

Universidade de Brasília - UnB
Faculdade UnB Gama - FGA
Engenharia de *Software*

Identificação de Exceções de Segurança e Vulnerabilidades em Certificados Digitais Utilizados em Portais e Páginas da Internet

Autor: Yuri Moraes Mota
Orientador: Prof. Dr. Edson Alves da Costa Júnior

Brasília, DF
2015



Yuri Moraes Mota

**Identificação de Exceções de Segurança e
Vulnerabilidades em Certificados Digitais Utilizados em
Portais e Páginas da Internet**

Monografia submetida ao curso de graduação em Engenharia de *Software* da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de *Software*.

Universidade de Brasília - UnB

Faculdade UnB Gama - FGA

Orientador: Prof. Dr. Edson Alves da Costa Júnior

Brasília, DF

2015

Yuri Moraes Mota

Identificação de Exceções de Segurança e Vulnerabilidades em Certificados Digitais Utilizados em Portais e Páginas da Internet/ Yuri Moraes Mota. – Brasília, DF, 2015-

62 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Edson Alves da Costa Júnior

Trabalho de Conclusão de Curso – Universidade de Brasília - UnB
Faculdade UnB Gama - FGA , 2015.

1. Certificados Digitais. 2. Exceções de Segurança. I. Prof. Dr. Edson Alves da Costa Júnior. II. Universidade de Brasília. III. Faculdade UnB Gama. IV. Identificação de Exceções de Segurança e Vulnerabilidades em Certificados Digitais Utilizados em Portais e Páginas da Internet

CDU 02:141:005.6

Yuri Moraes Mota

Identificação de Exceções de Segurança e Vulnerabilidades em Certificados Digitais Utilizados em Portais e Páginas da Internet

Monografia submetida ao curso de graduação em Engenharia de *Software* da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de *Software*.

Trabalho aprovado. Brasília, DF, 09 de julho de 2015:

Prof. Dr. Edson Alves da Costa Júnior
Orientador

Prof. Dr. Fernando William Cruz
Convidado 1

Prof. Dr. Tiago Alves Fonseca
Convidado 2

Brasília, DF
2015

Este trabalho é dedicado a Deus.

Agradecimentos

Agradeço a Deus, por sustentar minha fé e me encher de esperanças quando não parecia haver solução; à minha mãe e irmãs, que me serviram de inspiração de perseverança nos momentos em que nada parecia valer à pena; Agradeço aos meus amigos, que estiveram comigo nos momentos felizes, e me apoiaram nos momentos tristes. Agradeço aos professores, que não desistiram de mim. Agradeço à minha Pequena, que me fez notar que as grandes bênçãos não se prendem a grandes coisas. E finalmente, agradeço ao meu grande amigo, Maddox, eternamente vigilante.

*“Aquele que habita no abrigo do Altíssimo
e descansa à sombra do Todo-Poderoso
Pode dizer ao Senhor:
Tu és o meu refúgio e minha fortaleza,
o meu Deus, em quem confio.”
(Bíblia Sagrada, Salmos 91, 1-2)*

Resumo

O objetivo desse trabalho é avaliar as vulnerabilidades de segurança em decorrentes de problemas em certificados digitais, através da verificação de certificados em uso. Os erros que dão origem às principais vulnerabilidades serão identificados e classificados. Posteriormente serão apontados os possíveis ataques que podem explorar estes erros, evidenciando os principais riscos a que estão expostos os sites que utilizam certificados apresentam tais erros.

Palavras-chaves: Certificação Digital. *Internet*. Verificação de Certificados. Criptografia.

Abstract

The objective of this work is to evaluate the security vulnerabilities due to problems in digital certificates by verifying certificates. The errors that return the main vulnerabilities are identified and classified. Then, it will be appointed the possible attacks that can exploit such errors, highlighting the main risks the sites are exposed to while using certificates that present such errors.

Key-words: Digital Certification. Internet Security. Certificate Verification. Cryptography.

Lista de ilustrações

Figura 1 – Processo de Cifração e Decifração	26
Figura 2 – Processo de Cifração e Decifração com Chave Privada	27
Figura 3 – Processo de Cifração em Chave Pública	27
Figura 4 – Processo de Decifração em Chave Pública	28
Figura 5 – Processo de Cifração do DEA (CRYPTO, 2005)	28
Figura 6 – Certificado de Chave Pública em Uso (STALLINGS, 2011, p. 430)	31
Figura 7 – Certificado X.509 (STALLINGS, 2011, p. 431)	32
Figura 8 – Árvore Simplificada de Autoridades Certificadoras Brasileiras (ITI, 2015)	33
Figura 9 – Taxa de Ocorrência dos Erros	51
Figura 10 – Taxa de Erros Relativos	52

Lista de tabelas

Tabela 1 – Tabela de Componentes de Hardware	35
Tabela 2 – Tabela de Softwares Utilizados	35
Tabela 3 – Tabela de Comandos <i>OpenSSL</i> na Verificação	44

Lista de abreviaturas e siglas

AC	Autoridade Certificadora
ASN.1	<i>Abstract Syntax Notation One</i>
Cipher	Algoritmo de Cifração
OpenSSL	<i>Open Source Toolkit para SSL e TLS</i>
PKCS	<i>Public-Key Cryptography Standards</i> (Padrões de Criptografia de Chave Privada)
RSA	Algoritmo de Criptografia de Dados inventado por R. Rivest, A. Shamir, e L. Adleman
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>

Sumário

1	INTRODUÇÃO	23
1.1	Objetivo Geral	23
1.2	Objetivos Específicos	23
1.3	Metodologia	23
1.4	Organização do Trabalho	24
2	FUNDAMENTAÇÃO TEÓRICA	25
2.1	Criptografia e Protocolos	25
2.2	Algoritmos e Chaves	27
2.3	Certificados Digitais	30
3	METODOLOGIA	35
3.1	Ferramentas	35
3.2	Aquisição dos Certificados	35
3.3	Verificação dos Certificados	44
4	RESULTADOS	51
4.1	Sem Erro	51
4.2	Erro 02 - Unable to get issuer Certificate	52
4.3	Erro 10 - Certificate has Expired	53
4.4	Erro 18 - Self Signed Certificate	53
4.5	Erro 20 - Unable to get Local Issuer Certificate	54
5	CONCLUSÃO	55
	Referências	57
	ANEXOS	59
	ANEXO A – TABELA DE RETORNOS DO VERIFY DA OPENSSEL	61

1 Introdução

Certificados digitais são uma forma comum, atualmente, de comprovar a identidade de pessoas, físicas ou jurídicas, em meios digitais. Essa ferramenta de identificação precisa ser robusta, do contrário colocaria em dúvida a confiabilidade do sistema de identificação digital, entretanto, essas falhas existem e dificilmente são tratadas com a devida importância. Para garantir a segurança dos usuários de certificação digital, é necessário expor e identificar tais falhas.

Pela da exposição das falhas mais comuns entre os certificados digitais avaliados, nesse estudo, realiza-se uma análise acerca de quais fatores levam a essas falhas, se elas podem ser sanadas, e quais as principais implicações ocasionadas pela ocorrência das mesmas.

1.1 Objetivo Geral

Este trabalho se foca na identificação, por amostragem em sites que utilizam certificação digital, de quais são as principais vulnerabilidades de segurança causadas por certificados digitais que apresentam erros, utilizados em ambiente real.

1.2 Objetivos Específicos

Por estes mesmos meios, se busca:

- Conhecer as estruturas internas dos certificados digitais utilizados em ambiente real;
- Elucidar formas de contornar exceções de segurança causadas por problemas em certificados digitais.

1.3 Metodologia

Dentro do padrão X.509, os tipos de erros serão divididos em grupos para que a análise esclareça quais as formas pelas quais esses erros podem se apresentar, e assim seja possível entender a origem e razão de tais erros. Todos os grupos de erros serão originários, e baseados, dos erros encontrados pela verificação realizada com a ferramenta *OpenSSL*, uma ferramenta aberta utilizada para realizar esse tipo de verificação.

1.4 Organização do Trabalho

Na primeira parte deste trabalho, é apresentada uma introdução à teoria envolvida na criptografia, tendo como foco as razões pelas quais ela se faz necessária, os tipos de ameaças digitais conhecidas, e as medidas tomadas para contornar esses problemas.

Uma vez que esses detalhes estão esclarecidos, será discutida a forma como a criptografia age para possibilitar a existência, e uso, dos certificados digitais e os algoritmos envolvidos em sua aplicação.

Essa informação servirá para descrever as características que permeiam os certificados digitais, e que permitem que eles sejam considerados como seguros em um ambiente real de aplicação, onde eles devem carregar informações suficientes para atestar a identidade de um indivíduo, ou grupo, em meio digital.

2 Fundamentação Teórica

Neste capítulo a principal meta é inteirar o leitor sobre a importância do uso e da qualidade de certificados digitais, de forma correta. Inicialmente serão apresentados detalhes sobre o que é comunicação segura, e a criptografia. Em seguida, serão abordados e apresentados os detalhes da criptografia, tanto simétrica quanto assimétrica. Por fim, serão discutidos certificados digitais e sua importância, assim como seu uso.

2.1 Criptografia e Protocolos

No contexto da computação, as redes de computadores têm se tornado cada vez maiores, esperasse um trânsito elevado de informações, e o uso dessas redes de computadores para a troca de informações é esperado.

Nesse quadro, dois indivíduos pretendem trocar informações e desejam trocar suas mensagens de forma segura, eles desejam confidencialidade. Para esse fim, eles podem escolher utilizar a criptografia. A criptografia em si, possui muitos fins:

- **Confidencialidade** - Proteger a informação contida em uma mensagem, de forma que apenas o emissor e o receptor conheçam seu conteúdo.
- **Autenticação** - Dar a possibilidade do receptor identificar a origem de uma mensagem.
- **Integridade** - Permitir que o receptor tenha certeza que aquela mensagem não foi modificada por um terceiro.
- **Não-Repúdio** - Um remetente não deve ser capaz de negar falsamente o envio de uma mensagem.

Os indivíduos de nosso exemplo serão, figurativamente, chamados de A e B , e suas mensagens serão chamadas de m_A e m_B , respectivamente. Chamando a mensagem original, m_A , de **texto plano**, ela pode ser alterada através de *Cifração* para gerar um **texto cifrado**, en_A , e retornará ao seu estado original passando por uma *Decifração* (SCHNEIER, 1996, p. 15), como vemos na Figura 1.

Porém, a comunicação em si pode não estar completamente segura apenas com o uso da criptografia, caso um algoritmo ou chave de Cifração secretos sejam expostos, esses casos caracterizam quebras de segurança (STALLINGS, 2011, p. 399):

- **Quebra Total** - Um indivíduo externo descobriu a *chave* do algoritmo.

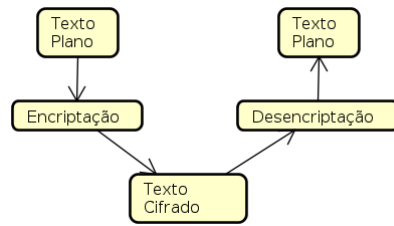


Figura 1 – Processo de Cifração e Decifração

- **Dedução Global** - Um indivíduo externo encontra um algoritmo equivalente, sem conhecer a *chave*.
- **Dedução Seletiva** - Um indivíduo externo consegue acesso ao *texto plano* de um *texto cifrado*.
- **Dedução Existencial** - Um indivíduo externo tem acesso a uma parcela de informação da *chave* ou do *texto plano*.

Para reduzir as chances de possíveis vazamentos de mensagens, é possível seguir protocolos de comunicação, esses *protocolos* se fazem úteis tanto para padronizar a forma como as informações são trocadas quanto para ajudar na interpretação do que está sendo falado pelos envolvidos.

Um **protocolo criptográfico** é aquele protocolo que aplica criptografia (SCHNEIER, 1996, p. 31), como por exemplo o protocolo de comunicação *HTTPS*. Os protocolos ajudam a gerar confiança entre os indivíduos, eles podem exigir uma troca de chaves secretas. Isso pode ser feito para convencer os participantes de que são quem verdadeiramente afirmam. Deve-se ter em mente, também, que o protocolo deve se limitar ao que se propõe em cada caso, para aumentar a segurança dos indivíduos.

A criptografia em si pode ser reforçada por outros métodos que tornariam a troca de mensagens ainda mais segura, é possível então que os indivíduos insiram na sua forma de comunicação um **protocolo**. Um *protocolo* é um processo realizado pelos participantes de uma atividade (no caso a comunicação) para realizar essa atividade, sendo que esse processo apresenta passos bem definidos e que devem ser seguidos (SCHNEIER, 1996).

Como exemplo é possível imaginar dois estranhos se vendo pela primeira vez, imagine que o protocolo social que se segue é cumprimentar as pessoas com um aperto de mão. Caso os dois estranhos se encontrem na rua, e se cumprimentem com um aperto de mãos, eles dirão um ao outro seus respectivos nomes, e iniciarão uma conversa. Caso o aperto de mãos não ocorra, isso seria uma quebra de protocolo, e a comunicação entre eles terminaria ali.

2.2 Algoritmos e Chaves

Existem duas formas mais populares de se tratar com chaves de segurança, mantendo-as em segredo (*chaves secretas*), na **criptografia de chave simétrica**, ou tornando-as acessíveis (*chaves públicas*) em par com *chaves privadas*, na **criptografia de chave assimétrica**. Cada um dos casos apresenta suas próprias vantagens, e desvantagens, sendo possível trabalhar com ambos objetivando uma troca segura de informações.

Nos algoritmos de chave privada, a chave é compartilhada pelos envolvidos na troca de informações. Utilizando de um mesmo algoritmo conhecido, eles irão enviar suas mensagens, e recebê-las, utilizando uma mesma chave secreta para o processo de cifrar e *Decifrar* as informações trocadas, como visto na Figura 2. Na atualidade, é comum que essas chaves privadas sejam monitoradas por **KDCs** (*Key Distribution Centers*), **Centros de Distribuição de Chaves**, afim de arbitrar a distribuição e consenso em relação à chave utilizada em uma troca.

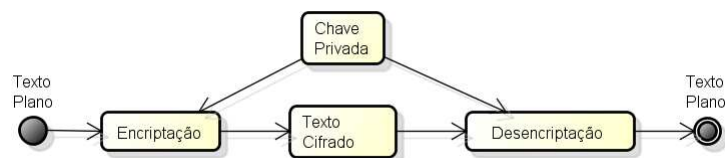


Figura 2 – Processo de Cifração e Decifração com Chave Privada

Já os algoritmos de chave pública seguem uma ideia diferente, existe uma chave conhecida publicamente e uma chave privada, idealmente conhecida apenas pelo usuário. Através da Cifração utilizando a chave pública de um indivíduo, exemplo na Figura 3, os algoritmos de chave assimétrica irão garantir que apenas a chave privada do indivíduo seja capaz de Decifrar a mensagem, visto na Figura 4. Da mesma forma, utilizar a própria chave privada para cifrar um conteúdo irá garantir que apenas a chave pública seja utilizada para Decifrar corretamente aquela mensagem, atestando a origem daquela mensagem.

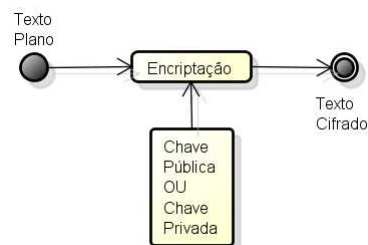


Figura 3 – Processo de Cifração em Chave Pública

Nesse contexto, a Cifração com a própria chave privada serviria como meio de assinar um conteúdo, ainda no contexto da Figura 3, de forma a garantir a autenticidade e a não-repúdio. Em se tratando de uma comunicação que necessite de maior segurança,

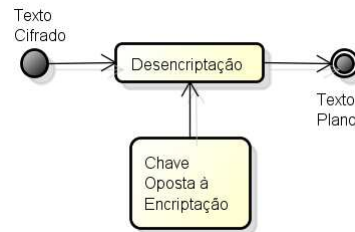


Figura 4 – Processo de Decifração em Chave Pública

é possível empregar mais de uma Cifração, com o objetivo de garantir que um conteúdo seja lido apenas pelo destinatário, e que seja provada a identidade do remetente.

Entretanto, para garantir que essas trocas sejam feitas, e que haja consenso em como cifrar e Decifrar essas informações, é necessário que os algoritmos utilizados no processo sejam conhecidos por ambas as partes. Diferente de algoritmos que se tornam seguros através do segredo do algoritmo em si, algoritmos que utilizam chaves, geralmente, tem sua segurança embasada nas chaves em si, sendo os algoritmos públicos. Historicamente, existem diversos algoritmos de criptografia conhecidos e utilizados, vale citar dois desses algoritmos: o DES e o RSA (STALLINGS, 2011).

Um dos primeiros algoritmos utilizados em larga escala, o DES (Data Encryption Standard) na verdade se trata de um padrão, detentor do algoritmo DEA (Data Encryption Algorithm). Em seu funcionamento, esse algoritmo adota a Função de Feistel, que realiza a Cifração através de quatro estágios. A função-F (como é conhecida a função de Feistel) é repetida diversas vezes dentro do algoritmo, observado na Figura 5, de forma que ao final de diversas repetições será alcançado o texto cifrado.

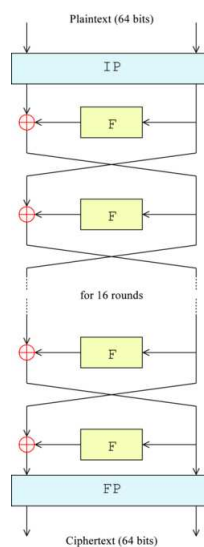


Figura 5 – Processo de Cifração do DEA (CRYPTO, 2005)

Já o RSA, nomeado assim em referência aos seus criadores, é utilizado para a Ci-

fração utilizando chaves assimétricas. Seu funcionamento difere, pois certas formalidades são exigidas para gerar as chaves a serem utilizadas nesse algoritmo. As chaves utilizadas dependem de dois números primos grandes (o que matematicamente diminui as chances de uma quebra de segurança) que irão ser utilizados em sua geração, que se dá de forma que:

1. Dois números primos grandes p e q , são escolhidos;
2. É calculado $n \equiv pq$;
3. Utiliza-se a função- φ onde $n : \varphi(n) \equiv (p - 1)(q - 1)$;
4. É escolhido um valor e (inteiro) maior que 1 e menor que $\varphi(n)$, de forma que e e $\varphi(n)$ sejam primos entre si.
5. Calcula-se d como inverso multiplicativo de e , onde $\text{mod} \varphi(n)$

Assim gerando uma chave pública através do par (e, n) , e uma chave privada do conjunto (p, q, d) ou apenas (d, n) , o segundo caso sendo uma abordagem mais lenta, pois o descriptador não conhece os primos originais. A Cifração e Decifração se dão, respectivamente, pelas fórmulas: (*onde m é o texto plano, e c é o texto cifrado*)

1. $c = m^e \text{ mod } n$
2. $m = c^d \text{ mod } n$

Existem muitos algoritmos de cifração de chave pública, porém a maioria é impraticável por questões de desempenho. É importante notar que a complexidade envolvida nesses algoritmos desse tipo se deve a existência da própria chave pública, pois os procedimentos envolvidos para gerá-la não são simples, nem mais eficientes que algoritmos simétricos (STALLINGS, 2011). Para se trabalhar com esse tipo de sistema, é necessário que o algoritmo e a chave pública não sejam suficientes para descobrir a chave privada (RSA, 1993). Essa mesma capacidade de gerar chaves públicas em par com chaves privadas permite que algoritmos assimétricos gerem um texto cifrado a partir de um texto plano usando uma chave pública, e que a chave privada seja a única capaz de decifrar aquele texto cifrado gerado (RSA, 2012).

Originalmente o que foi proposto por Diffie-Hellman para as aplicações de algoritmos de chave pública permitia apenas a Troca de Chaves, já na abordagem RSA se tornou possível utilizar Assinaturas Digitais (RSA, 2012, p. 12) e esquemas de Cifração/Decifração (RSA, 2012, p. 15); o uso do RSA se tornou difundido pela sua aplicabilidade e a impraticabilidade de ataques por conta do tamanho e administração de suas chaves.

Pela capacidade de gerar novas chaves públicas, e possuir uma chave privada, os algoritmos assimétricos servem aos seguintes propósitos (STALLINGS, 2011, p. 275):

- **Cifração/Decifração** - O remetente pode cifrar uma mensagem com a *chave pública* do receptor.
- **Assinatura Digital** - Um remetente pode assinar uma mensagem com sua *chave privada*. A assinatura pode ser alcançada por métodos diferentes, de acordo com os *protocolos* utilizados.
- **Troca de Chaves** - Duas entidades em conjunto geram uma **chave de sessão**. Assim como na assinatura digital, existem diversas aproximações para que isso seja alcançado.

2.3 Certificados Digitais

No contexto da comunicação segura, a ideia de saber a identidade do outro indivíduo é essencial. Não é desejável que um desconhecido se faça passar pela receptor, ou mesmo pelo emissor, um “*man-in-the-middle*”. Para garantir essa comunicação de um para um, é desejável que sejam apresentadas credenciais que garantam que a mensagem foi transmitida sem desvios, e pelo emissor esperado. Acerca disso, Schneier exemplifica:

“Um certificado público é a chave pública de alguém, assinada por alguém confiável. Certificados são usados para frustrar tentativas de substituir uma chave por outra [879]. O certificado de Bob, numa base de dados de chaves-públicas, possui muito mais que sua chave pública. Ela contém informações sobre Bob -seu nome, endereço, e por aí vai- e é assinado por alguém em quem Alice confia: Trent (comumente conhecido como uma autoridade certificadora, ou AC)...” (SCHNEIER, 1996, p. 163, com adaptações).

Em suma, o que o autor diz é que a forma mais simples de atestar a identidade de uma pessoa é utilizando um **certificado de chave pública**. Pensando numa situação onde aparecem os indivíduos **A**, **B**, e **C**, um certificado apresenta várias informações sobre um *indivíduo A*, e é assinado por um *indivíduo C* externo, para que o *indivíduo B* passe a confiar no *indivíduo A*. Para que esse certificado seja confiável e válido, é necessário que o *indivíduo A* e o *indivíduo B* confiem no *indivíduo C*. No caso o indivíduo C seria então conhecido como uma **Autoridade Certificadora**.

Neste trabalho tratar-se-a um *certificado seguro* como aquele que não apresenta erros, não gerando *vulnerabilidades* no processo de comunicação que esteja sendo realizado. Uma *vulnerabilidade* seria uma possibilidade de interferência ou interceptação nas informações que estejam sendo trocadas pelos indivíduos que se comunicam. Estas *vul-*

nerabilidades podem ser resultados de *exceções*, que seriam certificados aceitos apesar da detecção de erros durante a verificação.

Para que esses certificados possam seguir um padrão, foram criados os **Public-Key Cryptography Standards**, ou *PKCS*, e dentre elas, especificamente a *PKCS #10* (RSA, 2000), cujo objetivo é padronizar os dados contidos em *certificados digitais*, assim como definir quais tipos de informações devem estar contidas em um *certificado digital* e o modelo que deve ser seguido para se requisitar um. O certificado é construído como se observa na Figura 6:

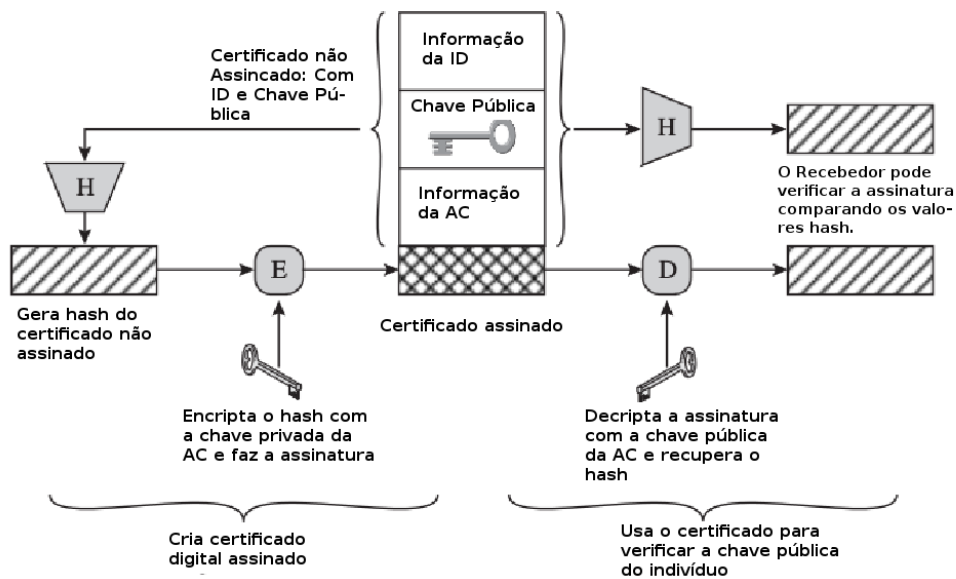


Figura 6 – Certificado de Chave Pública em Uso (STALLINGS, 2011, p. 430)

Esses certificados utilizam o padrão **X.509**. O *X.509* não dita um *cipher* específico, entretanto ele aconselha que seja utilizado o *RSA* para a implementação da *criptografia de chave pública* e das *assinaturas digitais*. Na Figura 7 é possível observar a estrutura de um certificado:

E esses certificados *X.509* podem ainda se mostrar de duas formas, em formato **DER** ou **PEM**. Quando se encontram em codificação *DER* (*Distinguished Encoding Rules*), esses certificados se apresentam em formato binário, legíveis apenas através dos devidos interpretadores por parte da máquina. Por outro lado, os *PEM* (*Privacy Enhanced Mail*) usam codificação **ASCII**, facilitando sua interpretação e leitura, assim como a distinção das informações contidas em seu corpo.

Como já foi dito, a ideia de um certificado é atestar a identidade dos indivíduos envolvidos numa transação de informações. Para isso, pode ser necessário que uma terceira parte se envolva, caso aqueles que se comunicam não conheçam os certificados um do outro de antemão, e esse terceiro envolvido seria uma autoridade certificadora, de confiança mútua entre os envolvidos. Essa terceira entidade, geralmente, conhecida como

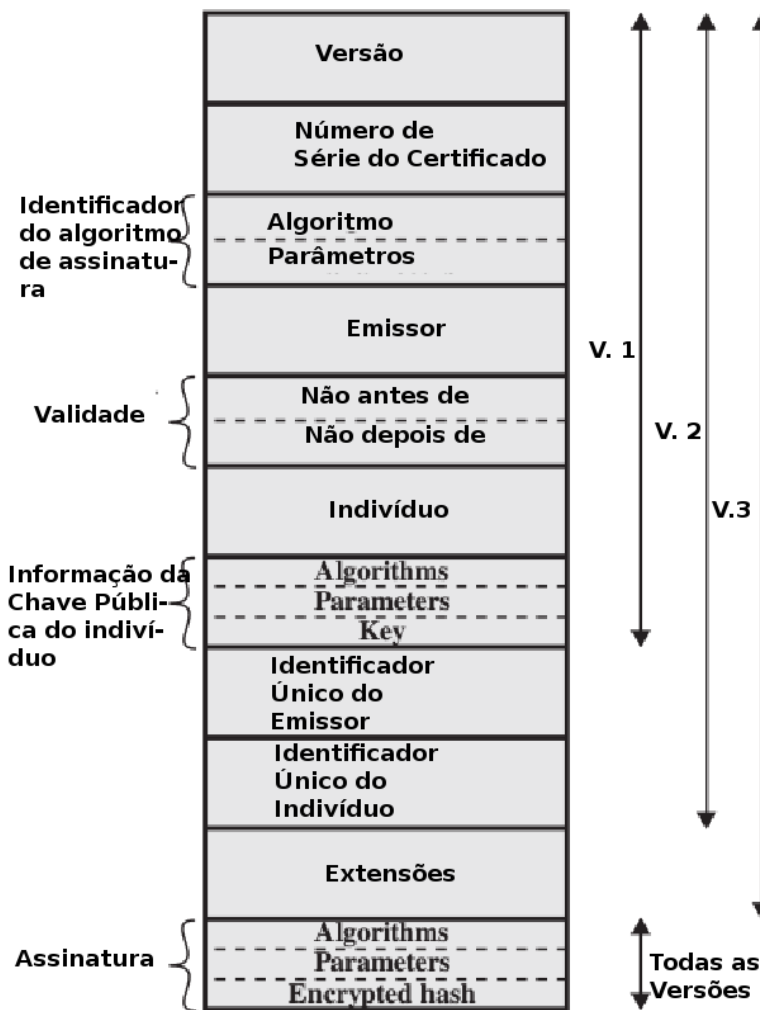


Figura 7 – Certificado X.509 (STALLINGS, 2011, p. 431)

Autoridade Certificadora, é responsável por emitir e assinar os certificados digitais que circulam em determinados domínios. Por exemplo, no domínio brasileiro, temos a **AC Raiz**, como autoridade certificadora raiz, definindo quem pode ser visto como um agente certificador e emitindo certificados para tais indivíduos.

Na figura 8 podemos observar a estrutura simplificada da árvore de certificação brasileira.

Entretanto, esses certificados também podem apresentar erros, ou falhas, e comprometer a confiabilidade da troca de informações por diversos fatores, que podem acarretar em quebras de segurança, esses erros são explicitados através de verificações realizadas por ferramentas de geração e análise de certificados digitais (entre outras funções). No Anexo A vemos os erros identificáveis através da ferramenta **OpenSSL**.

Cada um desses retornos (*com exceção do caso zero*) envolve uma vulnerabilidade de segurança, e se não tratados, certificados que apresentam essas falhas podem

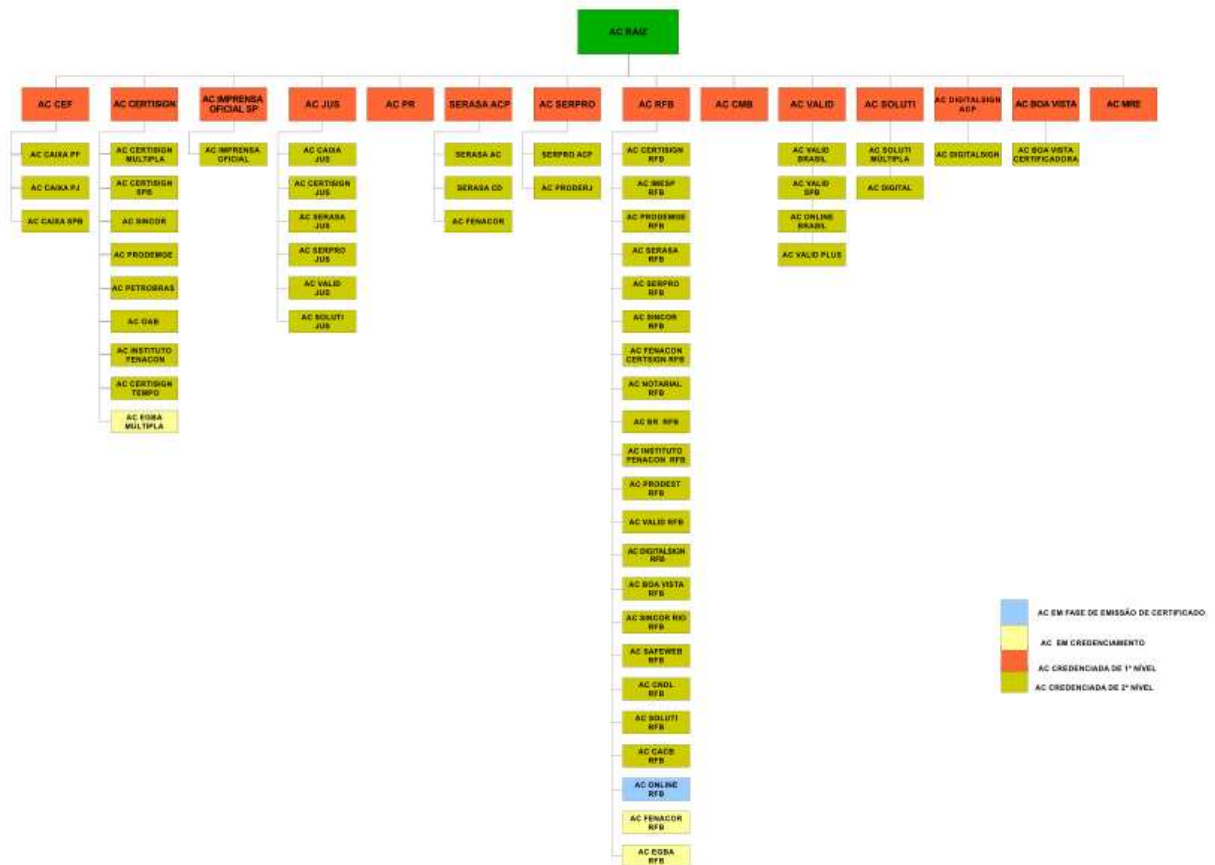


Figura 8 – Árvore Simplificada de Autoridades Certificadoras Brasileiras (ITI, 2015)

representar brechas de segurança. Notemos os Erros 02, 10, 18, 20 e 23.

O retorno **02 - unable to get issuer certificate** caracteriza que um ou mais certificados da cadeia não puderam ser encontrados, ou acessados, e por essa razão, não é possível atestar que aquele certificado foi realmente emitido por aquela autoridade. Se não for possível atestar o emissor de um certificado, não é possível admitir a identidade do indivíduo certificado, abrindo uma brecha na confiabilidade.

Já o retorno **10 - certificate has expired** determina que a data de validade do certificado já expirou, e por essa razão o certificado não deve ser considerado válido em datas posteriores. Isso pode ocorrer para a proteção da chave privada, ou por motivos corporativos. O que importa é que a partir daquela data, não é possível atestar o real portador daquelas informações, a não ser que o certificado seja renovado.

No retorno **18 - self signed certificate** vemos um certificado auto-assinado. Este não é necessariamente um erro, como os outros. Essa situação é comum caso o certificado em questão fosse emitido para uma raiz de certificação. Também é normal encontrar certificados auto-assinados em ambientes como PGP (Pretty Good Privacy), cujo funcionamento se baseia em *redes de confiança*, e nesses casos toda a comunicação segue um padrão de mensagens OpenPGP (CALLAS et al., 2007).

Entretanto, essa situação não deve ocorrer em outros casos, pois não existe uma relação de confiança para atestar a identidade do indivíduo, a não ser que aquele certificado já fosse conhecido. Qualquer um, nesse caso, poderia se passar por outro indivíduo, ou mesmo se passar por uma autoridade certificadora, na falta de referências.

E o retorno **20 - unable to get local issuer certificate** mostra que ao recuperar os certificados, alguns dos certificados de emissores podem não coincidir com o que era esperado, ou não podem ser lidos. Por alguma razão, esses certificados que deveriam ter sido providos/acessados não estão presentes, impedindo que a verificação siga adiante. Nesse caso, se alcança o mesmo impasse visto no **retorno 02**.

O retorno **23 - revoked certificate** constata um certificado revogado, um certificado que, por uma série de razões não deveria mais estar em circulação. Essas razões, sugeridas na RFC 5280 são ([COOPER et al., 2008](#), p. 90):

- Desuso
- Chave Comprometida
- Autoridade Certificadora Comprometida
- Mudança de Afiliação
- Substituído
- Encerramento da Operação
- Certificado Suspenso
- Perda de Privilégios
- Attribute Authority Comprometido

Um certificado não necessariamente precisa estar revogado para que ocorra esse retorno, ele pode estar suspenso em caso de suspeita do acontecimento de alguma outra irregularidade. Para que seja de conhecimento público quais certificados foram revogados, existem as CRLs (*Certificate Revocation Lists*) ([COOPER et al., 2008](#)), que são periodicamente atualizadas pelas autoridades certificadoras.

Uma vulnerabilidade envolvida nesse contexto é a possibilidade de um certificado revogado ser utilizado antes que a informação das CRLs seja atualizada, impossibilitando a identificação do uso indevido deste certificado, colocando a comunicação em risco.

3 Metodologia

Neste capítulo o objetivo é apresentar as ferramentas e métodos que foram adotados com o objetivo de alcançar resultados significativos para o trabalho. Na primeira parte do capítulo serão apresentadas as ferramentas, e as razões pelas quais foram escolhidas certas tecnologias capazes de auxiliar e facilitar o alcance dos resultados. Em seguida, são apresentados os métodos e *Scripts* gerados, de forma a automatizar e auxiliar o processo de análise dos certificados digitais obtidos.

3.1 Ferramentas

Para o desenvolvimento deste trabalho de avaliação dos certificados digitais, foi configurado um ambiente com as seguintes especificações apresentadas nas Tabelas 1 e 2. A conexão com a internet é um pré-requisito para a execução do trabalho, para que seja

Tabela 1 – Tabela de Componentes de Hardware

Componente	<i>Hardware Especificação</i>
Processador	<i>Intel Core i3-3217U 1.8GHz</i>
Memória	<i>4,00 Gb</i>
Placa de Rede	<i>Realtek RTL8139/810x Fast Ethernet Adapter</i>

Tabela 2 – Tabela de Softwares Utilizados

Software	<i>Versão</i>
Sistema Operacional	<i>Ubuntu GNOME 12.04</i>
Python	<i>3.4.3</i>
Java VM	<i>OpenJDK 1.7</i>
<i>OpenSSL</i>	<i>1.0.0</i>
OpenOffice	<i>4.0.0</i>

possível a busca de links, e o download dos certificados digitais utilizados em cada um dos domínios identificados, que empregam o protocolo *HTTPS* em suas vias de acesso.

3.2 Aquisição dos Certificados

Para a coleta dos certificados são utilizadas duas etapas bem definidas:

1. A coleta da URL de *sites* que apresentem o protocolo *HTTPS*;

2. O download dos certificados através de comunicação via porta 443;

Os certificados digitais identificados foram adquiridos através de comunicação com a porta 443, padrão utilizado no protocolo *HTTPS* para a requisição e comunicação de segurança. O processo de handshake foi ignorado durante a aquisição dos certificados, de modo a evitar que certificados que apresentam erros sejam descartados durante a coleta. Esta escolha permitiu que todos os certificados fossem avaliados da mesma forma, posteriormente, pelo *OpenSSL*.

Os passos definidos foram executados através de *Scripts*. Todos os *Scripts* desenvolvidos e/ou utilizados neste trabalho realizam tarefas bem definidas, e devem ser executados na ordem descrita para seu devido funcionamento. O primeiro *Script* a ser executado é apresentado no Código 3.1.

Código 3.1 – FunnyCrawler.java

```
import java.io.IOException;
2 import java.util.HashSet;
import java.util.Set;
4 import java.util.regex.Matcher;
import java.util.regex.Pattern;
6 import org.jsoup.Jsoup;
import org.jsoup.nodes.Document;
8 import org.jsoup.nodes.Element;
import org.jsoup.select.Elements;
10
public class FunnyCrawler {
12
    private static Pattern patternDomainName;
14 private Matcher matcher;
private static final String DOMAIN_NAME_PATTERN
16 = "[a-zA-Z0-9]([a-zA-Z0-9\\-]{0,61}[a-zA-Z0-9])?\\.([a-
    zA-Z]{2,6})";
static {
18     patternDomainName = Pattern.compile(
        DOMAIN_NAME_PATTERN);
}
20
public static void main(String[] args) {
22
    FunnyCrawler obj = new FunnyCrawler();
24     Set<String> result;
```

```
    for(int i = 0; i < 100; i++){
26         result = obj.getDataFromGoogle("+https", i);
           for(String temp : result){
28             System.out.println(temp);
           }
30         System.out.println(result.size());
       }
32     }

34     public String getDomainName(String url){

36         String domainName = "";
           matcher = patternDomainName.matcher(url);
38         if (matcher.find()) {
               domainName = matcher.group(0).toLowerCase().trim
                   ();
40         }
           return domainName;
42     }

44     private Set<String> getDataFromGoogle(String query, int
           number) {

46         Set<String> result = new HashSet<String>();
48         //String request = "https://www.google.com.br/search?
           q=login+%2Bhttps&start=" + number + "0";
           //String request = "https://www.google.com.br/search?
           q=sign+in+%2Bhttps&start=" + number + "0";
50         //String request = "https://www.google.com.br/search?
           q=register+%2Bhttps&start=" + number + "0";
           //String request = "https://www.google.com.br/search?
           q=%2Bhttps&start=" + number + "0";
52         String request = "https://www.google.com.br/search?q=
           buy+%2Bhttps&start=" + number + "0";

54         System.out.println("Sending request... " + request);

56         try {
```

```

58     // need http protocol, set this as a Google bot
        agent :)
Document doc = Jsoup
60     .connect(request)
        .userAgent("Mozilla/5.0 (Macintosh; U;
            Intel Mac OS X 10.4; en-US; rv
            :1.9.2.2) Gecko/20100316 Firefox/3.6.2
            ")
62     .referrer("http://www.google.com")
        .timeout(5000).get();

64

        // get all links
66     Elements links = doc.select("a[href]");
    for (Element link : links) {

68

        String temp = link.attr("href");
70     if(temp.startsWith("/url?q=")){
        //use regex to get domain name
72         result.add(getDomainName(temp));
        }

74

    }

76

    } catch (IOException e) {
78         e.printStackTrace();
    }

80

    return result;
82 }

84 }

```

O Código 3.1 foi escrito a partir de um tutorial da ferramenta JSON, da plataforma Java, disponibilizado na internet (YONG, 2015). Sua função é analisar os resultados de uma pesquisa Google e retornar os links disponibilizados pela mesma na forma de um conjunto (SET). As seguintes strings de busca foram utilizadas:

- "HTTPS://www.google.com.br/search?q=login+%2BHTTPS&start="+ number + "0"

- ```
1;
```
- "HTTPS://www.google.com.br/search?q=sign+in+%2BHTTPS&start="+ number + "0";
  - "HTTPS://www.google.com.br/search?q=register+%2BHTTPS&start="+ number + "0";
  - "HTTPS://www.google.com.br/search?q=%2BHTTPS&start="+ number + "0";
  - "HTTPS://www.google.com.br/search?q=buy%2BHTTPS&start="+ number + "0".

Os retornos, no caso links para resultados das buscas, foram direcionados para um arquivo de texto (UTF-8), onde os links são colocados de forma que cada link ocupa uma única linha do arquivo.

```
“...
www.wpbeginner.com
www.wpwhitesecurity.com
stackoverflow.com
en.support.wordpress.com
security.stackexchange.com
github.com
webcache.googleusercontent.com
...”
```

Utilizando a lista de links que foi organizada, o *Script 3.2* inicia conexões via porta 443 utilizando o *OpenSSL* e recuperando os certificados, quando existentes, salvando localmente uma cópia `.pem` do certificado que foi tocado durante o processo de comunicação.

---

#### Código 3.2 – DOWNLOAD.py

---

```
from subprocess import *
2 from glob import glob
 #coding: utf-8
4
 def download(url):
6 httpsPort = str(url.replace("\n", ":443"))
 resultado = str(url.replace("\n", ".pem"))
8
 comandoCriarArquivo = ['touch', resultado]
10
```

---

<sup>1</sup> O parâmetro “number” é utilizado para a navegação em diferentes páginas, durante a busca.

```

processoCriarArquivo = Popen(comandoCriarArquivo, stdout=
 PIPE)
12 [response, error] = processoCriarArquivo.communicate()
processoCriarArquivo.wait()
14
certificado = open(resultado, 'w')
16
comando_a = ['openssl', 's_client', '-showcerts', '-
 connect', httpsPort]
18 comando_b = ['openssl', 'x509', '-outform', 'PEM']
#openssl s_client -showcerts -connect matriculaweb.unb.br
 :443 | openssl x509 -outform PEM > mycert.pem
20
process_a = Popen(comando_a, stdout=PIPE)
22 process_b = Popen(comando_b, stdin=process_a.stdout,
 stdout=certificado)
[response, error] = process_b.communicate()
24 process_b.wait()
26
certificado.close()
pass
28
if __name__ == '__main__':
30 with open('links.lnk') as f:
 listaDeLinks = f.readlines()
32
 f.close()
34
 for link in listaDeLinks:
36 download(link)

```

Nesse momento, os certificados salvos localmente estão prontos para a análise posterior. Porém, os certificados não são baixados com toda sua cadeia de certificação, em alguns dos casos, e por conta disso o certificado digital do seu emissor, a CA, precisa ser copiado localmente, para evitar falso-positivos entre os resultados.

Para solucionar essa falta, se utiliza o seguinte *Script*.

---

#### Código 3.3 – LOAD\_ROOT.py

---

```

from subprocess import *
2 from glob import glob

```

```
4 def download_root(certificado):
 comando_um = ['openssl', 'x509', '-in', certificado, '-
 text']
6
 process = Popen(comando_um, stdout=PIPE)
8 [response, error] = process.communicate()
 process.wait()
10
 tokens = response.split()
12
 foundIssuers = False
14 foundScore = False
16
 download_link = ""
18
 #procura o link do CA Issuers e joga em download_link
 for token in tokens:
20 if foundIssuers and foundScore:
 download_link = str(token)
22 foundIssuers = False
 if token == 'Issuers':
24 foundIssuers = True
 foundScore = False
26 if token == '-':
 foundScore = True
28
 ##tirando os primeiros quatro caracteres "URI:" e
 impurezas
30 download_link = download_link[4:]
 #download_link = download_link.split(":")[-1]
32 #download_link = 'http:' + download_link
 print download_link
34
 #nome do arquivo baixado
36 nome_download = download_link.split("/")[-1]
 print nome_download
38
 comando_dois = ['wget', download_link]
```

```
40 process = Popen(comando_dois, stdout=PIPE)
42 [response, error] = process.communicate()
43 process.wait()
44
45 #determinando o nome final do arquivo
46 na_root = str(certificado.replace(".crt", ""))
47 na_root = na_root + '.root'
48 print na_root
49
50 #comando para passar de DER para PEM
51 comando_tres = ['openssl', 'x509', '-in', nome_download,
52 '-inform', 'der', '-out', na_root, '-outform', 'pem']
53
54 process = Popen(comando_tres, stdout=PIPE)
55 [response, error] = process.communicate()
56 process.wait()
57
58 #comando para deletar o DER original
59 comando_quatro = ['rm', '-r', nome_download]
60
61 process = Popen(comando_quatro, stdout=PIPE)
62 [response, error] = process.communicate()
63 process.wait()
64
65
66 if __name__ == '__main__':
67
68 files = glob("*.crt")
69
70 for certificado in files:
71 download_root(certificado)
```

---

No *Script 3.3*, a função `download_root()` realiza todo o trabalho de acessar o conteúdo textual de um certificado, separá-lo em tokens, e a partir desses tokens extrair o endereço para download do certificado do emissor. Uma vez com o certificado do emissor em mãos, esse certificado é tratado e passado do formato DER para o formato PEM, e esse novo arquivo PEM tem sua extensão definida, para fins de controle, como `.root`.

Uma vez recuperados os certificados dos emissores, foi executado o *Script* apresentado no *Script 3.4*, com a finalidade de listar quais certificados possuem o certificado da CA armazenado localmente.

Código 3.4 – LISTA.py

```
from subprocess import *
2 from glob import glob
 # coding: utf-8
4
def listar():
6 file = open('lista.dupla', 'w')

8 temp_a = ""
 temp_b = ""
10 output = ""

12 CRT = glob("*.crt")
 ROOT = glob("*.root")
14

 match = False
16

 for temp_a in CRT:
18 temp_a = str(temp_a.replace(".crt",""))
 match = False
20 for temp_b in ROOT:
 temp_b = str(temp_b.replace(".root",""))
22 if (temp_a == temp_b) and (match == False):
 dados = (temp_a + '.crt', temp_b + '.root')
24 output = '%s,%s\n'%dados
 match = True
26 if (match == False):
 dados = (temp_a + '.crt')
28 output = '%s,-\n'%dados

30 if match == True:
 file.write(output)
32 else:
 file.write(output)
34

 file.close()
```

```

36 if __name__ == '__main__':
37
38 listar()

```

---

A função do *Script 3.4* é pegar todos os arquivos `.pem` presentes no mesmo diretório que ele e pesquisar se para eles existe um arquivo `.root` associado. O *Script* então gera uma lista pareada de `.pem`'s e `.root`'s na qual, caso não haja um par, o `.pem` será pareado com um hífen ( - ), para identificação dos arquivos sem `.root` quando for feita a verificação dos certificados.

### 3.3 Verificação dos Certificados

A *OpenSSL* foi amplamente utilizada no processo de aquisição e verificação dos certificados por permitir, através de suas funções, que a comunicação pela porta 443 fosse feita e que os processos de comunicação pela mesma fossem estabelecidos. Em um momento posterior, esta mesma biblioteca foi utilizada para permitir a verificação local dos certificados coletados.

A Tabela 3 apresenta os nomes das funções inseridas nos scripts e os comandos *OpenSSL* por elas utilizados para a verificação e validação dos certificados coletados.

Tabela 3 – Tabela de Comandos *OpenSSL* na Verificação

| Comando                  | Descrição                                                               |
|--------------------------|-------------------------------------------------------------------------|
| <code>cmdVerify</code>   | <code>\$ OpenSSL verify certificado.crt</code>                          |
| <code>cmdCAverify</code> | <code>\$ OpenSSL verify -CAfile certificado.root certificado.crt</code> |

Esses comandos, entretanto, não são utilizados diretamente via terminal, estando presentes no corpo dos *Scripts* (quando se fazem necessários) responsáveis por sua execução automatizada. A automatização do processo de verificação se fez necessária pelo tamanho do corpo de certificados que foram coletados para a verificação.

Para a validação dos certificados, foi executado o *Script* listado no Código 3.5.

Código 3.5 – SEPARAR.py

---

```

from subprocess import *
2 from glob import glob

4 def erros():
 erros = {0 : 'ok',
6 1 : 'ok',

```

```
2 : 'unable to get issuer certificate',
8 3 : 'unable to get certificate CRL',
 4 : 'unable to decrypt certificate\'s signature',
10 5 : 'unable to decrypt CRL\'s signature',
 6 : 'unable to decode issuer public key',
12 7 : 'certificate signature failure',
 8 : 'CRL signature failure',
14 9 : 'certificate is not yet valid',
 10 : 'certificate has expired',
16 11 : 'CRL is not yet valid',
 12 : 'CRL has expired',
18 13 : 'format error in certificate\'s notBefore field'
 ,
 14 : 'format error in certificate\'s notAfter field',
20 15 : 'format error in CRL\'s lastUpdate field',
 16 : 'format error in CRL\'s nextUpdate field',
22 17 : 'out of memory',
 18 : 'self signed certificate',
24 19 : 'self signed certificate in certificate chain',
 20 : 'unable to get local issuer certificate',
26 21 : 'unable to verify the first certificate',
 22 : 'certificate chain too long',
28 23 : 'certificate revoked',
 24 : 'invalid CA certificate',
30 25 : 'path length constraint exceeded',
 26 : 'unsupported certificate purpose',
32 27 : 'certificate not trusted',
 28 : 'certificate rejected',
34 29 : 'subject issuer mismatch',
 30 : 'authority and subject key identifier mismatch',
36 31 : 'authority and issuer serial number mismatch',
 32 : 'key usage does not include certificate signing'
 ,
38 50 : 'application verification failure'}
return erros
40
def find_subject(certificado):
42 comando_um = ['openssl', 'x509', '-in', certificado, '-
 text']
```

```
44 process = Popen(comando_um, stdout=PIPE)
45 [response, error] = process.communicate()
46 process.wait()

48 tokens = response.split('0=')

50 token = ""
51 token = tokens[2]
52 micro = token.split(',')
53 subject = micro[0]
54 sub = subject.split('/')
55 return str(sub[0])

56
57 def find_issuer(certificado):
58 comando_um = ['openssl', 'x509', '-in', certificado, '-
59 text']

60 process = Popen(comando_um, stdout=PIPE)
61 [response, error] = process.communicate()
62 process.wait()

64 tokens = response.split('0=')

66 token = ""
67 token = tokens[1]
68 micro = token.split(',')
69 issuer = micro[0]
70 iss = issuer.split('/')
71 return str(iss[0])

72
73 def separador_c():
74 certificados = []
75 c = ""
76 arquivo = open('lista.dupla', 'r')
77 for line in arquivo:
78 c = str(line.split(',')[0])
79 certificados.append(str(c))
80 return certificados
```



```
82 def separador_r():
 roots = []
84 r = ""
 arquivo = open('lista.dupla','r')
86 for line in arquivo:
 r = str(line.split(',') [1])
88 roots.append(str(r.replace("\n","")))
 return roots

90
def verifica_c(certificado):
92 args = ['openssl', 'verify', certificado]

94 process = Popen(args, stdout=PIPE)
 [response, error] = process.communicate()
96 process.wait()

98 tokens = response.split()

100 issuer = find_issuer(certificado)
 company = '-'
102

 foundError = False
104 errorCode = 1

106 for token in tokens:
 if foundError:
108 errorCode = int(token)
 foundError = False

110

 if token == 'error':
112 foundError = True

114 error_list = erros()

116 message = ""
 message = error_list[int(errorCode)]
118

 dados = (errorCode, message, certificado, issuer)
```

```
120 return dados
122
123 def verifica_rc(certificado, root):
124 args = ['openssl', 'verify', '-CAfile', root, certificado
125]
126
127 process = Popen(args, stdout=PIPE)
128 [response, error] = process.communicate()
129 process.wait()
130
131 issuer = find_issuer(certificado)
132 company = '-'
133
134 tokens = response.split()
135
136 foundError = False
137 errorCode = 1
138
139 for token in tokens:
140 if foundError:
141 errorCode = int(token)
142 foundError = False
143
144 if token == 'error':
145 foundError = True
146
147 error_list = erros()
148
149 message = ""
150 message = error_list[int(errorCode)]
151
152 if errorCode == 1:
153 errorCode = 0
154
155 dados = (errorCode, message, certificado, issuer)
156
157 return dados
```

```
158 if __name__ == '__main__':
 certificado = separador_c()
160 root = separador_r()

162 for c, r in zip(certificado, root):
 if (r == "-"):
164 dados = verifica_c(c)
 print '%d,%s,%s,%s' % dados
166 else:
 dados = verifica_rc(c, r)
168 print '%d,%s,%s,%s' % dados
```

---

O *Script 3.5* foi então o responsável pela verificação dos certificados. Primeiro ele gera getou dois vetores pareados usando o arquivo gerado pelo *Script 3.4* e cuja ordem é foia a mesma da lista gerada por tal *Script*. Uma vez determinados, esses vetores pareados foram verificados utilizando comandos *OpenSSL* na Tabela 3.

Através do último *Script* (o *Script 3.5*) foi possível gerar um arquivo .csv (comma separated value) com o nome de cada certificado e os resultados de suas avaliações automatizadas. Cada resultado corresponde a um único erro relacionado ao certificado, acusado pela verificação do *OpenSSL* e extraído automaticamente.

O resultado do Código 3.5 apresenta, além do número do erro e de informações relativas ao certificado, qual a natureza do erro apontado, de acordo com a lista de retornos do comando *verify* do *OpenSSL*, que podem ser um resultado de verificação positiva ou um dentre os trinta e dois erros previstos de serem encontrados. Estes erros são listados e descritos no Anexo A.

No próprio arquivo .csv resultante foi utilizada a função `SUMIF()`, nativa da ferramenta OpenOffice Math, que adiciona termos ao somatório quando estes atendem a condição especificada dentro de seus parâmetros.



## 4 Resultados

Através da verificação automática feita utilizando a ferramenta OpenSSL, em conjunto com os *códigos*, foram alcançados resultados, vistos na Figura 9. Esses resultados retornaram uma tabela, cujos valores incluem se as verificações encontraram algum erro e qual foi o erro encontrado, além de identificarem em quais certificados foram encontrados cada um dos erros.

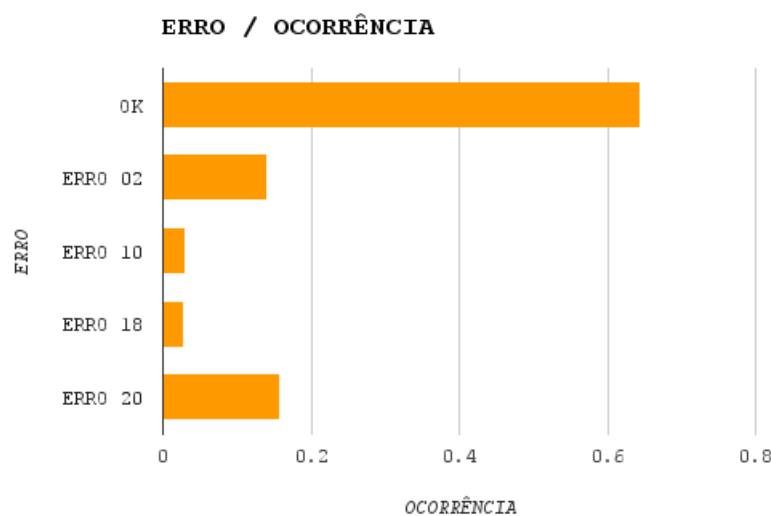


Figura 9 – Taxa de Ocorrência dos Erros

Os números com que os erros se repetiram foram um dos dados extraídos da tabela, que se baseia na verificação de 799 (setecentos e noventa e nove) certificados digitais. Vale notar, também, que destes certificados verificados, foram considerados certificados de pessoa jurídica, ou física, em sites de qualquer domínio.

Os erros constatados são apresentados em proporção à suas ocorrências, como visto na Figura 10.

### 4.1 Sem Erro

Os certificados que não apresentaram erros na verificação representam aproximadamente 64,45% (sessenta e quatro por cento) dos certificados verificados no primeiro momento do trabalho. Esses certificados estão, de acordo com a verificação feita pela ferramenta OpenSSL, de acordo com as exigências dos PKCSs que adotam o padrão x509 como formato final.

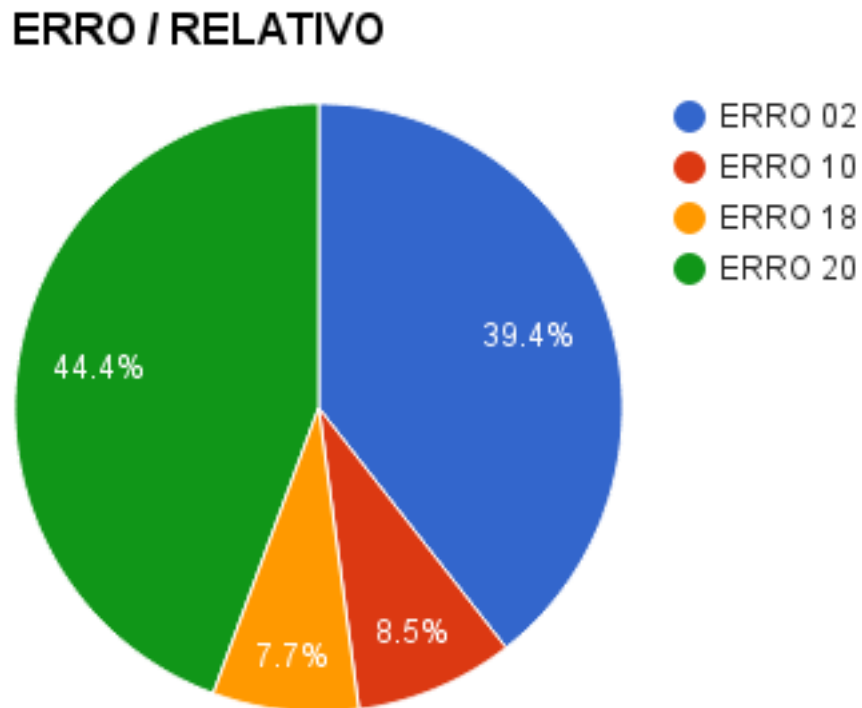


Figura 10 – Taxa de Erros Relativos

Esses certificados são certificados ideais, cuja confiança reside na cadeia de certificação, reconhecida e atestada pelos métodos de avaliação utilizados pelos envolvidos na comunicação. As assinaturas e as autoridades por toda a cadeia são atestadas e apenas os certificados de Autoridades Certificadoras no topo de suas hierarquias são auto-assinados.

## 4.2 Erro 02 - Unable to get issuer Certificate

Na documentação da ferramenta OpenSSL, o erro 02 (dois) identifica que a verificação retornou a mensagem: Incapaz de conseguir o certificado do emissor. Esse erro se apresenta quando a cadeia de certificados não está completa na listagem disponível no certificado analisado. O erro 02 (dois) se apresentou em aproximadamente 14% (quatorze por cento) dos certificados verificados.

Uma das principais consequências que se pode ter ao encontrar esse erro vem da incapacidade de verificar a certificação do emissor em questão. Como forma de forjar um certificado, um indivíduo pode gerar um certificado inválido e assiná-lo com outro

certificado inválido, ocultando o de maior posição na cadeia de certificação, ele poderia forjar um certificado duvidoso sem se denunciar como um certificado auto-assinado.

A incapacidade de encontrar referências válidas na cadeia de certificação deixa a análise do certificado vulnerabilizada, assim como a confiança do outro indivíduo envolvido, o que dificultaria a garantia de identidade e acarretando em uma séria situação. Visto em outro quadro, essa situação pode ser constrangedora, pois um certificado assinado sem referências acessíveis não é capaz de cumprir o objetivo a que se propõe, de identificar através do atestado de terceiros.

### 4.3 Erro 10 - Certificate has Expired

Na documentação da ferramenta OpenSSL, o erro 10 (dez) identifica que a verificação retornou a mensagem: O certificado expirou. Esse erro se apresenta se, e somente se, o certificado estiver sendo utilizado além de sua validade original. Um certificado digital tem um período de validade especificado no momento em que ele é emitido, e uma vez que esse prazo se cumpriu, ele deixa de ser reconhecido como válido. O erro 10 (dez) se apresentou em aproximadamente 3% (três por cento) dos certificados verificados.

A ocorrência desse erro é preocupante pois, uma vez que a validade de um certificado se vá, outros detalhes sobre ele não são mais confiáveis, não se sabe se aquele portador ainda é o mesmo que se identifica no certificado. Mais comumente, certificados são utilizados por pessoas jurídicas e quem responde por aquele nome, quem pode responder por aquela marca, nem sempre são os mesmos indivíduos de tempos em tempos. A informação contida no certificado pode estar desatualizada. A comunicação pode estar sendo feita com um portador anterior, que já não é mais autorizado a utilizar-se daquela identidade, ou acessar certa informação.

### 4.4 Erro 18 - Self Signed Certificate

Na documentação da ferramenta OpenSSL, o erro 18 (dezoito) identifica que a verificação retornou a mensagem: Certificado auto-assinado. Neste caso em específico, duas condições foram encontradas irregulares no certificado. A primeira e mais evidente é que o alvo da certificação e o emissor do certificado são a mesma entidade; a segunda que se apresenta é que o certificado não se encontra na lista de certificados confiáveis, o que significa que ele não é uma autoridade certificadora raiz. O erro 18 (dezoito) se apresentou em aproximadamente 2,75% (dois vírgula setenta e cinco por cento) dos certificados verificados.

Esses certificados nem sempre devem ser tidos como erros, por exemplo no caso de algumas autoridades certificadoras cujos certificados precisam ser auto-assinados para

indicar o fim da cadeia de certificação. Logicamente, nesses casos, esses certificados se diferenciam dos outros.

Porém, quando utilizados em outros contextos, esses certificados não servem como prova de identidade, pois não é um fator definitivo de identidade, assumindo um contexto em que desconhecidos usam certificados digitais para se identificar. Esse tipo de erro daria brechas para que qualquer um assumisse a identidade que lhe fosse interessante. Em um ataque como o *Man-In-The-Middle Attack*, o atacante poderia facilmente se certificar como um, ou mesmo ambos, os indivíduos da comunicação, interceptando e controlando toda a informação trocada.

## 4.5 Erro 20 - Unable to get Local Issuer Certificate

Na documentação da ferramenta OpenSSL, o erro 20 (vinte) identifica que a verificação retornou a mensagem: Incapaz de acessar o emissor local do certificado. Um erro que ocorre quando o certificado do emissor não pôde ser encontrado. Nesse caso o certificado do emissor é inicialmente procurado através da referência presente no certificado em análise, e quando o acesso não oferece um retorno positivo, a ferramenta verificadora procura o certificado localmente, analisando o certificado do emissor passado na verificação, retornando esse erro caso ainda haja incoerências na verificação do certificado. O erro 20 (vinte) representa 15,75% (quinze vírgula setenta e cinco por cento) dos certificados verificados.

É um erro parecido com o *Erro 02*, porém, se estende, no sentido de que, ao tentar conseguir o certificado do emissor de forma remota e receber uma resposta negativa, a cadeia foi procurada localmente e também não foi encontrada. As vulnerabilidades apresentadas são as mesmas vulnerabilidades que se vê no *erro 02*.

Nesse trabalho acadêmico esse erro não se apresenta pela falta de referências locais, pois os métodos utilizados buscam a fonte dos certificados para disponibilizar a cadeia localmente. Esse erro pode ser considerado, então, uma extensão do *erro 02* em suas razões.



## 5 Conclusão

Os resultados apresentam um número notável de exceções de segurança, sendo disparadas pela verificação realizada pelo *OpenSSL*. Estas, encontradas em ambiente controlado de estudo, mostram que existem falhas em certificados obtidos de um ambiente real, um dado preocupante, visto que todos os certificados apresentados deveriam ser seguros. Essas exceções podem se tornar um risco de falhas maiores de segurança, em ambiente real, resultando em riscos na comunicação, que supostamente deveria ser segura.

Um número percentual de exceções pode ser notado no corpo de certificados estudados, entretanto não é possível afirmar uma única causa para todos os erros. Foi observado que um grande número de certificados apresentaram o *Erro 02* ao serem analisados e isso serve como um forte indicador de que a origem dos problemas pode estar na *cadeia de assinaturas digitais* que se faz presente em todo certificado digital. Essa cadeia, que deveria ser confiável, pode não estar funcionando de forma ideal, e suas razões devem ser investigadas.

Dentro desse contexto, os certificados que apresentaram o *Erro 20* também foram numerosos, e sua natureza leva a crer que os mesmos riscos advindos do *Erro 02* podem se repetir nesse cenário. Isso leva a crer que existe uma grande vulnerabilidade, atualmente, em como está sendo tratada a cadeia de certificação e suas referências. A própria ideia da razão dos certificados digitais dependeria dessa cadeia, que é a justificada na confiabilidade através de terceiros.

A presença do *Erro 10* no estudo pode apresentar casos circunstanciais, em que a falta de um controle mais rígido levou à repetição da detecção deste erro dentro do estudo. A natureza do erro e sua incidência não se apresentam de forma tão alarmante, seria necessário analisar pontualmente para entender se os casos são maliciosos.

Já o *Erro 18*, diferente do *Erro 10* de recorrência similar, pode apresentar casos mais perigosos, onde a brecha de segurança seria mais facilmente explorada. Esses casos, possuem suas exceções, mas a natureza das exceções deixa claro que sua recorrência não deveria se mostrar como um valor tão significativo quanto foi visto.

Os *erros* retornados em menor número durante as verificações podem indicar casos isolados. A ocorrência desses erros também é preocupante, pois podem acarretar em problemas de segurança, se caracterizando como falhas dependendo de como forem explorados. Isso deixa claro que erros de segurança existem, e podem ser encontradas em certificados em uso, um fator alarmante, uma vez que o uso de certificados digitais é cada vez mais um recurso explorado como forma de aumentar a segurança nas transações realizadas por vias de comunicação digitais.



# Referências

- CALLAS, J. et al. <https://tools.ietf.org/html/rfc4880>. [S.l.]: IETF, 2007. Citado na página 33.
- COOPER, D. et al. <https://tools.ietf.org/html/rfc5280>. [S.l.]: IETF, 2008. Citado na página 34.
- CRYPTO, M. <https://en.wikipedia.org/wiki/FILE:DES-main-network.png>. [S.l.]: Matt Crypto, 2005. Citado 2 vezes nas páginas 15 e 28.
- ITI. [www.iti.gov.br/icp-brasil/estrutura](http://www.iti.gov.br/icp-brasil/estrutura). [S.l.]: Instituto Nacional de Tecnologia da Informação, 2015. Citado 2 vezes nas páginas 15 e 33.
- RSA, L. Pkcs #8 private key information syntax standard. Redwood City, CA, 1993. Citado na página 29.
- RSA, L. Pkcs #10 certification request syntax standard. Bedford, MA, 2000. Citado na página 31.
- RSA, L. Pkcs #1 rsa cryptography standard. Cambridge, MA, 2012. Citado na página 29.
- SCHNEIER, B. *Applied cryptography protocols, algorithms, and source code in C*. [S.l.]: Wiley, 1996. ISBN 9780471128458. Citado 3 vezes nas páginas 25, 26 e 30.
- STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. [S.l.]: Prentice Hall, 2011. ISBN 9780136097044. Citado 7 vezes nas páginas 15, 25, 28, 29, 30, 31 e 32.
- YONG, M. K. <http://www.mkyong.com/java/jsoup-send-search-query-to-google/>. [S.l.]: mkyong, 2015. Citado na página 38.



# Anexos



# ANEXO A – Tabela de Retornos do Verify da OpenSSL

| <b>Valor Associado</b> | <b>Retorno</b>                                        |
|------------------------|-------------------------------------------------------|
| 0                      | <i>ok</i>                                             |
| 2                      | <i>unable to get issuer certificate</i>               |
| 3                      | <i>unable to get certificate CRL</i>                  |
| 4                      | <i>unable to decrypt certificate's signature</i>      |
| 5                      | <i>unable to decrypt CRL's signature</i>              |
| 6                      | <i>unable to decode issuer public key</i>             |
| 7                      | <i>certificate signature failure</i>                  |
| 8                      | <i>CRL signature failure</i>                          |
| 9                      | <i>certificate is not yet valid</i>                   |
| 10                     | <i>certificate has expired</i>                        |
| 11                     | <i>CRL is not yet valid</i>                           |
| 12                     | <i>CRL has expired</i>                                |
| 13                     | <i>format error in certificate's notBefore field</i>  |
| 14                     | <i>format error in certificate's notAfter field</i>   |
| 15                     | <i>format error in CRL's lastUpdate field</i>         |
| 16                     | <i>format error in CRL's nextUpdate field</i>         |
| 17                     | <i>out of memory</i>                                  |
| 18                     | <i>self signed certificate</i>                        |
| 19                     | <i>self signed certificate in certificate chain</i>   |
| 20                     | <i>unable to get local issuer certificate</i>         |
| 21                     | <i>unable to verify the first certificate</i>         |
| 22                     | <i>certificate chain too long</i>                     |
| 23                     | <i>certificate revoked</i>                            |
| 24                     | <i>invalid CA certificate</i>                         |
| 25                     | <i>path length constraint exceeded</i>                |
| 26                     | <i>unsupported certificate purpose</i>                |
| 27                     | <i>certificate not trusted</i>                        |
| 28                     | <i>certificate rejected</i>                           |
| 29                     | <i>subject issuer mismatch</i>                        |
| 30                     | <i>authority and subject key identifier mismatch</i>  |
| 31                     | <i>authority and issuer serial number mismatch</i>    |
| 32                     | <i>key usage does not include certificate signing</i> |
| 50                     | <i>application verification failure</i>               |