CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

INFORMÁTICA

ANÁLISE DE SEGURANÇA SOBRE APLICATIVO DE MENSAGEM INSTANTÂNEA: WHATSAPP COMO ESTUDO DE CASO

Antonio Marcos de Castro Mota[1], Paulo Roberto Corrêa Leão[2]
Pós-graduado em Perícia Computacional[1], Mestre em Gestão do Conhecimento e Tecnologia da Informação[2]

RESUMO: O vazamento de informações da agência norte-americana NSA (National Security Agency) por um de seus analistas, Edward Snowden, em 2013, trouxe à tona múltiplas informações sobre programas de vigilância e monitoramento de comunicações digitais geridos pela agência e que tinham como parceiros grandes provedores da Internet. Tal episódio, desencadeador de grande repercussão na comunidade internacional, instigou ainda mais precauções e cuidados por parte dos gestores e especialistas em segurança de comunicações, sobretudo quanto à necessidade de robustecimento de práticas relativas à salvaguarda de privacidade de dados na grande rede. Em meio a esse contexto, dada a popularização de ferramentas de troca de mensagens e do aumento do tráfego de voz sob IP em dispositivos móveis, uma pesquisa a respeito dos aspectos de segurança envolvidos nesse tipo de serviço, bem como um estudo de caso realizado sobre o WhatsApp (com enfoque no tráfego de dados e na quebra de privacidade e autenticidade) poderia resultar em importante conhecimento a ser compartilhado e divulgado à imensa quantidade de usuários finais da ferramenta, bem como aos estudiosos da área de Segurança e de Perícia Forense. Assim, o Artigo Técnico proposto referenciou o funcionamento das comunicações de voz sobre IP, percorrendo os principais métodos de criptografia e os atributos de segurança da informação. Para a realização do estudo empírico foi realizada uma pesquisa exploratória, tendo por base a pesquisa aplicada, a revisão bibliográfica, os padrões conhecidos sobre o tema e um estudo de caso seguido da respectiva análise e conclusão.

Palavras-chave: Segurança da Comunicação. VoIP. Forense Computacional. Análise de Tráfego.

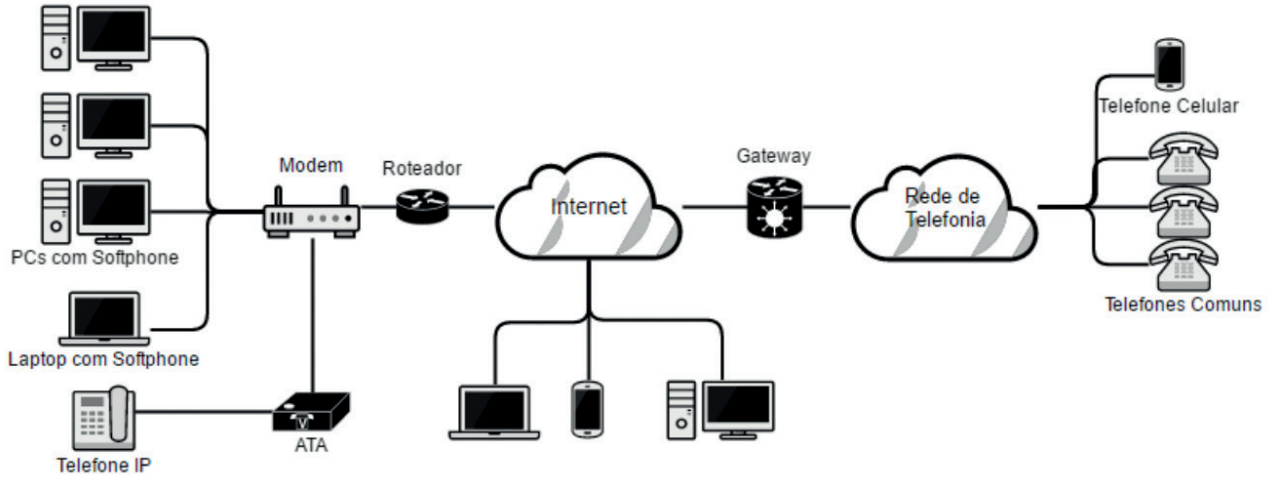
INTRODUÇÃO

Os aplicativos de mensagens instantâneas passaram por um amplo processo de massificação nesta última década. Em busca de tornar os softwares mensageiros atrativos, as empresas desenvolvedoras passaram a agregar várias funcionalidades aos seus projetos de comunicação, assim, além do envio de textos, tornou-se possível em um mesmo aplicativo a troca de arquivos como gifs animados, planilhas, documentos em formato portátil, músicas, entre outras.

A integração de chamadas de voz sobre IP (VoIP) aos softwares de troca de mensagens, certamente foi um dos mais importantes passos na ampliação dessa convergência de serviços em aparelhos telefônicos.

Os sistemas VoIP trazem inúmeras vantagens, tais como redução de custo operacional (em virtude de uma mesma rede para transporte de dados e voz), flexibilidade (uma vez que proporciona grande variedade de serviços), mobilidade (pois usuários podem fazer e receber chamadas de voz a partir de uma infinidade de pontos geográficos), entre outras características. Na Figura 1 estão elencadas algumas possibilidades de interconexão de dispositivos VoIP.

FIGURA 1 Arquitetura típica de rede VoIP.



Fonte: o autor, 2016.

À medida que tais aplicativos de mensagens (e voz) tornaram-se amplamente utilizados cresceram também os problemas relacionados à segurança. A interceptação de sinais, a invasão de dispositivo e a popularização de métodos de crimes cibernéticos são fatores que demonstram a necessidade do aprofundamento de estudos que envolvam o envio e recebimento de tráfego de dados e VoIP, bem como de medidas que possam mitigar possíveis ataques ou ameaças.

> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (NBR ISO 27002/2005, p. 10).

Assim, pesquisas atinentes à segurança das informações em tais tipos de softwares revestem-se de relevância, vez que podem vir a subsidiar novas técnicas, metodologias, códigos e “retratos” que visem aprimorar os cuidados com as comunicações de dados e de voz sobre IP.

Este artigo tem como objetivo geral a elaboração de uma análise de segurança de informações sobre um aplicativo de mensagem instantânea. Para tanto, montou-se uma rede privada (em laboratório) em que foram colocados em prática métodos de análise de tráfego e MAC spoofing objetivando-se levantar e identificar possíveis brechas.

A organização deste escrito estrutura-se da seguinte forma: a seção 2 trata da metodologia da pesquisa, dos instrumentos e procedimentos, bem como da pormenorização do estudo de caso em si; a seção 3 trata dos resultados e discussões; e a seção 4 exibe a parte final com as conclusões do autor sobre o tema estudado.

1 METODOLOGIA E MATERIAIS

A seguir estão elencados o tipo de metodologia aplicada, os instrumentos, os procedimentos e a implementação do estudo de caso.

1.1 METODOLOGIA

Para subsidiar este artigo realizou-se uma pesquisa bibliográfica em meio a literatura de tecnologia da informação sobre assuntos como segurança da informação, criptografia e VoIP.

Foram realizadas também consultas em artigos e trabalhos de conclusão de curso, bem como explorações em sites especializados da internet.

> Determinados o objetivo da pesquisa e a abordagem cientÍfica que irá orientar a investigação, é necessário decidir que método de pesquisa melhor se aplica à condução do estudo. (DRESCH, 2015, p. 16).

Conforme a mesma autora, pode-se

dizer que o artigo em questão está enquadrado conforme os seguintes tipos científicos elencados:

a) quanto à natureza – trata-se de uma pesquisa aplicada a Sistemas de Informação;

b) quanto à forma de abordagem do problema – trata-se de uma pesquisa qualitativa, realizada com o objetivo de levantar o envio e recebimento de dados de voz e texto e a constatação da camada de segurança;

c) quanto aos fins – trata-se de uma pesquisa descritiva, pois busca expor algumas características de segurança em aplicativo de uso generalizado; e

d) quanto aos meios – trata-se de um estudo de caso, pois aprofunda-se na análise da segurança das informações trafegáveis em um ambiente montado e dedicado para tal finalidade.

1.2 INSTRUMENTOS E PROCEDIMENTOS

Para a execução do estudo de caso foi montado um ambiente de testes em que se utilizaram os dispositivos a seguir:

- dois celulares Motorola Moto G 2014 XT 1064 8GB (2ª Geração) (SO Android 5.0.2);
- um notebook Lenovo G40-70 (SO Windows 10); e
- um notebook Dell Inspiron 14 (SO Windows 8.1).

Ambos celulares utilizados nesse estudo possuíam o aplicativo WhatsApp (versão 2.12.539 para Motorola) instalado em seus sistemas. Os notebooks tinham acesso ao WhatsApp Web que é uma variante do mensageiro e que podem ser acessadas por browsers (desde que ocorra uma autenticação por meio de um QR Code). As mensagens enviadas e recebidas são completamente sincronizadas entre o aplicativo de um aparelho celular e o computador, podendo ser vistas em ambos dispositivos.

1.3 ESTUDO DE CASO

Este estudo de caso pretende demonstrar a possibilidade de se duplicar a conta de WhatsApp de um usuário que pertence a uma mesma rede de um falsário. Dessa forma, seria possível a um falsário ter acesso às mensagens e contatos da vítima a partir de outro celular.

De acordo com o método utilizado, se faz necessário a aquisição do endereço MAC (Media Access Control) do telefone do usuário alvo. O MAC é um endereço único, com 12 dígitos hexadecimais que identifica a placa de rede do dispositivo.

Neste teste, os dispositivos (celulares e notebooks) estão ligados a uma mesma rede local e conectados a um modem, o que torna possível o uso de um programa como o Wireshark, que é um analisador de protocolos e que permite a captura e navegação interativa no tráfego de uma rede de computadores em tempo de execução, para esmiuçar a rede e descobrir o endereço MAC do smartphone do usuário alvo.

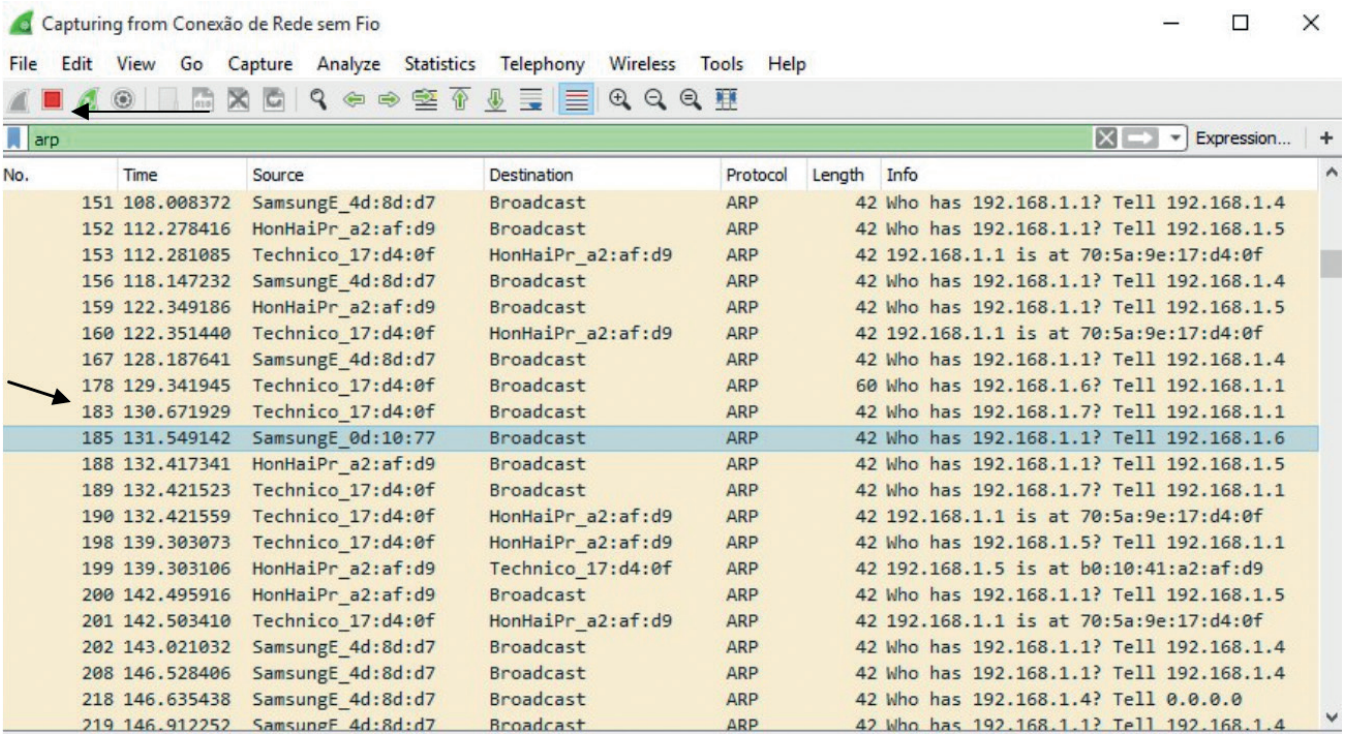
O protocolo ARP (Address Resolution Protocol) permite conhecer o endereço físico de uma placa de rede que corresponde a um endereço IP.

Para fazer a correspondência entre os endereços físicos registrados nas placas de rede pelos fabricantes (MAC) e os endereços lógicos (IP), o protocolo ARP interroga as demais máquinas da rede em busca do endereço físico.

Assim, com a utilização de um filtro, no programa Wireshark, que separe os pacotes por tipo de protocolo (e nesse caso queremos apenas ARP) é possível verificar o tráfego de todos os pacotes desejados. A Figura 2 mostra

o momento em que é realizada a captura.

FIGURA 2 Captura de pacotes de rede com protocolos do tipo ARP.

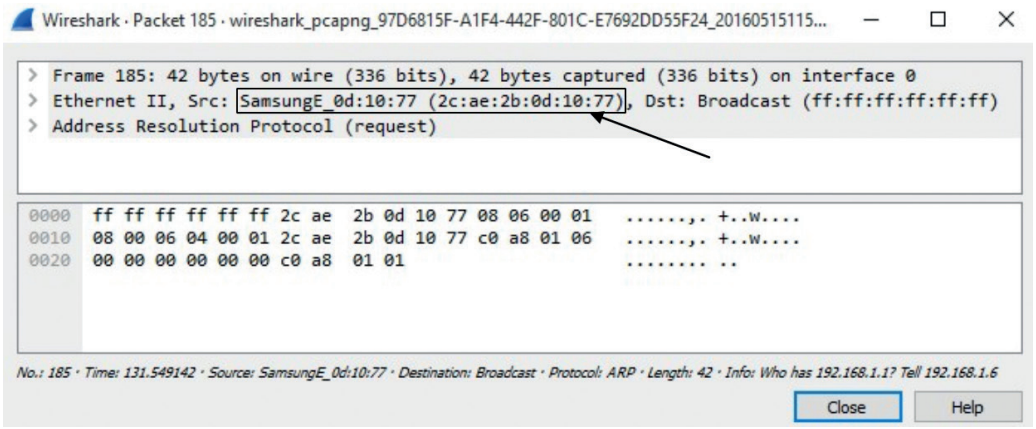


Fonte: o autor, 2016.

A partir da observação dos pacotes identifica-se o dispositivo que se deseja adquirir mais informações, no teste em questão estamos buscando o endereço MAC do dispositivo de rede (um telefone da marca Samsung e cujo número IP é o 192.168.1.6). Ao se identificar o pacote procurado podemos expandir suas informações para adquirirmos seu endereço MAC.

A Figura 3 mostra esse detalhamento.

FIGURA 3 Detalhamento do pacote 185 com descrição do MAC do dispositivo procurado.



Fonte: o autor, 2016.

De posse do endereço MAC da vítima e com acesso root no dispositivo que será utilizado para clonar a conta WhatsApp, se faz a atualização do endereço MAC do aparelho do falsário. Esse passo pode ser executado com o auxílio de um aplicativo que substitua ou mascare o endereço MAC original pelo endereço MAC da vítima.

Neste estudo de caso foi utilizado o software KingRoot para se obter privilégios de superusuário que permitissem a realização do mascaramento do endereço MAC.

Para finalizar a clonagem, reinstala-se o aplicativo WhatsApp no dispositivo do falsário.

Para que a instalação seja concluída é preciso ter em mãos o código de confirmação enviado por mensagem SMS. Importa ressaltar que o código é enviado para o aparelho que possui o chip correspondente ao número de telefone vinculado à conta do WhatsApp que se deseja clonar, neste caso ao celular da vítima.

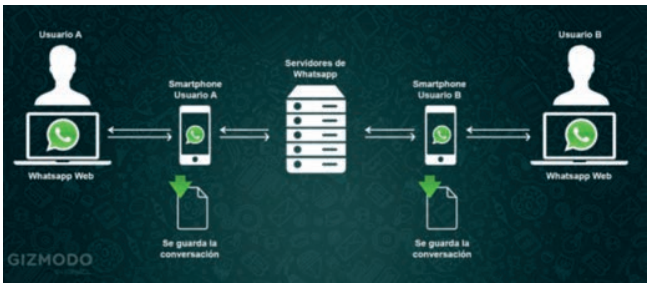
2 RESULTADOS E DISCUSSÕES

Com base em Anglano C. (2014), os serviços de mensagens instantâneas são cada vez mais usados, não só para atividades legítimas, mas também para ilícitas.

O WhatsApp é um aplicativo multiplataforma e possibilita a troca de mensagens entre diferentes dispositivos (celulares, tablets, notebooks etc.) e entre os mais variados sistemas operacionais, tais como Android, Windows, BlackBerry, iOS e outros.

A figura 4 exibe sua arquitetura de funcionamento.

FIGURA 4 Arquitetura de funcionamento do WhatsApp



Fonte: Gizmodo, 2015.

O WhatsApp, por ser líder de mercado, evidentemente torna-se alvo de cibercriminosos, logo, estudos voltados para a área de segurança da informação conjugados ao aplicativo citado fazem-se necessários.

De acordo com Goodrich et al (2013), tradicionalmente, a segurança da informação está relacionada com os seguintes atributos: confidencialidade, integridade, disponibilidade e autenticidade. É com base nestes atributos que estruturou-se a discussão construída nesta seção a partir dos resultados do estudo de caso.

Na seção 2 deste artigo, evidenciou-se a possibilidade da revelação não autorizada de dados contidos em conversas da conta clonada. Tal situação, indubitavelmente prejudica a confidencialidade na comunicação da vítima com seus contatos.

Al-Saadawi & Varol (2017) explicam que em redes IP, os dados são digitalizados e transmitidos em formato de pacotes. Tais pacotes são roteados baseados em alguns protocolos. No laboratório, a aquisição do endereço MAC do dispositivo alvo pôde ser efetuada porque o atacante estava conectado à mesma rede da vítima. Assim, o atacante de posse de um software analisador de rede pôde verificar todo o trâfego de pacotes.

> Um usuário com acesso a um terminal local pode tentar a intrusão sem usar uma rede intermediária. (...) Assim, a violação de sistemas é uma área na qual as preocupações relativas à segurança de rede e à segurança de computadores se sobrepõem. (STALLINGS, 2008).

No estudo de caso realizado, o atacante era parte da lista de usuários habilitados. Assim, podia “escutar” a rede. Tal situação, mesmo induzida (por ocasião da montagem do cenário do laboratório) traz à tona a importância da implementação do controle de acesso em redes privadas.

> O controle de acesso é a capacidade de limitar e dominar o acesso aos sistemas e aplicações por meio de links de comunicação. Para conseguir isso, cada entidade que tenta obter acesso precisa primeiro ser identificada, ou autenticada, de modo que os direitos de acessos possam ser ajustados ao indíviduo. (STALLINGS, 2008).

No caso de redes públicas totalmente abertas, a intecerptação de dados por cibercriminosos é ainda mais facilitada, motivo pelo qual especialistas recomendam a não utilização destes tipos de conexões para a execução de procedimentos críticos que envolvam informações sensíveis. Em redes privadas, o controle de acesso poderá ser mais uma ação

para mitigar adesões de usuários mal-intencionados.

O estudo de caso revelou, na versão estudada do aplicativo mensageiro, uma carência de atenção quanto à autenticação e autorização.

Para se completar a instalação e para se confirmar a identidade, a administração do WhatsApp encaminhava um token (enviado por SMS) que após ser digitado em campo específico habilitava o usuário a utilizar o aplicativo. Esse conjunto de procedimentos demonstrou-se pouco adequado para impedir que atacantes consiguissem o token, até porque, conforme preceituam Krombholz et al (2013), cibercriminosos têm lançado mão de ataques cada vez mais sofisticados, inclusive com o uso de engenharia social.

A despeito disso, versões posteriores do WhatsApp passaram a implementar verificação em duas etapas, com envio do token para o e-mail e com o cadastro de uma senha como “recurso opcional” para situações em que os usuários necessitem instalar o programa novamente.

Importa ressaltar que o laboratório fora realizado em ambiente isolado e que a metodologia de duplicação de conta descrita neste artigo talvez não seja bem-sucedida ao ser aplicada em aparelhos pertencentes a redes diferentes.

Hoje, existem diversos métodos para se conseguir endereços MAC de maneira não-autorizada. Como preceitua Mota Filho (2013), a análise de tráfego em redes TCP/IP permite entre outras possibilidades: monitorar relevantes mensagens de sistema não reveladas pelas aplicações, bem como instruir-se sobre o funcionamento de protocolos e serviços pela observação. O software Wireshark utilizado no estudo de caso possibilitou realizar a análise dos dados que trafegavam na rede. Filtrando-se o protocolo ARP, o atacante conseguiu, sem muita dificuldade, importantes informações como o endereço IP e o endereço MAC do dispositivo alvo.

Também é perfeitamente possível duplicar os endereços físicos das placas de rede. A utilização de aplicativos é uma das formas de se chegar a esse objetivo conforme ficou demonstrado no estudo. Existem inclusive dispositivos piratas que vêm de fábrica com a numeração de suas placas de rede já duplicadas.

Por ocasião da execução do estudo de caso, o dispositivo (do falsário) utilizado para se alterar o número MAC e para se clonar a conta do WhatsApp apresentou problemas em seu sistema operacional quando foi reinicializado, provavelmente em função de conflitos quanto ao reconhecimento do MAC modificado, o que exigiu a reconfiguração de fábrica para restabelecer as funcionalidades do aparelho celular.

Outro aspecto da segurança da informação comprometido foi a integridade dos dados. No profile clonado foi possível interferir em conversas de forma não autorizada.

Por fim, quanto à disponibilidade do serviço, este funcionou por todo o período dos testes. Não houveram tentativas de tirá-lo do ar.

CONCLUSÃO

Com mais de um bilhão de usuários ativos (informação essa divulgada em fevereiro de 2016 pela própria empresa), o WhatsApp bem como outros serviços de mensagem tende a contar por muito tempo ainda com índices elevados de popularidade e adesão aos seus serviços.

Toda essa notoriedade acaba por tornar o aplicativo de mensagens um grande atrativo para pessoas mal-intencionadas e organizações criminosas que enxergam no elevado número de usuários possibilidades infinitas para o cometimento de crimes.

Por mais que as empresas desenvolvedoras invistam pesado na criação e aperfeiçoamento de metodologias para mitigação de riscos, o aumento no nível de segurança não necessariamente garante a segurança total dos sistemas.

Não é por acaso que quase diariamente são veiculados noticiários e divulgações de novas vulnerabilidades, malwares, ameaças e brechas.

O WhatsApp é um aplicativo de mensagens multiplataforma, que tem um modelo negocial de baixo ou nenhum custo para seus usuários, apresenta relativa facilidade de uso e possui um enorme tráfego de dados entre os milhares de dispositivos que fazem uso de seus serviços. Por tudo isso tal tipo de programa apresenta-se como um relevante objeto de pesquisas.

O presente artigo foi realizado com a intenção de estudar e testar a aplicação e identificar possíveis falhas de segurança.

Para ajudar a subsidiar o escrito foi produzido um estudo teórico a respeito de voz sobre IP e segurança da computação.

O estudo de caso, descrito neste artigo, contemplou a análise de tráfego de dispositivos de uma mesma rede, onde foi possível capturar, com o auxílio de uma ferramenta de inspeção de pacotes, o número físico da placa de rede de um dos dispositivos.

Em seguida foi utilizado um software para rotear um aparelho de telefone e outro aplicativo para mascarar o endereço MAC. A partir daí foi possível instalar o WhatsApp de outro aparelho de telefone e ter acesso às informações de outro usuário.

Conclui-se que ainda é inteiramente possível fazer uso de técnicas para contornar a autenticidade dos usuários quando da instalação do aplicativo de mensageria WhatsApp. Além do mais, a partir do acesso à conta se pode consultar e enviar mensagens atacando também os princípios da privacidade e integridade de dados.

Por fim, destaca-se a importância de se aplicar sempre novas camadas de segurança em aparelhos e aplicativos com o objetivo contínuo de se incrementar possibilidades de segurança ao acesso de redes, aparelhos e softwares.

Sugere-se o estudo de metodologias de segurança e proteção aplicados a serviços e aplicativos de troca de mensagens.

Sugere-se também um Estudo de Caso que verifique a viabilidade de aquisição de endereço MAC e a duplicação de uma mesma conta do WhatsApp em dispositivos que pertençam a redes diferentes. Uma pesquisa sobre a eficiência de aplicativos e implementações que oferecem proteção e bloqueio a mensageiros e comunicadores instantâneos através de PIN e senhas também poderia ser de grande pertinência.

SECURITY ANALYSIS ON INSTANT MESSAGING APPLICATION: WHATSAPP AS CASE STUDY

Abstract. The leakage of information from the US National Security Agency (NSA) by one of its analysts, Edward Snowden, in 2013, brought to the forefront multiple information on surveillance and monitoring programs for digital communications managed by the agency and which had large partners providers. This event, which had a major impact on the international community, further instigated precautions by communications security managers and specialists, especially regarding the need to strengthen data protection practices in the large network. Given this context, due to the popularization of messaging tools and the increase of voice traffic under IP on mobile devices, a research on the security aspects involved in this type of service, as well as a case study carried out on WhatsApp (focusing on data traffic and breaking privacy and authenticity) could result in important knowledge to be shared and disseminated to the vast number of end-users of the tool, as well as scholars in the area of Security and Forensic Skills. Thus, the proposed technical article referred to the operation of voice over IP communications, covering the main methods of encryption and information security attributes. For the accomplishment of the empirical study an exploratory research was carried out, based on the applied research, the bibliographic revision, the known protocols on the subject and a case study followed by the respective analysis and conclusion.

Keyword: Communication Security. VoIP. Computational Forensics. Traffic Analysis. Instant Messaging Application.

REFERÊNCIAS

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO 27.002/2005 – Tecnologia da Informação – **Técnicas de Segurança – Código de prática para a gestão de segurança da informação**. Rio de Janeiro, ABNT, 2004.

AL-SAADAWI, Hussein; VAROL, Asaf. **Voice over IP forensic approaches: A review**. Conference: 2017 5th International Symposium on Digital Forensic and Security. Romenia, 2017, DOI: 10.1109/ISDFS.2017.7916507

ANGLANO C, **Forensic analysis of WhatsApp Messenger on Android smartphones**, Digital Investigation, 2014, http://dx.doi.org/10.1016/j.diin.2014.04.003

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança**: o guia oficial RSA. Rio de Janeiro: Elsevier, 2002.

CARUSO, Carlos A. A; STEFFEN, Flávio D. **Segurança em informática e de informações**. 3ª ed. São Paulo: Editora Senac São Paulo, 2006.

DRESCH, Aline; LACERDA, Daniel P.; JUNIOR, José J.A.V.A. **Design Science Research – Método de pesquisa para avanço ciência e tecnologia**. Porto Alegre: Editora Bookman, 2015.

GOODRICH, Michael. T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

KROMBHOLZ, Katharina & Hobel, HEIDELINDE & Huber, MARKUS & Weippl, Edgar. **Social engineering attacks on the knowledge worker**. - Proceedings of the 6th International Conference on Security of Information and Networks, 2013. 10.1145/2523514.2523596

MOTA FILHO, João Eriberto. **Análise de tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. São Paulo: Novatec Editora, 2013.

STALLINGS, William. **Criptografia e segurança de redes**. São Paulo: Pearson Prentice Hall, 2008.

Antonio Marcos de Castro Mota é graduado em Ciência da Computação (2008), pós-graduado em Perícia Digital (2016), ambas, junto à Universidade Católica de Brasília (UCB). Atualmente, trabalha na Divisão de Controle de Produtos Químicos, unidade integrante do Departamento de Polícia Federal, órgão em que ocupa cargo efetivo de Agente Administrativo e pode ser contactado pelo email antonio.amcm@dpf.gov.br.

Paulo Roberto Corrêa Leão é formado pela Academia Militar das Agulhas Negras (1977), pós-graduado em análise de sistemas, supervisão escolar, gestão estratégica da informação e mestrado em Gestão do Conhecimento e da Tecnologia da Informação, pela Universidade Católica de Brasília (2004). Atualmente está cursando o doutorado em Educação na Universidade Católica de Brasília(UCB).