Uma análise dos certificados digitais usados na assinatura de aplicação Android

Jonata Fröhlich[1], **Claudia Angelita Fagundes Raupp**[1], **Luciano Ignaczak**[1]

[1]Universidade do Vale do Rio dos Sinos(UNISINOS)
Av. Unisinos, 950 – 93.022-000 – São Leopoldo – RS – Brasil

jonatafrohlich@gmail.com,{rauppcaf,lignaczak}@unisinos.br

Abstract. *The number of Android platform users is growing every day, and the number of available applications grows in similar proportion. Currently, each application installed on the Android platform must be digitally signed, but there is no control of the safety criteria used in used certificates, leaving to the developer himself the task of selecting information and characteristics of the certificate. This paper analyzed security characteristics of 397 digital certificates used for application signing on Android platform and demonstrated that the validity periods are very long, reaching like thousands of years. The results also shows that are differences between data inserted in the digital certificates and registered in the searched virtual store.*

Resumo. *O número de usuários da plataforma Android cresce a cada dia e o número de aplicativos disponíveis cresce em proporção semelhante. Atualmente, cada aplicativo instalado na plataforma Android deve ser assinado digitalmente, porém não existe um controle dos critérios de segurança nos certificados digitais utilizados, deixando para o próprio desenvolvedor a tarefa de selecionar as informações e características do certificado. Este artigo analisou características de segurança de 397 certificados digitais utilizados na assinatura de aplicativos da plataforma Android e demonstrou que os prazos de validade são muitos longos, chegando a alcançar milhares de anos. Os resultados também apresentam que existem diferenças entre os dados inseridos nos certificados digitais e o cadastrados na loja virtual pesquisada.*

1. Introdução

Os smartphones deixaram de ser um dispositivo de comunicação e tornaram-se um componente essencial na vida de muitas pessoas em todo mundo. É isso que a pesquisa do IDC (International Data Corporation) publicada em fevereiro desse ano apresenta. Segundo o IDC, no ano de 2013 foram comercializados mais de 1 bilhão de dispositivos em todo mundo, o que equivale a um aumento de 39,2% quando comparado com o ano de 2012. Segundo a mesma pesquisa do IDC o sistema operacional mais utilizado em smartphones é o sistema Android com 78,6%[IDC 2014]. Com o expressivo aumento dos dispositivos móveis, o número de aplicativos para o sistema operacional Android cresce na mesma ordem. No mês de maio de 2013 eram 782.038 aplicativos disponíveis para *download* na loja oficial do Google Play. Já no mês de maio de 2014, esse número passou para 1.229.672 aplicativos, um aumento de 57,24% de aplicativos[APPBrain 2014].

A fim de garantir a segurança, durante o processo de instalação de um aplicativo algumas verificações são efetuadas. Entra elas podemos destacar a *Update Integrity*,

que efetua uma verificação quanto a integridade do aplicativo, ou seja, é verificado se não houve nenhuma modificação desde que o código foi assinado pelo seu desenvolvedor. Em seguida o Android decidirá se a instalação se trata de um novo aplicativo ou somente uma atualização. Caso seja uma atualização é feita uma comparação da assinatura digital do aplicativo já instalado com a nova versão. Esse processo garante que somente o desenvolvedor legítimo do aplicativo seja capaz de lançar novas versões do aplicativo[Barrera et al. 2012].

A assinatura digital deve possibilitar que os usuários consigam verificar a autoria de um aplicativo, através da sua associação com o certificado digital. Nesse sentido, a plataforma Android obriga os desenvolvedores a assinar digitalmente os aplicativos antes de disponibilizá-los aos usuários. No entanto, a plataforma Android possibilita que o desenvolvedor utilize certificados auto-assinados na criação da assinatura digital[Gunasekera 2012]. Ao atribuir a tarefa de emissão de um certificado digital ao desenvolvedor, o Android possibilita que ele selecione as informações e características do certificado digital emitido, o que pode resultar no comprometimento da segurança provida pela assinatura digital.

Este artigo tem como objetivo realizar uma análise dos certificados digitais usados na assinatura de aplicações para plataforma Android. Para alcançar o objetivo foi efetuado o *download* de 397 aplicativos da loja Google Play e foi realizado a extração do certificado digital de cada aplicativo. A análise envolveu cinco características dos certificados digitais que podem comprometer a sua segurança ou a credibilidade da assinatura de código.

O restante do artigo está dividido em quatro seções. Na segunda seção são apresentados trabalhos publicados recentemente que discutem a utilização do uso de certificados digitais em aplicativos Android, problemas no modelo atual e outras pesquisas estatísticas relacionadas. A terceira seção apresenta a metodologia. Na quarta seção os autores discorrem sobre os resultados obtidos com a análise dos certificados digitais. Por fim, os autores apresentam suas considerações finais.

2. Trabalhos Relacionados

A segurança proporcionada pelo uso de assinaturas digitais baseadas em certificados digitais como busca de credibilidade vem sendo discutida em diversos trabalhos. No artigo [Barrera and van Oorschot 2011] é apresentado que o desenvolvedor é responsável em efetuar a assinatura de código, sem nenhum envolvimento da loja virtual. Na mesma publicação é abordado que a assinatura digital é utilizada somente em atualizações , uma vez que não existe processo de verificação do desenvolvedor na primeira instalação. No trabalho de [Vargas et al. 2012] os autores apresentam os controles de segurança adotados pelo Android, entre eles é citado a utilização de certificados digitais para a assinatura de código, porém é apresentado que o certificado digital não precisa ser emitido por um autoridade de certificação confiável, ou seja, o próprio desenvolvedor emiti o certificado, o que é chamado de certificado auto assinado.

Mesmo utilizando certificados digitais para assinar digitalmente os aplicativos Android, os trabalhos atuais mostram que o modelo atual possui algumas fragilidades. No trabalho [Barrera et al. 2012] os autores citam que o Android tem uma abordagem de confiança no primeiro uso, ou seja, o desenvolvedor não é autenticado na primeira instalação, autenticando somente o desenvolvedor caso ocorra uma atualização, com isso

caso algum aplicativo seja modificado por um usuário mal intencionado, o sistema operacional identificará e não será possível realizar a instalação, porém caso o usuário mal intencionado assine a aplicação com outro certificado será possível realizar a instalação novamente, pois será considerada uma nova instalação. No trabalho publicado por [Zheng et al. 2014] os autores apresentam uma análise dos vários *firmware* que são baseados em Android e alerta para a possibilidade dessas versões possuírem vulnerabilidades. O autores citam uma vulnerabilidade, *Master Key*, que o usuário mal intencionado explora a falta de verificação de nomes duplicados nas entradas dos arquivos .apk e então são criados dois arquivos com o mesmo nome, contornando a verificação de assinatura realizada durante o processo de instalação e atualização de um aplicativo.

Atualmente estão sendo desenvolvidas diversas análises estatísticas quanto ao uso de aplicativos na plataforma Android. Em [Fahl et al. 2012] é realizada uma análise de 13.500 aplicativos gratuitos mais populares do Google Play procurando identificar vulnerabilidades que permitam ataques *Man-in-the-Middle* e foi identificado que 8% dos aplicativos examinados estavam potencialmente vulnerável. No trabalho de [Enck et al. 2011] foi analisados o código fonte de 1.100 aplicativos gratuitos mais populares da loja virtual do Google. A análise descobriu o uso generalizado e indevido de identificadores pessoais do telefone, porém não foram encontradas vulnerabilidades exploráveis de *malware* nas aplicações estudadas.

Embora os trabalhos apresentados realizem análises de vulnerabilidades associadas aos aplicativos da plataforma Android, os trabalhos não analisam as características e os dados inseridos no certificado digital utilizado na assinatura do aplicativo. A inclusão de dados de forma indiscriminada e o uso de certificados auto assinados podem comprometer a credibilidade do aplicativo. A contribuição deste trabalho é avaliar características de cinco campos dos certificados digitais usados na assinatura de aplicativo e analisar seu impacto na credibilidade do aplicativo.

3. Metodologia

A primeira etapa do trabalho consistiu em definir os critérios de análise dos certificados digitais, para isso foi selecionada uma amostra inicial de certificados digitais usados na assinatura de aplicações Android. A partir disso foi realizada uma análise dos valores atribuídos aos campos da estrutura x.509 que poderiam resultar na perda de credibilidade da aplicação. Com base nesta amostra foram selecionados os seguintes critérios para análise: 1) Prazo de validade: Análise do tempo, em anos, que o certificado permanecerá válido; 2) Tamanho da chave: Analisado qual o tamanho da chave pública; 3) Possibilidade de revogação do certificado: Analisado se o certificado possuía alguma informação que possibilite a consulta do seu *status* de revogação; 4) Auto assinado: Verificado se o certificado é auto assinado ou emitido por um autoridade certificadora; e 5)Dados do Titular: Nesse campo foram verificados se o Common Name (CN) e/ou o campo Organization (O), presentes no campo Nome do titular, são condizentes com o nome do desenvolvedor publicado na loja virtual do Google Play.

Na segunda etapa, foi definido o tamanho da amostra de certificados digitais analisados. Para isso foi definido um nível de confiança de 95% e com margem de erro de 5 pontos percentuais. Para atingir os critérios acima foi necessário uma amostra de 385 certificados digitais. Para seleção dos aplicativos da amostra, os autores usaram como

critério o *ranking* dos aplicativos gratuitos mais populares na Google Play. A partir disso foi extraída uma listagem com 410 aplicativos gratuitos mais populares.

A etapa seguinte, consistiu em coletar os certificados digitais das aplicações que fizeram parte da amostra. Para isso, inicialmente foi realizado o *download* dos aplicativos listados na etapa anterior. Os aplicativos listados, foram baixados em um dispositivo Android que foram instalados. Após a instalação foi efetuado o *backup* do aplicativo para que fosse possível ter o aplicativo em extensão .apk. De posse dos aplicativos na extensão .apk, eles foram transferidos para um computador e descompactado. Uma vez possuindo os arquivos descompactados, foi necessário o uso do OpenSSL para extrair o certificado digital. Nessa etapa foram descartados 13 aplicativos devido a impossibilidade de efetuar o *download* por não estarem mais disponíveis na loja virtual.

Na quarta etapa foi realizada a análise e tabulação dos dados coletados. Para isso foi gerado uma planilha com os 397 aplicativos foi preenchida com os dados conforme realizada a analise individual dos certificados digitais. Por fim a última etapa consistiu em realizar uma análise dos resultados obtidos. Para isso foi realizado uma análise de modo quantitativo onde foram efetuados cálculos de porcentagem, cruzamento de informações e médias afim de identificar o impacto na credibilidade dos aplicativos.

4. Resultados

Nesta seção é realizada a discussão dos resultados obtidos a partir da análise dos 397 certificados digitais. A discussão foi dividida em subseções que abordam as diferentes análises realizadas. Em cada subseção, após a análise dos dados, os autores apresentam algumas consequências das características presentes nos certificados digitais.

4.1. Análise do Prazo de Validade e Comprimento da Chave

A primeira análise levou em consideração duas variáveis: o período de validade e o comprimento da chave. Inicialmente, foi realizada uma análise isolada do período de validade, com o objetivo de conhecer o tempo de duração dos certificados digitais usados em assinatura aplicativos na plataforma Android. Para essa análise os autores definiram três intervalos de tempo de validade: até 50 anos; entre 51 e 100 anos; e acima de 100 anos. Posteriormente, foram utilizados testes t para diferença entre duas médias, com amostras independentes, para verificar se há diferença significativa no comprimento das chaves públicas dos certificados digitais nos três intervalos de tempo definidos. A Tabela 1 apresenta os resultados desta análise.

Tabela 1. Prazo de validade x Tamanho de chave pública

Prazo de Validade	Certificados	% do total	Intervalo de confiança	Comprimento médio da chave	σ
1 -50	235	59,2	54,4 - 64,0	1.436,26	624,55
51- 100	105	26,4	22,1 - 30,8	1.149,59	337,52
Mais de 100	57	14,4	10,9 - 17,8	1.611,85	785,72

A análise constatou que 235 (59,2% do total) certificados digitais dos aplicativos possuem prazo de validade de 50 anos ou menos. Ao considerar um período maior de validade dos certificados digitais, entre 51 e 100 anos, a análise identificou que 105 (26,4%

do total) certificados digitais continham essa característica. Uma terceira verificação identificou certificados digitais com um período de validade superior a 100 anos, onde foram encontrados 57 certificados digitais (14,4% do total).

Com base nesses dados é possível concluir, com 95% de confiança, que entre 54,4% e 64% dos certificados digitais utilizados na assinatura de código de aplicativos possuem um prazo de validade igual ou inferior à 50 anos; entre 22,1% e 30,8% dos certificados digitais têm prazo de validade entre 51 e 100 anos; e, por fim, entre 10,9% e 17,8% dos certificados digitais têm prazo de validade acima de 100 anos.

Ainda sobre os período de validade dos certificados digitais, a análise constatou que apenas um aplicativo foi assinado digitalmente com um certificado digital com tempo de validade inferior a 10 anos. Por outro lado, 28 aplicativos foram assinados com certificados digitais que possuem um período de validade de 999 anos e 16 aplicativos foram assinados com certificados com período de validade de 1000 anos ou superior. O maior tempo de validade encontrado em um certificado digital da amostra foi 2738 anos.

Embora no site do Android, ao apresentar uma estratégia para assinatura de aplicações, recomende o uso de certificados digitais com um período de validade de 25 anos ou mais, garantindo assim a assinatura das atualizações da aplicação durante o seu ciclo de vida [Android 2014], essa característica pode resultar em uma vulnerabilidade no médio ou longo prazo, pois o aumento da capacidade de processamento poderá reduzir a quantidade de tempo necessário para comprometer as chaves do certificado digital.

Ao comparar o comprimento médio da chave pública, os certificados digitais com prazo de validade superior a 100 anos possuem o tamanho médio da chave pública foi de 1611,85, com desvio-padrão de 785,72. Já nos certificados com prazo de validade inferior a 100 anos, o tamanho médio da chave pública foi de 1349,41, com desvio-padrão de 565,67. Ao nível de 5% de significância, pode-se afirmar que essa diferença é significativa, ou seja, aplicativos com validade maior tem, em média, tamanho de chave menor.

O teste realizado no tamanho das chaves demonstra novos elementos que podem resultar em vulnerabilidades na utilização dos certificados digitais usados na assinatura de aplicações Android no médio ou longo prazo. A partir dela é possível conhecer que os certificados digitais emitidos com uma validade maior estão associados a chaves com tamanhos menores. Ou seja, além dos responsáveis pela emissão estenderem significativamente o prazo de validades dos certificados digitais, eles estão usando como base o comprimento mínimo das chaves consideradas seguras na atualidade.

4.2. Comparação dos dados dos Certificados Digitais com informações da loja

Uma segunda análise comparou os dados contidos no certificado digital do desenvolvedor usado na assinatura de aplicativos com os dados cadastrados por ele na Google Play. Esta análise levou em consideração a identificação do desenvolvedor do aplicativo, apresentada pela Google Play no momento do *download*, em relação a duas informações do certificado digital que deveriam estar associadas a ela: o nome e a organização requerente. Nesta análise foram considerados apenas os certificados digitais que continham nome ou organização do requerente, pois muitos não possuíam tais dados. Por isso, o número de certificados digitais das análises distingue do tamanho da amostra

Na amostra de aplicativos analisados, um total de 94 (23,7%) possuem o nome do

requerente do certificado digital relacionado ao nome da empresa divulgada na loja virtual e 249 (62,7%) certificados digitais, o nome do requerente não está relacionado. Por fim, em 54 (13,6%) certificados digitais não consta a informação do nome do requerente. Com base nesses dados é possível concluir, com 95% de confiança, que entre 57,9% e 67,5% do aplicativos são assinados com certificados digitais que não possuem o nome do requerente relacionado ao nome da empresa divulgada na loja virtual.

Na amostra de aplicativos, em 211 (53,1%) o nome da organização do requerente do certificado digital está relacionado ao nome da empresa divulgada na loja virtual e em 145 (36,5%), o nome não está relacionado ao nome da empresa divulgada na loja virtual. Além disso, 41 (10,3%) certificados digitais não possuem a informação da organização do requerente. Com base nesses dados pode-se concluir, com 95% de confiança, que entre 31,8% e 41,2% dos aplicativos são assinados com certificados digitais cujo o nome da organização requerente contida nele não está relacionado ao nome da empresa divulgada na loja virtual.

Em um segundo momento, a análise associou os três intervalos de período de validade dos certificados digitais com a relação existente entre os dados dos requerentes dos certificados digitais e os apresentados na loja virtual Google Play. Para definir se há ou não a existência de associação entre o período de validade do certificado e a relação entre as informações do certificado e da loja virtual foi utilizado o teste qui-quadrado, onde foi considerada uma associação significativa probabilidades superiores a 5%. A Tabela 2 apresenta o resultado desse cruzamento.

Tabela 2. Prazo de validade x Nome do requerente

Prazo de Validade (Anos)	Associação entre dados do certificado e loja virtual			
	Possui relação entre nome do requerente e site		Possui relação entre organização do requerente e site	
	Sim	Não	Sim	Não
1-50	59 (29,8%)	139 (70,2%)	132 (62,9%)	78 (37,1%)
50-100	20 (21,5%)	73 (78,5%)	51 (52,6%)	46 (47,4%)
>100	15 (28,8%)	37 (71,2%)	28 (57,1%)	21 (42,9%)

Ao analisar os certificados digitais que não possuem o nome do requerente relacionado ao nome da empresa divulgada na loja virtual, foram identificados 136 (67,7%) certificados com validade entre 1 e 50 anos, 74 (78,7%) certificados digitais entre 50 e 100 anos e 35 (72,9%) certificados digitais com mais de 100 anos. A partir desses dados não foi possível perceber uma associação significativa entre prazo de validade e o nome do requerente contido nele estar relacionado ao nome da empresa divulgada na loja virtual.

Ao analisar os certificados digitais que não possuem o nome da organização requerente relacionado ao nome da empresa divulgada na loja virtual, foram identificados 76 (36,7%) certificados com validade entre 1 e 50 anos, 47 (48%) certificados digitais entre 50 e 100 anos e 19 (41,3%) certificados digitais com mais de 100 anos. A partir desses dados não foi possível perceber uma associação significativa entre o prazo de validade e o nome da organização requerente contido nele estar relacionado ao nome da empresa divulgada na loja virtual

A partir dessas análises é possível concluir que não há um cuidado em relacionar

as informações do certificado digital usado na assinatura das aplicações Android com os dados cadastrados na loja virtual. A partir disso é possível concluir que a assinatura de código na plataforma Android não está cumprindo o seu papel de atribuir credibilidade às aplicações, pois o usuário não consegue relacionar os dados da identidade usada na assinatura com a empresa ou desenvolvedor responsável por ela.

4.3. Dados de Revogação e modelo de confiança

A análise do item Dados de Revogação levou em consideração se o certificado utilizado na assinatura do aplicativo continha alguma informação de revogação do mesmo. A análise verificou se o certificado possuía um link que possibilitasse a revogação, independentemente do protocolo utilizado. Para realizar a análise do modelo de confiança foi verificado se o certificado utilizado na assinatura digital era auto assinado. A análise constatou que nenhum dos certificados analisados possuía algum dado que possibilitasse a revogação de um certificado utilizado para a assinatura de aplicações da plataforma Android. Essa característica pode ser considerada uma vulnerabilidade de segurança, pois caso algum desses certificados seja comprometido, não será possível verificar a sua revogação.

Para efetuar a análise do modelo de confiança foi verificado o nome do requerente do certificado e o nome do emissor do certificado. Se ambos os nomes fossem iguais o certificado era auto assinado. A análise constatou que todos os certificados eram auto assinados, ou seja todos os certificados utilizados para a assinatura de código foram emitidos pelos próprios desenvolvedores comprometendo a segurança proporcionada pela assinatura digital.

5. Considerações Finais

O presente artigo realizou uma análise de 397 certificados digitais utilizados na assinatura digital dos aplicativos gratuitos mais populares do Google Play. Após a análise foi possível constatar que os certificados digitais possuem prazos de validade muito longos, como, por exemplo o fato de 44 certificados possuírem o período de validade de 999 anos ou mais. Quando comparado a validade dos certificados digitais com o tamanho da chave constatou-se que quanto maior o prazo de validade menor o tamanho da chave, ou seja, além dos responsáveis pela emissão estenderem significativamente a validade dos certificados digitais, eles estão usando como base o comprimento mínimo das chaves consideradas seguras na atualidade.

Quando comparado os dados dos certificados digitais com informações da loja, constatou-se que não existe um cuidado por parte dos desenvolvedores em relacionar as informações contidas no certificado digital com as informações cadastradas na loja virtual, pois verificou-se que somente 23,7 % dos certificados analisados possuem o nome do requerente do certificado digital relacionado ao nome divulgado na loja virtual e que 53,1% possuem o nome da organização requerente do certificado digital relacionado ao nome divulgado na loja virtual. Portanto pode-se concluir que a assinatura de código na plataforma Android não está cumprindo o seu papel, que é atribuir credibilidade às aplicações, pois o usuário não consegue relacionar os dados entre o certificado digital e as informações divulgadas na loja virtual.

Por fim foi identificado que nenhum dos certificados utilizados para assinatura de aplicativos da plataforma Android possuía dados de revogação. É possível afirmar

que essa característica pode ser considerada uma vulnerabilidade no modelo de confiança adotado pela plataforma Android, pois caso um desenvolvedor tenha a segurança do seu certificado digital comprometida, ele não possui meios de tornar o certificado inválido.

Novas análises poderão ser iniciadas a partir dos resultados desta pesquisa, pois ainda é escasso o número de trabalhos que analisam o uso de certificados digitais nas plataformas em uso em dispositivos móveis. Como trabalho futuro é sugerida a análise dos certificados digitais usados em assinatura de aplicações em outras plataformas ou é possível realizar a análise de aplicativos de segmentos específicos na plataforma Android, como, por exemplo, aplicativos corporativos. Além disso pode-se sugerir um novo modelo de confiança para o uso de assinatura para aplicativos de plataforma Android.

Referências

Android, D. (2014). Signing Your Applications. http://developer.android.com/tools/publishing/app-signing.html. Acessado em 2014-07-15.

APPBrain (2014). APPBrain,Number of Android applications. http://www.appbrain.com/stats/number-of-android-apps. Acessado em 2014-05-29.

Barrera, D., Clark, J., McCarney, D., and van Oorschot, P. C. (2012). Understanding and improving app installation security mechanisms through empirical analysis of android. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '12, pages 81–92, New York, NY, USA. ACM.

Barrera, D. and van Oorschot, P. (2011). Secure Software Installation on Smartphones. *Security & Privacy Magazine*, 9(3):42–48.

Enck, W., Octeau, D., McDaniel, P., and Chaudhuri, S. (2011). A study of android application security. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 21–21, Berkeley, CA, USA. USENIX Association.

Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B., and Smith, M. (2012). Why eve and mallory love android: An analysis of android ssl (in)security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 50–61, New York, NY, USA. ACM.

Gunasekera, S. (2012). *Android Apps Security*. Apress, Berkely, CA, USA, 1st edition.

IDC (2014). Android and iOS Continue to Dominate the Worldwide Smartphone Market with Android Shipments Just Shy of 800 Million in 2013, According to IDC. http://www.idc.com/getdoc.jsp?containerId=prUS24676414. Acessado em 2014-05-29.

Vargas, R., Huerta, R., Anaya, E., and Hernandez, A. (2012). Security controls for android. In *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on*, pages 212–216.

Zheng, M., Sun, M., and Lui, J. C. (2014). Droidray: A security evaluation system for customized android firmwares. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pages 471–482, New York, NY, USA. ACM.