RBTI – Revista Brasileira em Tecnologia da Informação
Volume 06, Número 02 – 2024
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

Segurança da informação em smartphones: uma análise sobre escalonamento de permissões em Sistema Android

Roseline Machaca
roseline.machaca@fatec.sp.gov.br
Deborah Eduarda Azevedo Sousa
deborah.sousa@fatec.sp.gov.br
Fabio Codo
fabio.codo@fatec.sp.gov.br

RESUMO

O presente artigo tem por objetivo explicar como as permissões funcionam nos dispositivos ANDROID tendo como base estudos teóricos e documentações oficiais disponíveis ao público. Como aplicativos podem explorar as vulnerabilidades do sistema, obtendo permissões de terceiros e acesso a dados restritos do usuário. Buscando mostrar formas que aplicativos terceiros conseguem se aproveitar da vulnerabilidade no sistema, além disso demonstrar como melhores práticas de instalação são essenciais para a segurança do dispositivo.

Palavras-Chave: Android OS; Backdoor; Phishing; Rootkits; Segurança da informação.

Artigo Submetido: 16/04/2023

Artigo Aceito Publicação: 01/08/2024

Information security in smartphones: an analysis on scaling permissions in android system

ABSTRACT

Often, the users themselves are the device's main vulnerabilities. When the individual does not have a general knowledge of the attacks that have occurred on the network, he can end up providing permissions giving access to private data and control of the device itself to third parties. In view of this problem, the article was designed to explain, based on theoretical studies, how permissions work. It seeks to show ways that third parties can take advantage of vulnerabilities in the system, in addition to demonstrating how best installation practices are essential for device security.

Keywords: Android OS; Backdoor; Information Security; Phishing; Rootkits.

1 Introdução

Em plena era da comunicação e junto com as tecnologias emergentes, percebemos o aumento da notoriedade dos smartphones. Aplicativos especializados no roubo de informações por escalonamento de permissões, podem ter acesso à lista de contatos restritos, fotos e vídeos pessoais ou comprometedores, dentre outros dados sensíveis.

Em comparação com outros sistemas (como IOS ou Windows), os dispositivos móveis que usam o sistema operacional ANDROID são amplamente ameaçados por aplicativos maliciosos. Isso pode ser devido à sua popularidade e ao aumento na gama de aplicativos de fontes não confiáveis disponíveis para esta plataforma. Por um lado, uma variedade de aplicativos atrai novos usuários e, por outro lado, torna-os mais suscetíveis a aplicativos de fontes não verificadas.

Segundo S. Alsoghyer and I. Almomani (2020, p. 94): “Muitos sistemas de detecção de ransomware ANDROID foram desenvolvidos na literatura como tentativas de prevenir o ransomwares de serem instalados nos dispositivos e sistemas ANDROID dos usuários”. Porém, sendo habitual o uso de permissões que habitualmente são ignoradas pelos usuários na instalação de seus apps, representando uma possível via de acesso à malwares vindouros.

Sendo este ataque atrativo pela quantidade e tipo de informações armazenadas e popularidade de aplicativos de terceiros. É fundamental a gerência de permissões em smartphones, para assegurar a integridade das informações pessoais de cada usuário ANDROID.

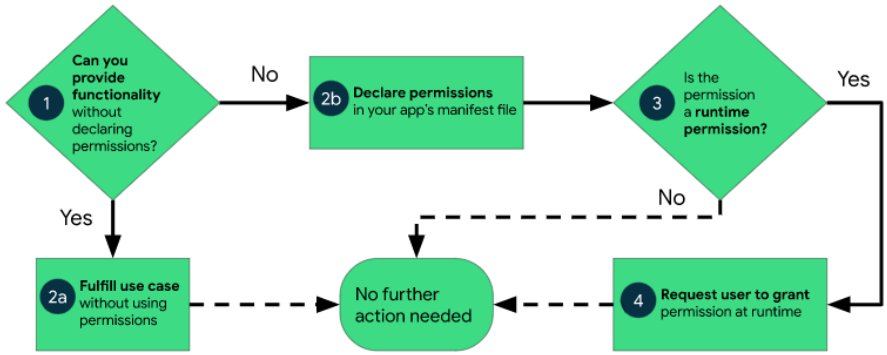
Neste artigo, busca-se demonstrar as principais funções do ataque de escalonamento em smartphones e o controle de permissão em dispositivos móveis com o sistema operacional ANDROID, para evitar que aplicativos maliciosos explorem as permissões de terceiros. Além disso, como as melhores práticas ao instalar aplicativos móveis reduzem o risco de ser vítima de roubo de dados por desenvolvedores mal-intencionados.

2 Referencial teórico

2.1. Sistema Android – Análise da metodologia de segurança aplicada aos aplicativos instalados

A segurança da informação no sistema ANDROID apoia-se principalmente na separação de tipos de acessos e permissões envolvidas. Os tipos de acesso são: acesso a dados restritos e acesso a ações restritas. Dados restritos dizem respeito ao estado do sistema e contatos do usuário, ações restritas dizem respeito por exemplo à gravação de áudio ou pareamento a outros dispositivos. Os aplicativos podem ou não necessitar do acesso a dados ou ações restritas e seu uso depende das permissões adquiridas. A figura 1 demonstra o fluxo de trabalho de permissões. Atualmente os tipos de permissões são: permissão em tempo de instalação, permissões de execução e permissões especiais que serão detalhadas nos tópicos seguintes.

Figura 1 - Diagrama do fluxo de trabalho de permissões.



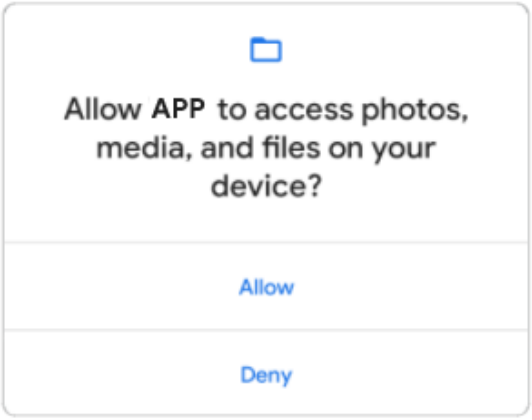
Fonte: Alsoghyer; Almomani (2020)

Permissão em tempo de instalação definem permissões de acesso limitado aos dados restritos e a ações restritas que concernem minimamente o sistema. A permissão em tempo de instalação possui duas sub permissões: as normais e as de assinatura. Permissões normais permitem o acesso aos dados e ações que apresentam pouco risco à privacidade do usuário e à operação de outros aplicativos. Permissões de assinatura baseia-se em certificado que por sua vez pode ser compartilhado por outros aplicativos e seu funcionamento depende de sua assinatura no momento da instalação.

Permissão de execução dão acesso adicional aos dados e ações restritas, trata-se do tipo de permissão considerado o mais crítico. Por este motivo, é necessário solicitar permissão de execução, sendo normalmente apresentado ao usuário uma tela de

solicitação de permissão. Em sua maioria, permissões de execução acessam dados particulares um tipo especial de dado restrito que inclui informações potencialmente confidenciais. Como exemplo: contatos e localização. A figura 2 apresenta um exemplo de tela solicitando permissão de acesso em tempo de execução.

Figura 2 - Exemplo de solicitação de acesso aos dados de fotos, mídia e arquivos do dispositivo em tempo de execução de um aplicativo fictício APP.



Fonte: Elaboração própria

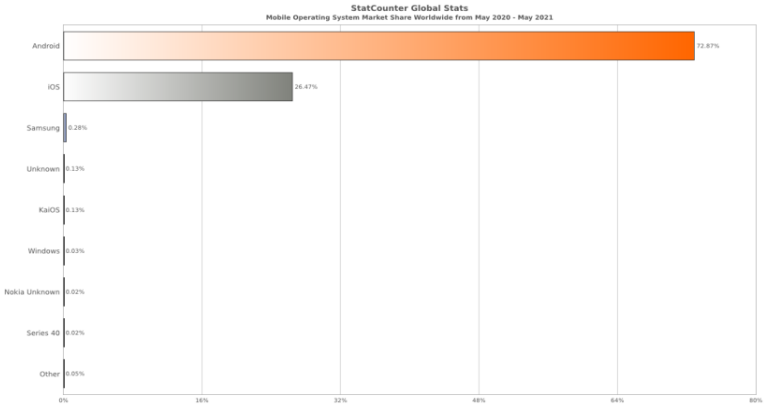
Permissões especiais são permissões que correspondem a operações específicas. Somente a plataforma e os OEMs (OEM - Sigla para "*Original Equipment Manufacturer*" que, em tradução livre, significa "Fabricante Original de Equipamento") podem definir permissões especiais. Geralmente definem permissões especiais quando querem proteger o acesso a ações especialmente poderosas, como sobrepor outros aplicativos.

3 Android – Popularidade vs Segurança

Segundo a StatCounter GlobalStats [4] na pesquisa de participação no mercado de sistemas operacionais móveis em todo o mundo (maio de 2020 a maio de 2021), o ANDROID está em primeiro lugar com 72,72% do total, sendo seus concorrentes: IOS 26,47%, Samsung 0,4%, KaiOS 0,17%, Desconhecido 0,15% e Nokia Desconhecido 0,02%, como mostra a figura 3.

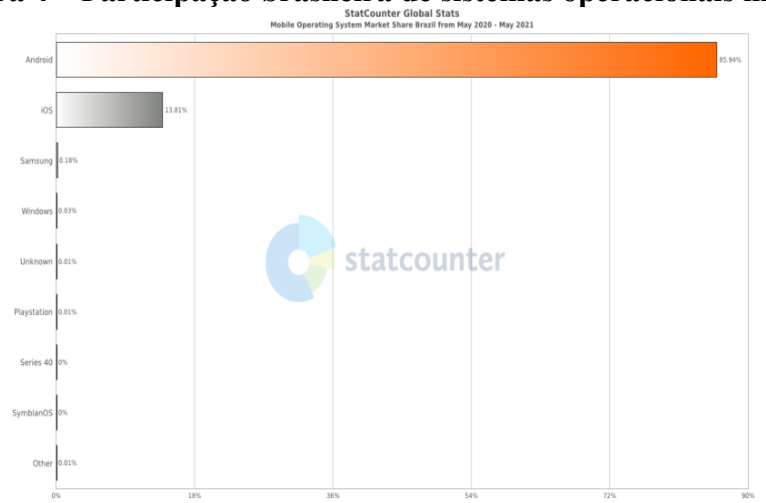
Mudando de localidade, sendo agora para pesquisa de participação no mercado de sistemas operacionais móveis em todo o Brasil (maio de 2020 a maio de 2021) [3] a popularidade do ANDROID sobe para 86,9% a do IOS desce para 12,82%, Samsung 0,23%, Windows aparece na pesquisa com 0,02%, desconhecido 0,01 e Série 40 0,01, como mostra a figura 4.

Figura 3 – Participação mundial de sistemas operacionais móveis



Fonte: Elaboração própria

Figura 4 – Participação brasileira de sistemas operacionais móveis



Fonte: Elaboração própria

A popularidade do ANDROID é refletida pela sua acessibilidade, dispositivos que operam o sistema tendem a possuir compatibilidade com recursos essenciais diversos, tais como por exemplo carregadores, fones de ouvido ao se tratar de hardware e aplicativos oficiais e não oficiais ao se tratar de softwares.

O ANDROID pertence a GOOGLE e conta com Google Play Protect que verifica todos os aplicativos recebendo atualizações de segurança periódicas [2], porém apesar de existirem diversas formas de manter um dispositivo ANDROID seguro contra ameaças à segurança da informação [1], diversos usuários não sabem como utilizá-las ou simplesmente as ignoram, fazendo do usuário o maior risco a segurança do sistema.

4 Ataque de escalonamento de permissões

Os métodos que usamos para implementar políticas de autorização (controle de acesso, privilégios ou permissões do usuário) são projetados para proteger informações confidenciais de visualização, compartilhamento, modificação ou exclusão não autorizados. Essas estratégias também podem impedir que aplicativos não autorizados sejam executados no dispositivo.

O indivíduo que tenta apoderar-se de informação no mundo tecnológico é conhecido como hacker, segundo Mitnick e Simon (2003, p.6) “a mente do hacker é orientada para encontrar maneiras de burlar as poderosas salvaguardas da tecnologia da segurança." Sendo assim toda tentativa de subtração da informação de forma não autorizada, é considerado um ataque.

Espiões maliciosos, criminosos ou partes envolvidas em espionagem cibernética (seja por motivos econômicos, sociopolíticos ou notórios) são tentados a contornar as estratégias de autorização para obter dados sensíveis ou confidenciais. Esses invasores geralmente começam comprometendo contas de usuários. Eles também podem procurar vulnerabilidades que podem ser usadas para controlar computadores ou aplicativos.

Para Sêmola (2014, p.45) ameaças " São agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades". Essas vulnerabilidades podem ser um grande risco de uma determinada ameaça utilizar dessas vulnerabilidades para realizar um ataque à segurança da informação.

Por meio desses ataques iniciais, o invasor obterá certos direitos de acesso. Em seguida, o invasor investigará gradualmente o sistema infectado para obter mais privilégios do que aquele que possuía originalmente, para poder acessar informações confidenciais de outras contas e até obter controle administrativo total sobre o sistema. Quando um invasor expande seu acesso não autorizado original dessa maneira, esse método é chamado de ataque de escalonamento de privilégios.

O escalonamento de privilégios Vertical ocorre quando o usuário ou processo é capaz de obter um nível de acesso mais alto do que o pretendido por um administrador ou desenvolvedor de sistemas. Esse acesso pode permitir que os usuários alterem as

configurações do sistema, criem usuários, autorizem atividades e se envolvam em uma ampla variedade de outros danos.

O escalonamento de privilégios horizontal ocorre quando um aplicativo permite que o invasor obtenha acesso a recursos que normalmente estariam protegidos de um aplicativo ou usuário. O invasor tenta assumir os direitos e privilégios de outro usuário que tem os mesmos privilégios que a conta atual. O resultado é que o aplicativo executa ações com o mesmo usuário, mas com contexto de segurança diferente do pretendido pelo desenvolvedor do aplicativo ou administrador do sistema. Depois de ter acesso a um sistema e obter privilégios suficientes, é hora de comprometer o sistema e realizar o ataque. O invasor executa diferentes aplicativos em um sistema com objetivos específicos em mente.

Aplicações do tipo Backdoors são projetadas para comprometer o sistema de tal forma que permita o acesso posterior.

> Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo. Após incluído, o backdoor é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado. A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. (CERT.BR,2015).

Uma das formas de ataque são os RootKits que são um pacote de software criado para permanecer oculto no seu computador enquanto fornece controle e acesso remotos.

> Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os rootkits atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.” (CERT.BR, 2015).

Os Rootkits controlam o dispositivo sem o conhecimento ou consentimento do usuário. (“Root” significa Raiz que se refere à conta administrativa em um dispositivo) Como essa conta pode acessar tudo no dispositivo e possui todos os privilégios de usuário, ela tem o maior nível de controle no sistema (“kit” é a forma que esse acesso raiz é desbloqueado) O cibercriminoso cria um kit de software que concede privilégios na raiz do sistema de destino.

Permissões invasivas podem servir de phishing para infectar o dispositivo com malwares, ou o desenvolvedor por trás do aplicativo pode lucrar com o uso de adwares, esses ataques podem vir em aplicativos falsos disponíveis na Google Play Store. O Phishing é uma forma de golpe em que um atacante tenta, de forma fraudulenta, adquirir informações de uma vítima personificando uma entidade em que esta confia, (Jagatic et al. 2007).

FluBot é um malware instalado no aparelho por meio de mensagens de texto afirmando ser de uma empresa de entrega, que pede aos usuários para clicar em um link com o intuito de rastrear a entrega do pacote, uma vez que o link em questão redireciona o usuário para uma página que faz o download de um aplicativo que se passa por uma ferramenta de rastreio de entregas. Mas que na realidade é um Phishing usado para roubar informações de smartphones com ANDROID.

5 Metodologia

Para a realização desta pesquisa, a metodologia aplicada consiste no embasamento teórico, e através deste método será gerado dados com base em nosso objetivo para explicar como funciona e exemplos de como evitar, para que o usuário possa identificar e relatar roubo de dados, e se é verificado a segurança de tais aplicativos antes de utilizar em seus dispositivos móveis.

Foi realizada uma análise aprofundada dos artigos selecionados, buscando mostrar a importância e a relação do tema proposto, identificando e separando aspectos por tópicos para apresentar cenários do conceito abordado.

Com isso foi utilizado entre 5 a 10 artigos científicos exemplificando a maneira de como a segurança em smartphones é vista por meio dos usuários, e através desses artigos foram gerados informações e dados que mostram o comportamento dos usuários com a segurança no smartphone.

Considerações finais

Devido ao aumento dos casos referente a segurança da informação através de aplicativos maliciosos, isso nos mostra o quanto isso é necessário ser revisado e averiguado, criar modalidades para evitar tais tipos de erros dentro do mundo virtual. Com a tecnologia em expansão é possível relatar algumas soluções, e ter como base a pesquisa para verificar quais novos métodos podem ser utilizados para futuramente serem implementados.

Contudo, quanto mais procuramos informações para resolver o problema da segurança, são encontradas mais questões para serem resolvidas, então podemos dizer que estamos em constante evolução e nada é impossível para solucionar problemas. Portanto esta pesquisa foi gerada para auxiliar aqueles que buscam conhecimento da segurança em smartphones e identificar quais pontos podem ser melhorados de acordo com dados que foram gerados através dos usuários.

REFERÊNCIAS

ALSOGHYER, S.; ALMOMANI, I. On the Effectiveness of Application Permissions for Android Ransomware Detection. In: **CONFERENCE ON DATA SCIENCE AND MACHINE LEARNING APPLICATIONS (CDMA)**, 6., 2020, Riyadh, Saudi Arabia. **Anais [...]**. Riyadh, Saudi Arabia: IEEE, 2020. p. 94-99. DOI: 10.1109/CDMA47397.2020.00022.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). **Cartilha de Segurança para Internet**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://www.cert.br/docs/whitepapers/ddos/. Acesso em: 17 maio 2021.

DALLAS, T. **13 Must-Know Tips for Keeping Your Phone Secure**. [S. l.]: Android Gadget Hacks, [2017]. Disponível em: https://android.gadgethacks.com/how-to/android-security-13-must-know-tips-for-keeping-your-phone-secure-0162723/. Acesso em: 11 out. 2017.

JAGATIC, Tom N. et al. Social phishing. **Communications of the ACM**, v. 50, n. 10, p. 94-100, 2007.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar**. São Paulo: Pearson Education, 2003.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva**. 2. ed. São Paulo: Elsevier, 2014.

SEU smartphone fica protegido com a segurança integrada. [S. l.]: Android, [2021]. Disponível em: https://www.android.com/intl/pt-BR_br/what-is-android/. Acesso em: 6 jun. 2021.

STATCOUNTER. **Participação de mercado do sistema operacional móvel em todo o mundo**. [S. l.], [2021]. Disponível em: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202005-202105-bar. Acesso em: 6 jun. 2021.

STATCOUNTER. **Participação de mercado do sistema operacional móvel no Brasil**. [S. l.], [2021]. Disponível em: https://gs.statcounter.com/os-market-share/mobile/brazil/#monthly-202005-202105-bar. Acesso em: 6 jun. 2021.