Análise de segurança da distribuição de raízes na ICP-Brasil

Bruno C. Dias Ribeiro, Edson Floriano S. Junior[1], Diego F. Aranha[2]

[1] Departamento de Ciência da Computação – Universidade de Brasília (UnB)

[2]Instituto de Computação – Universidade Estadual de Campinas (Unicamp)

Abstract. *This work presents a security analysis of the distribution of root certificates in the Brazilian Public Key Infrastructure (ICP-Brasil). A simple proof of concept is provided to replace a root certificate downloaded from the official repository with a fake certificate, compromising the trusted store of the client machine even when the suggested verification procedure is strictly followed. Finally, some recommendations are offered to strengthen the certificate distribution processin hope of contributing to make ICP-Brasil more robust.*

Resumo. *Este trabalho analisa a distribuição de certificados raízes na ICP-Brasil do ponto de vista de segurança. Uma prova de conceito simples é apresentada para substituir o certificado raiz distribuído no repositório oficial por um certificado falso, comprometendo a base de certificados confiados da máquina cliente, mesmo quando o procedimento sugerido de verificação é respeitado. Finalmente, algumas recomendações são apresentadas para fortalecer a distribuição de certificados, na esperança de contribuir para tornar a ICP-Brasil mais robusta.*

1. Introdução

A certificação digital se propõe a resolver o problema de obtenção de chaves públicas autênticas, atuando como uma "terceira parte confiável" que atesta a titularidade de uma chave pública [Kohnfelder 1978]. Este papel é desempenhado pelas Autoridades Certificadoras (AC) e Autoridades de Registro (AR), cuja hierarquia caracteriza uma Infraestrutura de Chaves Públicas (ICP) [Kuhn et al. 2001].

As ACs são portanto elemento chave do modelo e também sua maior fraqueza [AccessNow 2011], já que o comprometimento de uma AC pode implicar comprometimento de toda estrutura abaixo dela. Falhas de segurança em sua operação podem levar a verdadeiros desastres, como o ocorrido no caso DigiNotar em 2011 [Prins 2011], com o comprometimento de várias ACs. Um problema central para a segurança de ICPs é a instalação de certificados raízes de ACs, dado que sua manipulação maliciosa permite ataques posteriores difíceis de detectar. Sob controle da chave privada correspondente a um certificado maliciosamente instalado, um atacante pode emitir certificados reconhecidos como válidos para personificar qualquer domínio na Internet.

Neste trabalho, foi realizada uma análise de segurança do processo de distribuição de certificados raízes na ICP-Brasil, com o objetivo de colaborar com a robustez da infraestrutura contra atividade maliciosa. É apresentada uma prova de conceito que demonstra a substituição do certificado raiz legítimo por um fraudulento, mesmo quando os procedimentos recomendados de verificação são seguidos. Esse problema não é exatamente novo para a comunidade científica brasileira, mas parece ser a primeira vez que aparece discutido de forma sistemática, com recomendações para mitigação e aprimoramento.

2. Trabalhos Relacionados

O caso de comprometimento da DigiNotar [Prins 2011] é um exemplo notório de desastre na área da certificação digital. A empresa teve cerca de 30 ACs de diversos níveis (inclusive raízes) comprometidas, sendo que em pelo menos 6 delas foram encontradas evidências de abuso por parte dos atacantes. Todas faziam parte do mesmo domínio *Active Directory* (AD), com isso, uma vez obtidos privilégios de administrador no domínio, o atacante conseguiu invadir quantas ACs julgou necessário.

Falhas como esta possibilitam ataques "*man-in-the-middle*" (MITM), como demonstrado em [Huang et al. 2014], em que um atacante fabrica certificados para domínios arbitrários de seu interesse, tornando-se capaz de controlar todo o tráfego entre cliente e servidor. Como estratégia de mitigação, os autores propõem um método para detectar certificados falsos através do uso de um pequeno *plugin* nos navegadores de clientes. Através da análise de características como tamanho da cadeia de certificados, tamanho das chaves, domínio no campo *Common Name* e emissor do certificado, o *applet* conclui, com grande probabilidade de acerto, se um certificado é verdadeiro ou não.

Estes problemas colocam em evidência a necessidade de um rápido e eficiente tratamento de incidentes nas ICPs. Como mostrado na literatura [Cooper 1998, Li and Feigenbaum 2001], os ataques podem inclusive atuar na tentativa de burlar o processo de revogação de certificados. Se o processo de revogação não for feito de maneira eficiente, o atacante pode tanto impedir que o certificado seja revogado, quanto continuar a se passar pela vítima mesmo após a revogação do mesmo. O modelo de confiança em ACs também é questionado na literatura [Leavitt 2011, Roosa and Schultze 2013]. Isto porque qualquer AC dita "confiável" pode emitir um certificado atestando a titularidade de uma determinada chave pública e este será automaticamente aceito. Com isso, muitas vezes a verificação de identidade efetuada pelas autoridades de registro é a única defesa contra a obtenção de certificados fraudulentos.

Cientes do risco, navegadores modernos estabelecem níveis rigorosos de segurança e transparência para admitir certificados raízes em sua cadeia de certificados confiados. Por exemplo, a Mozilla instituiu o *CA Certificate Program*, um processo rigoroso de avaliação que determina implantação de boas práticas e requer auditorias independentes regulares [WebTrust 2011, WebTrust 2017]. Os requisitos costumam ser ainda mais rigorosos para ICPs governamentais, dado o interesse evidente de alguns governos em personificar serviços para promover censura e vigilância [Mozilla 2015]. Além da admissão, a operação de autoridades certificadoras é cuidadosamente acompanhada por esforços como o *Certificate Transparency* [Laurie et al. 2013], que mantém um registro temporal de certificados emitidos e observados, já utilizado anteriormente para detectar emissão de certificados fraudulentos com sucesso [Kerner 2015].

3. ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é responsável por garantir autenticidade, integridade e validade jurídica aos documentos eletrônicos com certificação digital no Brasil[1]. A ICP-Brasil conta atualmente com 14 ACs de primeiro nível credenciadas, responsáveis pela emissão, distribuição, gerenciamento e revogação de certificados

[1] `https://www.iti.gov.br/icp-brasil`

para ACs de próximo nível ou diretamente ao usuário final. Embora a ICP-Brasil seja instituída de modo governamental, tanto entidades públicas quanto privadas podem requerer credenciamento para atuarem como ACs e ARs. Desta forma, é possível a atuação de empresas no ramo da certificação digital como parte integrante da hierarquia, comercializando certificados digitais a pessoas físicas ou jurídicas.

Representada pelo Instituto Nacional de Tecnologia da Informação (ITI), a ICP-Brasil já emitiu um total de 6 certificados auto-assinados (raízes). Com validade inicial de 10 anos, a primeira raiz foi emitida em 2001 utilizando o algoritmo RSA com chaves de 2048 *bits* e função de resumo SHA-1. Os parâmetros foram mantidos na segunda raiz (v1), quando o prazo de validade foi estendido para 13 anos. A terceira raiz (v2) foi emitida em 2010 e também utilizou RSA com o dobro de tamanho de chaves, mas adotou a função de resumo SHA-512, mantida desde então. A quarta raiz (v3) deu início à utilização de assinaturas ECDSA sobre curvas elípticas, mas terminou revogada após suspeitas sobre as curvas padronizadas pelo *National Institute of Standards and Technology* (NIST) [Bernstein et al. 2015]. Raízes posteriores utilizaram curvas Brainpool [Merkle and Lochter 2010] (v4) e RSA com 4096 *bits* (v5).

4. Distribuição de certificados

Um problema desafiador para qualquer ICP é promover a distribuição de suas raízes, que se torna ainda mais complexo no caso de infraestruturas governamentais, ao ser reconhecido o risco adicional [Mozilla 2015]. Após negociação com a empresa Microsoft, o ITI conseguiu introduzir a raiz v2 do certificado raiz em versões do Windows a partir do XP[2]. Aparentemente, não houve o mesmo sucesso para raízes subsequentes, que continuam ausentes no sistema operacional, mesmo havendo certificados já emitidos para serviços populares sob essas raízes. Um exemplo de serviço é o Expresso[3], utilizado para comunicação institucional em órgãos do governo federal. Além disso, sistemas operacionais alternativos, como GNU/Linux ou *Android*, ou ainda navegadores que não confiam incondicionalmente na base de certificados fornecida pelo sistema operacional, como o *Mozilla Firefox*, continuam apresentando alerta de segurança indicando a ausência do certificado raiz para encerrar a verificação de um certificado final.

Para resolver esse problema, a ICP-Brasil utiliza o procedimento de instalação manual, documentado em páginas específicas para cada navegador[4]. Há severas limitações nessa abordagem. Em primeiro lugar, o repositório raiz de certificados é fornecido utilizando o protocolo HTTP[5]. Apesar das informações lá contidas serem de caráter público, não exigindo a propriedade de confidencialidade fornecida pelo transporte sobre SSL/TLS, perde-se também a propriedade vital de autenticação. Para esse novo problema, o ITI serve páginas com valores de *hash* para verificação de integridade dos pacotes de certificado, também servidos via HTTP[6]; ou HTTPS sob certificado da própria ICP-Brasil, reduzindo o problema a si próprio. Não sendo possível a autenticação da página que oferece os certificados para instalação manual, o usuário não consegue determinar se o con-

[2] https://www.microsoft.com/brasil/setorpublico/temas/icp-brasil.mspx
[3] https://expressobr.serpro.gov.br/
[4] http://www.iti.gov.br/navegadores
[5] http://acraiz.icpbrasil.gov.br
[6] http://iti.gov.br/repositorio/84-repositorio/489-certificados-das-acs-da-icp-brasil-arquivo-unico-compactado

junto correto de certificados foi obtido e será instalado, até porque tanto os certificados quanto informações para verificação de integridade podem ser sutilmente substituídos por um adversário com controle da rede, sem produzir qualquer alerta visível. A prova de conceito descrita na Seção 5 apresenta em detalhes um ataque dessa natureza. Não obstante, por vezes os valores de *hash* publicados pelo ITI estavam simplesmente incorretos, conforme pode ser verificado na versão de Junho de 2016 da página arquivada no *Internet Archive Wayback Machine* que possui nome de arquivo e valor de *hash* incorretos[7].

A solução encontrada por outras ACs lançadas recentemente, como a *Let's Encrypt*, foi realizar assinatura cruzada de seus certificados intermediários, permitindo a verificação com sucesso de certificados em sua árvore até que a raiz tenha sido propagada[8]. Entende-se que essa abordagem não é de aplicação trivial, dado que é problemático confiar a soberania da ICP-Brasil a uma AC comercial já devidamente instalada em navegadores modernos, por isso outras abordagens serão sugeridas na Seção 6.

A solução ideal para distribuição das raízes ICP-Brasil é sua inclusão nos repositórios de certificados confiados por navegadores modernos. O ITI procura há 9 anos satisfazer requisitos impostos pela Mozilla, mas sem sucesso. Há uma longa discussão no fórum da organização[9], com participação de funcionários do ITI e ocasional ruído, que demonstra as dificuldades. Primeiramente, fica evidente que a falta de documentação em Inglês das normas e procedimentos dificulta o entendimento sobre a organização da iniciativa, agravado pela natureza peculiar da ICP-Brasil, que possui mais de uma dezena de ACs subordinadas comerciais e governamentais operadas de maneira independente. O termo utilizado para raízes desse tipo é *Super-CA*, com tratamento compatível ao aplicado às ICPs governamentais da Venezuela e Índia (comentário #122 na discussão).

A determinação da equipe Mozilla para o caso é que cada uma das ACs subordinadas da ICP-Brasil participe do processo de credenciamento em caráter individual, para apenas após a finalização do procedimento, as raízes poderem ser inseridas com sucesso. Isso não parece viável a curto prazo para o grande número de ACs da ICP-Brasil. Mais recentemente, há também questionamentos sobre escolha da empresa de auditoria de práticas na ICP-Brasil (comentário #155), que já esteve envolvida em auditorias deficientes em outros países. A leitura de toda a discussão é fascinante e fortemente recomendada para pesquisadores e profissionais da indústria envolvidos com certificação digital.

5. Prova de conceito de ataque

Baseando-se nos problemas de distribuição dos certificados raiz da ICP-Brasil, foi desenvolvida uma prova de conceito para exercitar um ataque em ambiente de testes.

5.1. Objetivo

A prova de conceito tem o objetivo de executar um ataque MITM contra um usuário que deseja ter acesso a qualquer serviço ou funcionalidade dependente da ICP-Brasil. O usuário simulado deseja proteger o conteúdo de todas suas informações de tráfego e

[7] https://web.archive.org/web/20160609022631/http://www.iti.gov.br/icp-brasil/repositorio/144-icp-brasil/repositorio/3886-repositorio-de-certificados-arquivo-unico-compactado

[8] https://letsencrypt.org/2015/06/04/isrg-ca-certs.html

[9] https://bugzilla.mozilla.org/show_bug.cgi?id=438825

navegação com o protocolo HTTPS, mas o ataque não levanta qualquer suspeita ou alerta do navegador ou do sistema operacional utilizado.

5.2. Detalhamento

O ataque MITM é uma interceptação maliciosa da comunicação entre duas partes de modo que essas partes julgam estar se comunicando diretamente entre si. Essa interceptação pode ser passiva, apenas observar o conteúdo das informações em trânsito, como também ativa, alterando as informações.

No cenário da prova, essa ação é executada por um atacante contra uma vítima conectada à mesma rede local. Antes da vítima acessar um serviço na Internet, o atacante convence mutuamente o computador atacado de que sua máquina representa o roteador da rede e vice-versa. Assim, o atacante passa a ser capaz de interceptar qualquer comunicação feita pela vítima, um ataque chamado *ARP spoofing*. Caso a vítima, no entanto, acesse serviços HTTPS, em que há autenticação do usuário e dados privados, existe uma camada criptográfica que o atacante não seria, em princípio, capaz de derrotar. O serviço em HTTPS possui um certificado digital válido atrelado ao seu endereço emitido por uma AC confiada por navegadores e sistemas operacionais que não poderia ter sido forjado por um atacante.

Uma técnica conhecida para contornar o uso de HTTPS pela vítima no ataque MITM é a *ssl-strip* ou *protocol downgrade* na qual as requisições HTTPS são reduzidas para HTTP pelo atacante, forçando, assim, uma conexão sem proteção criptográfica do usuário com o serviço. A adversidade é que, atualmente, os navegadores exibem um alerta visual quando não há a conexão HTTPS, podendo criar a suspeita pelo próprio usuário. Não somente, também há um parâmetro na resposta de requisições chamado *HTTP Strict Transport Security* (HSTS) que permite que servidores *Web* instruam os navegadores a interagir estritamente via protocolo HTTPS. Se ativa, esta política é guardada pelo navegador após a primeira comunicação com o servidor, portanto um ataque dessa natureza seria ineficaz caso a vítima tenha previamente acessado o serviço correto.

A prova de conceito para o ataque consiste exatamente em explorar as fragilidades na distribuição das ACs raízes da ICP-Brasil de modo a enviar ao usuário uma substituição maliciosa da raiz desejada, gerada pelo atacante. Assim, o sistema da vítima passa a confiar em certificados emitidos por essa raiz maliciosa, tornando possível também a substituição posterior dos certificados SSL de serviços HTTPS por certificados efêmeros emitidos pelo atacante. Isso torna possível o ataque MITM inclusive sobre o protocolo HTTPS, já que a entidade maliciosa se torna capaz de decifrar e recifrar o tráfego de informação, tendo acesso a todo seu conteúdo, cenário com maior impacto.

5.3. Metodologia

A implementação do ataque foi realizada através de uma instalação Kali Linux[10], uma distribuição GNU/Linux voltada para testes de penetração e análises de segurança. Esta distribuição facilita o uso de várias ferramentas, entre elas a *arpspoof* e *mitmproxy*, que serão usadas para interceptar o tráfego entre a vítima e o roteador; e para tratar as requisições e respostas tendo acesso ao conteúdo dos pacotes, respectivamente.

[10] `https://www.kali.org/`

O primeiro passo é criar um certificado de chave pública auto-assinado que mimetize a raiz da ICP-Brasil. Essa tarefa pode ser executada através da interface de linha de comando do *OpenSSL*[11]. Ao definir o *Common Name* do certificado, adicionamos o prefixo *ROGUE* ao nome da AC raiz brasileira para evidenciar de que este é o certificado malicioso. Para filtrar as comunicações e permitir a manipulação das informações trafegadas, foi criado um programa em *Python*, a ser acoplado à execução da ferramenta *mitmproxy*. O filtro é responsável pelas seguintes adulterações:

1. Aplicar ataque de *downgrade*: o programa irá substituir todos os links HTTPS por HTTP enquanto ainda não temos a raiz maliciosa confiada pela vítima. Esse ataque demonstra como é inócuo criar *links* HTTPS a partir de páginas HTTP, pois esta já pode estar sob ataque, removendo os recursos de proteção adicionados pelo transporte SSL/TLS.
2. Identificar o *download* de um certificado de autoridade certificadora através do *header Content-Type* da resposta do servidor e fazer a substituição pelo certificado raiz malicioso.
3. Substituir *hash* de verificação do certificado original pelo *hash* do malicioso.

Definido o comportamento do filtro na máquina com o sistema Kali Linux, foi habilitado o modo *IP forwarding* e em seguida aplicado o ataque *ARP Spoofing* para interceptar o tráfego de rede entre roteador e vítima, fazendo com que a comunicação entre eles passe pela máquina do atacante. Resta modificar o conjunto de regras da tabela de IPs da máquina atacante com o intuito de desviar o tráfego HTTP e HTTPS para passar pelo *proxy* da aplicação *mitmproxy* e, por fim, sua execução com o filtro e a autoridade certificadora maliciosa criada anteriormente.

5.4. Ataque

O ataque montando foi executado em ambiente de teste controlado, com todas as partes cientes e acompanhando o processo. No início, a vítima, em computador pessoal com sistema operacional Windows e navegador Firefox, acessa seu suposto *webmail* provido por `https://expressobr.serpro.gov.br/`. O acesso é imediatamente interrompido pela mensagem de erro da Figura 1, pois o certificado de SSL do serviço não foi emitido por uma autoridade certificadora de confiança do navegador.

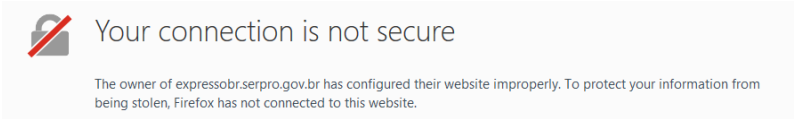

Figura 1. Erro de conexão desprotegida exibido pelo navegador.

A vítima, agora sob ataque, acessa a página do ITI para seguir os passos de configuração para o seu navegador, disponível em `http://iti.gov.br/navegadores/2-uncategorised/106-mozilla-firefox`. Ao clicar no *link* da cadeia v5, cadeia sob a qual está o certificado SSL do serviço desejado, o navegador irá sugerir à vítima a configuração de confiança para a raiz maliciosa, identificada pelo prefixo *ROGUE*, adulteração que passaria completamente despercebida pela vítima caso o desejado fosse gerar certificado com idêntico *Subject Name* da raiz brasileira v5.

[11] `https://www.openssl.org`

A página com os passos de configuração oferece um *link* para o valor do *hash* SHA-512 do arquivo da cadeia obtido, caso o usuário deseje verificar sua integridade, uma medida de segurança que é ineficaz contra o ataque proposto, que também permite adulterar o valor para concordar com o certificado malicioso. A Figura 2 exibe a página com o resumo criptográfico do arquivo sob ataque, evidenciado novamente pelo prefixo *ROGUE* adicionado.

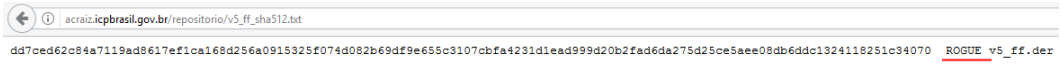

Figura 2. Página com resumo criptográfico do certificado raiz sob ataque.

Concluindo a configuração da confiança do certificado pelo navegador, a vítima retorna à página do *webmail*, agora com acesso positivo, validado pelo navegador, sem qualquer alerta de segurança (Figura 3). Por detrás da navegação usual, o atacante passa a ser capaz de examinar ou modificar o conteúdo de todo o tráfego da vítima, não somente no serviço de *webmail*, mas de qualquer outro *site* ou recurso acessado, uma vez que a aplicação do atacante é capaz de utilizar a raiz maliciosa para emitir dinamicamente certificados com endereço de qualquer domínio sendo acessado.

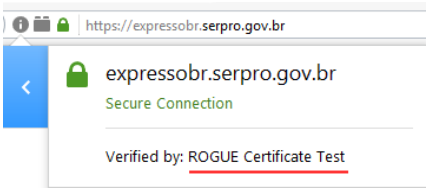

Figura 3. Página acessada pela vítima com certificado malicioso validado.

6. Recomendações

A tarefa de se projetar, implementar e manter uma infraestrutura de certificação digital é reconhecidamente desafiadora. Além dos aspectos técnicos e marco legal para validação jurídica de assinaturas digitais, há ainda dezenas de procedimentos para emissão de certificados, manutenção dos algoritmos criptográficos suportados, produção de carimbos de tempo e revogação de certificados cujas chaves privadas foram comprometidas. Esses desafios são ainda maiores para ICPs governamentais, que precisam aderir a conjuntos de práticas mais rigorosos, pelo risco inerente envolvido.

Desta forma, este trabalho apresentou uma análise de segurança das práticas vigentes na ICP-Brasil para distribuição de certificados raízes. A curto prazo, recomenda-se aprimoramento dos canais de distribuição de raízes para utilizar autenticação fornecida pelo protocolo HTTPS. Uma sugestão é utilizar as ACs de primeiro nível para descentralizar a distribuição, utilizando a solução adotada pela certificadora *Let's Encrypt*. Ou seja, permitir a certificação cruzada de certificados intermediários para também possibilitar que as ACs tenham páginas via SSL/TLS para distribuição de certificados e/ou verificação de integridade. Páginas com origem autenticada podem então ser utilizadas para distribuição de cadeias inteiras de certificados. O principal argumento de suporte à essa estratégia é que as ACs da ICP-Brasil já são confiadas do ponto de vista operacional, e podem também ser confiadas para distribuição das cadeias de certificados para instalação manual. A inclusão posterior de alguma AC em repositórios confiados facilitará a tarefa de distribuição de certificados raízes e fornecerá uma solução definitiva para o problema estudado aqui.

Referências

AccessNow (2011). The weakest link in the chain: vulnerabilities in the SSL certificate authority system and what should be done about them. https://www.accessnow.org/cms/assets/uploads/archive/docs/Weakest_Link_in_the_Chain.pdf.

Bernstein, D. J., Chou, T., Chuengsatiansup, C., Hülsing, A., Lambooij, E., Lange, T., Niederhagen, R., and van Vredendaal, C. (2015). How to manipulate curve standards: A white paper for the black hat. In *SSR*, volume 9497 of *LNCS*, pages 109–139. Springer. http://bada55.cr.yp.to.

Cooper, D. A. (1998). A Closer Look at Revocation and Key Compromise in Public Key Infrastructures. In *Proceedings of the 21st National Information Systems Security Conference*. NIST.

Huang, L. S., Rice, A., Ellingsen, E., and Jackson, C. (2014). Analyzing Forged SSL Certificates in the Wild. In *IEEE Symposium on Security and Privacy*, pages 83–97.

Kerner, S. M. (2015). Symantec Issues Fraudulent Google SSL Cert. http://www.esecurityplanet.com/network-security/symantecissues-fraudulent-google-ssl-cert.html.

Kohnfelder, L. M. (1978). Towards a practical public-key cryptosystem. B.S. Thesis, supervised by L. Adleman.

Kuhn, D. R., Hu, V., Polk, W. T., and Chang, S.-j. H. (2001). SP 800-32. Introduction to Public Key Technology and the Federal PKI Infrastructure. Technical report, Gaithersburg, MD, United States.

Laurie, B., Langley, A., and Kasper, E. (2013). Certificate transparency. RFC 6962: https://www.rfc-editor.org/rfc/rfc6962.txt.

Leavitt, N. (2011). Internet Security under Attack: The Undermining of Digital Certificates. *Computer*, 44(12):17–20.

Li, N. and Feigenbaum, J. (2001). Nonmonotonicity, user interfaces, and risk assessment in certificate revocation. In *Financial Cryptography*, volume 2339 of *LNCS*, pages 157–168. Springer.

Merkle, J. and Lochter, M. (2010). Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639: https://www.rfc-editor.org/rfc/rfc5639.txt.

Mozilla (2015). The MCS Incident and Its Consequences for CNNIC. https://blog.mozilla.org/security/files/2015/04/CNNIC-MCS.pdf.

Prins, J. (2011). DigiNotar Certificate Authority breach: "Operation Black Tulip". Interim report, Cybercrime Business Unit.

Roosa, S. B. and Schultze, S. (2013). Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model. *IEEE Internet Computing*, 17(3):18–25.

WebTrust (2011). Trust Service Principles and Criteria for Certification Authorities v2.0. http://www.webtrust.org/homepage-documents/item54279.pdf.

WebTrust (2017). Principles and criteria for certification authorities: Ssl baseline with network security v2.2. http://www.webtrust.org/principles-and-criteria/docs/item83987.pdf.

