UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO APLICADA

PAULO ROBERTO UHLIG

AVALIAÇÃO DO IMPACTO DE SEGURANÇA DE DISPOSITIVOS MÓVEIS VIA ABORDAGEM FUZZY

DISSERTAÇÃO DE MESTRADO

CURITIBA

2019

PAULO ROBERTO UHLIG

AVALIAÇÃO DO IMPACTO DE SEGURANÇA DE DISPOSITIVOS MÓVEIS VIA ABORDAGEM FUZZY

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação Aplicada da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Mestre em Computação Aplicada" – Área de Concentração: Engenharia de Sistemas Computacionais.

Orientador: Prof. Dr. Luiz Nacamura Junior

CURITIBA

2019

Dados Internacionais de Catalogação na Publicação

Uhlig, Paulo Roberto
Avaliação do impacto de segurança de dispositivos móveis via abordagem *fuzzy* [recurso eletrônico] / Paulo Roberto Uhlig.-- 2019.
1 arquivo eletrônico (94 f.) : PDF ; 2,07 MB.

Modo de acesso: World Wide Web.
Texto em português com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Computação Aplicada. Área de Concentração: Engenharia de Sistemas Computacionais, Curitiba, 2019.
Bibliografia: f. 85-93.

1. Computação - Dissertações. 2. Computação móvel - Medidas de segurança. 3. Computadores de bolso - Medidas de segurança. 4. Aplicativos móveis - Desenvolvimento. 5. Sistemas operacionais (Computadores) - Avaliação. 6. Lógica difusa. 7. Proteção de dados. 8. Crime por computador - Prevenção. 9. Empresas - Redes de computação - Medidas de segurança. 10. Métodos de simulação. I. Nacamura Júnior, Luiz, orient. II. Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Computação Aplicada. III. Título.

CDD: Ed. 23 -- 621.39

Biblioteca Central do Câmpus Curitiba - UTFPR
Bibliotecária: Luiza Aquemi Matsumoto CRB-9/794

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação

ATA DA DEFESA DE DISSERTAÇÃO DE MESTRADO Nº 75

DISSERTAÇÃO PARA OBTENÇÃO DO TÍTULO DE MESTRE EM COMPUTAÇÃO APLICADA
PROGRAMA DE PÓS-GRADUAÇÃO EM: COMPUTAÇÃO APLICADA
ÁREA DE CONCENTRAÇÃO: ENGENHARIA DE SISTEMAS COMPUTACIONAIS
LINHA DE PESQUISA: REDES E SISTEMAS DISTRIBUÍDOS

No dia 13 de agosto de 2019 às 10h00 reuniu-se na Sala B-205 da Sede Centro a banca examinadora composta pelos pesquisadores indicados a seguir, para examinar a dissertação de mestrado do candidato Paulo Roberto Uhlig**,** intitulada: Avaliação do Impacto de Segurança de Dispositivos Móveis Via Abordagem Fuzzy.

Orientador: Prof. Dr. Luiz Nacamura Junior

Após a apresentação, o candidato foi arguido pelos examinadores que, em seguida à manifestação dos presentes, consideraram o trabalho de pesquisa: ( ) Aprovado. ( ) Aprovado com restrições. Revisor indicado para verificação: _____. ( ) Reprovado.

Observações:

_____

_____

_____

Nada mais havendo a tratar, a sessão foi encerrada às __h__, dela sendo lavrado a presente ata, que segue assinada pela Banca Examinadora e pelo Candidato.

O candidato está ciente que a concessão do referido título está condicionada à: (a) satisfação dos requisitos solicitados pela Banca Examinadora; (b) entrega da dissertação em conformidade com as normas exigidas pela UTFPR; (c) atendimento ao requisito de publicação estabelecido nas normas do Programa; e (d) entrega da documentação necessária para elaboração do Diploma. A Banca Examinadora determina um **prazo máximo de _____ dias**, considerando os prazos máximos definidos no Regulamento Geral do Programa, para o cumprimento dos requisitos (desconsiderar caso reprovado), sob pena de, não o fazendo, ser desvinculado do Programa sem o Título de Mestre.

Prof. Luiz Nacamura Junior, Dr. Presidente - UTFPR _____

Profa. Ana Cristina Vendramin, Dra. - UTFPR _____

Prof. Mauro Sérgio Pereira Fonseca, Dr. - UTFPR _____

Prof. Altair Olivo Santin, Dr. - PUC-PR _____

Prof. Carlos Alberto Maziero, Dr. - UFPR _____

Assinatura do Candidato: _____

Reservado à Coordenação

DECLARAÇÃO PARA A OBTENÇÃO DO TÍTULO DE MESTRE

A Coordenação do Programa declara que foram cumpridos todos os requisitos exigidos pelo Programa de Pós-Graduação para a obtenção do título de Mestre.

Curitiba, _____de _____de 20____.

Carimbo e Assinatura do(a) Coordenador(a) do Programa

“Lust und Liebe sind die Fittiche zu großen Taten.”

(A alegria e o amor são as asas para os grandes feitos.)

Johann Wolfgang von Goethe.

À minha amada esposa por todo apoio, carinho, incentivo e dedicação.

AGRADECIMENTOS

Inicialmente gostaria de agradecer à Deus por ter me dado sabedoria e coragem para enfrentar todos os desafios de minha jornada. Aos meus pais, estes que me ensinaram com retidão os valores morais e éticos, uma educação exemplar na qual se fundamenta todas as conquistas de minha vida.

Agradeço cordialmente ao Dr. Luiz Nacamura Jr. por todo o aprendizado, aconselhamento e paciência nesta minha trajetória acadêmica. Adicionalmente, aos professor com os quais eu tive contato, estes sem dúvidas deixaram a sua contribuição e auxiliaram no êxito deste trabalho.

Minha amada esposa, Janine Rafaela Dums Uhlig, uma pessoa que me apoiou incondicionalmente em cada momento vivido durante a realização deste curso de mestrado, nutriu-me de forças para que eu sempre desse um passo em direção ao sucesso. A você, Janine, não tenho palavras para mensurar nem explicar o quanto eu sou grato e admiro a sua pessoa.

Durante a maior parte da realização das atividades das disciplinas e também da redação desta dissertação, eu estive em companhia da minha cachorrinha, Tigresa. O seu olhar meigo e tranquilizador, de alguma forma, me faziam relaxar e buscar inspiração para a conclusão das tarefas. Infelizmente, ao redigir o capítulo final deste estudo, ela faleceu com aproximadamente 17 anos de idade. Seu amor, doçura e companheirismo jamais serão esquecidos.

A todos os meus amigos, sejam eles de infância ou aqueles que eu cativei durante o curso - especialmente ao cursar as disciplinas de redes e sistemas fuzzy, que de alguma forma contribuíram com ideias e principalmente momentos de relaxamento para a renovação de energias, o meu fraterno muito obrigado. Em especial, Fernando José Muchalski, Patrick Vicente e Carlos Alberto Cipriano Korovsky.

De igual forma, agradeço à Prefeitura Municipal de São Bento do Sul por ter acreditado no meu potencial e no êxito da execução desta formação acadêmica.

RESUMO

UHLIG, Paulo Roberto. AVALIAÇÃO DO IMPACTO DE SEGURANÇA DE DISPOSITIVOS MÓVEIS VIA ABORDAGEM FUZZY. 93 f. Dissertação de Mestrado – Programa de Pós-Graduação em Computação Aplicada , Universidade Tecnológica Federal do Paraná. Curitiba, 2019.

Smartphones e *tablets* são equipamentos comumente utilizados tanto para fins pessoais quanto para atividades voltadas ao trabalho. O número de empresas que adotam a política de permitir que seus usuários utilizem seus próprios equipamentos para realizar atividades pessoais e laborais é crescente. Esta política, denominada *Bring Your Own Device (BYOD)*, oferece vantagens como redução de custos na aquisição de equipamentos por parte da empresa, aumento da mobilidade e produtividade. Entretanto, a adoção do *BYOD* oferece riscos, pois estes equipamentos podem possuir configurações customizáveis do sistema operacional demasiadamente permissivas e também armazenar informações de alta relevância. Desta forma, as configurações customizáveis do sistema operacional do dispositivo móvel podem impactar diretamente na segurança do aparelho e como consequência, ameaças digitais como *malware*, furto de dados e prejuízo financeiro podem ocorrer. Neste trabalho é proposto a coleta e avaliação dos parâmetros das configurações customizáveis do sistema operacional aliada à quantificação dos dados armazenados pelo usuário no dispositivo móvel. Desta forma, pode-se avaliar o impacto de segurança oferecido pelo equipamento e assim, qualificá-lo a acessar informações corporativas cuja relevância é compatível com o grau de impacto de segurança apresentado pelo aparelho. Para validar a proposta, o aplicativo *Fuzzy BYOD (FBYOD)* foi desenvolvido. Este aplicativo utiliza a lógica *fuzzy* como componente principal para a análise dos equipamentos. O *FBYOD* foi avaliado em ambiente corporativo não simulado, onde dispositivos móveis executam o sistema operacional *Android* e são compatíveis com a política de *BYOD*. Os resultados obtidos demonstram a eficácia da proposta e também revelam que usuários negligenciam aspectos importantes de segurança e que adicionalmente, quantidades de arquivos acima da média reportada pela literatura são armazenadas nos dispositivos.

Palavras-chave: BYOD, configuração customizável, furto de dados, fuzzy

ABSTRACT

UHLIG, Paulo Roberto. SECURITY IMPACT EVALUATION OF MOBILE DEVICES USING FUZZY APPROACH. 93 f. Dissertação de Mestrado – Programa de Pós-Graduação em Computação Aplicada , Universidade Tecnológica Federal do Paraná. Curitiba, 2019.

Smartphones and tablets are commonly used equipment for personal purposes as well as for work-oriented activities. The number of companies that adopt the policy of allowing their users to use their own equipment to carry out personal and work activities is increasing. This policy, called Bring Your Own Device (BYOD), offers advantages such as reduced costs in the acquisition of equipment by the company, increased mobility and productivity. However, the adoption of BYOD offers risks because these devices may have operating system's customizable configurations that are too permissive and also they may store highly relevant information. The customizable settings of the mobile device's operating system can directly impact on the security of the equipment and as a consequence, digital threats such as malware, data theft and financial loss might occur. In this work it is proposed the collection and evaluation of the parameters of the operating system's customizable configurations allied to the quantification of the data stored by the user in the mobile device. It is possible to evaluate the security impact offered by the equipment and thus, qualify it to access corporate information whose relevance is compatible with the degree of security impact presented by the device. To validate the proposal, the Fuzzy BYOD (FBYOD) application has been developed. This application uses fuzzy logic as the main component for the analysis of equipment. FBYOD has been evaluated in a non-simulated corporate environment where mobile devices run Android operating system and are compliant with BYOD policy. The results obtained demonstrate the effectiveness of the proposal and also reveal that users neglect important aspects of security and that in addition, above-average amounts of files, which is reported in the literature, are stored in the devices.

Keywords: BYOD, customizable configuration, data theft, fuzzy

LISTA DE FIGURAS

FIGURA 1 – Tipos de informação mais importantes para os usuários. 24
FIGURA 2 – Objetivos do ataque, distribuição e infecção e aquisição de privilégios do *malware*. 25
FIGURA 3 – Funcionamento típico de uma rede sem fio. 28
FIGURA 4 – Funcionamento do ataque *eavesdropping*. 29
FIGURA 5 – Funcionamento do ataque *hijacking* com a variante *Man-in-the-Middle.* .. 30
FIGURA 6 – Funcionamento do protocolo *WPA* no modo de operação *WPA Enterprise*. 33
FIGURA 7 – Funções de pertinência do tipo triangular, trapezoidal e gaussiana. 36
FIGURA 8 – Método de defuzificação "Média dos Máximos". 37
FIGURA 9 – Método de defuzificação "Centróide". 38
FIGURA 10 – Componentes de um sistema *fuzzy* típico. 38
FIGURA 11 – Fluxo de trabalho proposto. 57
FIGURA 12 – Estrutura do protótipo do aplicativo *FBYOD*. 61
FIGURA 13 – Fluxo de trabalho do *FBYOD*. 63
FIGURA 14 – Universo onde a variável de entrada oriunda da saída do processamento do módulo "coletor de configurações customizáveis" é fuzificada. 65
FIGURA 15 – Universo onde a variável de entrada oriunda da saída do processamento do módulo "contador de arquivos" é fuzificada. 66
FIGURA 16 – Conjuntos *fuzzy* que fazem parte do universo da saída do sistema. 67
FIGURA 17 – Estrutura do banco de dados do *FBYOD*. 68
FIGURA 18 – Tela de *login* do *FBYOD*. Após a inserção dos dados de *login*, a avaliação do dispositivo é automaticamente iniciada. 69
FIGURA 19 – FBYOD: tela de arquivos disponíveis e descrição do índice de impacto de segurança que o dispositivo apresenta no momento da avaliação. 69
FIGURA 20 – Distribuição das versões do sistema operacional *Android* entre os dispositivos avaliados. 70
FIGURA 21 – Resultados das configurações customizáveis coletadas pelo *FBYOD*. 71
FIGURA 22 – Utilização de autenticação via impressão digital. 73
FIGURA 23 – Quantidade de mensagens *SMS* encontradas nos dispositivos avaliados pelo *FBYOD*. 77
FIGURA 24 – Configurações fundamentais ajustadas de modo inseguro. 78
FIGURA 25 – Quantidade de arquivos de dados do usuário encontrados pelo *FBYOD* nos dispositivos avaliados. 78
FIGURA 26 – Quantidade de arquivos de dados do usuário encontrados pelo *FBYOD* em dispositivos sem a proteção de senha. 79

LISTA DE TABELAS

TABELA 1 – Histórico de novas vulnerabilidades dos sistemas operacionais *Android* e *iOS*. 18
TABELA 2 – Customização de configurações e respectivas vulnerabilidades. 21
TABELA 3 – Padrões *IEEE* para redes *WLAN*. 28
TABELA 4 – String de busca utilizada. 41
TABELA 5 – Comparação desta dissertação com os trabalhos relacionados mais relevantes. 49
TABELA 6 – Configurações customizáveis e recomendações de segurança. 52
TABELA 7 – Descrição dos níveis de impacto de segurança causado por configurações customizáveis caso estejam ajustadas de modo não seguro. 55
TABELA 8 – Formatos comumente utilizados para arquivos do tipo documento, áudio, vídeo e imagem. 55
TABELA 9 – Configurações do *Android* coletadas pelo *FBYOD* e respectivos níveis de impacto de segurança. 60
TABELA 10 – Regras fuzzy desenvolvidas para uso no aplicativo FBYOD. 66
TABELA 11 – Itens avaliados pelo *FBYOD* que compõe a categoria “senha”. 72
TABELA 12 – Itens avaliados pelo *FBYOD* que compõe a categoria “rede”. 73
TABELA 13 – Itens avaliados pelo *FBYOD* que compõe a categoria “permissão”. 74
TABELA 14 – Itens avaliados pelo *FBYOD* que compõe a categoria “sistema”. 75
TABELA 15 – Itens avaliados pelo *FBYOD* que compõe a categoria “conteúdo”. 76
TABELA 16 – Qualificação dos dispositivos avaliados para acesso de informações disponíveis no módulo *Storage* do *FBYOD*. 80

LISTA DE SIGLAS

BYOD	Bring Your Own Device
DoS	Denial of Service
CVE	Common Vulnerabilities and Exposures
SC	Security Category
SMS	Short Message Text
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
IEEE	Institute of Electrical and Electronics Engineers
AP	Access Point
DSL	Digital Subscriber Line
ONT	Optical Network Termination
MAC	Media Access Control
MDM	Mobile Device Management
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA-PSK	Pre-Shared Key
AES	Advanced Encryption Standard
SAE	Simultaneous Authentication of Equals
KRACK	Key Reinstallation Attack
VPN	Virtual Private Network
GPS	Global Positioning System
PIN	Personal Identification Number
TLS	Transport Layer Security
FBYOD	Fuzzy BYOD
API	Application Programming Interfaces

SUMÁRIO

1 INTRODUÇÃO 13
1.1 MOTIVAÇÃO E JUSTIFICATIVA 14
1.2 OBJETIVOS 15
1.2.1 Objetivos específicos 15
1.3 CONTRIBUIÇÕES 15
1.4 ESTRUTURA DO DOCUMENTO 16
2 SEGURANÇA EM AMBIENTES *BYOD* 17
2.1 INTRODUÇÃO SOBRE DISPOSITIVOS UTILIZADOS PARA *BYOD* 17
2.1.1 Vulnerabilidades relacionadas ao uso de *BYOD* 18
2.1.2 Ameaças geradas através de configurações customizáveis 20
2.1.3 Relevância dos dados e informações 21
2.1.4 Ataques e furto de dados 24
2.1.5 Ataques à rede sem fio ampliados pelo uso de políticas *BYOD* 27
2.2 PROTEÇÃO DAS INFORMAÇÕES DISPONIBILIZADAS AO *BYOD* 31
2.2.1 Segurança de redes sem fio 32
2.3 LÓGICA *FUZZY* 34
2.4 OUTROS MÉTODOS DE APOIO À DECISÃO 38
2.5 CONCLUSÃO 39
3 REVISÃO DA LITERATURA 41
3.1 MÉTODO DE PESQUISA 41
3.2 TRABALHOS RELACIONADOS 42
3.2.1 BYOD security engineering: A framework and its analysis 42
3.2.2 Developing a NATO BYOD security policy 43
3.2.3 Towards enforcing on-the-fly policies in BYOD environments 44
3.2.4 Benchmarking user-defined security configurations of android devices 44
3.2.5 Understanding users' requirements for data protection in smartphones 45
3.2.6 On the need for different security methods on mobile phones 45
3.2.7 A risk assessment method for smartphones 45
3.2.8 Security Benchmarks 46
3.3 USO DE LÓGICA FUZZY PARA SEGURANÇA 46
3.3.1 Fuzzy logic-based implicit authentication for mobile access control 46
3.3.2 Fuzzy inference based intrusion detection system: FI-Snort 47
3.3.3 Fuzzy logic based android malware classification approach 47
3.4 DISCUSSÃO 48
3.5 CONCLUSÃO 49
4 UM MODELO PARA AVALIAÇÃO DO IMPACTO DE SEGURANÇA DE DISPOSITIVOS MÓVEIS 50
4.1 VISÃO GERAL 50

4.2 CONFIGURAÇÕES CUSTOMIZÁVEIS 51
4.2.1 Ameaças relacionadas a configurações customizáveis 53
4.3 DADOS GRAVADOS EM DISPOSITIVOS MÓVEIS 55
4.4 ACESSO A INFORMAÇÕES CORPORATIVAS 55
4.5 LIMITAÇÕES 57
4.6 CONCLUSÃO 58
5 VALIDAÇÃO E RESULTADOS OBTIDOS 59
5.1 VISÃO GERAL 59
5.2 ATRIBUIÇÃO DE NÍVEIS DE IMPACTO DE SEGURANÇA 59
5.3 ESTRUTURA DO *FBYOD* 61
5.4 IMPLEMENTAÇÃO DO *FBYOD* 64
5.4.1 Implementação do módulo coletor de configurações customizáveis 64
5.4.2 Implementação do módulo contador de arquivos 65
5.4.3 Implementação do módulo controlador *fuzzy* 65
5.4.4 Implementação do banco de dados 67
5.4.5 Implementação do módulo de autenticação 68
5.4.6 Implementação do módulo *Storage* 68
5.4.7 Interfaces do *FBYOD* 69
5.5 ESTUDO DE CASO E RESULTADOS OBTIDOS 69
5.5.1 Configurações relacionadas à categoria “Senha” 71
5.5.2 Configurações relacionadas à categoria “Rede” 73
5.5.3 Configurações relacionadas à categoria “Permissão” 74
5.5.4 Configurações relacionadas à categoria “Sistema” 75
5.5.5 Configurações relacionadas à categoria “Conteúdo” 76
5.5.6 Configurações fundamentais 77
5.5.7 Arquivos de dados do usuário 77
5.5.8 Níveis de acesso 79
5.6 DISCUSSÃO 79
5.7 CONCLUSÃO 81
6 CONCLUSÃO E TRABALHOS FUTUROS 82
6.1 LIMITAÇÕES E AMEAÇAS À VALIDADE 83
6.2 TRABALHOS FUTUROS 84
REFERÊNCIAS 85

1 INTRODUÇÃO

Com a consolidação do uso de redes sem fio, o perfil do usuário corporativo tem evoluído continuamente. Há algumas décadas, os escritórios dos ambientes empresariais eram constituídos principalmente de computadores *desktop*, impressoras e *scanners*. Entretanto, a coexistência destes esquipamentos com aplicações de *smartphones* para fins corporativos já é uma realidade.

A utilização de equipamentos pessoais, como *smartphones* por exemplo, para fins laborais é denominada *BYOD* (MILLER et al., 2012). A política de *BYOD* permite que o mesmo equipamento seja utilizado tanto para as necessidades pessoais quanto para o trabalho. O emprego do *BYOD* fornece vantagens tanto para o usuário quanto para a empresa, como aumento de produtividade e mobilidade (BLIZZARD, 2015; DOWNER; BHATTACHARYA, 2016).

O uso desta política também pode oferecer inconvenientes, principalmente relacionados à segurança. Por tratar-se de um dispositivo que possui função dupla - pessoal e laboral, a empresa, normalmente, não possui o mesmo grau de gerenciamento sobre esses equipamentos. Assim, um aparelho utilizado para *BYOD* pode conter ameaças digitais como *malware* ou configurações do sistema operacional do dispositivo excessivamente permissivas. Desta forma, o uso do *BYOD* pode causar prejuízo financeiro em decorrência de furto de dados desencadeado por ameaças digitais e também pela violação dos princípios da confidencialidade, integridade e disponibilidade. O furto de dados é caracterizado pela transferência de informações para outros equipamentos sem o devido consentimento, seja ela de forma maliciosa ou não (KO et al., 2014).

As configurações customizáveis do sistema operacional de um dispositivo móvel desempenham um papel importante no tocante da segurança. A parametrização de determinadas configurações customizáveis de modo permissivo, mesmo que tal ajuste seja válido, pode gerar vulnerabilidades tanto para o furto dos dados contidos no próprio aparelho quanto para as informações remotas que o dispositivo acessa.

Na literatura utilizada para a elaboração deste trabalho, encontram-se descritas dife-

rentes abordagens para a mitigação do furto de dados e suas consequências. Entretanto, os trabalhos pesquisados não relacionam o impacto de segurança causado pela parametrização insegura das configurações customizáveis do sistema operacional do equipamento utilizado para *BYOD* em conjunto com os arquivos de informações que o usuário armazena naquele equipamento. Um dispositivo móvel pode conter dados de alta relevância ou criticidade e estes podem estar sob ameaça de furto em virtude de configurações customizáveis ajustadas de modo não seguro.

Para atenuar este inconveniente, este trabalho apresenta um modelo para avaliar o impacto de segurança causado por dispositivos utilizados para *BYOD*. A parametrização das configurações customizáveis do dispositivo sob análise são coletadas e ponderadas no quesito segurança. Adicionalmente, a quantidade de arquivos de dados que o usuário armazena no equipamento é computada. Desta forma, torna-se possível calcular o impacto geral de segurança que o dispositivo causa no ambiente empresarial. Assim, classifica-se o aparato a acessar somente informações corporativas cuja relevância é compatível com o impacto de segurança apresentado pelo aparelho.

Os resultados obtidos comprovam a eficácia do modelo proposto e desta forma, o impacto causado pelo furto de dados oriundo de dispositivos utilizados para o *BYOD* é mitigado.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Os dispositivos utilizados para *BYOD* armazenam dados cuja relevância é variável. Desta forma, no caso da ocorrência do furto ou indisponibilidade de dados, o impacto causado por este inconveniente é relacionado diretamente com a relevância do dado sob sinistro (BEN-ASHER et al., 2011; MUSLUKHOV et al., 2012). Assim, o nível de proteção relacionado à segurança que um dispositivo móvel possui deve ser compatível com a importância dos dados que ele acessa ou armazena.

Em análise das soluções propostas na literatura para a mitigação do furto de dados e outras ameaças, encontram-se descritas soluções baseadas, principalmente, em perfil de acesso, políticas de segurança visando o bloqueio e necessidade de aplicativos e *frameworks* de recomendações de segurança. Entretanto, estas são ferramentas estáticas e podem tornar-se incompatíveis, ao decorrer do uso, com a importância dos dados que o equipamento acessa.

Um dos pontos vinculados a vulnerabilidades de segurança é a parametrização das configurações customizáveis do sistema operacional do dispositivo móvel. Uma configuração ajustada de modo inseguro, mesmo que válida, pode expor os dados a vulnerabilidades de níveis

de impacto de segurança distintos pois o usuário padrão não possui conhecimento acerca dos fundamentos de segurança (BECHER et al., 2011; VECCHIATO, 2016).

A literatura pesquisada aponta as vulnerabilidades causadas pela parametrização equivocada de configurações customizadas. Entretanto, nenhum trabalho avaliado considera o relacionamento entre o impacto de segurança causado por configurações customizáveis inseguras e a relevância das informações que o aparelho móvel armazena e acessa remotamente.

Este trabalho apresenta um novo modelo para mitigação das consequências do furto de dados através da avaliação dinâmica do impacto de segurança provocado pelas configurações customizáveis e dos arquivos de dados do usuário armazenados no dispositivo. O objetivo é tornar possível qualificar o dispositivo móvel a acessar somente as informações cuja relevância seja compatível com o impacto de segurança apresentado pelo aparelho.

1.2 OBJETIVOS

O objetivo geral deste trabalho é apresentar e validar um modelo para a mitigação do impacto causado pelo furto de dados originado de dispositivos utilizados em um ambiente *BYOD*.

1.2.1 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho encontram-se elencados na sequência:

- Coletar os parâmetros das configurações customizáveis do sistema operacional do dispositivo móvel e avaliá-los quanto à segurança;
- Quantificar os arquivos de dados do usuário armazenados no equipamento sob avaliação;
- Qualificar o dispositivo móvel sob avaliação a acessar informações corporativas compatíveis com o grau de impacto de segurança apresentado pelo aparelho.

1.3 CONTRIBUIÇÕES

Este trabalho desenvolve em um ambiente *BYOD* uma abordagem inovadora no tocante da mitigação do impacto causado pelo furto de dados. O modelo proposto permite a avaliação, em modo dinâmico, das configurações customizáveis do sistema operacional e dos

arquivos de dados que o usuário armazena no dispositivo. Assim, o equipamento é constantemente qualificado para que acesse somente informações cuja relevância seja compatível com o grau de impacto de segurança apresentado pelo aparelho. Adicionalmente, o seguinte artigo foi publicado:

- UHLIG, P. R.; NACAMURA JUNIOR, L. FBYOD: A Fuzzy Logic-based System for Safe BYOD Adoption. **International Journal of Engineering Trends and Technology**, v.9, n.4, p.40-53, Setembro 2019, doi: 10.14445/22492593/IJCOT-V9I4P307.

1.4 ESTRUTURA DO DOCUMENTO

Este documento encontra-se divido da seguinte forma: o capítulo dois apresenta a fundamentação teórica relacionada à segurança de ambientes *BYOD* e adicionalmente, uma breve introdução sobre a lógica *fuzzy*; o capítulo três descreve a revisão bibliográfica realizada; o capítulo quatro retrata a solução proposta; o capítulo cinco apresenta a validação da proposta e os resultados obtidos, por fim, o trabalho é concluído no capítulo seis.

2 SEGURANÇA EM AMBIENTES *BYOD*

Este capítulo apresenta a fundamentação acerca da segurança em ambientes *BYOD*. Adicionalmente, uma breve introdução sobre a lógica *fuzzy* é exposta, pois a mesma é empregada na validação da proposta deste trabalho.

2.1 INTRODUÇÃO SOBRE DISPOSITIVOS UTILIZADOS PARA *BYOD*

Equipamentos aderentes à política de *BYOD*, tais como computadores *desktop*, *notebooks*, *smartphones* ou *tablets*, podem ser utilizados dentro do ambiente físico corporativo ou para efetuar o acesso aos serviços de rede da empresa de modo remoto (SOUPPAYA; SCARFONE, 2016). Neste estudo, os dispositivos utilizados para a política de *BYOD* estão restritos a *smartphones* e *tablets* que utilizam o sistema operacional *Google Android* e *Apple iOS*.

Os *smartphones* e *tablets* possuem características em comum se comparados a um computador *desktop*. Entretanto, no tocante da segurança, há diferenças significativas entre dispositivos móveis e computadores *desktop* (POLLA et al., 2013; VECCHIATO, 2016):

- *Mobilidade*: como os aparelhos móveis não encontram-se limitados a um único espaço físico, estes podem ser furtados ou perdidos;
- *Maior customização do dispositivo*: normalmente equipamentos móveis não são compartilhados com outros usuários. Desta forma, há forte customização das configurações e aplicações instaladas;
- *Conectividade*: *smartphones* e *tablets* normalmente possuem suporte a variados meios para acessar redes corporativas e Internet, como redes sem fio locais e redes 3G ou 4G, por exemplo;
- *Tecnologia convergente*: um equipamento móvel combina múltiplas tecnologias, tais como: telefone móvel, câmera digital e reprodutor de músicas. Deste modo, há mais pontos a serem explorados por um eventual atacante.

Dispositivos utilizados para *BYOD* normalmente não possuem o mesmo grau de controle se comparados a um equipamento pertencente à própria corporação, pois podem não possuir os mesmos aplicativos necessários instalados, bem como configurações de segurança. Desta forma, um *malware* pode estar instalado no equipamento sem que o usuário saiba, por exemplo. Assim, é possível que ocorra furto de dados corporativos, sendo esta uma das ameaças mais graves a uma empresa (KAO et al., 2015).

2.1.1 VULNERABILIDADES RELACIONADAS AO USO DE *BYOD*

Uma vulnerabilidade corresponde a uma deficiência que pode ser explorada e assim comprometer a segurança de um determinado sistema (FELT et al., 2011; ZHOU; JIANG, 2012; VECCHIATO, 2016). A tabela 1 ilustra o histórico de vulnerabilidades encontradas nos sistemas operacionais *Android* e *iOS* nos anos de 2014, 2015 e 2016.

Tabela 1: Histórico de novas vulnerabilidades dos sistemas operacionais *Android* e *iOS*.

Ano	Android	iOS	Total
2014	12	178	190
2015	89	463	552
2016	316	290	606

Fonte: Symantec (2017).

De um modo geral, vulnerabilidades podem ser exploradas por *malware* e desta forma obter controle daquele dispositivo. Os softwares denominados *malware* possuem o intuito de furtar e indisponibilizar dados, podendo causar prejuízos financeiros (ENCK, 2011; DANG-PHAM; PITTAYACHAWAN, 2015). A infecção de um dispositivo por *malware* dá-se, normalmente, pela instalação de aplicativos oriundos de locais não confiáveis, não utilização de *patches* de segurança do sistema operacional e pelo não emprego de aplicação *anti-malware*. A seguir, encontram-se descritos os tipos mais comuns de *malware* [1] (FELT et al., 2011; POLLA et al., 2013; JAMIL; SHAH, 2016):

- *Vírus*: o *vírus* é um software que possui a capacidade de se autorreplicar. Diferentes réplicas de um mesmo vírus podem infectar aplicações legítimas e setores de inicialização onde reside o *boot* do sistema operacional. Comumente, o *vírus* insere seu código em uma aplicação genuína. Deste modo, seu código sempre é executado quando aquela aplicação é chamada;

[1] Estas ameaças digitais possuem variantes para *smartphones, tablets*, computadores *desktop* e *notebooks*.

- *Trojan*: o *trojan* é uma aplicação maliciosa que não possui a capacidade de se replicar automaticamente. Entretanto, este tipo de aplicação possibilita uma interface de comunicação entre um usuário mal intencionado e o computador infectado pelo *trojan*. Normalmente o *trojan* possui funcionalidades úteis aos usuários, podendo mascarar o comportamento malicioso deste *malware*. Por exemplo, um usuário instala um aplicativo de *chat* em seu *smartphone*. Este aplicativo fornecerá a função de *chat* desejada pelo usuário, entretanto executará também ações maliciosas, como furto de dados, sem que o usuário perceba e assim caracterizando o *trojan*;

- *Worm*: ao contrário do *trojan*, o *worm* é uma aplicação que replica-se automaticamente entre computadores e dispositivos móveis através da rede. Diferentemente do *vírus*, o *worm* não insere seu código em aplicações legítimas. O *worm* normalmente explora as vulnerabilidades de segurança do sistema operacional do dispositivo para executar a infecção. Desta forma, o *worm* pode consumir rapidamente os recursos de rede durante sua replicação. Adicionalmente, este tipo de *malware* causa instabilidade nos equipamentos infectados e pode oferecer furto de dados;

- *Botnet*: uma *botnet* é uma coleção de computadores e dispositivos móveis infectados por *malware* que dão ao executor do ataque a possibilidade de controlar estes equipamentos remotamente. As *botnets* representam um risco de segurança, pois normalmente são desenvolvidas por organizações criminosas que geram ataques cibernéticos com o objetivo de causar prejuízos financeiros. Os ataques mais comuns gerados por estas organizações incluem o envio de *spam*, ataques de negação de serviço *DoS* ou simplesmente coletar informações dos equipamentos para que estas sejam utilizadas ilegalmente;

- *Ransomware*: este tipo de *malware* codifica os dados armazenados nos dispositivos. Assim, documentos, acesso a sistemas e fotos, por exemplo, tornam-se indisponíveis. O objetivo do *ransomware* é que a vítima pague uma quantia financeira para que o acesso às informações codificadas sejam restauradas;

- *Rootkits*: o *rootkit* atinge seu objetivo malicioso infectando diretamente o sistema operacional dos dispositivos. Deste modo, processos maliciosos são criados no *user-space*. Estes processos podem desabilitar ferramentas como *anti-vírus* e bem como instalar outras ameaças digitais como *trojans*, por exemplo. Como o *rootkit* altera diretamente componentes do sistema operacional, esta categoria de *malware* pode controlar mais amplamente o equipamento infectado.

Além do *malware*, as vulnerabilidades também podem ser exploradas por pessoas in-

tencionadas a deliberar este ato, como por exemplo, um funcionário insatisfeito com seu trabalho ou um *hacker*. Deste modo, as consequências causadas são similares ao ataque do *malware* (DANG-PHAM; PITTAYACHAWAN, 2015).

2.1.2 AMEAÇAS GERADAS ATRAVÉS DE CONFIGURAÇÕES CUSTOMIZÁVEIS

Uma configuração *customizável de dispositivo móvel* pode ser definida como um ajuste de parâmetros que o usuário realiza no sistema operacional do seu equipamento. Desta forma, essa configuração pode impactar na segurança daquele dispositivo (VECCHIATO, 2016; CIS, 2018). A customização de configurações representa uma parcela das atividades realizadas pelos usuários em seus *smartphones* e *tablets*. Estas atividades são motivadas por situações diversas, como por exemplo, alterar as configurações de rede para acessar uma determinada rede sem fio, permitir a instalação de *software* de outras *Application Stores*, alterar o papel de parede da tela de espera do dispositivo, dentre outras.

Os ajustes em um equipamento geram impactos diferenciados no sistema. Do ponto de vista da segurança, por exemplo, trocar a foto do papel de parede do dispositivo é irrelevante, ao passo que definir uma senha fraca de desbloqueio de tela pode facilitar o acesso ao aparelho a pessoas não autorizadas (VECCHIATO, 2016).

Cada fabricante de *smartphone* e *tablet* pode inserir seus parâmetros padrão nas configurações customizáveis pelo usuário. Desta forma, caso estes ajustes não atendam a necessidade do utilizador, o usuário pode inserir valores convenientes ou selecionar outros valores fornecidos pelo sistema para aquela configuração.

Entretanto, o conhecimento de um usuário padrão relacionado à segurança é baixo, pois normalmente estes não são capazes de entender o real objetivo e principalmente as consequências de se alterar uma determinada configuração customizável. Mesmo que de modo não intencional e válido, pode-se gerar vulnerabilidades graves de segurança que podem ser exploradas por *malware* ou pessoas mal intencionadas (KRITZINGER; SOLMS, 2010; BECHER et al., 2011). A tabela 2 apresenta as configurações mais comumente customizadas e as respectivas vulnerabilidades caso sejam inseguramente parametrizadas.

Os itens apresentados pela tabela 2, mesmo que parametrizados de modo inseguro, são válidos e aceitos pelo sistema operacional. Determinadas parametrizações podem possuir relações com vulnerabilidades já conhecidas. A plataforma *CVE* relaciona as vulnerabilidades conhecidas de aplicações, inclusive dos sistemas operacionais *Google Android* e *Apple iOS* (MITRE, 2018). O trabalho de Vecchiato (2016) apresenta em detalhes o relacionamento de

Tabela 2: Customização de configurações e respectivas vulnerabilidades.

Customização da configuração	Vulnerabilidade gerada caso ajustada de modo inseguro
Senha de acesso ao equipamento	Caso esta configuração seja customizada com senhas de tamanho reduzido, caracteres sequenciais, senha do tipo padrão dedutível ou mesmo desabilitar o seu uso, o acesso ao equipamento é facilitado a terceiros.
Bloqueio de tela após uso do dispositivo	Quando o usuário deixa o dispositivo ocioso, a tela pode ser bloqueada automaticamente. Deste modo, quanto maior for o tempo ajustado nesta configuração, maior é o tempo que o dispositivo permanece ocioso sem solicitar a senha de desbloqueio. Assim, o acesso a terceiros é facilitado.
Redes sem fio	Caso o acesso a redes sem fio públicas seja permitido, os dados trafegados podem ser capturados e furtados, pois não estão protegidos por codificação. Do mesmo modo, salvar senhas de redes sem fio permite que pessoas mal intencionadas se conectem a essas redes caso obtenham acesso ao dispositivo.
Aplicativos de fontes não oficiais	Ao customizar a configuração que permite o uso de aplicativos oriundos de outras lojas de *software* que não sejam oficiais do sistema operacional do dispositivo, ameaças relacionadas a *malware* podem ser introduzidas no equipamento.
Encriptação do armazenamento	Caso a encriptação do armazenamento do equipamento seja desativada, os dados salvos no dispositivo não são protegidos por codificação e assim, o acesso ao conteúdo é facilitado a pessoas mal intencionadas e *malware*.
Alterar permissões de diretórios do sistema operacional	Ao aplicar parâmetros mais permissivos de acesso aos diretórios do sistema operacional do dispositivo, vulnerabilidades podem ser geradas em virtude do acesso de aplicativos e usuários a dados previamente exclusivos do sistema operacional.
Atualização do sistema operacional	Caso essa configuração seja parametrizada como desativada, correções de vulnerabilidades efetuadas pelo fabricante do sistema operacional não são aplicadas.

Fonte: Kritzinger e Solms (2010), Becher et al. (2011), Vecchiato (2016), CIS (2018).

configurações customizadas do sistema *Android* com vulnerabilidades reportadas pelo *CVE*.

2.1.3 RELEVÂNCIA DOS DADOS E INFORMAÇÕES

No decorrer da utilização do dispositivo *BYOD* é comum o crescente armazenamento e transmissões de informações. Estas informações incluem catálogo de endereços, senhas armazenadas, histórico de chamadas telefônicas, dados de localização geográfica, mensagens de e-mail, documentos corporativos, dentre outros. Assim, uma informação pode ser definida como um *ativo* do aparelho (JEON et al., 2011).

O uso de equipamentos *BYOD* oferece riscos e uma das consequências mais severas é o furto de dados (FELT et al., 2011; MILLER et al., 2012; POLLA et al., 2013; ROSE, 2013; KO et al., 2014; JAMIL; SHAH, 2016). Entretanto, as informações indisponibilizadas, divulgadas ou furtadas possuem impactos diferenciados no que refere-se a sua confidencialidade, integridade e disponibilidade. Como por exemplo, um *smartphone* utilizado para *BYOD* é infectado por um *malware* e os dados do aparelho são furtados. A divulgação da lista de contatos,

por exemplo, terá um impacto menor se comparada à divulgação de um documento contendo detalhes de um novo projeto técnico. De acordo com Page (2013), 34% dos aparelhos *BYOD* armazenam informações corporativas relevantes. Assim, caso equipamentos *BYOD* sofram um infortúnio, mais de um terço destes estarão suscetíveis ao furto de informações corporativas críticas.

As informações podem ser classificadas de acordo com seu valor, criticidade e requisitos legais (ISO27002..., 2013). Deste modo, os princípios da confidencialidade, integridade e disponibilidade são respeitados. A seguir, encontram-se descritos esses princípios de segurança (MACONACHY et al., 2001; ROSS; SWANSON, 2004):

- *Confidencialidade*: a confidencialidade estabelece políticas relacionadas ao acesso à informação. O controle de permissões de acesso é implementado e somente sistemas ou pessoas autorizadas podem acessar uma dada informação. Quando um documento, por exemplo, é furtado através da ação de um *malware* ou usuário, o principio da confidencialidade é quebrado;

- *Disponibilidade*: o princípio da disponibilidade determina que a informação esteja sempre disponível para o acesso legítimo de usuários e sistemas;

- *Integridade*: uma informação é considerada íntegra quando esta não sofreu nenhuma alteração não autorizada. Desta forma, a informação mantém-se isenta de quaisquer dados que não correspondam legitimamente a ela.

A violação da *confidencialidade*, *disponibilidade* ou *integridade* de informações pode causar diferentes níveis de impacto ao usuário ou à corporação conforme descrito a seguir (ROSS; SWANSON, 2004):

- *Baixo*: o efeito é baixo caso a violação de um ou mais destes princípios cause adversidades limitadas ao usuário ou à corporação. Por exemplo, no caso de ocorrências de furto de informações com violação temporária de *disponibilidade*, estas não impactam diretamente na continuidade das atividades da organização ou causam pequeno prejuízo financeiro;

- *Moderado*: a violação é considerada moderada quando a violação dos princípios causam impacto negativo considerável ao usuário ou corporação. Como por exemplo, em virtude de um furto de informações e quebra da *confidencialidade*, as atividades corporativas são temporariamente reduzidas ou interrompidas bem como ocorre prejuízo financeiro significativo;

- *Alto*: esta é a classificação mais elevada que uma violação pode receber. Assim, por exemplo, caso ocorra um furto de dados com violação de *integridade*, *confidencialidade* ou *disponibilidade* e esta violação desencadeie uma classificação nesta categoria, o usuário ou a corporação sofrem severos prejuízos financeiros ou inabilidade de continuar com suas atividades.

Entretanto, os princípios da *confidencialidade*, *disponibilidade* e *integridade* podem apresentar valores de categorias diferentes entre si. Por exemplo, caso uma informação confidencial seja divulgada erroneamente, o princípio da confidencialidade pode receber categoria *Moderado* enquanto a integridade e disponibilidade são classificadas como *Baixo*. Assim, uma informação recebe a seguinte notação de classificação (ROSS; SWANSON, 2004):

$$SC_{info} = \{(\text{confidencialidade, impacto}), (\text{disponibilidade, impacto}), (\text{integridade, impacto}) \}$$

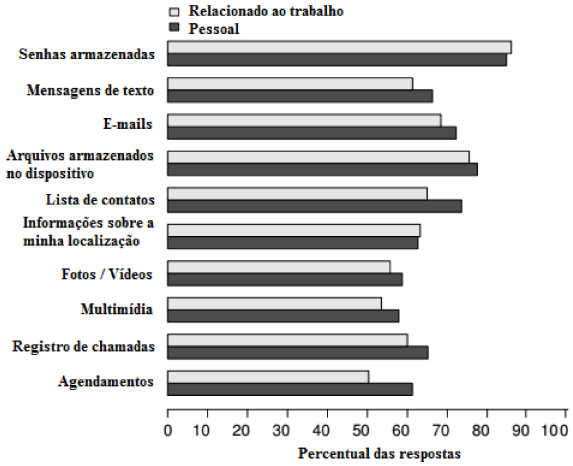
Conforme a notação acima demonstra, a *SC* ou categoria de segurança de uma determinada informação é composta pela combinação dos níveis de impacto de *confidencialidade*, *disponibilidade* e *integridade*. Como por exemplo: uma determinada empresa trabalha no ramo de seguros e permite que seus usuários utilizem equipamentos *BYOD* para manipular os dados relativos a clientes. Assim, estabeleceu-se que que a categoria de segurança destas informações é a seguinte:

$$SC_{seguro} = \{(\text{confidencialidade, alto}), (\text{disponibilidade, alto}), (\text{integridade, alto})\}$$

No exemplo acima, os três princípios foram pontuados com grau máximo, pois a violação de algum deles, naquela situação, causa severas consequências. Entretanto, algumas informações não se enquadram nos níveis de impacto *baixo*, *médio* e *alto* (ROSS; SWANSON, 2004). Como por exemplo, uma empresa que armazena informações públicas. Neste caso para o princípio da confidencialidade é atribuído o valor *Não Aplicável (NA)*, pois este princípio não é relevante para aquele conjunto de informações.

Em pesquisa realizada por Ben-Asher et al. (2011), demonstrou-se que a relevância das informações está relacionada com a violação de confidencialidade do usuário. Esta violação pode ser tanto no âmbito pessoal como no corporativo. A figura 1 ilustra quais tipos de informações são relevantes.

Figura 1: Tipos de informação mais importantes para os usuários.



Fonte: Adaptado de Ben-Asher et al. (2011).

A figura 1 ilustra nas esferas pessoal e corporativa quais tipos de informações são mais relevantes ao usuário. Senhas, arquivos armazenados no equipamento, e-mails e lista de contato estão entre as mais importantes. Esta figura também aponta que, exceto pela categoria de senha e informações sobre a localização atual, as informações no âmbito pessoal são consideradas mais importantes se comparadas a mesma categoria corporativa.

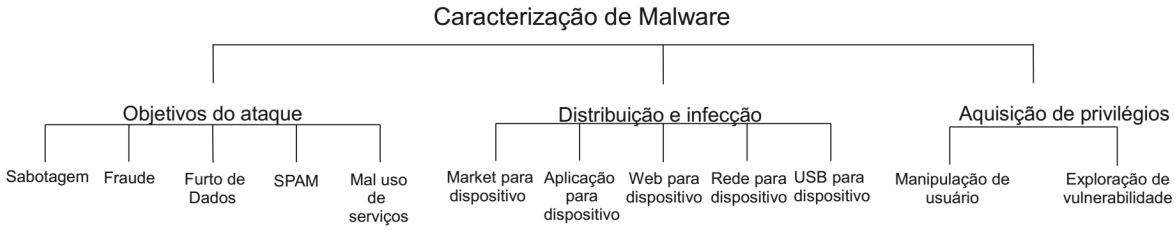
2.1.4 ATAQUES E FURTO DE DADOS

No ano de 2017 foram encontradas 26.579 novas variantes de *malware* para dispositivos móveis, um incremento de 54% em relação ao ano de 2016 (SYMANTEC, 2018). As categorias de *malware* que mais cresceram são aquelas relacionadas diretamente com o furto de dados financeiros, como *ransomware* e *trojans*. Comumente, o *malware* se disfarça como uma aplicação útil e assim induz o usuário a instalar ou utilizar o aplicativo infectado.

Um *malware* pode apresentar diversas características que são necessárias à realização de suas atividades. A figura 2 ilustra os *objetivos de ataque*, a *distribuição e infecção* e também a *aquisição de privilégios* do *malware* (BECHER et al., 2011; VIDAS et al., 2011; SUAREZ-TANGIL et al., 2014):

- *Objetivos do ataque*: o objetivo de ataque caracteriza o porquê daquele *malware* ter sido desenvolvido. A atividade maliciosa está envolvida essencialmente no furto de dados pessoais e laborais como número telefônico, senhas armazenadas, número de cartão de crédito, *logins* de sistema e documentos armazenados no equipamento. Desta forma, o próprio *malware* ou a entidade que o controla pode desencadear ações maliciosas como

Figura 2: Objetivos do ataque, distribuição e infecção e aquisição de privilégios do *malware*.



Fonte: Autoria própria

fraudes, sabotagem, furto de outros dados, envio de *SPAM* e abuso de serviços. Como por exemplo: o *smartphone* de um determinado usuário encontra-se infectado por um *trojan*. Este *trojan* furta os dados pessoais do usuário, inclusive o conteúdo de mensagens *SMS*. Em um determinado momento, o *malware* envia as informações de cartão de crédito e *login* do sistema corporativo ao atacante que controla o *trojan*. Assim que ele os recebe, compras *on-line* são feitas no cartão de crédito da vítima e alterações são feitas pelo atacante dentro do sistema corporativo. Adicionalmente, o *trojan* envia *e-mails* de *SPAM* a partir do equipamento do usuário e também registra o dispositivo junto a um serviço de recebimento de *SMS*. Neste exemplo, caracterizam-se o furto de dados, fraude, sabotagem, envio de *SPAM* e abuso de serviços;

- *Distribuição e infecção*: aplicações maliciosas possuem várias técnicas para que *malware* seja distribuído nos aparelhos das vítimas. Desta maneira, caso um canal de propagação não obtenha êxito, há outras técnicas que podem ser empregadas pelo *malware* para que ele possa ser distribuído no maior número de aparatos possível. Estas técnicas de distribuição podem ser divididas em:

  - *Market para dispositivo*: um *Application Market*, *Application Store* ou loja de aplicativos é um serviço de distribuição digital de *software* para *smartphones*, *tablets* e outros aparelhos. Dispositivos que utilizam o sistema operacional *Google Android* podem utilizar a *Application Store "Google Play"* e aparelhos da fabricante *Apple* que utilizam o sistema operacional *iOS* fazem uso da *"App Store"* (CHEN et al., 2015). Desta forma, caso algum *software* disponível naquela loja de aplicativos contenha *malware* e o usuário instale aquela aplicação infectada, o dispositivo estará contaminado. Entretanto, este vetor de infecção é comum em *Application Stores* não oficiais. As lojas oficiais *Google Play* e *App Store* possuem maior controle quanto à

segurança das aplicações disponíveis (MARTIN et al., 2017);

  - *Aplicação para dispositivo*: neste método de distribuição, o *malware* busca uma vulnerabilidade específica em uma determinada aplicação para se propagar. Diferentemente do vetor de propagação *Market para dispositivo*, o *malware* busca por aplicações já instaladas no equipamento. Como por exemplo, um *vírus* que dispara mensagens automáticas no aplicativo *Facebook*. Entretanto, para atingir seu objetivo malicioso, este *vírus* necessita de uma versão específica da aplicação *Facebook* instalada no equipamento. Assim, a vulnerabilidade contida na aplicação pode ser explorada;
  - *Web para dispositivo*: na propagação de *malware* denominada *Web para dispositivo*, o navegador (*Web Browser*) do dispositivo é utilizado. Trata-se de um tipo específico de *Aplicação para dispositivo*, pois as vulnerabilidades contidas no navegador são exploradas e assim o *malware* é disseminado;
  - *Rede para dispositivo*: esta estratégia de propagação é baseada na exploração de vulnerabilidades de rede incluindo configurações inseguras. Como por exemplo, uma rede sem fio com senha de acesso óbvia ou *bluetooth* do dispositivo cujo *firmware* apresenta vulnerabilidades. Deste modo, caso exista uma vulnerabilidade, o *malware* poderá explorá-la e propagar-se através da rede entre os dispositivos;
  - *USB para dispositivo*: a transferência de *malware*, neste caso, ocorre através da porta *USB*. Por exemplo, o usuário pode conectar seu *smartphone* através do cabo *USB* ao computador *desktop*. Caso o computador esteja infectado com alguma ameaça que explore dispositivos móveis, o equipamento conectado via *USB* poderá ser infectado.

- *Aquisição de privilégios*: para atingir o objetivo malicioso, o *malware* necessita de *privilégios*. Estes privilégios podem ser um acesso administrativo ao equipamento, uma senha de desbloqueio ou qualquer outra informação necessária para sua execução. Para isto há duas maneiras:

  - *Manipulação de usuário*: em determinadas situações os privilégios são concedidos ao *malware* pelo próprio usuário. Este fato ocorre pois o usuário pode não entender as consequências de atribuição de privilégios à uma aplicação. Desta forma, por exemplo, caso um reprodutor de áudio infectado com um *trojan* solicite permissão para acessar diretórios restritos do sistema operacional, o usuário equivocadamente poderá conceder os privilégios. Assim, a atividade maléfica do *malware* pode ser desencadeada;

– *Exploração de vulnerabilidades*: neste caso, para obter os privilégios necessários, o *malware* explora vulnerabilidades de *software* ou configurações de sistema ajustadas de modo inseguro. Como por exemplo: *bugs* do sistema operacional, vulnerabilidades em navegadores, interfaces *wireless*, *bluetooth* e configurações customizáveis.

Um fator determinante que influencia diretamente na segurança do *smartphone* ou *tablet* é o procedimento de *Jailbreak* ou *Root*. Os sistemas operacionais *Apple iOS* e *Google Android* possuem um sistema de permissões de acesso aos componentes do próprio sistema operacional, dados de aplicativos, dentre outros. Deste modo, um usuário ou um aplicativo não pode acessar ou alterar algumas regras, acessar diretórios exclusivos do sistema operacional, por exemplo. Ao aplicar o procedimento de *Jailbreak* ou *Root*, o usuário e as aplicações obtêm acesso administrativo ao equipamento. Assim, quaisquer restrições impostas pelo sistema operacional são desativadas (MILLER, 2011; LI; CLARK, 2013; ZHANG et al., 2015).

Além das consequências causadas por *malware* citadas nesta seção, o *malware* também pode facilitar e desencadear *ataques de rede*, principalmente em redes sem fio. Os detalhes destes ataques encontram-se descritos na seção seguinte.

2.1.5 ATAQUES À REDE SEM FIO AMPLIADOS PELO USO DE POLÍTICAS *BYOD*

Comunicação sem fio refere-se a transmissão de informações de um equipamento a outro através de meio sem fio. Desta forma, a comunicação ocorre através de ondas eletromagnéticas transmitidas no ar. Na atualidade existem diversas tecnologias para transmissão de dados via meio sem fio, tais como: *WiMax*, redes celulares 3G e 4G, *WLAN*, dentre outras (KUMAR; PAUL, 2016). Neste trabalho, o escopo de redes sem fio limita-se à *WLAN*.

Uma rede sem fio do tipo *WLAN*, seja ela residencial ou corporativa, comunica-se através do padrão *IEEE 802.11*. Este é um padrão internacional desenvolvido e mantido pela *IEEE* e é específico para a implementação de redes *WLAN*. Desta forma, a *WLAN* permite que equipamentos, como por exemplo, *smartphones*, computadores *desktop* e impressoras comuniquem-se entre si sem a necessidade de cabos (BIANCHI, 2000; HIERTZ et al., 2010). A tabela 3 ilustra uma visão geral dos padrões *IEEE* utilizados para *WLAN*.

Dentre os vários padrões *IEEE* para redes sem fio, o *802.11ac*, durante o desenvolvimento deste trabalho, é o mais recente. Este padrão opera na faixa de 5GHz e fornece oito canais de 866,7 Mhz cada. Como característica adicional, o *802.11ac* é compatível com os padrões *802.11b, 802.11a, 802.11g* e *802.11n* (SARRAFZADEH; SATHU, 2015). Detalhes acerca do padrão *802.11* e suas variantes podem ser consultados nas publicações de Crow et al.

Tabela 3: Padrões *IEEE* para redes *WLAN*.

Data de lançamento	Padrão	Frequência	Taxa de transferência
1997	802.11	2.4GHz	2 Mbps
1999	802.11b	2.4GHz	11 Mbps
1999	802.11a	5GHz	54 Mbps
2003	802.11g	2.4GHz	54 Mbps
2009	802.11n	2.4GHz	600 Mbps
2014	802.11ac	5GHz	1300 Mbps

Fonte: Sarrafzadeh e Sathu (2015).

(1997), Bianchi (2000), Hiertz et al. (2010), Bejarano et al. (2013).

Uma rede *WLAN* é constituída, normalmente, de um ou mais roteadores, *AP* e demais equipamentos que utilizam a rede para estabelecer a comunicação, tais como: *notebooks*, *smartphones* e impressoras (SOUPPAYA; SCARFONE, 2016). A figura 3 ilustra o funcionamento típico de uma rede sem fio.

Figura 3: Funcionamento típico de uma rede sem fio.

Fonte: Adaptado de SPIRO (2018).

No cenário exposto pela figura 3, o sinal da rede sem fio é distribuído pelo *roteador principal* aos demais *notebooks* e *desktops*. O *roteador principal* também conecta-se ao *DSL*, *Cable Modem* ou *ONT* e assim fornece acesso à Internet aos equipamentos conectados.

A utilização de redes *wireless* é fundamental para a adoção do *BYOD*. Entretanto, esta

política pode potencializar os ataques de rede que podem levar ao furto de dados e a indisponibilidade de serviços de rede. Neste trabalho, as redes denominadas *cabeadas* estão fora do escopo da abordagem. A seguir encontram-se descritos os ataques de rede que podem ser intensificados através do emprego do *BYOD* (HOQUE et al., 2015; MUTAKIN et al., 2016; ZHANG et al., 2016):

- *Ataque do tipo eavesdropping*: este é o tipo de ataque mais comum à uma rede sem fio e tem por objetivo obter dados confidenciais tais como *logins* e senhas. O princípio desta ameaça consiste em captar o sinal da rede sem fio e assim, os pacotes que trafegam na rede podem ser capturados e decodificados através de aplicações específicas. A figura 4 ilustra o funcionamento do ataque de *eavesdropping*.

Figura 4: Funcionamento do ataque *eavesdropping*.

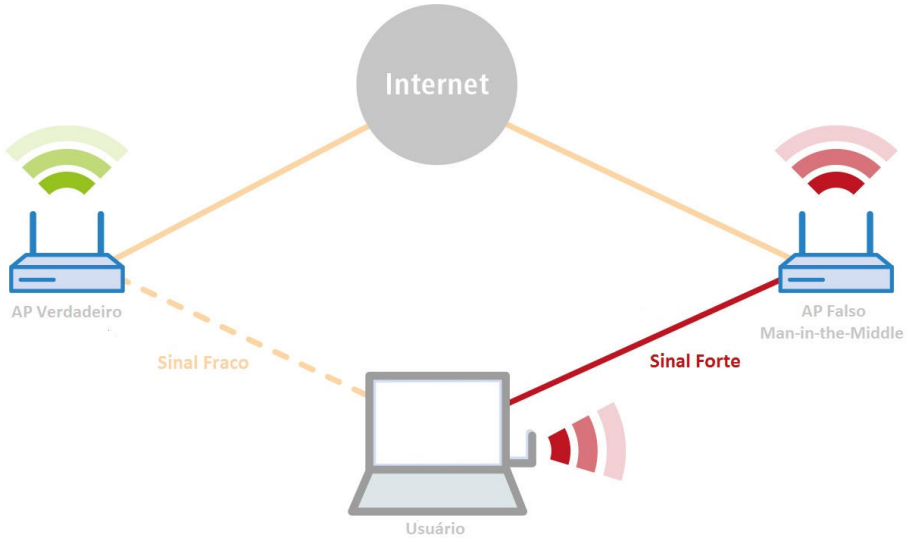
Fonte: Autoria própria.

Na figura 4 observa-se que os pacotes de rede trafegam normalmente entre o dispositivo do usuário e a Internet. Entretanto, os pacotes de rede são copiados, sem que o usuário saiba, para o atacante denominado *eavesdropper*;

- *Ataque hijacking*: o ataque do tipo *hijacking* ou *sequestro* consiste em um usuário não autorizado obter o controle de uma conexão *WLAN* de um usuário autorizado. Uma variante comum do ataque *hijacking* é o *Man-in-the-Middle*. Nesta situação, o atacante está posicionado entre dois equipamentos válidos dentro da rede sem fio com o intuito de interceptar sua comunicação e instalar um *Access Point (AP)* falso. Esta instalação dá-se por enfraquecer o sinal do *AP* verdadeiro, seja por ruído ou inundação de tráfego, enquanto o sinal do *AP* falso encontra-se íntegro. Desta forma, comunicação ocorre através do *AP*

falso onde as informações são interceptadas e furtadas. A figura 5 ilustra o funcionamento deste ataque.

Figura 5: Funcionamento do ataque *hijacking* com a variante *Man-in-the-Middle.*



Fonte: Autoria própria.

A figura 5 ilustra o usuário conectado na rede sem fio fornecida pelo *AP Verdadeiro*. O atacante instala o *AP Falso* com as mesmas configurações do *AP Verdadeiro* e desta forma enfraquece o sinal daquele *AP*. Assim, o usuário conecta-se equivocadamente ao *AP Falso* e deste modo o ataque é concretizado e o furto de dados pode ocorrer;

- *Ataque de negação de serviço*: um dos inconvenientes das redes sem fio é a usabilidade restrita de sua banda passante. O ataque de negação de serviço ou *Denial of Service (DoS)* em uma *WLAN* consiste em saturar a rede com pacotes de forma que os serviços por ela oferecidos fiquem indisponíveis. Como por exemplo, considerar um atacante que já esteja autenticado em uma rede sem fio. Este atacante dispara inúmeros pacotes de *ping* contra diversos destinos dentro da rede sem fio e deste modo, a banda da rede ficará saturada pelos pacotes oriundos daquele atacante. Assim, os serviços legítimos oferecidos pela rede sem fio tornam-se indisponíveis;

- *MAC Address Spoofing*: uma técnica utilizada para mitigar os riscos de segurança em redes *WLAN* é restringir o acesso de dispositivos através de seu endereço *MAC*. Entretanto, caso o atacante descubra algum endereço *MAC* válido, este poderá substituir o endereço *MAC* inválido de um determinado dispositivo com o endereço *MAC* aceito pela rede. Desta forma, o ataque de *MAC address spoofing* consiste em empregar um endereço *MAC* válido em um equipamento cujo endereço *MAC* é inválido e assim conseguir acesso

à rede sem fio.

Os ataques descritos anteriormente podem levar a *intrusões*. Intrusão é uma tentativa de acessar ou manipular informações não autorizadas e deliberar ações que resultem em sistemas instáveis ou inutilizáveis (LIAO et al., 2013).

2.2 PROTEÇÃO DAS INFORMAÇÕES DISPONIBILIZADAS AO *BYOD*

Antes do ingresso de um dispositivo que será utilizado para *BYOD*, o usuário deve verificar quais são as políticas de segurança adotadas pela empresa. Assim, pode-se avaliar se aquele equipamento está apto a ser usado dentro do ambiente corporativo ou acessar informações remotamente. A seguir encontram-se descritas as principais recomendações de segurança para estes equipamentos (SOUPPAYA; SCARFONE, 2016):

- *Aplicar controles físicos de segurança*: aplicar um controle físico de segurança refere-se a impedir que terceiros acessem diretamente o dispositivo;
- *Criptografar o armazenamento do aparelho*: Ao encriptar as informações contidas no aparelho, somente o possuidor da chave de encriptação poderá acessá-las. Este fato deve-se, dependendo do método de encriptação empregado, a necessidade de inserir uma senha para a decodificação dos dados. Sem esta senha, os dados são ilegíveis;
- *Executar backups periódicos*: caso algum problema ocorra com o aparelho, como por exemplo: falha de *software* ou *hardware*, furto ou qualquer outra situação que cause a inacessibilidade dos dados, uma cópia de segurança deve estar disponível para restauração. Assim, evita-se que dados sejam perdidos e que prejuízos financeiros ocorram;
- *Destruir informações quando estas não são mais necessárias*: quando uma determinada informação não é mais necessária, a mesma deve ser destruída. Armazenar dados que não são mais necessários pode abrir uma superfície de ataque e consequentemente resultar em furto de dados e prejuízo financeiro. Uma informação não necessária não significa que ela não seja mais válida. Como por exemplo, um usuário que mudou de departamento. As informações do departamento anterior não são mais necessárias a ele, mas ainda assim são válidas para a empresa;
- *Apagar informações de um dispositivo perdido ou furtado*: caso um equipamento seja perdido ou furtado, as informações nele contidas devem ser removidas remotamente.

Este procedimento pode ser executado por aplicações *MDM*. Uma aplicação *MDM* possui a capacidade de gerenciar dispositivos móveis através de um console de administração central. Dentre outras características, o *MDM* possui a função de remover dados remotamente assim que o dispositivo for conectado a uma rede. Entretanto, isto somente será possível caso a aplicação do *MDM* tenha sido instalada no dispositivo em questão previamente.

Cada situação pode requerer uma diferente combinação de opções de segurança. Os itens relatados anteriormente podem não ser suficientes a uma determinada empresa, pois depende diretamente do valor da informação a ser protegida. Normalmente, as corporações aplicam os mesmos requisitos e recomendações de segurança para todos os tipos de informação. Este fato deve-se a dificuldade em diferenciar quais informações são realmente importantes das que não possuem relevância (SOUPPAYA; SCARFONE, 2016).

2.2.1 SEGURANÇA DE REDES SEM FIO

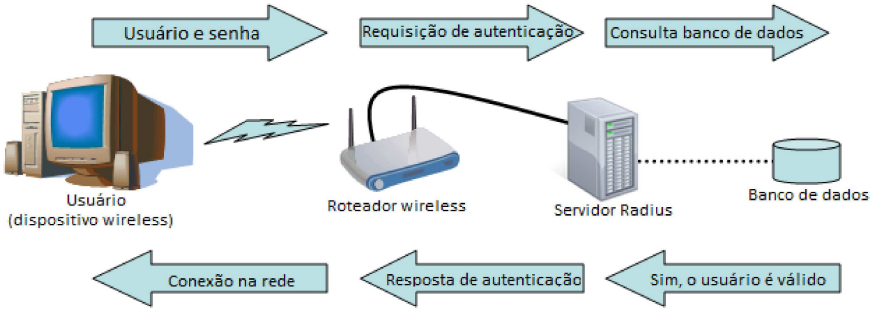
Para proteger os dispositivos conectados na rede sem fio, as redes denominadas *WLAN* oferecem *protocolos de segurança* com o intuito de fornecer encriptação e autenticação. Desta forma, os princípios da confidencialidade, disponibilidade e integridade podem ser preservados (NAKHILA et al., 2015; NOH et al., 2018). A seguir, estes protocolos de segurança encontram-se descritos:

- *WEP*: o protocolo *WEP* faz parte do padrão *IEEE 802.11* e é o primeiro protocolo de segurança a fornecer autenticação e encriptação na comunicação entre dispositivos sem fio. Em sua primeira versão, o *WEP* fornece encriptação de 40 bits, posteriormente suportando chaves de 104 bits (TEWS, 2007). Este protocolo possui os seguintes objetivos (BORISOV et al., 2001; HASSAN; CHALLAL, 2005):
  - *Confidencialidade*: manter o princípio da confidencialidade é o objetivo principal do protocolo *WEP*. Desta forma, o ataque *eavesdropping* pode ser mitigado;
  - *Controle de acesso*: o controle de acesso tem por objetivo proteger o acesso à rede sem fio. O padrão *IEEE 802.11* possui uma característica opcional de descartar todos os pacotes de rede que não estejam encriptados pelo *WEP*. Deste modo, somente os clientes de rede protegidos pelo *WEP* podem se comunicar;
  - *Integridade de dados*: o protocolo *WEP* garante a integridade dos pacotes de rede trafegados. Deste modo, os pacotes não podem ser alterados durante a transmissão.

Entretanto, o protocolo *WEP* apresenta vulnerabilidades de segurança, assim seus objetivos não podem ser plenamente atingidos. As vulnerabilidades e ataques contra este protocolo podem ser consultadas nos trabalhos de Borisov et al. (2001), Stubblefield et al. (2002) e Tews et al. (2007);

- *WPA*: em virtude das deficiências de segurança apresentadas pelo *WEP*, o protocolo *WPA* foi desenvolvido com o intuito de ser seu substituto. Deste modo, o *WPA* corrige as vulnerabilidades apresentadas pelo *WEP*. Além desta melhoria, o *WPA* possui dois modos de operação, conforme descritos a seguir (MAVRIDIS et al., 2011; CARVALHO et al., 2012):
  - *WPA-PSK*: o modo de operação *WPA-PSK* é normalmente utilizado para pequenos escritórios e ambientes domésticos. Diferentemente do protocolo *WEP*, o *WPA* emprega criptografia de até 256 bits e qualquer *string* alfanumérica pode ser utilizada para compor a chave de acesso à rede. Por exemplo, a chave de acesso à rede sem fio é configurada no dispositivo *AP* e a mesma chave deve ser inserida em cada equipamento que deseja conectar-se a rede;
  - *WPA Enterprise*: este modo de operação é utilizado principalmente por corporações de médio e grande porte. Diferentemente do *WPA-PSK*, o *WPA Enterprise* utiliza um servidor *Radius* externo para autenticação dos dispositivos ingressantes da rede. Um servidor *Radius* tem por objetivo centralizar o cadastramento, autenticação dos usuários e bem como fornecer políticas de acesso à rede (LASHKARI et al., 2009). Desta forma, cada usuário possui um *login* próprio. A figura 6 ilustra o funcionamento deste modo de operação.

Figura 6: Funcionamento do protocolo *WPA* no modo de operação *WPA Enterprise*.



Fonte: Adaptado de CISCO (2018).

Conforme ilustrado pela figura 6, o usuário informa seu *login*. Assim, a requisição de autenticação é processada ao enviar estes dados para o servidor *Radius*. Consequentemente, o servidor *Radius* verifica em seu banco de dados se aquele *login* é válido e em caso afirmativo, a conexão à rede sem fio é efetuada.

- *WPA2*: o protocolo *Wi-Fi Protected Access 2 (WPA2)* é uma evolução do *WPA*. A principal diferença entre eles está no algoritmo de encriptação. O *WPA2* utiliza o algoritmo *AES* para realizar a codificação, entretanto o *WPA* e *WPA2* são compatíveis entre si, inclusive o *WPA2* possui os mesmos modos de operação do seu antecessor (NAKHILA et al., 2015). O *AES* é utilizado como algoritmo de codificação padrão pelo governo federal dos Estados Unidos da América em virtude de sua alta confiabilidade (ORS et al., 2004);

- *WPA3*: em virtude das vulnerabilidades de segurança apresentadas pelo *WPA2*, o *Wi-Fi Protected Access 3 (WPA3)* foi lançado em junho de 2018 (WIFI-ALLIANCE, 2019). A principal alteração que o *WPA3* apresenta é o protocolo de autenticação entre os dispositivos clientes e o *AP*. O novo protocolo introduz o uso de *SAE* que mitiga algumas das vulnerabilidades presentes *WPA2*, como o ataque do tipo *KRACK*. O ataque *KRACK* consiste em reutilizar a chave de sessão para assim analisar o tráfego de rede e obter a decodificação dos dados. Com o emprego do *SAE*, a reutilização de chaves de sessão não é mais possível (KOHLIOS; HAYAJNEH, 2018; SAHINASLAN, 2019).

Os detalhes de codificação, funcionamento e vulnerabilidades dos protocolos *WEP, WPA*, *WPA2* e *WPA3* estão fora do escopo deste trabalho. Os trabalhos de Hassan e Challal (2005), Gonzales et al. (2010), Mavridis et al. (2011), Khasawneh et al. (2014), Kuo et al. (2018), Noh et al. (2018), Kohlios e Hayajneh (2018), Sahinaslan (2019), Bednarczyk e Piotrowski (2019) fornecem elucidação sobre este tema.

A utilização do protocolo *WPA3* é preferida em virtude de sua evolução ante ao *WPA*, *WPA2* e o *WEP*. Em contrapartida, o protocolo *WEP*, em razão de suas vulnerabilidades, deve ser utilizado somente caso seja a única opção disponível e que ainda assim seja em ambientes onde inexista acesso a informações relevantes. Assim, caso algum equipamento *BYOD* acesse algum sistema corporativo através de uma rede sem fio protegida pelo *WEP*, faz-se necessário uso de outras medidas protetivas, como uma *VPN*, por exemplo. Medidas adicionais de proteção como permitir a conexão somente de equipamentos cujo *MAC address* é válido e adotar chaves de rede cujos caracteres são diversificados, adicionam uma camada extra de segurança. Entretanto, ataques como *MAC address spoofing* e *hijacking*, apesar de menor probabilidade, ainda podem ocorrer e lograr êxito (SOUPPAYA; SCARFONE, 2016).

2.3 LÓGICA *FUZZY*

Na lógica tradicional, há somente duas possibilidades, *falso* e *verdadeiro*. Consequentemente, na teoria clássica dos conjuntos, um elemento pertence ou não à um determinado

conjunto. Na lógica *fuzzy*, o conceito de falso e verdadeiro é abordado pela variação do grau de verdadeiro, o quanto um dado elemento pertence à um conjunto em específico (BUSTINCE et al., 2015) . Desta forma, um elemento pode tanto pertencer à um conjunto quanto para outro, dependendo apenas do seu grau de pertinência. O grau de pertinência, definido no intervalo [0,1], demonstra o quanto um elemento pertence a um conjunto (NAIK, 2015; SHAO et al., 2016; FATIMA et al., 2017). As expressões 1 e 2 comparam o grau de pertinência dos elementos entre conjuntos clássicos ou *crisp* e conjuntos *fuzzy*.

$$f(x) = \begin{cases} 1, & \text{se, e somente se, } x \in A. \\ 0, & \text{se, e somente se, } x \notin A. \end{cases} \tag{1}$$

$$\mu(x) = \begin{cases} 1, & \text{se, e somente se, } x \in A. \\ 0, & \text{se, e somente se, } x \notin A. \\ 0 \leq \mu(x) \leq 1, & \text{se } x \text{ pertence parcialmente a } A. \end{cases} \tag{2}$$

Conforme apresentado na expressão 1, na teoria clássica dos conjuntos, um elemento x pertence integralmente ao conjunto A ou não pertence. De outra maneira, a expressão 2 demonstra que na lógica *fuzzy* um dado elemento x pode pertencer integralmente ao conjunto A, não pertencer ao conjunto A e também, pertencer parcialmente ao referido conjunto, apenas com a variação do grau de pertinência de x. Assim, os elementos de um conjunto *fuzzy* são representados através através da seguinte notação (ZADEH, 1996):

$$A = \{(x, \mu_A(x)) | x \in X\} \tag{3}$$

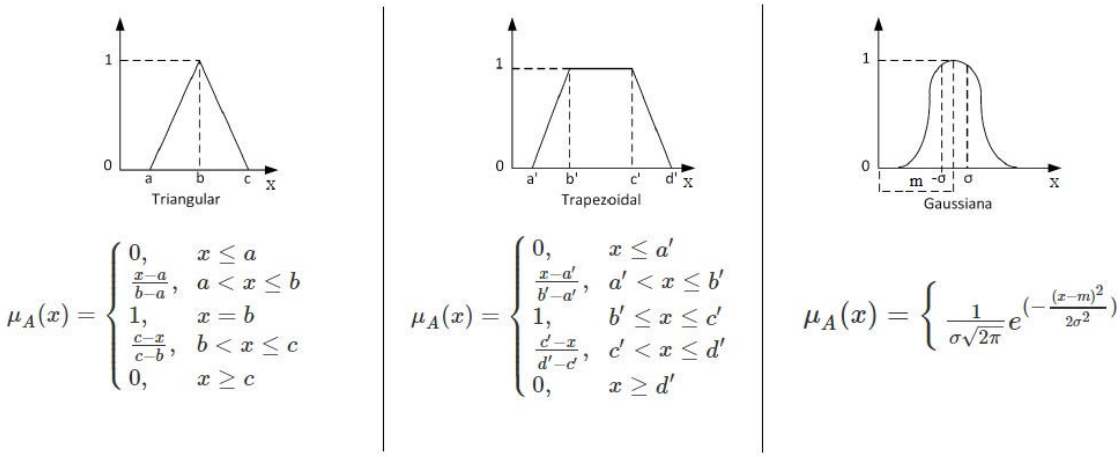
Conforme demonstrado pela notação 3, um conjunto *fuzzy* "A" é expresso pelo par ordenado "(x)" e "$\mu_A(x)''$ para todos os elementos pertencentes ao universo de discurso.

Baseado nesta premissa, a lógica *fuzzy* é recomendada em cenários onde a distinção entre os elementos dos conjuntos não encontra-se completamente definida. Esta lógica foi criada por Lotfi Zadeh em 1965 e assim permitiu o desenvolvimento de projetos como sistemas controladores de processos e sistemas de apoio à decisão. Os componentes básicos da lógica *fuzzy* encontram-se elucidados a seguir (ZADEH, 1996; YUNWU, 2009; ROUT; MOHANTY, 2015):

- *Processo de fuzificação*: na lógica *fuzzy*, os conjuntos descrevem termos linguísticos como "pouco", "bom", "baixo" e "alto", por exemplo, e as funções de pertinência de-

finem no intervalo [0,1] o grau de pertinência de um dado elemento naqueles conjuntos. As funções de pertinência mais comumente utilizadas são as do tipo triangular, trapezoidal e gaussiana. O processo de fuzificação consiste em correlacionar um valor de entrada, usualmente um valor numérico, com os conjuntos disponíveis através do grau de pertinência. A figura 7 ilustra o formato dos conjuntos *fuzzy* e a fórmula de cálculo de cada uma das funções de pertinência previamente citadas.

Figura 7: Funções de pertinência do tipo triangular, trapezoidal e gaussiana.



$$\mu_A(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a < x \leq b \\ 1, & x = b \\ \frac{c-x}{c-b}, & b < x \leq c \\ 0, & x \geq c \end{cases} \qquad \mu_A(x) = \begin{cases} 0, & x \leq a' \\ \frac{x-a'}{b'-a'}, & a' < x \leq b' \\ 1, & b' \leq x \leq c' \\ \frac{c'-x}{d'-c'}, & c' < x \leq d' \\ 0, & x \geq d' \end{cases} \qquad \mu_A(x) = \left\{ \frac{1}{\sigma\sqrt{2\pi}} e^{(-\frac{(x-m)^2}{2\sigma^2})} \right.$$

Fonte: Autoria própria.

Conforme exposto pela figura 7, cada função de pertinência possui formato e funções de cálculo distintas;

- *Base de regras*: o conteúdo da base de regras é inspirado na forma humada de tomar decisões. Um regra *fuzzy* é uma estrutura simples de decisão baseada em "SE-ENTÃO", onde as variáveis *fuzzy* são comparadas com termos linguísticos, tanto no antecedente quanto no consequente da regra. O antecedente e o consequente da regra podem conter mais de uma condição e são unidas pelos operadores 'E" ou "OU". A base de regras é normalmente criada por especialista da área , entretanto pode ser extraída através de algoritmos de *machine learning*. Por exemplo, uma regra *fuzzy* pode ser definida como "SE temperatura é "quente" ENTÃO velocidade do ventilador é "alta"";

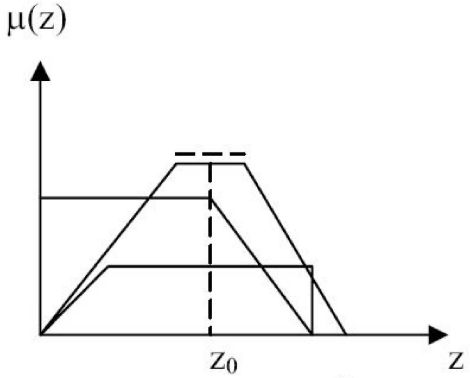
- *Inferência fuzzy*: a partir da inferência é possível obter conclusões lógicas, mesmo em cenários de incerteza, através do relacionamento dos valores de entrada com o que está definido na base de regras. O processo de inferência é similar ao modo humano de analisar dados e informações com o intuito de obter conclusões para a tomada de decisão. O processo de inferência inicia com a ativação das regras que mapeiam as entradas fornecidas pelo antecedente. O resultado da ativação de uma regra é um valor *fuzzy*, de-

rivado da agregação dos antecedentes através, por exemplo, da função mínimo para o operador lógico “E” ou a função máximo para o operador lógico “OU”, caso estes operadores estejam presentes na regra. Se os valores de ativação das regras resultarem no mesmo conjunto *fuzzy* do consequente, estas necessitam ser agregadas. Assim, a regra com maior valor prevalece em virtude desta já conter os valores das outras regras. Finalmente, os conjuntos de saída são delineados pelos valores de ativação resultantes da agregação das regras. Os métodos de inferência mais comumente utilizados são o método de *Mamdani* e o método de *Takagi-Sugeno* (CHADLI; BORNE, 2013). Detalhes acerca destes métodos podem ser obtidos nos trabalhos de Fukami et al. (1980), Mizumoto e Zimmermann (1982) e (JANG, 1993);

- *Processo de defuzificação*: a região de saída definida pelo mecanismo de inferência *fuzzy* configura, através de seus termos linguísticos, as possíveis saídas do sistema *fuzzy*. Entretanto, alguns cenários de aplicação necessitam de uma saída numérica apurada. Desta forma, o processo de defuzificação consiste em calcular uma saída numérica na região de saída. Estes cálculos podem ser feitos, por exemplo, através dos métodos “Média dos Máximos (MOM)” e “Centróide (COG)”. As figuras 8 e 9 apresentam o procedimento de cálculo de cada um destes métodos de defuzificação.

Figura 8: Método de defuzificação “Média dos Máximos”.

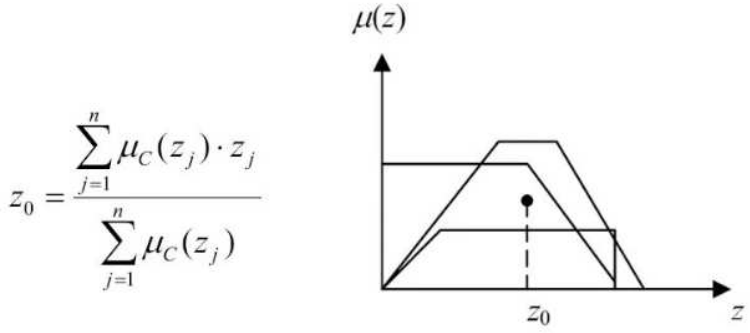
$$z_0 = \sum_{j=1}^{k} \frac{z_j}{k}$$



Fonte: Autoria própria.

Conforme ilustrado pela figura 8, este método de defuzificação consiste na média dos elementos que apresentam a maior pertinência. O componente *“z_j”* representa os elementos que atingem a maior pertinência, enquanto o componente *“k”* representa a quantidade de vezes que aqueles elementos ocorrem. De modo simular, o método de defuzificação representado pela figura 9 consiste em obter o centro de gravidade da figura delineada nos conjuntos *fuzzy* de saída. Assim, o componente *“C”* representa o conjunto *fuzzy* demarcado no universo de saída, enquanto o componente *“z_j”* representa todos os elementos

Figura 9: Método de defuzificação "Centróide".

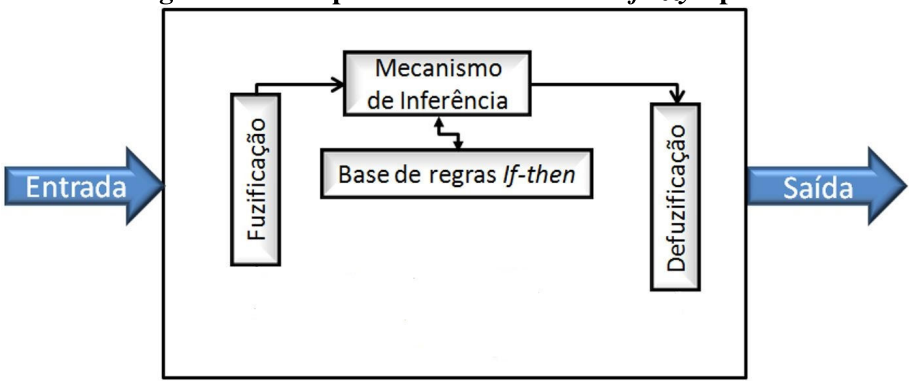


Fonte: Autoria própria.

quem compõe o referido conjunto.

A figura 10 ilustra um sistema *fuzzy* típico.

Figura 10: Componentes de um sistema *fuzzy* típico.



Fonte: Adaptado de Kanth (2016).

Conforme ilustrado pela figura 10, o sistema *fuzzy* recebe uma entrada numérica como variável de entrada. Então, o processo de fuzificação ocorre para atribuir graus de pertinência para a variável de entrada para cada conjunto *fuzzy* que faz parte da entrada. Depois deste processo, ocorre a inferência das regras e finalmente o processo de defuzificação é invocado.

2.4 OUTROS MÉTODOS DE APOIO À DECISÃO

Além da lógica *fuzzy*, o uso de *redes neurais artificias* e *algoritmos genéticos* podem ser empregados a sistemas de apoio à decisão. A rede neural artificial processa informações de modo distribuído e adquire conhecimento via treinamento através do processamento de exemplos (HODO et al., 2016). Os dados para processamento são recebidos por unidades denominadas *neurônios* ou *unidades neurais*. Os neurônios possuem pesos sinápticos para ponderar

cada valor de entrada (BURR et al., 2015). Assim, cada valor de entrada é multiplicado pelo respectivo peso sináptico e por fim estes produtos são somados. Deste modo, o valor de saída é obtido e, após ser processado por uma função de ativação, é enviado à próxima camada de neurônios. A união das camadas de neurônios formam a rede neural (WUERGES; BORBA, 2010; KARLIK; OLGAC, 2011; SAIED et al., 2016). O treinamento da rede neural determina os pesos sinápticos adequados para cada neurônio. Desde modo, a saída resultante do processamento dos neurônios da última camada são as mais próximas do resultado desejado para o problema que se deseja resolver (WUERGES; BORBA, 2010; CORTES et al., 2017).

Os algoritmos genéticos formam uma técnica de busca e otimização que é inspirada no princípio de Darwin para seleção natural (COSTA et al., 2010). Para buscar a solução ótima, de início, o algoritmo genético gera um conjunto de soluções randômicas para o problema para o qual foi desenvolvido. Após a geração deste conjunto, a *função de avaliação* calcula a aptidão de cada uma das soluções geradas. Assim, através de uma função de reprodução, as melhores soluções avaliadas são combinadas para formar novas soluções que, em tese, são melhores que suas antecessoras. O processo de avaliação e reprodução é repetido até que o conjunto de soluções não possa mais ser melhorado (WUERGES; BORBA, 2010; PANDEY, 2016; METAWA et al., 2017).

Os detalhes acerca das redes neurais artificiais e algoritmos genéticos estão fora do escopo desta dissertação. Os trabalho de Wuerges e Borba (2010), Karlik e Olgac (2011), Burr et al. (2015), Saied et al. (2016), Hodo et al. (2016), Cortes et al. (2017) e Metawa et al. (2017) fornecem elucidação sobre estes métodos de apoio à decisão.

2.5 CONCLUSÃO

O uso de políticas de *BYOD* ao contraponto de seus benefícios oferece riscos. Este capítulo apresentou as principais ameaças digitais e suas consequências que podem ser desencadeadas pela adoção do *BYOD*.

No que tange o dispositivo móvel, a parametrização por parte do usuário das configurações customizáveis do sistema operacional do equipamento é ponto chave no impacto de segurança causado no próprio dispositivo, demais equipamentos conectados à rede e também nas informações acessadas. Avaliar o modo em que estas configurações encontram-se parametrizadas fornece um indicador do impacto de segurança que o dispositivo pode causar. Do mesmo modo, o acesso indiscriminado a informações não classificadas em categorias de segurança pode permitir que aparelhos parametrizados do modo inseguro acessem dados de alta

relevância. Assim, em caso de eventual furto de dados, as consequências são acentuadas.

Este capítulo também demonstrou a fundamentação e a importância de métodos de apoio à decisão. Assim, o uso desses mecanismos pode auxiliar na resolução de inconvenientes na área da segurança computacional.

A seguir, o capítulo 3 apresenta em detalhes os trabalhos relacionados que compõe o estado da arte do tema abordado por esta dissertação.

3 REVISÃO DA LITERATURA

Este capítulo tem por objetivo apresentar os trabalhos relacionados com o tema de pesquisa desta dissertação e bem como suas contribuições. A seção 3.1 descreve o método de pesquisa utilizado para a seleção das publicações. Na sequência, as seções 3.2 e 3.3 apresentam em detalhes as publicações selecionadas. Uma breve discussão é proposta na seção 3.4 e por fim, o capítulo encerra-se com a conclusão na seção 3.5.

3.1 MÉTODO DE PESQUISA

O tema deste trabalho está vinculado ao uso seguro da política de *BYOD*. Dentre os riscos de segurança, as configurações customizáveis do dispositivo e os dados armazenados no equipamento são um dos pontos-chave a serem explorados por vulnerabilidades e atacantes. Desta forma, procedeu-se à pesquisa acerca de publicações que elucidem a importância dos dados armazenados no equipamento e o impacto causado pelas configurações customizáveis. Adicionalmente, publicações que aplicam técnicas para classificação de dados, como lógica *fuzzy*, também são apresentadas.

A tabela 4 apresenta os termos utilizados para executar a pesquisa das publicações que compõe o estado da arte.

Tabela 4: String de busca utilizada.

String A	Operador Lógico	String B
BYOD	AND	Custom configuration
Bring Your Own Device		Corporate data
Smartphone		Data leakage
		Sensitive information
		Security
		Risk assessment
		Fuzzy

Fonte: Autoria própria.

Conforme ilustrado pela tabela 4, para a execução da busca de publicações é utilizado

o operador lógico “OR” em conjunto com o operador lógico “AND” na seguinte regra:

$$(SA_1 \text{ OR } SA_2 \text{ ... OR } SA_n) \text{ AND } (SB_1 \text{ OR } SB_2 \text{ ... OR } SB_n)$$[1]

Após a formulação da *string* de pesquisa, as seguintes bibliotecas digitais foram selecionadas: IEEE Xplore[2], ACM Digital Library[3], Springer Link[4], Science Direct[5], Scopus[6] e Portal Capes[7].

Durante o processo de busca nas bibliotecas digitais citadas, sinônimos para os termos de pesquisa também foram utilizados. Como parâmetro de restrição, foram selecionados trabalhos publicados no período de 2010 até 2018 e escritos no idioma inglês. Para a consulta, os campos “Resumo”, “Título” e “Palavras Chave” *(Title, Abstract, Key Words)* foram considerados.

3.2 TRABALHOS RELACIONADOS

Esta seção apresenta em detalhes os trabalhos selecionados. Como forma de proporcionar maior organização e facilidade de leitura, os trabalhos encontram-se divididos em subseções intituladas conforme o título de cada publicação. Os trabalhos relacionados ao uso da lógica *fuzzy* encontram-se descritos na seção 3.3.

3.2.1 BYOD SECURITY ENGINEERING: A FRAMEWORK AND ITS ANALYSIS

O trabalho proposto por Zahadat et al. (2015) apresenta um *framework* com recomendações para o ciclo de vida do dispositivo utilizado para *BYOD*. Este ciclo de vida inicia-se com o registro do equipamento junto à corporação, provisiona as configurações e aplicativos necessários, bem como os procedimentos para o fim da vida útil daquele equipamento.

Especificamente, devem ser levadas em consideração, segundo os autores, se aquele equipamento que deseja ingressar à rede corporativa atende os requisitos mínimos, como suporte à autenticação de dois fatores, suporte a algoritmos de encriptação *WPA2* para redes sem fio e adicionalmente, a importância de conhecer a localização física do equipamento. A informação da localização é obtida através do módulo *GPS* do aparelho *BYOD*. Assim pode-se saber se algum equipamento cujas coordenadas *GPS* apontam para um local não autorizado pela

[1] SA refere-se ao conjunto de termos de “String A” e SB refere-se ao conjunto de termos de “String B”.
[2] http://ieeexplore.ieee.org
[3] http://dl.acm.org
[4] https://link.springer.com
[5] http://www.sciencedirect.com
[6] https://www.scopus.com
[7] https://www.periodicos.capes.gov.br

empresa e que está tentando acessar informações corporativas.

Além das configurações necessárias, os dados gravados no equipamento também são relevantes. Como por exemplo, um dispositivo do diretor da empresa pode armazenar documentos sigilosos e deste modo, necessita proteção adicional para prevenir o furto de dados, como encriptação de memória, por exemplo. O *framework* proposto também prevê medidas em caso de perda do equipamento, execução de *backup*, detecção de vulnerabilidades, dentre outros.

A validação do trabalho proposto foi realizada por meio de um questionário que foi respondido por 114 especialistas em segurança. Em conclusão, o *framework* desenvolvido é eficaz para solucionar ou mitigar os riscos oferecidos pelo *BYOD*.

O *framework* proposto pode ser utilizado por quaisquer corporações. Entretanto, o trabalho não apresenta nenhuma ferramenta automatizada para a execução deste processo.

3.2.2 DEVELOPING A NATO BYOD SECURITY POLICY

O trabalho proposto por Armando et al. (2016) argumenta acerca dos benefícios oferecidos pela política de *BYOD* e em contraponto, os riscos relacionados à segurança. De acordo com os autores, o maior risco é o furto de dados causado por *malware* ou por aplicações que possam armazenar dados corporativos sem a devida permissão.

Como proposta para oferecer o uso seguro do *BYOD*, políticas de acesso baseadas nas políticas de segurança fornecidas pela *Agência de Comunicações da OTAN (Organização do Tratado do Atlântico Norte)* são desenvolvidas. De acordo com estas políticas de segurança, dados e informações são ativos importantes e necessitam de controles de acesso específicos. Assim pode-se evitar a violação da confidencialidade, integridade e disponibilidade. Os aplicativos instalados no *smartphone BYOD*, somente os aparelhos baseados no sistema operacional *Android*, são verificados de acordo com as políticas de acesso definidas pelo administrador.

Para a automatização desta tarefa, o aplicativo *BYODroid* é modificado. Esta aplicação conta com um portal de administração, um servidor cuja função é armazenar as políticas criadas, verificar as aplicações a serem instaladas, dentre outras. O último componente é a aplicação cliente instalada diretamente no dispositivo móvel. Assim, o cliente comunica-se com o servidor para receber as políticas. As políticas podem, por exemplo, impedir a instalação de *softwares*, gravar e acessar determinados arquivos corporativos, dentre outros.

Em conclusão, os autores comentam que este trabalho foi inicialmente desenvolvido para a própria agência de comunicações da *OTAN* e em virtude do ambiente controlado, mais testes de campo são necessários para validar a eficácia da proposta em outros cenários.

3.2.3 TOWARDS ENFORCING ON-THE-FLY POLICIES IN BYOD ENVIRONMENTS

Costantino et al. (2013) comentam em seu trabalho que a adoção do *BYOD* é benéfica tanto para o usuário quanto para a empresa. Entretanto, o furto de dados ocorreu em aproximadamente 50% das corporações que implantaram esta política.

Como proposta, um *framework* que tem como foco atribuir políticas de segurança a determinados perfis de acesso é desenvolvido. De acordo com os autores, torna-se mais eficaz atribuir perfis de acesso aos dispositivos utilizados para *BYOD* do que protegê-los individualmente. Políticas de segurança contendo, por exemplo, permissões de acesso a aplicativos e recursos de rede corporativos são criadas pelo administrador e são atribuídas ao determinado perfil, como perfil de um diretor.

O *framework* é constituído pela aplicação cliente, instalada diretamente no dispositivo móvel, e pelo servidor de aplicação. Este servidor armazena as políticas definidas e as atribui automaticamente após o login do usuário através da aplicação cliente. Assim, o cliente e o servidor comunicam-se constantemente e caso existam alterações no perfil, elas são aplicadas automaticamente sem a necessidade de intervenção do usuário. Do mesmo modo, caso incidentes relacionados à violação das políticas de segurança ocorram, os mesmos podem ser reportados ao administrador ou ações automatizadas podem ser tomadas, como por exemplo, não permitir que o dispositivo continue a acessar o sistema. Em conclusão, os autores argumentam que se faz necessário experimentos com protótipo em ambientes não simulados, a fim de validar o *framework* proposto.

3.2.4 BENCHMARKING USER-DEFINED SECURITY CONFIGURATIONS OF ANDROID DEVICES

No trabalho proposto por Vecchiato (2016), aborda-se a popularização do *BYOD*, a crescente quantidade de informações armazenadas naqueles dispositivos e também duas das principais ameaças relacionadas: furto de dados e violação de privacidade. Como forma de mensurar o risco das ameaças de furto de dados e violação de privacidade, os autores aplicam uma abordagem voltada para a avaliação das configurações customizáveis do sistema operacional *Android*. Estas configurações, como por exemplo, *habilitar /desabilitar interface bluetooth*, *habilitar / desabilitar senha de desbloqueio de tela*, dentre outras, influenciam diretamente na segurança do equipamento. Deste modo, os parâmetros das configurações são coletados e comparados com valores seguros recomendados pela literatura.

O processo de coleta de informações é automatizado através ferramenta desenvol-

vida pelos próprios autores. Esta ferramenta proporciona quantificar quais configurações são mais negligenciadas pelos usuários e quais medidas corretivas adotar. Estas medidas incluem a notificação do usuário acerca dos parâmetros inseguros coletados, bem como o procedimento recomendado de correção.

3.2.5 UNDERSTANDING USERS' REQUIREMENTS FOR DATA PROTECTION IN SMARTPHONES

No trabalho proposto por Muslukhov et al. (2012), os autores abordam a importância das informações que usuários armazenam em *smartphones* de acordo com os princípios da confidencialidade, disponibilidade e integridade. Como forma de mensurar quais tipos de informações são armazenadas nos aparelhos e bem como sua importância, uma pesquisa com proprietários de *smartphones* foi realizada. Como resultado, revelou-se que senhas de aplicativos, documentos relacionados ao trabalho, fotos, vídeos, dentre outros dados armazenados no *smartphone* são considerados importantes, principalmente no que refere-se à confidencialidade. Resultados adicionais da pesquisa evidenciam que os usuários, em sua maioria, não adotam medidas protetivas para evitar o furto de dados ou preservação do princípio da disponibilidade, como a execução de *backups*. Deste modo, os autores concluem que estes dispositivos armazenam arquivos pessoais e corporativos sigilosos mas que não recebem a segurança necessária a fim que estas informações permaneçam protegidas.

3.2.6 ON THE NEED FOR DIFFERENT SECURITY METHODS ON MOBILE PHONES

Em seu trabalho, Ben-Asher et al. (2011) comentam sobre a necessidade de novos métodos de autenticação para proteger diferentes tipos de dados alocados em aparelhos móveis. Estes métodos baseiam-se no modelo biométrico, pois segundo os autores fornecem maior segurança no processo de autenticação do usuário. De acordo com a pesquisa, a utilização da autenticação *PIN* não fornece um nível de segurança adequado pois pode ser facilmente deduzido em função de seu curto tamanho, normalmente quatro caracteres numéricos. Em um *survey* realizado pelos autores, revelou-se que senhas, e-mails, arquivos armazenados no *smartphone* possuem um elevado grau de importância confidencial para os usuários, tanto no contexto pessoal quanto no corporativo.

3.2.7 A RISK ASSESSMENT METHOD FOR SMARTPHONES

O trabalho proposto por Theoharidou et al. (2012) apresenta um método para avaliação de risco de segurança para *smartphones*. Conforme os autores, a avaliação de risco para dispo-

sitivos móveis deve incluir além das ameaças tradicionais, como por exemplo: vulnerabilidades do sistema operacional e infecção por *malware*, o impacto da violação da confidencialidade, disponibilidade e integridade das informações contidas no aparelho. O método de avaliação de risco proposto é baseado na probabilidade e impacto de uma determinada ameaça ocorrer. Entretanto, os valores para probabilidade e impacto das ameaças são fornecidos pelo próprio usuário e nenhuma ferramenta foi desenvolvida para automatizar o processo de avaliação.

3.2.8 SECURITY BENCHMARKS

As publicações fornecidas por CIS (2018) têm por objetivo fornecer boas práticas para que os profissionais possam avaliar a segurança de sistemas corporativos. Denominadas *CIS Benchmarks*, essas publicações são em formato de documentos descritivos e encontram-se disponíveis para uma série de sistemas comerciais e *open source*, como por exemplo, *Apple iOS* e *Google Android*.

O conteúdo de cada documento é voltado para as configurações relevantes de cada sistema. Assim, descrições e esclarecimentos acerca de uma determinada configuração são fornecidos, bem como quais são os valores ou opções recomendadas para aquela configuração. As opções ou valores recomendados mitigam os riscos de segurança que aquela configuração poderia oferecer e assim, a segurança geral relacionada ao uso daquele sistema é ampliada. As orientações fornecidas pelos documentos são baseadas na experiência de profissionais. Entretanto, nenhuma ferramenta para automatização do processo de avaliação é fornecida.

3.3 USO DE LÓGICA FUZZY PARA SEGURANÇA

A lógica *fuzzy* permite o desenvolvimento de sistemas inteligentes (MENDEL, 2017). As subseções seguintes, intituladas conforme o título de cada publicação, apresentam os trabalhos que empregam a lógica *fuzzy* como elemento principal para a avaliação de segurança em ambientes computacionais.

3.3.1 FUZZY LOGIC-BASED IMPLICIT AUTHENTICATION FOR MOBILE ACCESS CONTROL

No trabalho desenvolvido por Yao et al. (2016), os autores propõe a utilização de lógica *fuzzy* para avaliar a legitimidade dos usuários de *smartphones*. A violação da confidencialidade dos dados contidos nos aparelhos é comum, principalmente em virtude da perda ou furto do dispositivo. Desta forma, os autores desenvolveram um protótipo de *software* que coleta deter-

minadas informações contidas no aparelho, tais como: quantidade mensagens *SMS* recebidas e enviadas, quantidade de chamadas de voz recebidas e realizadas, histórico de uso do navegador *web* e histórico de conexões a redes sem fio. Em seguida, estas informações são processadas por um sistema de inferência *fuzzy*. O perfil do usuário é criado e a medida que novos dados são coletados do aparelho e são processados pelo protótipo, os resultados são comparados. Assim, o grau de legitimidade do usuário daquele equipamento é mensurada. Em conclusão, os autores afirmam que a precisão fornecida pelo protótipo é superior a 90%.

3.3.2 FUZZY INFERENCE BASED INTRUSION DETECTION SYSTEM: FI-SNORT

A publicação de Naik (2015) propõe a utilização de lógica *fuzzy* para auxiliar na detecção de invasões em redes de computadores. As ferramentas tradicionais utilizadas para evitar invasões de rede somente aplicam ações corretivas ou alertam o administrador quando uma invasão já está em andamento. Para resolver este inconveniente, os autores desenvolvem um sistema de inferência *fuzzy* agregado à ferramenta de detecção de invasões *Snort*. O sistema de inferência desenvolvido recebe três dados do *Snort*: o tempo médio que um cliente de rede recebe um pacote de uma determinada origem, a quantidade de pacotes que um cliente de rede recebe de uma determinada origem e a quantidade de pacotes que um cliente de rede envia a um determinado destino. Assim, estas três informações são utilizadas como variáveis de entrada do sistema de inferência *fuzzy*. Desta forma, o sistema de inferência analisa os dados recebidos de acordo com suas regras e fornece um valor de saída. Este valor fornece ao administrador um indicador, dentro de uma escala de probabilidade, de uma invasão estar em curso. Em conclusão, os autores comentam que o protótipo proposto é válido, pois fornece ao administrador um nível de alerta para que ações corretivas sejam tomadas antes da invasão se concretizar.

3.3.3 FUZZY LOGIC BASED ANDROID MALWARE CLASSIFICATION APPROACH

O trabalho apresentado por Nayak et al. (2014) aborda a necessidade da classificação de *malware* em dispositivos com o sistema operacional *Android*. A seção 2.1.1 deste trabalho apresenta quais são as categorias de *malware* mais comumente encontradas. Um *malware* pode possuir características que o enquadrem em mais de uma categoria, como *trojan* e *ransomware*, por exemplo. Desta forma, para resolver este inconveniente, os autores propõe um sistema de inferência *fuzzy* que avalie as características de cada *malware*, baseando-se principalmente nas permissões requisitadas por este durante a instalação. Assim, é possível fornecer um enquadramento em uma ou mais categorias de *malware*. Em conclusão, o sistema *Fuzzy* proposto apresenta um índice de acerto próximo de 90% e demonstrou-se superior a modelos

que utilizam outras abordagens descritas naquele trabalho.

3.4 DISCUSSÃO

Este capítulo apresenta os trabalhos relacionados com o tema deste estudo. Estes trabalhos apontam os benefícios relacionados ao *BYOD* e em contrapartida, seus inconvenientes. A maioria das publicações evidenciam que o furto de dados e a violação dos princípios da disponibilidade, integridade e principalmente da confidencialidade são um dos maiores desafios relacionados ao uso da política *BYOD*.

O trabalho de Vecchiato (2016) avalia o impacto da parametrização, por parte dos usuários, das configurações customizáveis do sistema operacional *Android*. O autor baseia-se nos documentos fornecidos pela *CIS* e assim coleta as configurações de 561 dispositivos. Conforme demonstrado em seu trabalho, 71,15% dos aparelhos avaliados possuem deficiência no que refere-se à senha de acesso, 31,9% dos equipamentos apresentam permissões incorretas de sistemas e 47,09% apresentam configurações inseguras relacionadas à rede. Assim, a parametrização das configurações customizáveis pelo usuário pode influenciar não somente no furto de dados mas também violar princípios como a confidencialidade, integridade e disponibilidade. Entretanto, o trabalho não relaciona a relevância das informações gravadas no *smartphone* com o impacto de segurança das configurações customizáveis.

Os trabalhos de Ben-Asher et al. (2011), Muslukhov et al. (2012) e Armando et al. (2016) sugerem que diferentes tipos de informações necessitam de diferentes tipos de proteção. Assim, relacionar os arquivos corporativos armazenados no dispositivo *BYOD* com suas configurações customizadas pode fornecer uma avaliação para o risco de furto de dados.

Os trabalhos de Yao et al. (2016), Naik (2015) e Nayak et al. (2014) demonstram a flexibilidade fornecida pela *lógica fuzzy*. Com a utilização desta lógica estes autores obtiveram resultados mensuráveis e classificáveis através do relacionamento de diferentes dados.

A contribuição deste trabalho de dissertação está na proposta de classificar o impacto de segurança causado pelo dispositivo móvel através da avaliação dos parâmetros das configurações customizáveis e a quantificação dos arquivos de dados do usuário armazenados no equipamento. De acordo com a avaliação de risco, o equipamento é classificado a acessar informações corporativas cuja relevância é compatível com o grau de risco apresentado pelo aparelho. A tabela 5 apresenta um comparativo dos trabalhos relacionados.

A análise de risco fornece embasamento para mensurar o quanto um dado equipamento é vulnerável em um determinado aspecto (THEOHARIDOU et al., 2012). Assim, torna-se

Tabela 5: Comparação desta dissertação com os trabalhos relacionados mais relevantes.

Publicação	Ferramenta Segurança	Análise Risco	Informações Armazenadas	Análise Configurações	Políticas Acesso
Zahadat et al. (2015)			●		
Armando et al. (2016)	●		●		●
Costantino et al. (2013)					●
Vecchiato (2016)	●	●		●	
Muslukhov et al. (2012)			●		
Ben-Asher et al. (2011)			●		
Theoharidou et al. (2012)		●	●		
CIS (2018)				●	
Yao et al. (2016)	●				
Naik (2015)	●				
Nayak et al. (2014)	●				
Esta dissertação	●	●	●	●	

Fonte: Autoria própria.

possível avaliar parâmetros como configurações customizáveis e dados armazenados para então obter conclusões lógicas quanto a sua segurança. De maneira similar, a implementação de ferramentas de segurança permite a execução automatizada de cada proposta dos trabalhos aqui apresentados.

3.5 CONCLUSÃO

Este capítulo apresentou os trabalhos que compõe o estado da arte em relação ao tema desta dissertação. Dispositivos móveis armazenam dados relevantes tanto de cunho pessoal quanto profissional. Conforme demonstrado, o furto de dados é uma ameaça recorrente e um dos causadores é a parametrização insegura das configurações customizáveis do sistema operacional do equipamento. A seguir, o capítulo 4 apresenta um modelo para avaliação do impacto de segurança de dispositivos móveis para mitigar o impacto causado pelo furto de dados em ambientes *BYOD*.

4 UM MODELO PARA AVALIAÇÃO DO IMPACTO DE SEGURANÇA DE DISPOSITIVOS MÓVEIS

Este capítulo apresenta a proposta para a mitigação das consequências oriundas do furto de dados e outras ameaças digitais encontradas em ambientes onde a política de *BYOD* é adotada. A seguir, a visão geral da proposta é exibida. Na sequência, as configurações customizáveis consideradas por este trabalho, suas possíveis vulnerabilidades e níveis de impacto de segurança são descritas. Por seguinte, os dados que o usuário costumeiramente salva no dispositivo são elencados e bem como, o modelo de acesso a informações corporativas é apresentado. Por fim, o capítulo encerra-se na apresentação das limitações da proposta e a conclusão.

4.1 VISÃO GERAL

Os aparelhos utilizados para *BYOD* representam uma parcela dos dispositivos móveis empregados para fins corporativos. Como característica, estes equipamentos podem armazenar informações de distintas categorias de segurança. Assim, um destes dispositivos pode conter desde arquivos de conteúdo irrelevante até arquivos que são classificados em categorias de segurança de alta relevância. A discussão sobre as categorias de segurança nas quais as informações podem ser classificadas encontra-se na seção 2.1.3. Conforme descrito nos capítulos 2 e 3 deste trabalho, o uso de aparelhos utilizados para *BYOD* oferece riscos que podem desencadear o furto de dados, dentre outras ameaças.

As publicações de Ben-Asher et al. (2011), Muslukhov et al. (2012) e Armando et al. (2016) sugerem que as informações armazenadas no dispositivo móvel necessitam de proteção compatível com sua categoria de segurança. De forma similar, a obra de Vecchiato (2016) argumenta que quanto mais informações um equipamento armazena, maior é a probabilidade que este equipamento contenha informações críticas. Adicionalmente, o trabalho também apresenta os diferentes graus de impacto de segurança causados pela customização das configurações do sistema operacional do dispositivo móvel. Partindo da premissa de que quanto mais dados um equipamento móvel armazena, maior é a probabilidade de algum dado se encontrar na categoria de segurança de média ou alta relevância. Assim conclui-se que para mitigar os

impactos causados pelo furto de dados e outros inconvenientes, o risco de segurança oferecido pelas configurações customizáveis do aparelho deve ser o menor possível. Assim, este trabalho vislumbra a possibilidade de mensurar o impacto de segurança das configurações customizáveis do equipamento e relacionar com a quantidade de arquivos de dados armazenados pelo usuário. Desta maneira, pode-se qualificar o equipamento utilizado para *BYOD* a acessar somente informações cuja categoria de segurança seja compatível com o grau de impacto de segurança que o aparelho representa.

4.2 CONFIGURAÇÕES CUSTOMIZÁVEIS

A seção 2.1.2 apresenta a definição e as ameaças geradas pelas configurações customizáveis do dispositivo móvel. O ajuste de parâmetros de cada configuração gera um impacto de segurança diferenciado no sistema. Esse impacto pode aumentar o nível de segurança do dispositivo caso a configuração seja parametrizada seguramente e por outro lado, a parametrização insegura expõe o equipamento a riscos de segurança (KRITZINGER; SOLMS, 2010; BECHER et al., 2011; VECCHIATO, 2016).

A tabela 6 apresenta as configurações customizáveis dos sistemas operacionais *Apple iOS* e *Google Android* cujo impacto de segurança é relevante caso estas encontrem-se ajustadas de modo não seguro (VECCHIATO, 2016; CIS, 2018). Estes sistemas operacionais possuem aproximadamente 97% da participação no mercado de sistemas operacionais para dispositivos móveis. Por esse motivo, os demais sistemas foram descartados por este trabalho (HU et al., 2018). A tabela também apresenta recomendações de segurança, como por exemplo “instalar ferramenta anti-malware, “apagar todos os dados do aparelho antes de descartá-lo”, “verificar permissões de aplicativos periodicamente”, “manter aplicativos atualizados”, “conectar somente em redes *wi-fi* confiáveis” e “utilizar VPN quando conectado em rede pública”. Estas recomendações, quando seguidas, podem aprimorar a segurança do equipamento e assim evitar ameaças digitais (CIS, 2018).

A customização das configurações, em sua maioria, pode ser efetuada manualmente pelo usuário através da interface do próprio sistema operacional. Entretanto, situações onde se deseja obter privilégios e funções não disponíveis originalmente no sistema operacional, como efetuar o *root* ou *jailbreak*, alterar permissões dos diretórios “/system” e “/data”, as ações devem ser executadas a partir de ferramentas de terceiros (ZHOU; JIANG, 2012). O fabricante do sistema operacional *iOS* fornece um aplicativo denominado “Apple Configurator” [1] com o intuito de padronizar e automatizar a configuração daquele sistema operacional. Entretanto,

[1] https://support.apple.com/apple-configurator

Tabela 6: Configurações customizáveis e recomendações de segurança.

Configurações	iOS	Android	Valor recomendado
Categoria - Senha			
Uso de senha	X	X	Ativado
Permitir senha simples	X		Desativado
Uso de senha alfanumérica	X	X	Ativado
Uso de senha visível		X	Desativado
Aplicar remoção de dados do usuário após excessivas senhas inválidas	X	X	Ativado, 10 tentativas
Quantidade de tentativas para senhas inválidas	X		6
Configurar idade máxima para senha		X	Até 90 dias
Ativar o histórico de senhas		X	Mínimo de 24 senhas
Configurar tamanho mínimo da senha	X	X	6 iOS, 5 Android
Configurar tamanho mínimo de caracteres complexos	X	X	2
Visibilidade da senha tipo ”padrão”		X	Desativada
Categoria - Rede			
Remover Redes *Wi-Fi* conhecidas	X	X	Ativado
Notificação de rede	X	X	Desativada
Interface *Wi-Fi* quando não necessária	X	X	Desativada
Interface *bluetooth* quando não necessária	X	X	Desativada
Hotstpot pessoal quando não necessário	X	X	Desativado
Proteção do cartão *Subscriber Identity Module (SIM)*		X*	Ativada
Descoberta de *bluetooth*	X	X	Desativada
Função de auto reconectar para todas as redes sem fio	X	X*	Desativada
Conexão VPN quando não necessária	X	X*	Desativada
Conectar somente em redes *wireless* confiáveis	X	X	-
Assistente *Wi-Fi*		X*	Desativado
Utilizar VPN quando conectado em *wireless* pública	X	X	-
Categoria - Permissão			
Permissão de escrita no diretório /system		X	Desativada
Permissão de escrita no diretório /data		X	Desativada
Uso de “Jailbreak” (root)	X	X	Desativado
Categoria - Sistema			
Configurar tempo para bloqueio de tela	X	X	Máximo iOS 120, Android 90 segundos
Botão desliga ao ser pressionado bloqueia imediatamente a tela	X	X	Ativado
Encriptação do armazenamento de dados		X	Ativada
Opção para desenvolvedores		X	Desativada
Instalação de aplicativos de fontes desconhecidas		X	Desativada
Uso de serviços de localização quando não necessários	X	X	Desativado
Uso de localização simulada	X	X	Desativado
Ajuste automático de fuso horário	X	X	Ativado
Ajuste automático de data	X	X	Ativado
Instalar ferramenta anti-malware		X	Instalada
Descoberta do *AirDrop*	X		Desativada
Permitir discagem de voz enquanto aparelho estiver bloqueado	X		Desativado
Permitir o uso da ”Siri”enquanto o aparelho estiver bloqueado	X		Desativado
Desabilitar *previews* de aplicativo quando o aparelho estiver bloqueado	X		Desativado
Uso da função para não permitir a remoção do perfil do usuário	X		Ativado
Permitir que aplicativos gerenciados armazenem dados no *iCloud*	X		Desativado
Backups codificados no *iCloud*	X		Ativado
Forçar a encriptação de backups	X		Ativado
Permitir que usuários aceitem certificados TLS não confiáveis	X		Desativado
Permitir documentos de fontes não gerenciadas para destinos gerenciados	X		Desativado
Considerar *AirDrop* como um destino não gerenciado	X		Desativado
Permitir o uso de *Handoff*	X		Desativado
Mostrar central de controle quando a tela está bloqueada	X		Desativado
Aviso de fraude	X		Ativado
Gerenciamento de domínios do *Safari*	X		Ativado
Permitir notificações somente de aplicativos gerenciados	X		Ativado
Mostrar a Central de Notificações enquanto a tela está bloqueada	X		Desativado
SMS preview quando o aparelho estiver bloqueado	X	X*	Desativado
Acesso à Central de Controle quando o aparelho estiver bloqueado	X		Desativado
Apagar todos dados do aparelho antes de descartá-lo	X	X	-
Uso da função ”Encontre meu Dispositivo”	X	X*	Ativado
Verificar se *firmware* está atualizado	X	X*	Ativado
Uso do *Smart Lock*		X*	Desativado
Permitir a localização remota do dispositivo		X*	Ativado
Remover perfil de usuário convidado		X*	-
Verificar permissões de aplicativos periodicamente		X	-
Categoria - Conteúdo			
Limitar o número de mensagens SMS		X	Até 20
Limitar o número de mensagens Multimídia		X	Até 20
Permitir o usuário mover as mensagens desta conta de e-mail	X		Desativado
Manter aplicativos atualizados	X		-
Categoria Navegador			
Aceitar web cookies	X		Dos sites que visito ou site atual
Uso de “autocompletar formulários” no navegador	X	X*	Desativado
Uso de *plugins* do navegador		X*	Desativado
Lembrar senhas dentro do navegador	X	X*	Desativado
Verificação SSL de sites	X	X*	Ativada

Fonte: Vecchiato (2016), CIS (2018).

somente a parametrização das configurações autorizadas pela *Apple* pode ser executada. De maneira similar, o sistema operacional *Android* também permite a leitura e ajuste automatizado de configuração através de ferramenta de terceiros, exceto pelos itens marcados com um asterisco na tabela 6 (VECCHIATO, 2016).

4.2.1 AMEAÇAS RELACIONADAS A CONFIGURAÇÕES CUSTOMIZÁVEIS

Os itens descritos na tabela 6 podem gerar vulnerabilidades e, consequentemente, ampliar o espectro de ataques caso estes estejam ajustados para valores diferentes do recomendado. Os itens que compõe a categoria de "Senha" fornecem uma barreira inicial contra acessos não autorizados ao equipamento. A ativação de configurações que requerem senhas alfanuméricas, caracteres numéricos e caracteres complexos favorece o uso de senhas não triviais. Assim, torna-se menos provável o êxito de acesso não autorizado ao dispositivo através da dedução da senha de desbloqueio. De modo similar, desabilitar a visibilidade de senhas previne que pessoas próximas vejam eventuais caracteres digitados (SCHAUB et al., 2012; KAMBOURAKIS et al., 2016).

A utilização das interfaces *wireless* e *bluetooth* facilita acesso à Internet e a outros equipamentos. Entretanto, conforme reportado pelo *CVE*, o sistema operacional *Android* acumula 23 vulnerabilidades relacionadas ao uso do *Wi-Fi* e 55 vulnerabilidade relacionadas à tecnologia *bluetooth*. Da mesma maneira, o sistema operacional *Apple iOS* possui 18 vulnerabilidades relacionadas ao uso da interface *wireless* e 11 vulnerabilidades associadas ao *bluetooth* (MITRE, 2018). Entretanto, algumas dessas vulnerabilidades encontram-se vinculadas a versões específicas desses sistemas operacionais (MITRE, 2018). O uso indiscriminado destas tecnologias pode favorecer atividades maliciosas de *malware* e de pessoas intencionadas a executar a ação maliciosa. Similarmente, configurações relacionadas à localização do dispositivo podem ser exploradas e fornecer a localização do usuário a outros equipamentos e pessoas.

O uso de *"jailbreak"* permite que aplicações comuns sejam executadas com privilégios administrativos. Desta forma, estes aplicativos podem fazer alterações no sistema que normalmente não seriam permitidas. O equipamento que passou pelo processo de *"jailbreak"* amplia o espectro de ataque pois quaisquer dados podem ser acessados por quaisquer aplicativos instalados. Mesmo que o dispositivo móvel esteja isento do *"jailbreak"*, os diretórios /system e /data devem manter as permissões de acesso originais. O diretório /system armazena os arquivos do sistema operacional *Android* e de maneira similar, o diretório /data abriga informações relacionadas aos usuários do sistema operacional e aplicações instaladas. Assim, habilitar permissões fora do padrão recomendado nestes diretórios pode causar a violação dos princípios da

confidencialidade, integridade e disponibilidade (SHAO et al., 2014; ZHANG et al., 2015).

Configurações como “configurar tempo para bloqueio de tela” e “botão desliga ao ser pressionado bloqueia imediatamente a tela” fornecem proteção importante ao usuário. Caso, por exemplo, o usuário tenha desbloqueado o dispositivo através da sua senha e não há tempo, ou mesmo um tempo muito longo para bloqueio de tela configurado, o dispositivo comporta-se como se não tivesse a proteção de nenhum tipo de senha. Assim, após o primeiro desbloqueio, o dispositivo está pronto para ser consultado por quaisquer pessoas. De maneira similar, o botão desliga possui como uma de suas funções, desligar a tela do aparelho quando pressionado. Entretanto, o mesmo pode ser configurado para não exigir senha de acesso logo após ser pressionado, fato que favorece o furto de dados por invasores.

A instalação de aplicativos oriundos de lojas de *software* não oficiais pode gerar vulnerabilidades. Aplicações de terceiros, assim como aplicativos ainda em desenvolvimento, não passam pelo crivo da loja oficial de *software* do sistema operacional e desta forma, *malware* pode estar concatenado a este tipo de aplicativo. Todavia, mesmo que em menor probabilidade, aplicativos oficiais também podem conter ameaças digitais. O uso de ferramenta *anti-malware* é recomendado mesmo que os aplicativos sejam instalados somente através de lojas oficiais (ZHOU et al., 2012; SUAREZ-TANGIL et al., 2014).

As configurações relacionadas à encriptação fornecem uma camada adicional de proteção através da codificação dos dados, incluindo mensagens SMS e MMS, arquivos armazenados no dispositivo, mensagens de e-mail e *backups*. Desta forma, os dados somente podem ser acessados através de uma senha ou *token* de decodificação. De maneira similar, certificados do tipo *TLS* fornecem codificação na comunicação entre sistemas remotos. Entretanto, caso o usuário aceite e utilize um certificado *TLS* não confiável, vulnerabilidades podem ser geradas pois os princípios da confidencialidade, integridade e disponibilidade podem ser violados (RAYARIKAR et al., 2012; TEUFL et al., 2014; D’ORAZIO; CHOO, 2018).

Devido ao impacto de segurança, caso o dispositivo possua valores não recomendados atribuídos para qualquer uma das seguintes configurações: “uso de senha”, “configurar tempo para bloqueio de tela”, “uso de jailbreak (root)” e “instalação de aplicativos de fontes desconhecidas”, o impacto de segurança causado por este dispositivo é considerado alto. Estas quatro configurações são chamadas de *configurações fundamentais*.

Cada configuração customizável, caso ajustada incorretamente, gera impacto de segurança com diferente nível de severidade. A tabela 7 apresenta os níveis de impacto utilizados neste trabalho.

Tabela 7: Descrição dos níveis de impacto de segurança causado por configurações customizáveis caso estejam ajustadas de modo não seguro.

Nível de Impacto	Descrição	Descrição do Impacto
1	A configuração não é relevante e é muito improvável que esta configuração seja explorada caso esteja ajustada de modo inseguro.	Em caso de ataque, o impacto é mínimo.
2	A configuração é relevante e é improvável que esta configuração seja explorada caso esteja ajustada de modo inseguro.	Em caso de ataque, o impacto é limitado.
3	A configuração deve ser ajustada seguramente e pode ser explorada caso esteja ajustada de modo inseguro.	Em caso de ataque, o impacto pode favorecer o furto de dados e outras ameaças.
4	A configuração é importante e provavelmente será explorada caso esteja ajustada de modo inseguro.	Em caso de ataque, o furto de dados e outras ameaças podem ocorrer assim como prejuízo financeiro limitado.
5	A configuração é crítica e muito provavelmente será explorada caso esteja ajustada de modo inseguro .	Em caso de ataque, severo prejuízo financeiro assim como furto de dados e outras ameaças podem ocorrer.

Fonte: Vecchiato (2016).

Conforme demonstrado pela tabela 7, os níveis de impacto representam uma escala crescente na severidade do furto de dados, outras ameaças e consequente prejuízo financeiro caso as vulnerabilidades sejam exploradas.

4.3 DADOS GRAVADOS EM DISPOSITIVOS MÓVEIS

Os dispositivos móveis armazenam em média 500 arquivos dados do usuário (VECCHIATO, 2016). Estes arquivos podem ser de cunho pessoal e corporativo cuja relevância é classificada como baixa, média ou alta. Arquivos de áudio, imagem, vídeo e documentos podem conter dados sigilosos ou de importância corporativa, (BEN-ASHER et al., 2011; MUSLUKHOV et al., 2012; LEAVITT, 2013; VECCHIATO, 2016; CAHYANI et al., 2017). A tabela 8 ilustra os formatos mais comumente utilizados para esses tipo de arquivos.

Tabela 8: Formatos comumente utilizados para arquivos do tipo documento, áudio, vídeo e imagem.

Tipo de Arquivo	Formato
Documento	doc, docx, xls, xlsx, odt, ods, ppt, pptx, pdf
Áudio	mp3, ogg
Vídeo	avi, mpg, mpeg, mp4, 3gp, mov, flv
Imagem	jpg, png, bmp, tif, gif

Fonte: Cahyani et al. (2017).

4.4 ACESSO A INFORMAÇÕES CORPORATIVAS

Para que os riscos oferecidos pelos dispositivos utilizados para *BYOD* não se sobreponham às suas vantagens, cada equipamento deve acessar informações corporativas cuja cate-

goria de segurança seja compatível com o nível de impacto de segurança oferecido pelo equipamento. Cada item apresentado na tabela 6, caso esteja ajustado de modo não seguro, gera um impacto de segurança distinto no aparelho. Para avaliar o risco de segurança causado pelas configurações customizáveis no dispositivo, pode-se atribuir um nível de impacto de segurança, conforme apresentado pela tabela 7, para cada um daqueles itens da tabela 6. Desta forma, o grau de impacto de segurança que as configurações customizáveis representam em um aparelho utilizado para *BYOD* é obtido através da seguinte equação:

$$impacto = \sum_{i=1}^{N} C_i \tag{4}$$

Onde:

1. i representa o identificador da configuração inseguramente parametrizada;
2. N representa a quantidade de configurações inseguras avaliadas;
3. C_i representa o valor do impacto de segurança atribuído à configuração caso esteja incorretamente parametrizada.

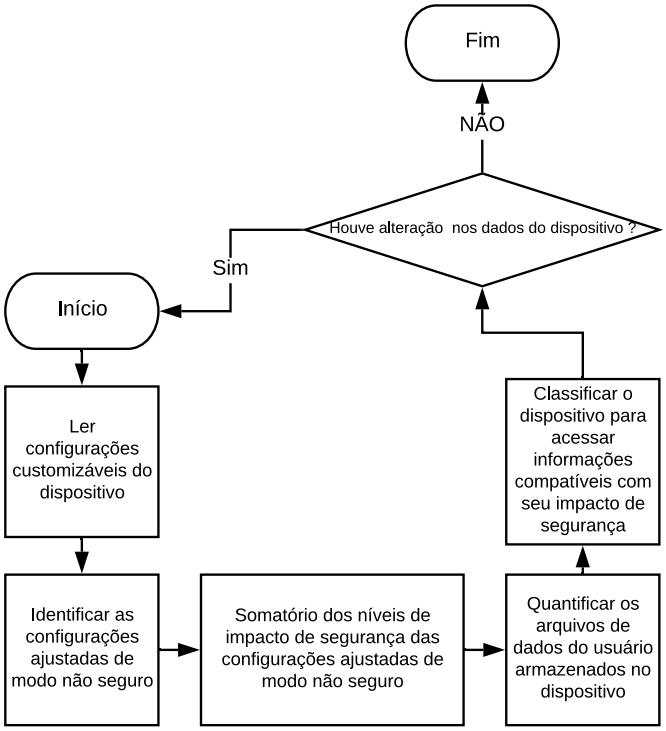
De modo simplificado, o impacto de segurança relacionado a configurações customizáveis é alcançado através do somatório dos níveis de impacto de segurança das configurações inseguramente parametrizadas.

Um aparelho com grau de impacto de segurança elevado favorece o furto de dados e pode desencadear prejuízo financeiro. Desta forma, quanto mais informações estiverem armazenadas no equipamento, maior é a probabilidade de dados relevantes existirem. Assim, estabelece-se uma relação entre o impacto de segurança causado pelas configurações customizáveis e a quantidade de arquivos de dados armazenados no equipamento. Esta relação baseia-se na premissa de que *quanto mais arquivos estiverem armazenados no dispositivo, menor deve ser o impacto de segurança causado pelas configurações customizáveis*.

Desta forma, o **impacto total de segurança** que um dispositivo utilizado para *BYOD* representa é medido através do relacionamento entre o impacto de segurança causado pelas configurações customizáveis e a quantidade de arquivos que o usuário armazena no equipamento.

Desta forma, quanto **menor** for o impacto de segurança causado pelo dispositivo **mais elevada** é a categoria de informações na qual ele está apto a acessar e vice-versa. A figura 11 ilustra o fluxo de trabalho proposto.

Figura 11: Fluxo de trabalho proposto.



Fonte: Autoria própria.

Conforme apresentado na figura 11, a avaliação do dispositivo inicia-se com a leitura das configurações customizáveis descritas na tabela 6. Após o término desta leitura, os itens coletados são comparados com os valores recomendados pela referida tabela. Em seguida, obtém-se o somatório dos níveis de impacto de segurança de todas as configurações que estão em desacordo e bem como são totalizados os arquivos de dados do usuário armazenados no dispositivo móvel. Após este processo, o aparelho é classificado podendo acessar informações cuja categoria de segurança é compatível com o grau de impacto de segurança apresentado. Caso o usuário do dispositivo efetue um reajuste das configurações ou altere a quantidade de arquivos armazenados, o processo é reiniciado.

4.5 LIMITAÇÕES

A proposta apresentada por este capítulo possui limitações e estas encontram-se descritas abaixo:

1. Os parâmetros customizados atribuídos aos itens da tabela 6 apenas são coletados. Desta forma, não são executadas quaisquer correções nas configurações não seguras;

2. A contagem de arquivos de dados que o usuário armazena no equipamento não leva em consideração a relevância de seu conteúdo. Desta forma, por exemplo, um dispositivo pode conter poucos arquivos cujo conteúdo é compatível com a categoria de segurança de alta relevância, ou por outro lado, conter centenas de arquivos sem quaisquer importância.

4.6 CONCLUSÃO

Este capítulo apresentou a proposta para mitigar o impacto causado por furto de dados e outras ameaças digitais em ambientes corporativos onde a política de *BYOD* é utilizada. Esta proposta baseia-se na avaliação de segurança das configurações customizáveis do dispositivo móvel e na quantificação dos arquivos de dados que o usuário nele armazena. Assim, pode-se obter o impacto total de segurança que o dispositivo representa. Com esta avaliação, torna-se possível classificar o equipamento a acessar informações corporativas cuja categoria de segurança é compatível com o impacto de segurança apresentado. No capítulo seguinte, a validação da proposta e os resultados obtidos são apresentados.

5 VALIDAÇÃO E RESULTADOS OBTIDOS

Este capítulo apresenta a validação da proposta e os resultados obtidos. Como parte do processo de validação, o aplicativo *FBYOD* foi desenvolvido e foi avaliado dentro do ambiente corporativo da Prefeitura Municipal de São Bento do Sul, Santa Catarina. Este capítulo está dividido da seguinte forma: inicialmente, a visão geral da validação da proposta é apresentada, na sequência os níveis de impacto de segurança das configurações customizáveis são expostos, na seção seguinte a estrutura do aplicativo *FBYOD* é exibida e na sequência apresenta sua implementação, estudo de caso e resultados obtidos. Por fim, uma breve discussão é proposta e o capítulo encerra-se na conclusão.

5.1 VISÃO GERAL

Para validar a proposta, o aplicativo *Fuzzy BYOD (FBYOD)* foi desenvolvido e encontra-se publicado na loja de aplicativos *Google Play* (UHLIG, 2018). O *FBYOD* foi concebido inicialmente para o sistema operacional *Android* versão 4.03 ou superior. A escolha deste sistema operacional fundamenta-se pela sua participação de aproximadamente 80% no mercado de sistemas operacionais para dispositivos móveis (ZHU et al., 2018). Como características, o *FBYOD* avalia o nível de impacto de segurança do dispositivo móvel de modo automático e também conta com um classificador baseado em lógica *fuzzy* para qualificar o dispositivo a acessar informações cuja categoria de segurança seja compatível com o nível de impacto de segurança apresentado pelo aparelho.

5.2 ATRIBUIÇÃO DE NÍVEIS DE IMPACTO DE SEGURANÇA

O *FBYOD* avalia as configurações customizáveis do sistema operacional *Android* conforme os itens descritos na tabela 6. Entretanto, este trabalho somente considera as configurações que podem ser coletadas via ferramenta automatizada. A tabela 9 apresenta os itens coletados pelo *FBYOD* juntamente com os respectivos níveis de impacto de segurança descritos pela tabela 7.

Tabela 9: Configurações do *Android* coletadas pelo *FBYOD* e respectivos níveis de impacto de segurança.

Configuração customizável	Nível de Impacto
Uso de senha	5 *
Uso de senha alfanumérica	5
Uso de senha visível	5
Aplicar remoção de dados do usuário após excessivas senhas inválidas	5
Configurar tempo para bloqueio de tela	5 *
Instalação de aplicativos de fontes desconhecidas	5 *
Uso de “Jailbreak” (root)	5 *
Botão desliga ao ser pressionado bloqueia imediatamente a tela	5
Configurar idade máxima para senha	4
Configurar tamanho mínimo da senha	4
Configurar tamanho mínimo de caracteres complexos	4
Encriptação do armazenamento de dados	4
Opção para desenvolvedores	4
Permissão de escrita no diretório /system	4
Permissão de escrita no diretório /data	4
Interface *Wi-Fi* quando não necessária	3
Interface *bluetooth* quando não necessária	3
Hotstpot pessoal quando não necessário	3
Ativar o histórico de senhas	3
Uso de serviços de localização quando não necessários	3
Uso de localização simulada	3
Instalar ferramenta anti-malware	3
Descoberta de *bluetooth*	3
Visibilidade da senha tipo ”padrão”	3
Limitar o número de mensagens Multimídia	2
Remover redes *Wi-Fi* conhecidas	2
Notificação de rede	2
Ajuste automático de fuso horário	2
Ajuste automático de data	2
Limitar o número de mensagens SMS	1

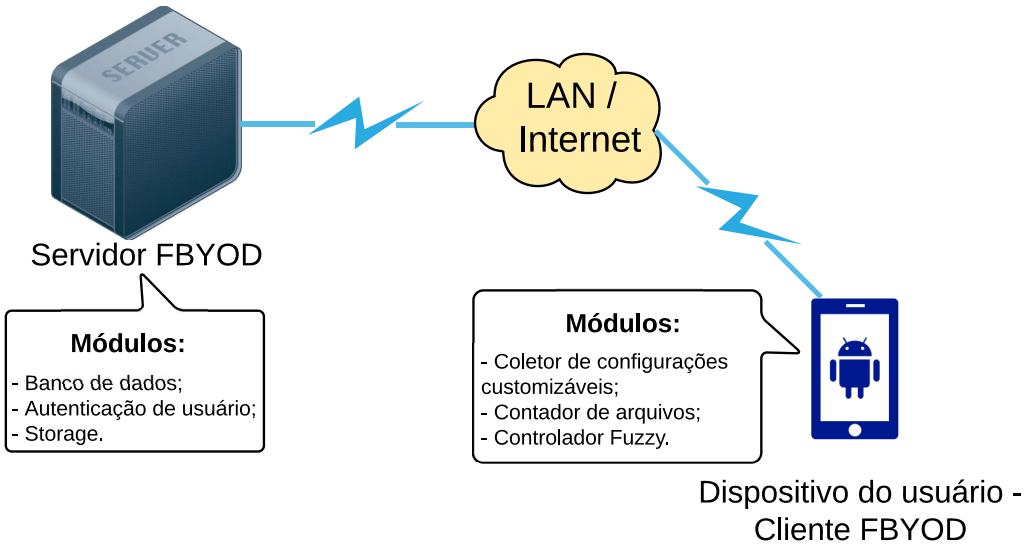
Fonte: Vecchiato (2016), CIS (2018).

De acordo com a tabela 9, os itens encontram-se ordenados pelo nível impacto de segurança. Os elementos marcados com um asterisco representam as “configurações fundamentais”. O parâmetro inseguro atribuído a qualquer um destes quatro itens gera grau máximo de impacto de segurança do aparelho sob avaliação. A atribuição do nível de impacto de segurança para cada um dos itens da tabela 9 fundamenta-se na relevância do item e adicionalmente, na severidade das vulnerabilidades geradas em caso de parametrização não segura.

5.3 ESTRUTURA DO *FBYOD*

O aplicativo *FBYOD* é baseado no modelo cliente-servidor. Desta forma, a aplicação cliente é instalada via loja de aplicativos *Google Play* no dispositivo móvel do usuário. Por outro lado, os serviços de banco de dados, autenticação do usuário e o armazenamento dos arquivos são executados remotamente em ambiente *cloud*. A figura 12 ilustra a estrutura geral do *FBYOD*.

Figura 12: Estrutura do protótipo do aplicativo *FBYOD*.



Fonte: Autoria própria.

Os módulos do cliente *FBYOD* encontram-se descritos na sequência:

- *Módulo coletor de configurações customizáveis*: este módulo verifica no dispositivo móvel em avaliação os itens contidos na tabela 9. Assim, para todos os itens encontrados no dispositivo sob avaliação e que estejam parametrizados de acordo com a tabela 6, o impacto de segurança do item é avaliado como *zero*. Todavia, caso a configuração esteja em desacordo, o impacto de segurança é registrado conforme o nível de impacto de segurança do item. Como saída do processamento, este módulo retorna a soma dos impactos de segurança de todos os itens avaliados e ajustados com parâmetros divergentes daqueles descritos pela tabela 6. Entretanto, caso qualquer uma das "quatro configurações fundamentais" esteja incorretamente ajustada, o módulo retorna valor equivalente ao somatório de todos níveis de impacto de segurança. Os parâmetros de cada item coletado por este módulo são enviados ao banco de dados;
- *Módulo contador de arquivos*: o módulo contador de arquivos procura no dispositivo

móvel arquivos cujas extensões sejam compatíveis com as apresentadas na tabela 8. Ao final do seu processamento, o módulo retorna o número total de arquivos;

- *Módulo controlador fuzzy*: o módulo controlador *fuzzy* é utilizado para computar o *índice de impacto de segurança do dispositivo*. Este índice, indicador geral da segurança do equipamento, é obtido através do relacionamento *fuzzy* entre o impacto de segurança causado pelas configurações customizáveis ajustadas de modo inseguro e a quantidade de arquivos encontrados pelo módulo contador de arquivos. Com o resultado deste relacionamento, o índice de impacto de segurança do dispositivo é calculado e através dele, o aparelho é classificado para acessar informações corporativas de baixa, média e alta relevância. Como parâmetros de entrada, o módulo controlador *fuzzy* recebe os valores de saída dos módulos "coletor de configurações customizáveis" e "contador de arquivos". Como saída deste módulo, o índice de impacto de segurança do dispositivo é calculado dentro do intervalo [0,100]. Assim, o valor 0 representa nenhum impacto de segurança enquanto o valor 100 representa o maior impacto de segurança que um dispositivo pode apresentar.

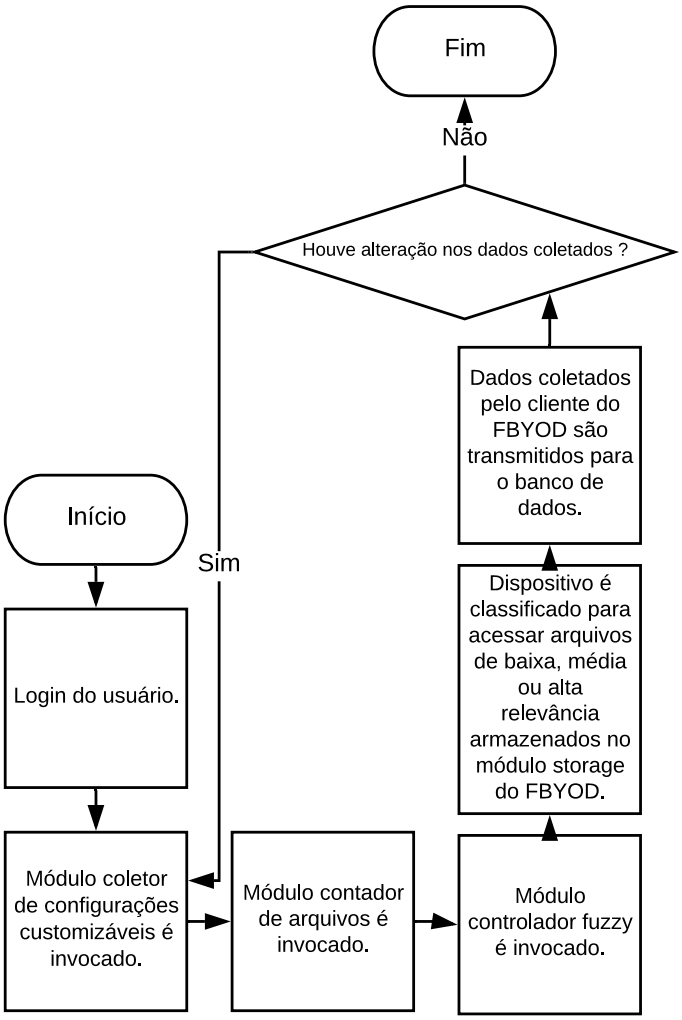
Os módulos do servidor *FBYOD* encontram-se descritos na sequência:

- *Módulo de banco de dados*: armazena as informações coletadas pelos módulos da aplicação cliente do *FBYOD*;
- *Módulo de autenticação*: este módulo armazena os dados relacionados ao *login* dos usuários do sistema *FBYOD*, como o nome de usuário e a senha;
- *Módulo storage*: este módulo armazena os arquivos corporativos disponibilizados pelo administrador. Assim, estes podem ser acessados através da interface da aplicação cliente do *FBYOD*. Entretanto, os arquivos necessitam de prévia classificação em diretórios distintos de acordo com sua relevância.

A seguir, a figura 13 ilustra o fluxo de trabalho do *FBYOD*. Após a aplicação cliente do *FBYOD* ter sido instalada no dispositivo móvel, o usuário efetua o *login* através de seu usuário e senha. Após o *login*, os módulos "coletor de configurações customizáveis" e "contador de arquivos" são automaticamente invocados. Desta forma, após o processamento, o módulo do "controlador fuzzy" é iniciado e ao final de seu processamento, o índice de impacto de segurança do dispositivo é calculado e então o equipamento sob avaliação é classificado para acessar arquivos de baixa, média ou alta relevância armazenados no *FBYOD storage*. Um dispositivo classificado para acessar arquivos de alta relevância, pode também acessar dados

classificados com o status de média e baixa relevância. Por outro lado, o contrário não se aplica. Como por exemplo, caso o equipamento seja classificado para acessar arquivos de baixa importância, as outras categorias de arquivos não estarão disponíveis. Por fim, os dados obtidos pelos módulos que compõe a aplicação cliente do *FBYOD* são transmitidos ao banco de dados. Caso ocorram alterações nas configurações customizáveis ou quantidade de arquivos do usuário armazenados no dispositivo, o fluxo de trabalho reinicia com a invocação do módulo "coletor de configurações customizáveis".

Figura 13: Fluxo de trabalho do *FBYOD*.



Fonte: Autoria própria.

5.4 IMPLEMENTAÇÃO DO *FBYOD*

O cliente *FBYOD* foi implementado utilizando o *Android Studio*. A escolha por esta ferramenta baseia-se em sua versatilidade e compatibilidade com o sistema operacional *Android* (GOOGLE, 2018c). A seguir, o processo de implementação dos módulos da aplicação cliente do *FBYOD* é descrito.

5.4.1 IMPLEMENTAÇÃO DO MÓDULO COLETOR DE CONFIGURAÇÕES CUSTOMIZÁVEIS

A implementação deste módulo fundamenta-se principalmente na execução de chamadas para as *API* de desenvolvimento do sistema operacional *Android*. Estas APIs, como por exemplo *WiFiManager* (utilizada para coleta de dados relacionados a interfaces *wireless*), *KeyguardManager* (utilizada para verificar se há senhas habilitadas no dispositivo), *DevicePolicyManager* (utilizada para leitura de políticas de senhas, tais como: tamanho mínimo, caracteres complexos, histórico, idade e remoção de dados após excessivas senhas inválidas) e *Settings.System* (configurações gerais do sistema operacional), dentre outras, fornecem métodos específicos para consultar atributos relacionados à configurações customizáveis. Desta forma, torna-se possível verificar se uma dada configuração está seguramente ajustada ou não. Entretanto, os seguintes itens foram implementados sem o uso de *APIs* específicas:

- *Uso de "Jailbreak" (root)*: para verificar se o dispositivo executa aplicações do usuário com privilégios administrativos, o *FBYOD* verifica se a aplicação "su" é encontrada no sistema. O "su" permite que aplicativos do usuário sejam executados com privilégios administrativos e como consequência, estes podem acessar quaisquer diretórios do sistema operacional (SHAO et al., 2014). Assim, caso o "su" seja detectado, o aparelho passou por processo de *"Jailbreak" (root)*;
- *Instalar ferramenta anti-malware*: o *FBYOD* possui uma lista contendo o nome do pacote de aplicações *anti-malware* disponíveis para o sistema operacional *Android*. Para a criação desta lista, uma pesquisa foi efetuada na loja *Google Play* (GOOGLE, 2018g). Nesta pesquisa, 142 ferramentas *anti-malware* foram encontradas[1]. Assim, caso algum destes pacotes seja encontrado no dispositivo móvel em avaliação, conclui-se que há um aplicativo *anti-malware* instalado.

A fundamentação acerca de quais APIs de desenvolvimento deveriam ser utilizadas

[1]Pesquisa efetuada em 14 de novembro de 2018.

para a implementação deste módulo do *FBYOD* foi obtida na documentação oficial do sistema operacional *Android* e também, no fórum de programadores *Stack Overflow* (GOOGLE, 2018a; STACKOVERFLOW, 2018).

5.4.2 IMPLEMENTAÇÃO DO MÓDULO CONTADOR DE ARQUIVOS

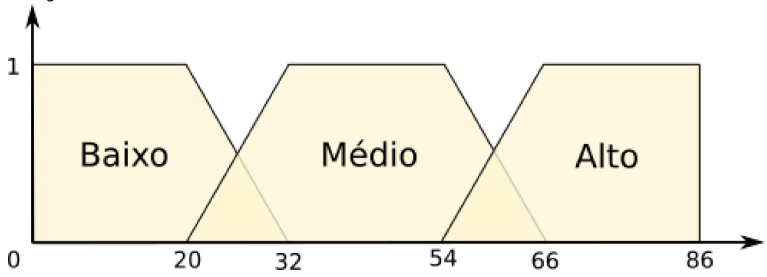
A pesquisa pelos arquivos que o *FBYOD* considera é efetuada no diretório padrão de armazenamento do usuário. Para obter o endereço deste diretório, o método *Environment.getExternalStorageDirectory().getPath()* é invocado. Por fim, o módulo retorna o total de arquivos encontrados.

5.4.3 IMPLEMENTAÇÃO DO MÓDULO CONTROLADOR *FUZZY*

O desenvolvimento do módulo do controlador *fuzzy* do *FBYOD* foi baseado na biblioteca de desenvolvimento *jfuzzy* (RADA-VILELA, 2017). Esta biblioteca foi desenvolvida em Java e é compatível com a ferramenta de desenvolvimento *Android Studio*. O fluxo deste módulo é idêntico ao representado pela figura 10 e é composto pelos seguintes itens:

- *Variáveis de entrada*: o módulo do controlador *fuzzy* do *FBYOD* utiliza como variáveis de entrada os valores de saída dos módulos "coletor de configurações customizáveis" e "contador de arquivos". Então, estas duas variáveis são fuzificadas nos respectivos universos através de função de pertinência do tipo trapezoidal (ZADEH, 1996). A escolha pela função trapezoidal dá-se em virtude de ser uma das funções mais utilizadas (SU et al., 2001; ORDOOBADI, 2009). As figuras 14 e 15 ilustram estes universos.

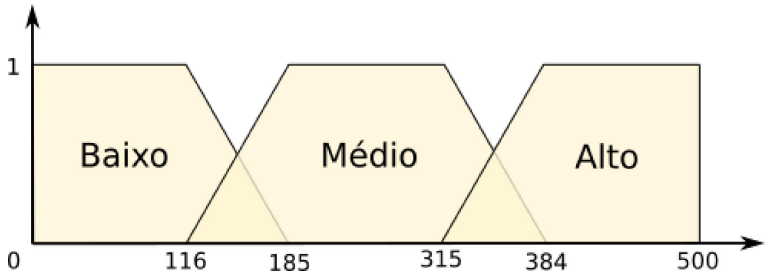
Figura 14: Universo onde a variável de entrada oriunda da saída do processamento do módulo "coletor de configurações customizáveis" é fuzificada.



Fonte: Autoria própria.

Os conjuntos *fuzzy* representados pela figura 14 possuem a faixa de valores no intervalo [0,86]. A escolha do valor final fundamenta-se na hipótese de todos os itens da tabela 9, exceto as configurações fundamentais, serem parametrizados inseguramente. Do mesmo

Figura 15: Universo onde a variável de entrada oriunda da saída do processamento do módulo "contador de arquivos" é fuzificada.



Fonte: Autoria própria.

modo, o valor final descrito pela figura 15 baseia-se na quantidade média de arquivos que um dispositivo móvel armazena;

- *Conjunto de regras*: este módulo utiliza o método de *Mamdani* e as regras são definidas por especialista. Para a agregação dos antecedentes das regras, o operador lógico "E" é empregado. A tabela 10 ilustra as regras criadas.

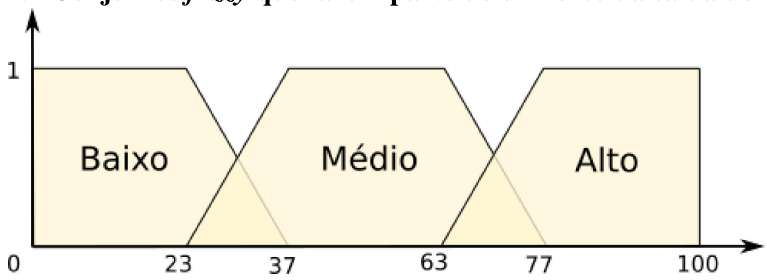
Tabela 10: Regras fuzzy desenvolvidas para uso no aplicativo FBYOD.

Regras Fuzzy
SE "Impacto das configurações" é *Baixo* E "Quantidade de Arquivos" é *Baixo* ENTÃO "Índice de Impacto de Segurança" é *Baixo*.
Se "Impacto das configurações" é *Baixo* E "Quantidade de Arquivos" é *Médio* ENTÃO "Índice de Impacto de Segurança" é *Baixo*.
SE "Impacto das configurações" é *Baixo* E "Quantidade de Arquivos" é *Alto* ENTÃO "Índice de Impacto de Segurança" é *Médio*.
SE "Impacto das configurações" é *Médio* E "Quantidade de Arquivos" é *Baixo* ENTÃO "Índice de Impacto de Segurança" é *Baixo*.
SE "Impacto das configurações" é *Médio* E "Quantidade de Arquivos" é *Médio* ENTÃO "Índice de Impacto de Segurança" é *Médio*.
SE "Impacto das configurações" é *Médio* E "Quantidade de Arquivos" é *Alto* ENTÃO "Índice de Impacto de Segurança" é *Alto*.
SE "Impacto das configurações" é *Alto* E "Quantidade de Arquivos" é *Baixo* ENTÃO "Índice de Impacto de Segurança" é *Médio*.
SE "Impacto das configurações" é *Alto* E "Quantidade de Arquivos" é *Médio* ENTÃO "Índice de Impacto de Segurança" é *Alto*.
SE "Impacto das configurações" é *Alto* E "Quantidade de Arquivos" é *Alto* ENTÃO "Índice de Impacto de Segurança" é *Alto*.

Fonte: Autoria própria.

- *Saída*: o valor numérico de saída do módulo controlador *fuzzy* é obtido através do método de defuzificação *centróide*. Este valor é denominado *índice de impacto de segurança*. A faixa de valores do universo de saída varia entre 0 e 100 e possui três conjuntos fuzzy nomeados da seguinte forma: *baixo, médio* e *alto*. Através da saída do controlador fuzzy, o dispositivo é classificado a acessar arquivos armazenados no módulo *Storage* do *FBYOD*. Para acessar arquivos de alta, média e baixa relevância, o índice de impacto de segurança deve ser inferior a 30. De maneira similar, se este índice estiver entre 30 e 60, o equipamento é classificado a acessar arquivos de média e baixa relevância. Caso o índice de impacto de segurança seja superior a 60, somente arquivos de baixa relevância são disponibilizados ao dispositivo. A figura 16 ilustra os conjuntos *fuzzy* que fazem parte da saída do sistema.

Figura 16: Conjuntos *fuzzy* que fazem parte do universo da saída do sistema.



Fonte: Autoria própria.

Com o intuito de validar a operação do módulo controlador fuzzy, o *software MATLAB* foi utilizado (MATLAB, 2019). A configuração criada pela biblioteca *jfuzzy* foi reproduzida naquele *software* e avaliada através dos mesmos valores numéricos para as variáveis de entrada em ambos cenários. Em conclusão, foi observado compatibilidade entre os resultados gerados pelo módulo controlador *fuzzy* do *FBYOD* e pelo *software MATLAB*. Assim, a operação deste módulo torna-se válida.

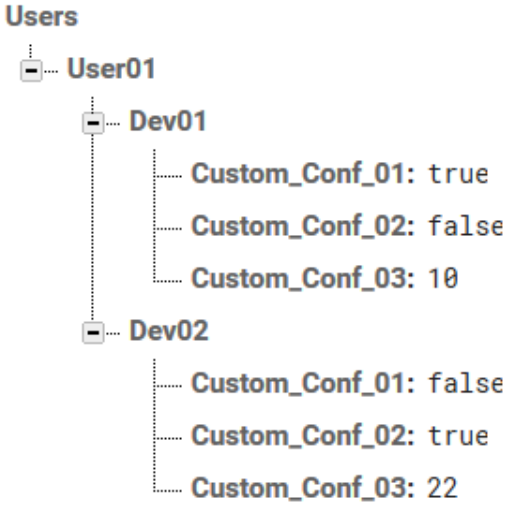
5.4.4 IMPLEMENTAÇÃO DO BANCO DE DADOS

O *FBYOD* utiliza o banco de dados *Google Firebase Realtime Database* (GOOGLE, 2018d). Este banco de dados é do tipo *NoSQL* e é hospedado em ambiente *cloud* diretamente nos servidores do próprio *Google*. A escolha por este banco de dados ampara-se na compatibilidade de suas bibliotecas de programação para o desenvolvimento de aplicações móveis e também, na segurança da transmissão de dados entre o dispositivo móvel e o próprio banco de dados. Como característica adicional, o *Firebase* implementa, automaticamente, a retransmissão de dados em caso de indisponibilidade de link de internet entre a aplicação desenvolvida e o banco de dados.

O banco de dados do *FBYOD* armazena os dados coletados pelos módulos da aplicação cliente e é organizado conforme ilustrado pela figura 17.

No exemplo apresentado pela figura 17, os nomes das configurações e seus respectivos parâmetros que representam os dados coletados são fictícios e são utilizados apenas para a demonstração da estrutura de dados. Essa estrutura mostra que os dados coletados estão vinculados a um dispositivo móvel e este por sua vez, vincula-se a um nome de usuário. Assim, um mesmo usuário pode utilizar mais de um dispositivo móvel.

Figura 17: Estrutura do banco de dados do *FBYOD*.



Fonte: Autoria própria.

5.4.5 IMPLEMENTAÇÃO DO MÓDULO DE AUTENTICAÇÃO

A autenticação dos usuários do *FBYOD* é feita através do par "usuário e senha". A base de autenticação adotada é o *Google Firebase Authentication* e sua escolha fundamenta-se na sua compatibilidade com o banco de dados adotado. O cadastramento dos usuários por parte do administrador é efetuado diretamente no console de administração do *Firebase* (GOOGLE, 2018e).

5.4.6 IMPLEMENTAÇÃO DO MÓDULO *STORAGE*

A plataforma escolhida para armazenerar e disponibilizar arquivos para o *FBYOD* é o *Google Firebase Storage* (GOOGLE, 2018f). Do mesmo modo que as outras soluções utilizadas para compor os módulos do servidor do *FBYOD*, o *Google Firebase Storage* é hospedado nos servidores do próprio *Google* e assim, um servidor local de armazenamento de arquivos não é necessário.

O módulo *Storage* utiliza três diretórios conforme descritos a seguir:

- *Baixo*: este diretório armazena os arquivos de baixa relevância;
- *Médio*: de modo similar ao item anterior, este diretório armazena arquivos de média relevância;
- *Alto*: dentro deste diretório encontram-se armazenados os arquivos de alta relevância.

No estágio atual de desenvolvimento do *FBYOD*, o administrador deve classificar e distribuir os arquivos dentro destes diretórios através do *Google Firebase Console*.

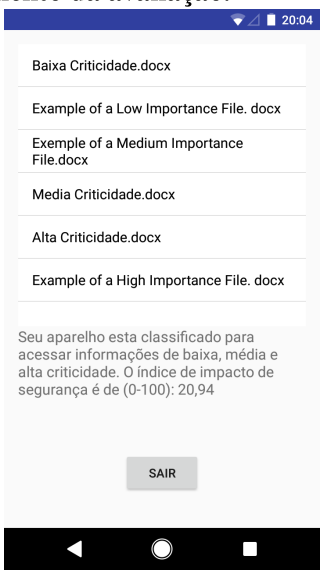
5.4.7 INTERFACES DO *FBYOD*

A aplicação cliente do *FBYOD* consiste em duas interfaces. A figura 18 ilustra a tela de *login* e a figura 19 mostra a interface com a listagem de arquivos disponíveis para aquele dispositivo. Abaixo da lista de arquivos, é descrito o índice de impacto de segurança apresentado por aquele dispositivo e bem como qual a categoria de relevância que está classificado a acessar.

Figura 18: Tela de *login* do *FBYOD*. Após a inserção dos dados de *login*, a avaliação do dispositivo é automaticamente iniciada.

Fonte: Autoria própria.

Figura 19: FBYOD: tela de arquivos disponíveis e descrição do índice de impacto de segurança que o dispositivo apresenta no momento da avaliação.



Fonte: Autoria própria.

No exemplo ilustrado pela figura 19, o dispositivo móvel possui índice de impacto de segurança de 20,94 e está apto a acessar informações de alta, média e baixa relevância.

5.5 ESTUDO DE CASO E RESULTADOS OBTIDOS

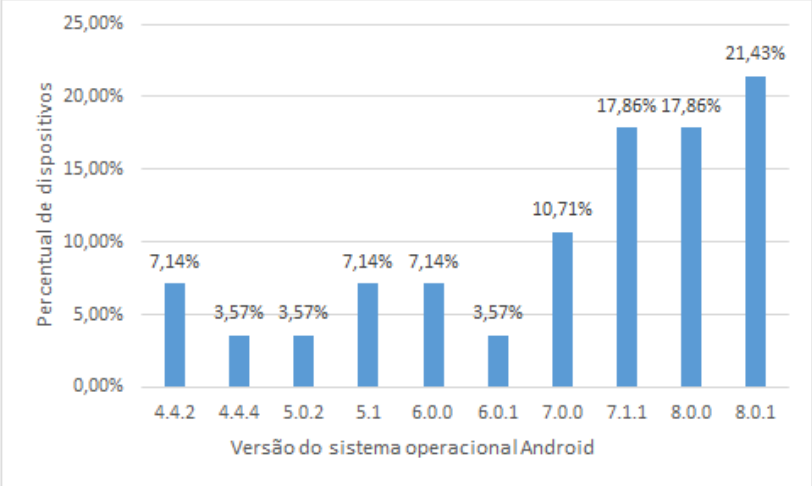
A validação do *FBYOD* foi realizada no ambiente corporativo da Prefeitura Municipal de São Bento do Sul, Santa Catarina - Brasil. O estudo consistiu na instalação do aplicativo *FBYOD* em dispositivos móveis com o sistema operacional *Android* compatível e de propriedade de colaboradores daquela prefeitura. Desta forma, uma política de *BYOD* pôde ser simu-

lada, visto que todos aparelhos participantes eram utilizados para fins pessoais.

A instalação do *FBYOD* foi procedida através do *Google Play* (UHLIG, 2018). Após a instalação, o *login* foi efetuado através do usuário criado para fins de validação. Nestes dispositivos, nenhum procedimento prévio como por exemplo, verificação manual das configurações customizáveis, instalação de aplicação *anti-malware* ou remoção de arquivos do usuário foi executado. Desta forma, foi possível avaliar a real situação dos equipamentos que participariam da política oficial de *BYOD*.

A coleta de dados foi realizada no mês de dezembro de 2018 e obteve 28 dispositivos participantes. A figura 20 ilustra a distribuição das versões do sistema operacional *Android* dos dispositivos avaliados.

Figura 20: Distribuição das versões do sistema operacional *Android* entre os dispositivos avaliados.



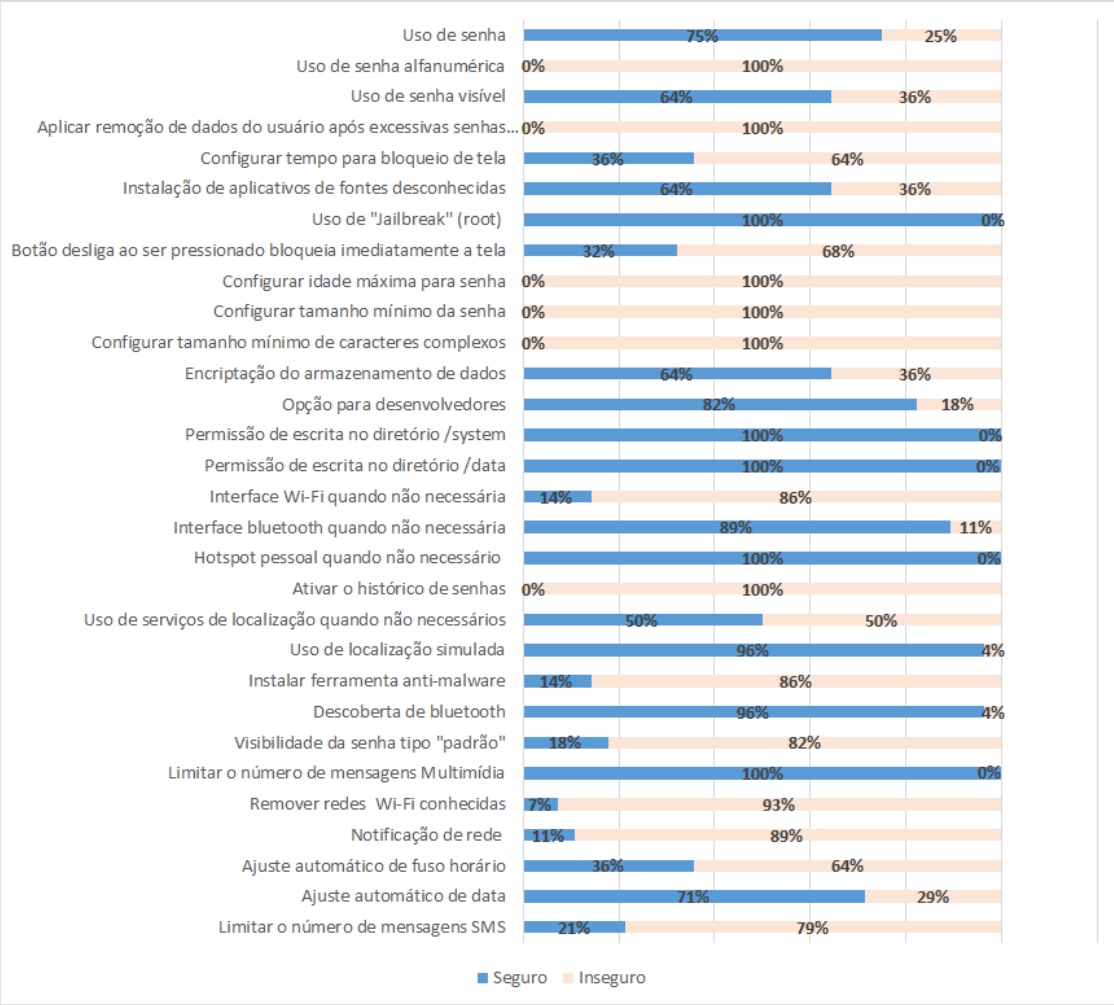
Fonte: Autoria própria.

Conforme ilustrado pela figura 20, 39,29% dos dispositivos executam versões recentes do sistema operacional (versão 8.0.0 e 8.1.0). Desta forma, vulnerabilidades de versões anteriores já encontram-se corrigidas (GOOGLE, 2018b).

No tocante da parametrização das configurações customizáveis dos dispositivos avaliados, a figura 21 ilustra os resultados obtidos. Para melhor entendimento, os dados referentes à figura 21 encontram-se divididos em categorias e explanados nas seguintes subseções:

1. **Subseção 5.5.1:** apresenta os resultados obtidos referente aos itens da categoria “senha”;
2. **Subseção 5.5.2:** apresenta os resultados obtidos referente aos itens da categoria “rede”;
3. **Subseção 5.5.3:** apresenta os resultados obtidos referente aos itens da categoria “permissão”;

Figura 21: Resultados das configurações customizáveis coletadas pelo *FBYOD*.



Fonte: Autoria própria.

4. **Subseção 5.5.4:** apresenta os resultados obtidos referente aos itens da categoria “conteúdo”.

5.5.1 CONFIGURAÇÕES RELACIONADAS À CATEGORIA “SENHA”

Os itens avaliados pelo *FBYOD* e que compõe a categoria “senha” encontram-se listados na tabela 11.

Conforme apresentado pela figura 21, usuários negligenciam aspectos importantes de segurança, principalmente relacionado aos itens descritos na tabela 11. Dentre o total de dispositivos avaliados, nenhum equipamento possui a configuração ajustada para requerer senha alfanumérica, tamanho mínimo de senha, tamanho mínimo de caracteres complexos, remover dados após excessivas senhas inválidas, idade máxima da senha e histórico de senha. De modo

Tabela 11: Itens avaliados pelo *FBYOD* que compõe a categoria "senha".

Configuração	Valor recomendado
Uso de senha	Ativado
Uso de senha alfanumérica	Ativado
Uso de senha visível	Desativado
Aplicar remoção de dados do usuário após excessivas senhas inválidas	Ativado, 10 tentativas
Configurar idade máxima para senha	Até 90 dias
Ativar o histórico de senhas	Mínimo de 24 senhas
Configurar tamanho mínimo da senha	5 caracteres
Configurar tamanho mínimo de caracteres complexos	2 caracteres
Visibilidade da senha tipo "padrão"	Desativado

Fonte: Vecchiato (2016), CIS (2018).

mais severo, 25% dos aparelhos não dispunham de nenhum tipo de proteção por senhas.

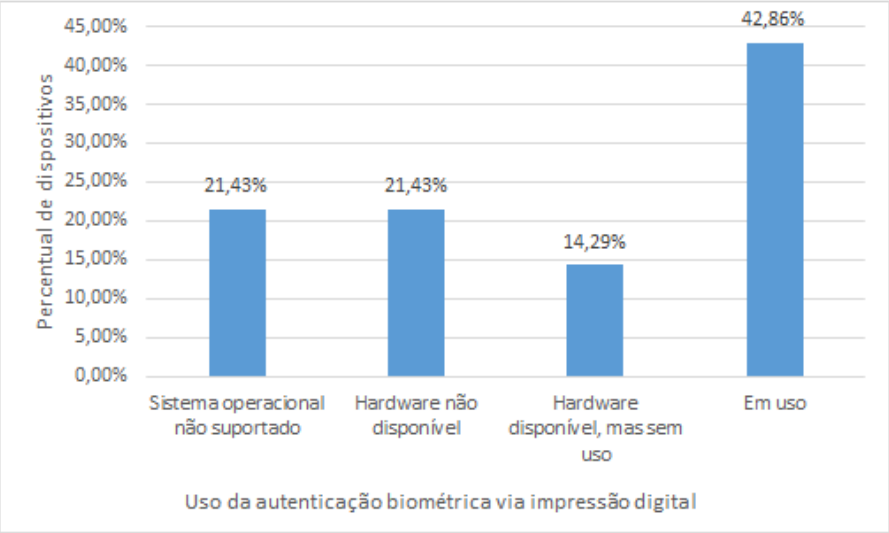
Sem o uso destas configurações, senhas de quaisquer tipos de força podem ser empregadas. Senhas óbvias como, por exemplo, números sequenciais e caracteres únicos podem ser utilizados e desta maneira facilitar que terceiros tenham acesso aos dados gravados no equipamento. Por outro lado, a não utilização de quaisquer tipos de senha, inclusive as óbvias, amplia a superfície de furto de dados e outros ataques pois não há esta proteção inicial de segurança.

As configurações "uso de senha visível" e "visibilidade da senha tipo "padrão"" permitem que pessoas próximas não visualizem, caso estejam ajustadas seguramente, os caracteres digitados e o padrão da senha sendo desenhado na tela do dispositivo móvel. Do total de dispositivos avaliados, 64% possuem a configuração "uso de senha visível" parametrizada corretamente, ao passo que apenas 18% dos equipamentos utilizam a senha do tipo padrão configurada seguramente.

De maneira adicional, o *FBYOD* verifica se a autenticação biométrica via impressão digital do usuário está disponível. Este método de autenticação está acessível a partir da versão 6.0 do *Android* e dá-se pelo cadastramento da impressão digital do usuário via sensor instalado no próprio aparelho. Desta maneira, após o cadastramento, o usuário apenas posiciona o dedo cadastrado e a impressão digital é comparada com as armazenadas em banco de dados do equipamento. Assim, em caso de compatibilidade, o acesso é concedido. Como vantagem, este método de autenticação não sofre as mesmas vulnerabilidades relacionadas ao uso de senhas convencionais. Entretanto, métodos tradicionais de autenticação continuam disponíveis em caso de falha no sensor de leitura, por exemplo (LUCA; LINDQVIST, 2015; MORSALIN et al., 2016; GOOGLE, 2019). A figura 22 ilustra os dados obtidos no tocante da autenticação via impressão digital.

De acordo com a figura 22, 42,86% dos aparelhos encontram-se com o recurso de

Figura 22: Utilização de autenticação via impressão digital.



Fonte: Autoria própria.

autenticação via impressão digital habilitado.

5.5.2 CONFIGURAÇÕES RELACIONADAS À CATEGORIA "REDE"

Os itens avaliados pelo *FBYOD* e que compõe a categoria "rede" encontram-se listados na tabela 12.

Tabela 12: Itens avaliados pelo *FBYOD* que compõe a categoria "rede".

Configuração	Valor recomendado
Remover redes *Wi-Fi* conhecidas	Ativado
Notificação de rede	Desativada
Interface *Wi-Fi* quando não necessária	Desativada
Interface *bluetooth* quando não necessária	Desativada
Hotstpot pessoal quando não necessário	Desativado
Descoberta de *bluetooth*	Desativada

Fonte: Vecchiato (2016), CIS (2018).

A utilização das tecnologias *Wi-Fi* e *Bluetooth* fornece benefícios e facilidades ao acesso à Internet e a outros equipamentos. Entretanto, o seu uso indiscriminado pode trazer riscos relacionados à segurança pois ambas tecnologias possuem vulnerabilidades conforme descrito na seção 4.2.1. A utilização da interface *wireless* no momento da avaliação do *FBYOD* estava disponível em 86% dos equipamentos. De maneira oposta, o uso da interface *bluetooth* estava ativa em apenas 11% equipamentos. Desta forma, a maioria dos equipamentos avaliados estavam expostos somente às vulnerabilidades oferecidas pelo uso da interface *wireless*.

Por outro lado, nenhum equipamento apresentou valores inseguros para a configuração "*hotstpot* pessoal quando não necessário". O uso do *hotspot* pessoal permite compartilhar a conexão de internet do dispositivo com outros equipamentos, desta forma vulnerabilidades relacionadas ao *wireless* podem ser exploradas. Do mesmo modo, apenas 4% dos equipamentos possuem valor inseguro para a configuração "descoberta de *bluetooth*". Com a descoberta do *bluetooth* ativado, o dispositivo pode procurar outros equipamentos com a mesma tecnologia e conectar-se a eles.

Dos equipamentos avaliados pelo *FBYOD*, 7% dos equipamentos possuem a configuração "remover redes *Wi-Fi* conhecidas" ajustada seguramente. O valor seguro de "0" é referente à quantidade de redes sem fio previamente conectadas salvas no dispositivo. Assim, caso existam redes salvas, o equipamento pode conectar-se automaticamente, mesmo que o aparelho esteja sob poder de terceiros. Desta forma, o acesso não autorizado aos serviços daquela rede sem fio pode ocorrer.

De modo similar, 11% dos equipamentos possuem a configuração "notificação de rede" parametrizada de acordo com a tabela 12. Esta configuração notifica o usuário acerca da existência de redes sem fio públicas nas proximidades, ou seja, sem autenticação. Desta forma, o usuário pode conectar-se a uma destas redes e sofrer ataques conforme descritos na seção 2.1.5.

5.5.3 CONFIGURAÇÕES RELACIONADAS À CATEGORIA "PERMISSÃO"

A tabela 13 apresenta os itens que compõe a categoria "permissão".

Tabela 13: Itens avaliados pelo *FBYOD* que compõe a categoria "permissão".

Configuração	Valor recomendado
Permissão de escrita no diretório /system	Desativada
Permissão de escrita no diretório /data	Desativada
Uso de "Jailbreak" (root)	Desativado

Fonte: Vecchiato (2016), CIS (2018).

Neste *dataset* avaliado, nenhum equipamento apresentou valores inseguros para os itens contidos na tabela 13. Desta maneira, 100% dos equipamentos encontravam-se íntegros no quesito permissões de acesso aos diretórios do sistema operacional. De igual modo, os privilégios de execução de aplicativos não foram afetados por procedimentos de *"jailbreak"*.

5.5.4 CONFIGURAÇÕES RELACIONADAS À CATEGORIA “SISTEMA”

Os itens avaliados pelo *FBYOD* relacionados à categoria “sistema” encontram-se na tabela 14.

Tabela 14: Itens avaliados pelo *FBYOD* que compõe a categoria “sistema”.

Configuração	Valor recomendado
Configurar tempo para bloqueio de tela	Máximo 90
Botão desliga ao ser pressionado bloqueia imediatamente a tela	Ativado
Encriptação do armazenamento de dados	Ativada
Opção para desenvolvedores	Desativada
Instalação de aplicativos de fontes desconhecidas	Desativada
Uso de serviços de localização quando não necessários	Desativado
Uso de localização simulada	Desativado
Ajuste automático de fuso horário	Ativado
Ajuste automático de data	Ativado
Instalar ferramenta anti-malware	Ativado

Fonte: Vecchiato (2016), CIS (2018).

A configuração “configurar tempo para bloqueio de tela” encontra-se parametrizada de modo inseguro em 64% dos dispositivos analisados pelo *FBYOD*. Esta configuração recomenda que a tela deva ser bloqueada após 90 segundos, no máximo, de inatividade do usuário. Um período de tempo longo de inatividade sem a solicitação da senha para desbloqueio gera uma vulnerabilidade na qual terceiros podem acessar o equipamento mesmo desconhecendo a senha. De forma similar, a configuração “botão desliga ao ser pressionado bloqueia imediatamente a tela” somente encontra-se ativa, no momento da avaliação, em 32% dos dispositivos móveis. Desta forma, ao pressionar o botão desliga dos 68% dos aparelhos cuja configuração encontra-se insegura, o dispositivo apenas desligará a tela mas não solicitará a senha no próximo acesso.

Entretanto, as configurações “encriptação do armazenamento de dados”, “opção para desenvolvedores” e “instalação de aplicativos de fontes desconhecidas” encontrava-se corretamente ajustada em 64%, 82% e 64% dos dispositivos, respectivamente. A encriptação fornece uma camada adicional de segurança através de codificação dos dados. Assim, por exemplo, os dados eventualmente furtados somente estariam disponíveis após sua decodificação. De maneira similar, os riscos relacionados à infecção de *malware* e furto de dados oriundos de aplicativos ainda em desenvolvimento e de fontes desconhecidas é parcialmente mitigado. Todavia, apenas 14% dos aparelhos empregam ferramenta *anti-malware* e desta forma, mesmo utilizando aplicativos de fontes confiáveis, a infecção por *malware* ainda é possível.

Os serviços de localização fornecem as coordenadas de onde encontra-se o aparelho e consequentemente o usuário. Aplicativos podem explorar vulnerabilidades relacionadas a este

serviço e expor a terceiros a localização do usuário e do equipamento. Na amostra de dados obtida, 50% dos equipamentos apresentam a configuração ajustada seguramente. De maneira similar, a configuração "uso de localização simulada" fornece uma localização falsa para aplicativos e estes podem funcionar de modo incorreto. Todavia, somente 4% dos equipamentos avaliados possuem esta configuração ativada.

O ajuste automático de data e fuso horário permitem que sistemas que baseiam-se na acuidade da data e horário funcionem corretamente. A configuração "ajuste automático de fuso horário" está seguramente ajustada em 36% dos equipamentos enquanto "ajuste de automático de data" encontra-se parametrizado conforme recomendado em 71% dos aparelhos avaliados. O ajuste incorreto do fuso horário e da data podem gerar discrepâncias nas propriedades de um arquivo, por exemplo, ou impedir acesso a sistemas.

5.5.5 CONFIGURAÇÕES RELACIONADAS À CATEGORIA "CONTEÚDO"

A tabela 15 apresentam os itens relacionados à categoria "conteúdo" avaliados pelo *FBYOD*.

Tabela 15: Itens avaliados pelo *FBYOD* que compõe a categoria "conteúdo".

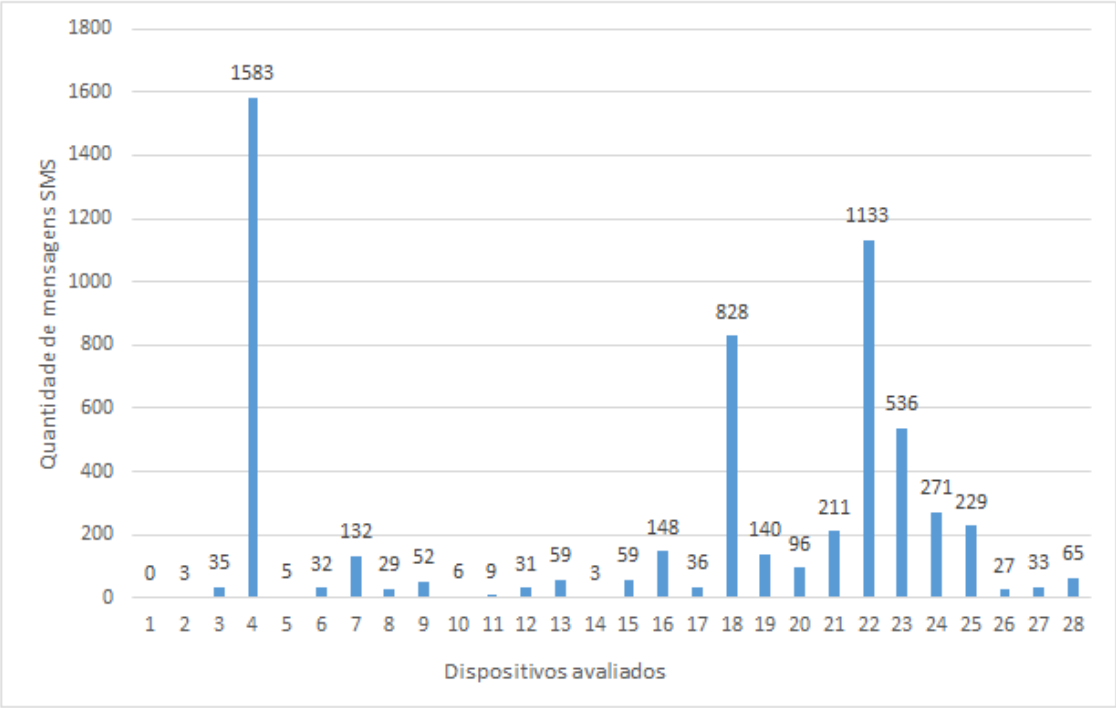
Configuração	Valor recomendado
Limitar o número de mensagens SMS	Até 20
Limitar o número de mensagens Multimídia	Até 20

Fonte: Vecchiato (2016), CIS (2018).

As mensagens *SMS* e multimídia *MMS* podem conter informações sigilosas ou conteúdo relevante. Quanto mais mensagens deste tipo o dispositivo armazena, maior é a possibilidade de informações pertencentes a categorias de segurança de alta relevância existirem. No tocante das mensagens multimídia, todos os equipamentos avaliados possuem menos de 20 mensagens deste tipo. Em contrapartida, o número de mensagens *SMS* encontradas é compatível com o recomendado em somente 21% dos aparelhos avaliados. A figura 23 ilustra os números relacionados à quantificação de mensagens *SMS*.

Conforme apresentado pela figura 23, apenas 6 equipamentos, equivalente a 21% do *dataset*, possuem até vinte mensagens, valor recomendado pela literatura. Em média, cada aparelho mantém 206,82 mensagens. Para avaliar a uniformidade deste conjunto de dados, a medida de dispersão "desvio padrão" foi utilizada. Quanto mais próximo de 0 for o valor do desvio padrão, mais homogêneos são os dados obtidos (BARBETTA et al., 2004). O desvio padrão obtido para os dados relacionados às mensagens *SMS* é de 376,36, demonstrando assim, um conjunto cujos valores encontram-se dispersos da medida central.

Figura 23: Quantidade de mensagens *SMS* encontradas nos dispositivos avaliados pelo *FBYOD*.



Fonte: autoria própria.

5.5.6 CONFIGURAÇÕES FUNDAMENTAIS

No tocante das configurações fundamentais, “uso de senha”, “configurar tempo para bloqueio de tela”, “uso de “jailbreak” (root)” e “instalação de aplicativos de fontes desconhecidas”, a figura 24 ilustra os resultados obtidos.

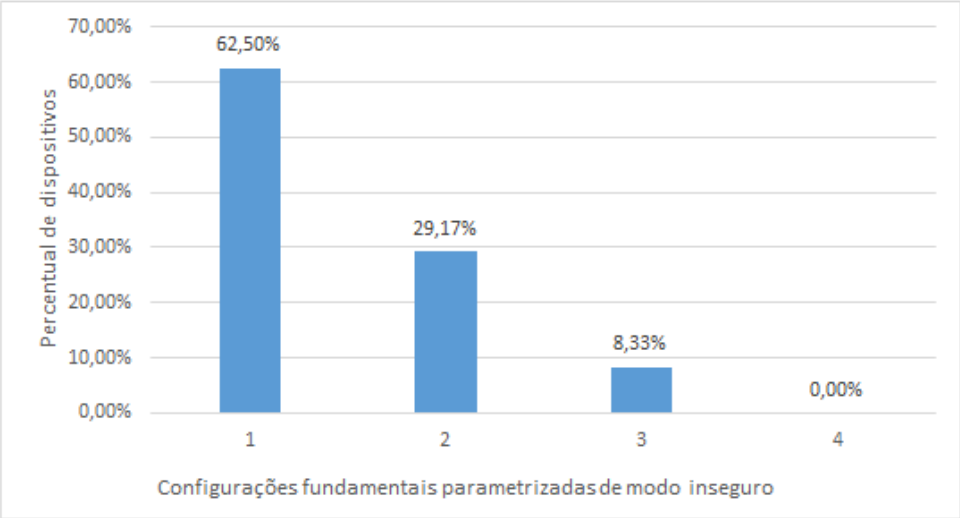
Do total de equipamentos avaliados pelo *FBYOD*, 85,71% apresentaram parametrização insegura de ao menos uma configuração fundamental. De acordo com a figura 24, a maior parte deste conjunto apresenta somente uma configuração fundamental ajustada de modo não seguro, do mesmo modo, 29,17% dos equipamentos apresentam 2 destas configurações não seguras e somente 8,33% dos dispositivos apresentaram 3 configurações inseguras. Como nenhum dos dispositivos avaliados violou a configuração “uso de jailbreak (root)”, não há dispositivos neste *dataset* com as quatro configurações fundamentais parametrizadas de modo não seguro.

5.5.7 ARQUIVOS DE DADOS DO USUÁRIO

O *FBYOD* avaliou os dispositivos no tocante da quantidade de arquivos de dados armazenados. A figura 25 ilustra os resultados obtidos.

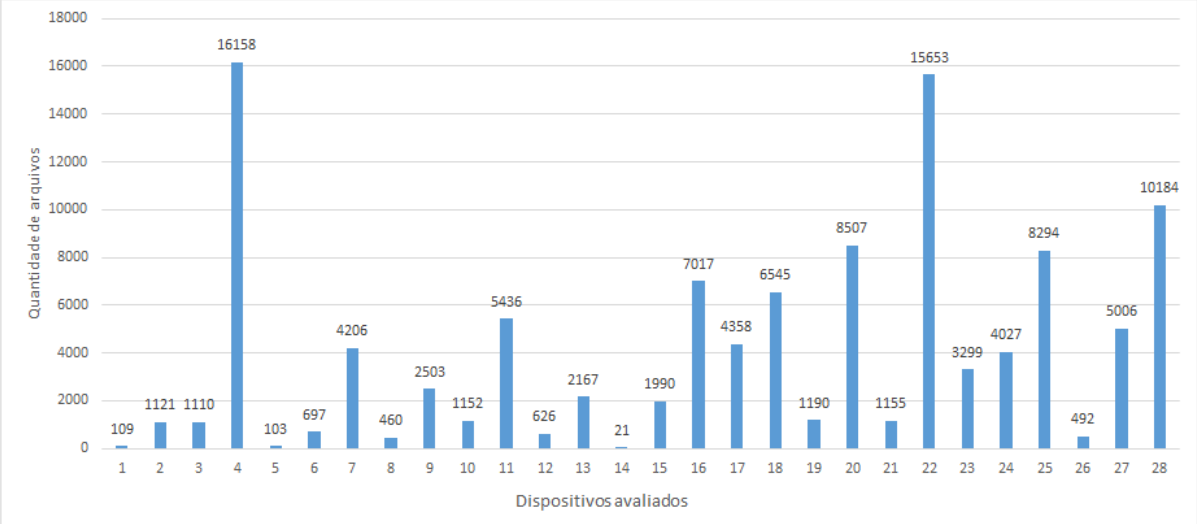
A média de arquivos encontradas deste *dataset* é de 4056,64 arquivos por dispositivo,

Figura 24: Configurações fundamentais ajustadas de modo inseguro.



Fonte: Autoria própria.

Figura 25: Quantidade de arquivos de dados do usuário encontrados pelo *FBYOD* nos dispositivos avaliados.

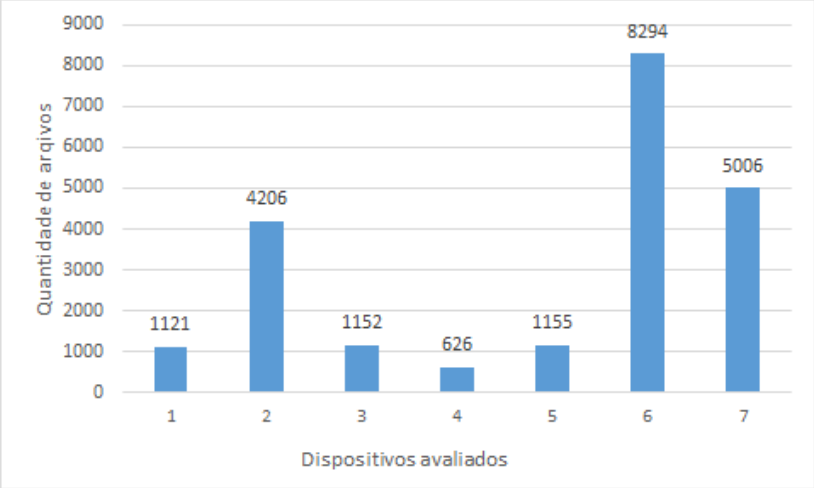


Fonte: Autoria própria.

oito vezes maior do que o número reportado na literatura. O desvio padrão para este conjunto foi computado com o valor de 4403,29, caracterizando elevada dispersão dos dados. De maneira similar, quantidades acima da média também foram encontradas nos dispositivos sem a proteção de qualquer tipo de senha. A figura 26 ilustra o resultado obtido.

Conforme apresentado pela figura 26, todos os equipamentos apresentam quantidades acima da média de dados armazenados. Assim, independentemente da categoria de segurança na qual os dados pertençam, o acesso é facilitado em virtude da inexistência de quaisquer tipos

Figura 26: Quantidade de arquivos de dados do usuário encontrados pelo *FBYOD* em dispositivos sem a proteção de senha.



Fonte: Autoria própria.

de senhas de acesso ao equipamento.

5.5.8 NÍVEIS DE ACESSO

Após a coleta dos parâmetros das configurações customizáveis e da quantidade de arquivos armazenados nos dispositivo avaliados, estes são qualificados a acessar informações de baixa, média ou alta relevância armazenadas no módulo *Storage* do *FBYOD*. A tabela 16 apresenta os resultados obtidos.

Conforme exposto pela tabela 16, apenas 3 aparelhos encontram-se aptos a acessar informações de alta, média e baixa relevância. Os demais dispositivos avaliados apenas podem acessar informações de baixa relevância em virtude do impacto de segurança apresentado. Exceto pelo “dispositivo 4”, todos os outros equipamentos classificados com “índice de impacto de segurança” igual a 100 violaram uma ou mais mais configurações fundamentais.

5.6 DISCUSSÃO

Após a análise dos resultados obtidos, observa-se que a maior parte dos usuários não utiliza de forma eficaz parte dos recursos de segurança disponíveis. Na categoria de senhas, as configurações relacionadas a políticas de senha (tamanho mínimo, senha alfanumérica, idade, histórico e caracteres complexos) não foram utilizados por nenhum dispositivo. Da mesma forma, o ajuste correto do tempo de bloqueio de tela, visibilidade da senha do tipo padrão e

Tabela 16: Qualificação dos dispositivos avaliados para acesso de informações disponíveis no módulo *Storage* do *FBYOD*.

Dispositivo	Índice de Impacto de Segurança	Nível de Acesso Qualificado
1	20,93	Arquivos de alta relevância e categorias de segurança inferiores
2	25,81	Arquivos de alta relevância e categorias de segurança inferiores
3	21,90	Arquivos de alta relevância e categorias de segurança inferiores
4	90,16	Arquivos de baixa relevância
5	100	Arquivos de baixa relevância
6	100	Arquivos de baixa relevância
7	100	Arquivos de baixa relevância
8	100	Arquivos de baixa relevância
9	100	Arquivos de baixa relevância
10	100	Arquivos de baixa relevância
11	100	Arquivos de baixa relevância
12	100	Arquivos de baixa relevância
13	100	Arquivos de baixa relevância
14	100	Arquivos de baixa relevância
15	100	Arquivos de baixa relevância
16	100	Arquivos de baixa relevância
17	100	Arquivos de baixa relevância
18	100	Arquivos de baixa relevância
19	100	Arquivos de baixa relevância
20	100	Arquivos de baixa relevância
21	100	Arquivos de baixa relevância
22	100	Arquivos de baixa relevância
23	100	Arquivos de baixa relevância
24	100	Arquivos de baixa relevância
25	100	Arquivos de baixa relevância
26	100	Arquivos de baixa relevância
27	100	Arquivos de baixa relevância
28	100	Arquivos de baixa relevância

Fonte: Autoria própria.

instalação de ferramentas *anti-malware* são adotados por apenas uma fração dos dispositivos avaliados.

De maneira positiva, configurações importantes tais como não utilizar *"jailbreak" (root)*, manter as permissões dos diretórios /system e /data, não instalar aplicativos de fontes desconhecidas e encriptar o armazenamento foram adotadas integralmente ou pela maioria dos usuários.

O usuário padrão não possui conhecimento acerca das consequências da não adoção de medidas de segurança (BECHER et al., 2011; FAGAN; KHAN, 2016). As medidas de segurança que foram negligenciadas por parte dos usuários pode embasar-se em falta de conhecimento de como procedê-las ou a sua real necessidade. Do mesmo modo, a execução de procedimentos de *"jailbreak"*, alteração das permissões de acesso dos diretórios do sistema operacional e instalação de aplicativos de fontes desconhecidas exigem conhecimento mais apu-

rado (ZHANG et al., 2015; KARTHICK; BINU, 2017).

Configurações relacionadas à categoria de rede, principalmente ao uso do *Wi-Fi*, fornecem praticidades ao usuário. Desta forma, salvar as redes sem fio costumeiramente utilizadas poupam o usuário da conexão manual e da consequente digitação da senha de acesso a cada nova conexão. De igual teor, a notificação acerca de redes sem fio públicas alertam o usuário sobre sua existência e o facultam a utilizá-las.

No tocante dos arquivos armazenados, constata-se quantidades de dados maiores ao reportado na literatura. Desta forma, possivelmente, arquivos de todas as categorias de segurança podem ser encontrados no dispositivo. Na seção 5.5.7 foi apresentado que 7 dispositivos, equivalente a 25% do *dataset*, armazenam grande quantidade de dados e sem a proteção de senha, e assim, corrobora com o não conhecimento do usuário acerca das consequências da não utilização de controles de segurança e adicionalmente, o valor de suas informações.

A utilização de lógica *fuzzy*, através de suas características, proporcionou relacionar o impacto de segurança causado pelas configurações customizáveis e a quantidade de determinadas informações que o usuário armazenada no dispositivo móvel. Desta forma, forneceu embasamento para mensurar o impacto de segurança causado pelos equipamentos avaliados e assim classificá-los, de forma dinâmica, a acessar somente informações compatíveis com o risco apresentado pelo aparelho.

A maior parte dos equipamentos avaliados demonstrou vulnerabilidades importantes. Então a adoção de níveis de acesso a informações corporativas mostrou-se eficaz. Sob eventual exploração destas vulnerabilidades, aqueles equipamentos apenas possuem acesso a informações de baixa relevância e caso ocorra o furto de dados, o impacto é limitado.

5.7 CONCLUSÃO

Este capítulo apresentou a validação da proposta através do aplicativo *FBYOD*. Os dados obtidos por este *software* são oriundos de dispositivos móveis compatíveis com a política de *BYOD* do ambiente corporativo da prefeitura municipal de São Bento do Sul - Santa Catarina.

Os resultados obtidos demonstram que as configurações customizáveis e a quantidade de arquivos do usuário armazenados no dispositivo desempenham papel fundamental na manutenção da segurança dos dispositivos. O *FBYOD* mostrou-se eficaz na avaliação do impacto de segurança causado por dispositivos móveis. Assim, pôde-se qualificar esses equipamentos ao acesso de informações cuja categoria de segurança é compatível com o grau de impacto de segurança apresentado pelo dispositivo.

6 CONCLUSÃO E TRABALHOS FUTUROS

A crescente oferta de mobilidade popularizou o uso de dispositivos móveis como *smartphones* e *tablets* para fins profissionais. Estes equipamentos podem ser utilizados para compor políticas de *BYOD* e assim, seus usuários podem usufruir da vantagem de utilizar o mesmo equipamento para fins pessoais e laborais.

O principal inconveniente relacionado a adoção do *BYOD* é o furto de dados. Um dos pilares que pode desencadear o furto de dados é a customização de configurações do sistema operacional do dispositivo móvel com parâmetros não seguros. Assim, mesmo que a parametrização da configuração seja válida, o ajuste pode provocar vulnerabilidades.

Este trabalho abordou a mitigação do impacto causado pelo furto de dados e outras ameaças digitais em ambientes onde políticas de *BYOD* são adotadas. A abordagem propôs a coleta dos parâmetros das configurações customizáveis do dispositivo móvel e a mensuração dos arquivos de dados que o usuário armazena no equipamento. Neste aspecto, pôde-se avaliar o risco de segurança que cada dispositivo representa. Com o resultado desta avaliação, cada equipamento é qualificado a acessar informações corporativas compatíveis com o impacto de segurança aferido.

O aplicativo *FBYOD* demonstrou a eficácia do modelo proposto e apontou que usuários negligenciam parâmetros importantes como uso de senhas de desbloqueio do dispositivo e demais configurações relacionadas à esta categoria, assim como a adoção de bloqueio de tela e ferramenta *anti-malware*. Caso todas as categorias de segurança das informações acessadas estivessem disponíveis a todos os aparelhos avaliados, sob eventual furto de dados, o impacto causado seria elevado.

De igual forma, observou-se quantidades de dados armazenados nos aparelhos cerca de oito vezes superiores à média reportada na literatura. Desta forma, fica evidente que os dispositivos móveis desempenham papel fundamental na comunicação e execução de trabalhos, necessitando de medidas de proteção compatíveis com a importância dos dados armazenados.

Por outro lado, o conhecimento limitado dos usuários acerca de procedimentos de

segurança pode ter sido importante na preservação de alguns pontos. Os processos de alteração de permissões dos diretórios do sistema operacional, assim como o uso de *root* ou *jailbreak*, requerem conhecimentos avançados. No *dataset* obtido, nenhum dos dispositivos violou estes aspectos de segurança.

6.1 LIMITAÇÕES E AMEAÇAS À VALIDADE

O trabalho aqui apresentado contém limitações e ameaças à validade. A seguir, estes itens encontram-se elencados:

1. A proposta deste trabalho não prevê nenhuma correção ou sugestão de ajuste das configurações customizáveis parametrizadas de modo inseguro do aparelho sob avaliação. Desta forma, somente os parâmetros atribuídos são coletados;

2. A coleta da quantidade de arquivos armazenados no dispositivo móvel leva em consideração somente os diretórios do usuário. A gravação destes dados em outros locais é possível caso o aparelho possua *"jailbreak" (root)*. Entretanto, a contagem poderia ser prejudicada pois não há distinção de quais são os arquivos do usuário e quais são do sistema operacional ou de aplicativos;

3. Referente ainda à quantidade de arquivos mensurados do dispositivo móvel, nenhum tipo de avaliação de conteúdo dos mesmos é efetuado. Um equipamento pode conter poucos arquivos de alta relevância enquanto outro pode conter inúmeros arquivos de baixa importância;

4. A lista de configurações pode tornar-se obsoleta e necessitar de atualizações. Desta forma, basta incluir ou remover itens e atribuir o nível de impacto de segurança compatível;

5. A lista de aplicações *anti-malware* pode tornar-se obsoleta. Entretanto, após nova pesquisa, torna-se possível incluir novos itens ou excluir itens inválidos;

6. A verificação de instalação de aplicativos de terceiros foi alterada na versão do *Android* 8 e superior. Observou-se a coleta incorreta destes dados em alguns equipamentos do fabricante *Samsung*;

7. Este trabalho baseia-se em conclusões de demais publicações. Desta forma, conclusões imprecisas das publicações referenciadas podem influenciar os resultados deste trabalho.

6.2 TRABALHOS FUTUROS

Os trabalhos futuros propostos visam aprimorar este trabalho e bem como, mitigar as ameaças à validade. A seguir os itens propostos encontram-se descritos:

1. *Sugestão ou correção de parâmetros inseguros das configurações coletadas*: a ferramenta desenvolvida pode corrigir parâmetros inseguros ou informar ao administrador e ao usuário sugestões e procedimentos acerca de sua correta parametrização;

2. *Avaliar a relevância dos arquivos armazenados*: para a precisa mensuração dos dados armazenados no aparelho, a avaliação do conteúdo dos arquivos é necessária, classificando em categorias de segurança os dados armazenados no equipamento;

3. *Avaliar arquivos armazenados em ambiente cloud*: soluções de armazenamento como *Google Drive* e *Dropbox* são comumente aplicadas para fins empresariais (DARYABAR et al., 2016). Deste modo, o uso destas aplicações pode indicar o uso de arquivos corporativos e auxiliar na classificação da relevância dos arquivos coletados;

4. *Coletar as atualizações do sistema operacional*: ao verificar quais *patches* de segurança encontram-se instalados, pode-se obter mais detalhes acerca da segurança do sistema operacional se comparada a simples coleta da versão do mesmo;

5. *Aplicar esta proposta a outro sistema operacional*: esta proposta pode ser aplicada a outros sistemas operacionais. Para isto, basta coletar as configurações customizáveis e aplicar os níveis de impacto de segurança individuais;

6. *Outro método para avaliação de impacto de segurança*: este trabalho utiliza a lógica *fuzzy* para auxiliar na classificação de impacto de segurança que o dispositivo apresenta. Entretanto, outras alternativas como o uso de algoritmos genéticos e redes neurais, por exemplo, podem ser utilizadas.

Este trabalho é uma singela contribuição à ciência. Espera-se que as informações aqui contidas sirvam de inspiração e embasamento a outros autores.

REFERÊNCIAS

ARMANDO, A. et al. Developing a nato byod security policy. In: IEEE. **Military Communications and Information Systems (ICMCIS), 2016 International Conference on**. [S.l.], 2016. p. 1–6.

BARBETTA, P. A.; REIS, M. M.; BORNIA, A. C. **Estatística: para cursos de engenharia e informática**. [S.l.]: Atlas São Paulo, 2004.

BECHER, M. et al. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In: IEEE. **Security and Privacy (SP), 2011 IEEE Symposium on**. [S.l.], 2011. p. 96–111.

BEDNARCZYK, M.; PIOTROWSKI, Z. Will wpa3 really provide wi-fi security at a higher level? In: INTERNATIONAL SOCIETY FOR OPTICS AND PHOTONICS. **XII Conference on Reconnaissance and Electronic Warfare Systems**. [S.l.], 2019. v. 11055, p. 1105514.

BEJARANO, O.; KNIGHTLY, E. W.; PARK, M. Ieee 802.11 ac: from channelization to multi-user mimo. **IEEE Communications Magazine**, IEEE, v. 51, n. 10, p. 84–90, 2013.

BEN-ASHER, N. et al. On the need for different security methods on mobile phones. In: ACM. **Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services**. [S.l.], 2011. p. 465–473.

BIANCHI, G. Performance analysis of the ieee 802.11 distributed coordination function. **IEEE Journal on selected areas in communications**, IEEE, v. 18, n. 3, p. 535–547, 2000.

BLIZZARD, S. Coming full circle: are there benefits to byod? **Computer Fraud & Security**, Elsevier, v. 2015, n. 2, p. 18–20, 2015.

BORISOV, N.; GOLDBERG, I.; WAGNER, D. Intercepting mobile communications: the insecurity of 802.11. In: ACM. **Proceedings of the 7th annual international conference on Mobile computing and networking**. [S.l.], 2001. p. 180–189.

BURR, G. W. et al. Experimental demonstration and tolerancing of a large-scale neural network (165 000 synapses) using phase-change memory as the synaptic weight element. **IEEE Transactions on Electron Devices**, IEEE, v. 62, n. 11, p. 3498–3507, 2015.

BUSTINCE, H. et al. A historical account of types of fuzzy sets and their relationships. **IEEE Transactions on Fuzzy Systems**, IEEE, v. 24, n. 1, p. 179–194, 2015.

CAHYANI, N. D. W. et al. Forensic data acquisition from cloud-of-things devices: windows smartphones as a case study. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, v. 29, n. 14, p. e3855, 2017.

CARVALHO, J. A. P. et al. Comparative performance studies of laboratory wpa ieee 802.11 g point-to-point links. In: IEEE. **Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on**. [S.l.], 2012. p. 1–4.

CHADLI, M.; BORNE, P. Multiple models approach in automation. In: **Takagi-Sugeno Fuzzy Systems**. [S.l.]: Wiley Online Library, 2013.

CHEN, K. et al. Finding unknown malice in 10 seconds: Mass vetting for new threats at the google-play scale. In: **USENIX Security Symposium**. [S.l.: s.n.], 2015. v. 15.

CIS. **Security Benchmarks**. 2018. `https://www.cisecurity.org`. Acessado em: 30/04/2018.

CISCO. **RADIUS: WPA2-Enterprise With EAP-TLS Using Microsoft NPS**. 2018. `https://documentation.meraki.com/MR/Encryption_and_Authentication/RADIUS%3A_WPA2-Enterprise_With_EAP-TLS_Using_Microsoft_NPS`. Acessado em: 03/05/2018.

CORTES, C. et al. Adanet: Adaptive structural learning of artificial neural networks. In: JMLR. ORG. **Proceedings of the 34th International Conference on Machine Learning-Volume 70**. [S.l.], 2017. p. 874–883.

COSTA, W. T. da et al. Identification of photovoltaic model parameters by differential evolution. In: IEEE. **2010 IEEE International Conference on Industrial Technology**. [S.l.], 2010. p. 931–936.

COSTANTINO, G. et al. Towards enforcing on-the-fly policies in byod environments. In: IEEE. **Information Assurance and Security (IAS), 2013 9th International Conference on**. [S.l.], 2013. p. 61–65.

CROW, B. P. et al. Ieee 802.11 wireless local area networks. **IEEE Communications magazine**, IEEE, v. 35, n. 9, p. 116–126, 1997.

DANG-PHAM, D.; PITTAYACHAWAN, S. Comparing intention to avoid malware across contexts in a byod-enabled australian university: A protection motivation theory approach. **Computers & Security**, v. 48, p. 281–297, Fevereiro 2015.

DARYABAR, F. et al. Forensic investigation of onedrive, box, googledrive and dropbox applications on android and ios devices. **Australian Journal of Forensic Sciences**, Taylor & Francis, v. 48, n. 6, p. 615–642, 2016.

D'ORAZIO, C. J.; CHOO, K.-K. R. Circumventing ios security mechanisms for apt forensic investigations: A security taxonomy for cloud apps. **Future Generation Computer Systems**, Elsevier, v. 79, p. 247–261, 2018.

DOWNER, K.; BHATTACHARYA, M. Byod security: A new business challenge. In: **Smart City/SocialCom/SustainCom (SmartCity), 2015 IEEE International Conference on**. [S.l.: s.n.], 2016.

ENCK, W. Defending users against smartphone apps: Techniques and future directions. In: SPRINGER. **International Conference on Information Systems Security**. [S.l.], 2011. p. 49–70.

FAGAN, M.; KHAN, M. M. H. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In: **Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)**. [S.l.: s.n.], 2016. p. 59–75.

FATIMA, H.; DASH, G. N.; PRADHAN, S. K. Soft computing applications in cyber crimes. In: **2017 2nd International Conference on Anti-Cyber Crimes (ICACC)**. [S.l.: s.n.], 2017. p. 66–69.

FELT, A. P. et al. A survey of mobile malware in the wild. In: ACM. **Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices**. [S.l.], 2011. p. 3–14.

FUKAMI, S.; MIZUMOTO, M.; TANAKA, K. Some considerations on fuzzy conditional inference. **Fuzzy sets and Systems**, Elsevier, v. 4, n. 3, p. 243–273, 1980.

GONZALES, H. et al. Practical defenses for evil twin attacks in 802.11. In: IEEE. **Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE**. [S.l.], 2010. p. 1–6.

GOOGLE. **Android Developer**. 2018. `https://developer.android.com/`. Acessado em: 08/01/2018.

GOOGLE. **Android Developer**. 2018. `https://developer.android.com/`. Acessado em: 01/03/2018.

GOOGLE. **Developers - Android Studio**. 2018. `https://developer.android.com/studio`. Acessado em: 23/09/2018.

GOOGLE. **Developers - Google Firebase**. 2018. `https://firebase.google.com`. Acessado em: 23/09/2018.

GOOGLE. **Google Firebase Administration Console**. 2018. `https://console.firebase.google.com`.

GOOGLE. **Google Firebase Storage**. 2018. `https://console.firebase.google.com`.

GOOGLE. **Google Play Store**. 2018. `https://play.google.com/store`. Acessado em: 14/11/2018.

GOOGLE. **Android Developer**. 2019. `https://developer.android.com/about/versions/marshmallow/android-6.0?hl=pt-br`. Acessado em: 04/03/2019.

HASSAN, H. R.; CHALLAL, Y. Enhanced wep: An efficient solution to wep threats. In: IEEE. **Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference on**. [S.l.], 2005. p. 594–599.

HIERTZ, G. R. et al. The ieee 802.11 universe. **IEEE Communications Magazine**, IEEE, v. 48, n. 1, 2010.

HODO, E. et al. Threat analysis of iot networks using artificial neural network intrusion detection system. In: IEEE. **2016 International Symposium on Networks, Computers and Communications (ISNCC)**. [S.l.], 2016. p. 1–6.

HOQUE, N.; BHATTACHARYYA, D.; KALITA, J. Botnet in ddos attacks: Trends and challenges. **IEEE Communications Surveys & Tutorials**, IEEE, v. 17, p. 2242–2270, Julho 2015.

HU, H.; BEZEMER, C.-P.; HASSAN, A. E. Studying the consistency of star ratings and the complaints in 1 & 2-star user reviews for top free cross-platform android and ios apps. **Empirical Software Engineering**, Springer, p. 1–34, 2018.

ISO27002 - Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação. [S.l.], September 2013.

JAMIL, Q.; SHAH, M. A. Analysis of machine learning solutions to detect malware in android. In: IEEE. **Innovative Computing Technology (INTECH), 2016 Sixth International Conference on**. [S.l.], 2016. p. 226–232.

JANG, J.-S. Anfis: adaptive-network-based fuzzy inference system. **IEEE transactions on systems, man, and cybernetics**, IEEE, v. 23, n. 3, p. 665–685, 1993.

JEON, W. et al. A practical analysis of smartphone security. In: SPRINGER. **Symposium on Human Interface**. [S.l.], 2011. p. 311–320.

KAMBOURAKIS, G. et al. Introducing touchstroke: keystroke-based authentication system for smartphones. **Security and Communication Networks**, Wiley Online Library, v. 9, n. 6, p. 542–554, 2016.

KANTH, B. K. A hybrid network architecture for applications of adaptive neuro fuzzy inference system. **International Journal of Current Trends in Engineering and Research (IJCTER)**, 2016.

KAO, Y.-C.; CHANG, Y.-C.; CHANG, R.-S. Managing bring your own device services in campus wireless networks. In: IEEE. **Computer Science and Engineering Conference (ICSEC), 2015 International**. [S.l.], 2015. p. 1–7.

KARLIK, B.; OLGAC, A. V. Performance analysis of various activation functions in generalized mlp architectures of neural networks. **International Journal of Artificial Intelligence and Expert Systems**, v. 1, n. 4, p. 111–122, 2011.

KARTHICK, S.; BINU, S. Android security issues and solutions. In: IEEE. **2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)**. [S.l.], 2017. p. 686–689.

KHASAWNEH, M. et al. A survey on wi-fi protocols: Wpa and wpa2. In: SPRINGER. **International Conference on Security in Computer Networks and Distributed Systems**. [S.l.], 2014. p. 496–511.

KO, R.; TAN, A.; GAO, T. A mantrap-inspired, user-centric data leakage prevention (dlp) approach. In: IEEE. **Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on**. [S.l.], 2014.

KOHLIOS, C.; HAYAJNEH, T. A comprehensive attack flow model and security analysis for wi-fi and wpa3. **Electronics**, Multidisciplinary Digital Publishing Institute, v. 7, p. 284, 2018.

KRITZINGER, E.; SOLMS, S. H. von. Cyber security for home users: A new way of protection through awareness enforcement. **Computers & Security**, Elsevier, v. 29, n. 8, p. 840–847, 2010.

KUMAR, A.; PAUL, P. Security analysis and implementation of a simple method for prevention and detection against evil twin attack in ieee 802.11 wireless lan. In: IEEE. **Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on**. [S.l.], 2016. p. 176–181.

KUO, E.-C.; CHANG, M.-S.; KAO, D.-Y. User-side evil twin attack detection using time-delay statistics of tcp connection termination. In: IEEE. **Advanced Communication Technology (ICACT), 2018 20th International Conference on**. [S.l.], 2018. p. 211–216.

LASHKARI, A. H.; DANESH, M. M. S.; SAMADI, B. A survey on wireless security protocols (wep, wpa and wpa2/802.11 i). In: IEEE. **2009 2nd IEEE International Conference on Computer Science and Information Technology**. [S.l.], 2009. p. 48–52.

LEAVITT, N. Today. **Computer**, IEEE, p. 16–19, 2013.

LI, Q.; CLARK, G. Mobile security: a look ahead. **IEEE Security & Privacy**, IEEE, v. 11, n. 1, p. 78–81, 2013.

LIAO, H.-J. et al. Intrusion detection system: A comprehensive review. **Journal of Network and Computer Applications**, Elsevier, v. 36, n. 1, p. 16–24, 2013.

LUCA, A. D.; LINDQVIST, J. Is secure and usable smartphone authentication asking too much? **Computer**, IEEE, v. 48, n. 5, p. 64–68, 2015.

MACONACHY, W. V. et al. A model for information assurance: An integrated approach. In: UNITED STATES MILITARY ACADEMY, WEST POINT. IEEE. **Proceedings of the 2001 IEEE Workshop on Information Assurance and Security**. [S.l.], 2001. v. 310.

MARTIN, W. et al. A survey of app store analysis for software engineering. **IEEE transactions on software engineering**, IEEE, v. 43, n. 9, p. 817–847, 2017.

MATLAB. **Matlab2019**. 2019. `https://www.mathworks.com/products/matlab.html`.

MAVRIDIS, I. et al. Real-life paradigms of wireless network security attacks. In: IEEE. **Informatics (PCI), 2011 15th Panhellenic Conference on**. [S.l.], 2011. p. 112–116.

MENDEL, J. M. Uncertain rule-based fuzzy systems. In: **Introduction and new directions**. [S.l.]: Springer, 2017. p. 684.

METAWA, N.; HASSAN, M. K.; ELHOSENY, M. Genetic algorithm based model for optimizing bank lending decisions. **Expert Systems with Applications**, Elsevier, v. 80, p. 75–82, 2017.

MILLER, C. Mobile attacks and defense. **IEEE Security & Privacy**, IEEE, v. 9, n. 4, p. 68–70, 2011.

MILLER, K. W.; VOAS, J.; HURLBURT, G. F. Byod: Security and privacy considerations. **It Professional**, IEEE, v. 14, n. 5, p. 53–55, 2012.

MITRE. **CVE - Common Vulnerabilities and Exposures**. 2018. `https://cve.mitre.org`. Acessado em: 01/05/2018.

MIZUMOTO, M.; ZIMMERMANN, H.-J. Comparison of fuzzy reasoning methods. **Fuzzy sets and systems**, Elsevier North-Holland, Inc., v. 8, n. 3, p. 253–283, 1982.

MORSALIN, S. et al. Machine-to-machine communication based smart home security system by nfc, fingerprint, and pir sensor with mobile android application. In: IEEE. **2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)**. [S.l.], 2016. p. 1–6.

MUSLUKHOV, I. et al. Understanding users' requirements for data protection in smartphones. In: IEEE. **Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on**. [S.l.], 2012. p. 228–235.

MUTAKIN, D.; KHAN, M.; IBRAHIM, J. Cyber risk management for wireless communication in organization. **International Journal of Scientific and Research Publications**, v. 6, p. 403–407, Janeiro 2016.

NAIK, N. Fuzzy inference based intrusion detection system: Fi-snort. In: IEEE. **Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on**. [S.l.], 2015. p. 2062–2067.

NAKHILA, O. et al. Parallel active dictionary attack on wpa2-psk wi-fi networks. In: IEEE. **Military Communications Conference, MILCOM 2015-2015 IEEE**. [S.l.], 2015. p. 665–670.

NAYAK, A.; YEN, K.; PONS, A. Fuzzy logic based android malware classification approach. **International Journal of Computer Networks and Security**, v. 24, n. 1, p. 8, 2014.

NOH, J.; KIM, J.; CHO, S. Secure authentication and four-way handshake scheme for protected individual communication in public wi-fi networks. **IEEE Access**, IEEE, 2018.

ORDOOBADI, S. M. Development of a supplier selection model using fuzzy logic. **Supply Chain Management: An International Journal**, Emerald Group Publishing Limited, v. 14, n. 4, p. 314–327, 2009.

ORS, S. B. et al. Power-analysis attack on an asic aes implementation. In: IEEE. **Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on**. [S.l.], 2004. v. 2, p. 546–552.

PAGE, L. The trade offs for bring your own devices. **IS Practices for SME Success Series**, v. 1, n. 1, 2013.

PANDEY, H. M. Performance evaluation of selection methods of genetic algorithm and network security concerns. **Procedia Computer Science**, Elsevier, v. 78, p. 13–18, 2016.

POLLA, M. L.; MARTINELLI, F.; SGANDURRA, D. A survey on security for mobile devices. **IEEE communications surveys & tutorials**, IEEE, v. 15, n. 1, p. 446–471, 2013.

RADA-VILELA, J. **fuzzylite: a fuzzy logic control library**. 2017. Disponível em: <http://fuzzylite.com>.

RAYARIKAR, R.; UPADHYAY, S.; PIMPALE, P. Sms encryption using aes algorithm on android. **International Journal of Computer Applications**, International Journal of Computer Applications, 244 5 th Avenue,# 1526, New ..., v. 50, n. 19, p. 12–17, 2012.

ROSE, C. Byod: An examination of bring your own device in business. **The Review of Business Information Systems (Online)**, The Clute Institute, v. 17, n. 2, p. 65, 2013.

ROSS, R. S.; SWANSON, M. M. **Standards for Security Categorization of Federal Information and Information Systems**. [S.l.], February 2004. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.

ROUT, G. P.; MOHANTY, S. N. A hybrid approach for network intrusion detection. In: **2015 Fifth International Conference on Communication Systems and Network Technologies**. [S.l.: s.n.], 2015. p. 614–617.

SAHINASLAN, O. Encryption protocols on wireless iot tools. In: AIP PUBLISHING. **AIP Conference Proceedings**. [S.l.], 2019. v. 2086, p. 030036.

SAIED, A.; OVERILL, R. E.; RADZIK, T. Detection of known and unknown ddos attacks using artificial neural networks. **Neurocomputing**, Elsevier, v. 172, p. 385–393, 2016.

SARRAFZADEH, A.; SATHU, H. Wireless lan security status changes in auckland cbd: A case study. In: IEEE. **Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on**. [S.l.], 2015. p. 1–6.

SCHAUB, F.; DEYHLE, R.; WEBER, M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In: ACM. **Proceedings of the 11th international conference on mobile and ubiquitous multimedia**. [S.l.], 2012. p. 13.

SHAO, G.-l. et al. A fuzzy detection approach toward different speed port scan attacks based on dempster shafer evidence theory. **Security and Communication Networks**, v. 9, n. 15, p. 2627–2640, 2016. ISSN 1939-0122. SCN-14-0841.R1. Disponível em: <http://dx.doi.org/10.1002/sec.1508>.

SHAO, Y.; LUO, X.; QIAN, C. Rootguard: Protecting rooted android phones. **Computer**, IEEE, v. 47, n. 6, p. 32–40, 2014.

SOUPPAYA, M.; SCARFONE, K. **User's Guide to Telework and Bring Your Own Device (BYOD) Security**. [S.l.], July 2016. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final>.

SPIRO. **What is wireless network?** 2018. `http://spiroprojects.com/blog/cat-view-more.php?blogname=What-is-wireless-network?&id=30`. Acessado em: 01/05/2018.

STACKOVERFLOW. **Stack Overflow**. 2018. `https://stackoverflow.com/`. Acessado em: 08/07/2018.

STUBBLEFIELD, A. et al. Using the fluhrer, mantin, and shamir attack to break wep. In: **NDSS**. [S.l.: s.n.], 2002.

SU, C.-T.; LII, G.-R.; TSAI, C.-C. Optimal capacitor allocation using fuzzy reasoning and genetic algorithms for distribution systems. **Mathematical and computer modelling**, Elsevier, v. 33, n. 6-7, p. 745–757, 2001.

SUAREZ-TANGIL, G. et al. Evolution, detection and analysis of malware for smart devices. **IEEE Communications Surveys & Tutorials**, IEEE, v. 16, n. 2, p. 961–987, 2014.

SYMANTEC. **Internet Security Threat Report - ISTR**. [S.l.], abr. 2017. Disponível em: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>.

SYMANTEC. **Internet Security Threat Report - ISTR**. [S.l.], abr. 2018. Disponível em: <https://resource.elq.symantec.com/e/f2>.

TEUFL, P. et al. Android encryption systems. In: IEEE. **2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)**. [S.l.], 2014. p. 1–8.

TEWS, E. Attacks on the wep protocol. **IACR Cryptology ePrint Archive**, v. 2007, p. 471, 2007.

TEWS, E.; WEINMANN, R.-P.; PYSHKIN, A. Breaking 104 bit wep in less than 60 seconds. In: SPRINGER. **International Workshop on Information Security Applications**. [S.l.], 2007. p. 188–202.

THEOHARIDOU, M.; MYLONAS, A.; GRITZALIS, D. A risk assessment method for smartphones. In: SPRINGER. **IFIP International Information Security Conference**. [S.l.], 2012. p. 443–456.

UHLIG, P. R. **Fuzzy BYOD - FBYOD**. 2018. `play.google.com/store/apps/details?id=mestrado.dissertacao.com.fbyod`.

VECCHIATO, D. A. **Benchmarking User-Defined Security Configurations of Android Devices**. Tese (Doutorado) — Unicamp - Universidade Estadual de Campinas, Campinas - Brasil, 2016.

VIDAS, T.; VOTIPKA, D.; CHRISTIN, N. All your droid are belong to us: A survey of current android attacks. In: **WOOT**. [S.l.: s.n.], 2011. p. 81–90.

WIFI-ALLIANCE. **Wi-Fi Alliance introduces Wi-Fi CERTIFIED WPA3 security**. 2019. `https://bit.ly/2ts2tci`. Acessado em: 01/09/2019.

WUERGES, A. F. E.; BORBA, J. A. Redes neurais, lógica nebulosa e algoritmos genéticos: aplicações e possibilidades em finanças e contabilidade. **JISTEM-Journal of Information Systems and Technology Management (Online)**, v. 7, n. 1, p. 163–182, 2010.

YAO, F. et al. Fuzzy logic-based implicit authentication for mobile access control. In: IEEE. **SAI Computing Conference (SAI), 2016**. [S.l.], 2016. p. 968–975.

YUNWU, W. Using fuzzy expert system based on genetic algorithms for intrusion detection system. In: **2009 International Forum on Information Technology and Applications**. [S.l.: s.n.], 2009. v. 2, p. 221–224.

ZADEH, L. A. Fuzzy sets. In: **Fuzzy Sets, Fuzzy Logic, And Fuzzy Systems: Selected Papers by Lotfi A Zadeh**. [S.l.]: World Scientific, 1996. p. 394–432.

ZAHADAT, N. et al. Byod security engineering: A framework and its analysis. **Computers & Security**, Elsevier, v. 55, p. 81–99, 2015.

ZHANG, H. et al. Optimal dos attack scheduling in wireless networked control system. **IEEE Transactions on Control Systems Technology**, IEEE, v. 24, n. 3, p. 843–852, 2016.

ZHANG, H.; SHE, D.; QIAN, Z. Android root and its providers: A double-edged sword. In: ACM. **Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security**. [S.l.], 2015. p. 1093–1104.

ZHOU, W. et al. Detecting repackaged smartphone applications in third-party android marketplaces. In: ACM. **Proceedings of the second ACM conference on Data and Application Security and Privacy**. [S.l.], 2012. p. 317–326.

ZHOU, Y.; JIANG, X. Dissecting android malware characterization and evolution. **Security and Privacy SP, 2012 IEEE Symposium on**, IEEE, p. 95–109, 2012.

ZHU, H.-J. et al. Droiddet: effective and robust detection of android malware using static analysis along with rotation forest model. **Neurocomputing**, Elsevier, v. 272, p. 638–646, 2018.