Journal of Strategic Security

Volume 6
Number 2 *Summer 2013*

Article 4

DigiNotar: Dissecting the First Dutch Digital Disaster

Nicole van der Meulen
VU University Amsterdam, n.s.vander.meulen@vu.nl

pp. 46-58

DigiNotar: Dissecting the First Dutch Digital Disaster

Abstract
In the middle of the night on September 2, 2011, the Dutch Minister of the Interior and Kingdom Relations held an emergency press conference. DigiNotar, a Certificate Authority (CA), had been electronically 'broken into' and as a result intruders had managed to generate falsified certificates. As a CA, DigiNotar issued digital certificates to secure digital communication, but as a result of the breach the authenticity of such certificates could no longer be verified. The Dutch government subsequently revoked its trust in all certificates issued by DigiNotar. This was the beginning of the first digital disaster in the Netherlands. As a pioneering disaster, this article focuses on the implications of DigiNotar as a vital case study for future scenarios of digital disaster management. The main focus of this article is on the underlying 'weaknesses' of the DigiNotar incident, which allowed the situation to evolve from a problem into a disaster. These include lack of oversight, lack of security attention and risk awareness and the absence of an effective mitigation strategy. By identifying and subsequently analyzing the underlying problems, this article aims to demonstrate how future situations can be better contained if sufficient attention is granted to these factors and subsequent changes are introduced.

Introduction

In the middle of the night on September 2, 2011, the Dutch Minister of the Interior and Kingdom Relations, Piet-Hein Donner, appeared in front of the camera for an emergency press conference.1 The morbid mood of the scene was only briefly interrupted as he wished everyone a good morning and quickly smiled at the last bit of humor he could muster. The Minister proceeded by introducing the emergency. DigiNotar, a Certificate Authority (CA), had been electronically 'broken into' and as a result intruders had managed to generate falsified certificates. These certificates, as stated by the Minister, are necessary to allow Internet traffic to take place securely. Nearly all digital communication relies on certificates, for its confidentiality, authenticity and integrity. Whilst Internet security, or more popularly known as cyber security, is a topic that receives widespread coverage in the media these days, the details and subsequent implications of cyber attacks remain difficult to grasp for non-experts.

DigiNotar was in that sense no different, which made the label of 'disaster' challenging to digest for the common public. Why was this situation worthy of an overnight press conference? There was no spectacular footage to show. No fire, blood or people in tears over loved ones. Instead, all the public received was a Minister in a grey suit reading from a piece of paper. This image introduced the public to a new type of disaster: the digital disaster. A type of disaster that lacks common features, which we have come accustomed to through our experiences with physical disasters, such as visible suffering. The consequences of a digital disaster are subtler. Intruders can access confidential and personal information, from businesses and private citizens, as well as governments in order to subsequently abuse it. Examples may include identity theft or other types of fraud. Authoritarian governments can access the content of emails from dissidents and infiltrate in their personal lives. Imported goods, such as fruits and vegetables, can no longer be verified at customs and must remain at the border, rotting away. All of these (potential) consequences taken together, demonstrate how a breach at a CA can disrupt business continuity, lead to crime and perhaps even death in the case of authoritarian governments spying on their citizens.

To understand the complexity of the DigiNotar breach, some preliminary knowledge about Internet communication in connection to CAs is necessary. Therefore, the first section of this article shall provide such background knowledge as a means to place this 'disaster' in its proper context. The second section details the breach at DigiNotar based on the authoritative forensic analysis carried out by Fox-IT, a Dutch information security company hired by DigiNotar and subsequently by the Dutch government to investigate the incident. The third section evaluates the direct causes of the breach. The direct causes generally include an evident neglect by DigiNotar for standard information security practices.

The fourth section introduces the core focus of this article: the underlying 'weaknesses' of the DigiNotar incident. These weaknesses arguably allowed the situation to evolve from a problem into a disaster. In the findings, I specifically discuss the following underlying weaknesses: lack of oversight, lack of security attention and risk awareness, and lack of mitigation strategy. Lack of oversight focuses on the absence of keeping the security practices of CAs sufficiently in check, especially considering their vital role in the overall chain of communication. Lack of risk attention and security awareness, on the other hand,

[1] "Persconferentie Donner over overheidswebsites," NOS, September 3, 2011, available at: *http://nos.nl/video/269611-persconferentie-donner-over-overheidswebsites.html.*

discusses the absence of security considerations on the side of the government itself. Whilst every party cared for its specific role in the chain, the system as a whole was not kept in mind by any of the parties. The escalation of the situation, however, also took place in large part due to the absence of an existing and effective mitigation strategy. This meant that improvisation was called for to limit damages.

The subsequent analysis in section five places the DigiNotar disaster along with its risks into a broader context. This is especially done through drawing connections with other prominent security companies that have experienced similar attacks, which have collectively introduced a serious threat to the cyber security landscape that I have labeled as a 'metavulnerability.' By identifying and subsequently analyzing the underlying problems, this article aims to demonstrate how future situations can be better contained if sufficient attention is granted to underlying weaknesses and subsequent changes are introduced.

Background

Two decades ago, in 1993, Peter Steiner wrote the following caption under one of his cartoons for the New Yorker: "On the Internet No One Knows You're a Dog." Whilst we have come a long way, identification on the Internet remains challenging. When we receive a message or go to a website, we find comfort in the thought that we know who we are communicating with. To facilitate this process of secure and reliable communication, we use digital certificates. Digital certificates are generally thought of as "digital passports." They fulfill three purposes:[2]

- To guarantee the authenticity of a website.
- To guarantee the authenticity and integrity of (email) messages, files or programming code through the generation of a digital signature. The signature can be verified with a 'public key' by the person who signed. Any alteration to the message, file or code shall lead to the signature no longer being accurate.
- To guarantee the confidentiality of an (email) message or file by encrypting it with the public key of the recipient. Only the recipient can decrypt the message through the usage of a private key.

Basically, through digital certificates, we know we can trust the website and enter our information, such as username and password. Or, alternatively, that we can believe the content of the message based on the digital signature which accompanies the content. Digital certificates therefore form a crucial link in the establishment of trust and security in Internet communication.

Digital certificates are issued by Certificate Authorities (CAs). CAs are also known as Trusted Third Parties (TTP). They verify the identity of the entity or person requesting the digital certificate. This is precisely why considerable trust is placed in the certificate itself, since the underlying assumption is that the identity of the recipient of the certificate has been verified by a TTP. We can draw a comparison with the ability to travel with a passport or enter a secured building with a token indicating the person in possession of said token has the necessary security clearance. When the issuer of certificates, the CA, is compromised through

[2] "Factscheet Veilig beheer van digitale certificaten," Nationaal Cyber Security Centrum (NCSC), September 27, 2012, available at: *https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html*.

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

a breach, all trust is revoked in its product, as happened with DigiNotar. Users do not possess the capacity to determine whether a certificate is falsified, only those whose name is being misused can do so.

The Breach

DigiNotar is a CA based in the Netherlands and started its operations in 1997. The company issued three different types of certificates. These included standard certificates, qualified certificates and Dutch Government certificates, also known as *PKIOverheid* certificates. On July 19, 2011, DigiNotar detected an intrusion, after the company found a mismatch between issued certificates and its administrative records. The intrusion itself had taken place more than a week earlier, on July 10, and had allowed intruders to generate rogue certificates. DigiNotar immediately revoked the corresponding serial numbers of the known rogue certificates and subsequently assumed the incident was under control.

This assumption turned out to be ill founded when several weeks later, on August 28, 2011, the intrusion finally found its way into the public eye. The first indication of a potential problem occurred when a worried Gmail user from Iran posted a comment on a Google forum.[3] In his forum post, the user details how he tried to log in to his Gmail-account and received a warning from his browser, which happened to be Google Chrome, about the trustworthiness of the certificate. Upon verification, he discovered how the certificate indeed appeared to be fraudulent. After the online disclosure, Cert-Bund, the German Government computer emergency response team came across the forum post and notified GOVCERT.NL, its Dutch counterpart. GOVCERT.NL notified Logius, the digital government service of the Netherlands, as well as software vendors. The latter already turned out to be up to date on the breach. Subsequently, DigiNotar revoked the rogue certificate used to infiltrate Gmail communication. The revocation, however, could not undo the damage that had already been done.

In its final report, Fox-IT, the Dutch information security company in charge of the investigation, describes how "[f]or weeks the rogue certificate had been abused in a large scale Man-In-The-Middle (MITM) attack on approximately 300,000 users that were almost exclusively located in the Islamic Republic of Iran." [4] A Man-in-the-Middle Attack is a type of attack where a perpetrator inserts himself into a conversation between two parties. Through the impersonation of both parties, he gains access to information that the two parties were trying to send to each other. As a result, the traffic intended for the Google subdomains was most likely intercepted or redirected during the MITM-attack. This potentially exposed the contents of the traffic and the Google credentials of the affected users. Whilst nearly all intercepted traffic concerned users in Iran, the breach also theoretically exposed other clients to the risks of rogue certificates.

The Gmail rogue certificate turned out to be merely the tip of the iceberg. The investigation by Fox-IT revealed how all servers had been compromised, including the qualified Certificate Authority (CA) server, which DigiNotar used to issue both accredited qualified certificates and *PKIOverheid* certificates.[5] Based on its forensic investigation, Fox-IT identified a total of

[3] Alibo, "Is this MITM attack on SSL's certificate?" *Google Forum*, August 27, 2011, available at: *http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en.*
[4] Hoogstraaten, Hans and Ronald Prins, *Black Tulip Report of the investigation into the DigiNotar Certificate Authority Breach* (The Netherlands, Fox-IT BV, 2012), 3.
[5] Ibid, 5.

531 rogue certificates with 140 unique distinguished names (DNs) and fifty-three unique common names (CNs).[6] These included the following:

- 26 – *google.com
- 22 – *skype.com
- 14 – *torproject.org
- 45 – Thawte Root CA
- 20 – Comodo Root CA
- 17 – addons.mozilla.org
- 4 – update.microsoft.com
- 25 – www.cia.gov

Once the Fox-IT investigation revealed how all servers were compromised, even those generating government certificates, the DigiNotar incident quickly evolved into a disaster as the Minister found himself in front of the camera. The compromise of a server means the authenticity of a certificate issued by DigiNotar can no longer be guaranteed, which is its core business. Therefore, the brand name DigiNotar itself can no longer be trusted. Originally the government believed only parts of DigiNotar were compromised, and subsequently underestimated the potential damage caused by the breach. The conclusions of Fox-IT however compelled the government to officially revoke the trust in all certificates issued by DigiNotar. This was merely the beginning of the crisis as revocation maintained considerable consequences due to the dependency on digital certificates for a myriad of business transactions and communication.

On September 20, 2011, DigiNotar voluntarily filed for bankruptcy after the breach. Since its primary business 'product' was trust through its delivery of digital certificates, the revocation of such trust after the breach could not be repaired.

Direct 'causes'

The first question on nearly everyone's mind after a breach, especially one which takes place at a security company, is how could this have happened? As a result, once the breach became public and DigiNotar realized how the incident had not been contained, as previously thought, the company asked Fox-IT to conduct an investigation into the intrusion. The conclusions published several days later revealed how DigiNotar neglected to implement basic security measures. This section briefly summarizes those in order to provide insight into the direct 'causes' of the breach.

With regard to basic security measures, a couple of conclusions are particularly worrisome. First, anti-virus software was absent on all investigated servers. [7] This resulted in malicious software being present on critical services, which normally could have been detected by anti-virus software. Second, DigiNotar had failed to update and patch software installed on the public webservers.[8] In total, the company had ignored thirty critical updates. Both the usage of anti-virus software, as well as the installation of updates and patches are fundamental security principles, which even the general public hears on a regular basis through security awareness campaigns.

[6] Ibid, 5.
[7] Prins, J.R., *DigiNotar Certificate Authority Breach. Operation Black Tulip. Interim Report* (The Netherlands, Fox-IT BV, 2011).
[8] Ibid.

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

Other security issues include a lack of separation of critical components. All CA servers were part of a single Windows domain, which meant all could be accessed through the acquisition of one username and password combination. Simultaneously, the single password used failed to be of sufficient strength as to resist a brute-force attack.[9]

Moreover, DigiNotar failed to respond to early signals which indicated they could be part of a targeted attack. While the actual intrusion is dated to July 10, the intruders had been preparing for the attack several weeks earlier. July 10 is the date on which they were actually successful in the generation of a rogue certificate. The intruders managed to take advantage of vulnerabilities introduced through outdated software, once again a security flaw, in an effort to prepare for further intrusion into the network of DigiNotar.

The enhancement of the problem occurred in part due to a lack of direct incident notification. ENISA, the European Network and Information Security Agency, specifically identifies the lack of such notification as one of three major issues.[10] The delay in notification allowed the incident to evolve into a more significant problem since rogue certificates could be abused without the knowledge of potential victims as well as remaining clients of DigiNotar. Moreover, the lack of notification is in direct violation of legal requirements. The Dutch Telecommunications Act states how registered CAs maintain an obligation to report all changes which could be of influence to their registration. A similar notification requirement is present in the TTP.nl system (see 'Lack of oversight'), which states how "any change in organization, management, activities and/or management system during the validity of the certificate must be reported to the Certification Body without delay."[11] The requirement obliges CAs, including DigiNotar, to notify Logius of any compromises or other relevant incidents.

Underlying 'weaknesses'

Besides the direct causes, there are also underlying 'weaknesses' which indirectly facilitated the incident to both occur and subsequently evolve into a disaster. These weaknesses deserve closer inspection since they can potentially influence future scenarios, either positively or negatively depending on the (policy) response, or lack thereof. As Hallam-Baker states "[w]e need to make it more difficult for an attacker to obtain a fraudulent server credential, but we also need to address the underlying weaknesses in the applications and services that use them."[12] Many factors influenced the successful nature of the intrusion and the subsequent disaster, but the primary focus in this section is on three core aspects: lack of oversight, lack of security attention and risk awareness, and the absence of an effective mitigation strategy. Based on the research conducted by both public and private organizations, these factors are recurring themes and as such deserve the majority of our attention. The list below is not meant to be exhaustive, since many different factors 'facilitated' the incident to escalate.

---

[9] Ibid.
[10] "Operation Black Tulip: Certificate authorities lose authority," *European Network and Information Security Agency (ENISA),* 2011, available at: http://www.enisa.europa.eu/media/news-items/operation-black-tulip.
[11] "Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig Bereikt*," Qtd. in Onderzoeksraad voor de Veiligheid (OVV*), December 12, 2012, 59, available at: *http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2012/11/12/brief-met-reactie-op-rapport-het-diginotar-incident-waarom-digitale-veiligheid-de-bestuurstafel-te-weinig-bereikt.html*.
[12] Phillip Hallam-Baker, "The Changing Threat Model," Comodo Blogs, March 25, 2011, available at: *http://blogs.comodo.com/it-security/data-security/the-changing-threat-model/.*

Lack of oversight

Lack of corporate responsibility, as detailed above, was the primary cause for the breach. Such an absence, however, becomes more problematic due to a subsequent underlying weakness. There is little disagreement among those involved in researching DigiNotar about one particular underlying weakness: inadequate oversight. [13] In the Netherlands, CAs and the provision of certificates are in principle unregulated. They are theoretically in the position to regulate themselves and their business processes of applications, production and issuance of certificates. The main exception is the issuance of qualified certificates. These certificates are subject to regulatory requirements.

The 1999 European Union Electronic Signatures Directive sets out regulatory requirements for CAs that issue qualified certificates. The directive specifically contains provisions on liability and security practices.[14] Moreover, qualified certificates must also adhere to the more stringent provisions in the Dutch Telecommunications Act.[15] To obtain the legal right to issue qualified certificates, CAs must register themselves with the Onafhankelijke Post en Telecommunicatie Autoritei (OPTA), the Dutch Telecommunications Authority. DigiNotar registered itself in 2003, shortly after the implementation of the Electronic Signature Act in the Netherlands.[16]

Whilst legally speaking there are only two types of certificates, qualified certificates and other certificates, *PKIOverheid* certificates deserve specific mentioning. The introduction of Public Key Infrastructure (PKI) for the Dutch Government took place in 1999. The primary goal was to secure government communication, both within the government, between the government and its citizens, and between the government and private corporations. To assure the reliability of such communication, the government uses digital certificates better known as *PKIOverheid* certificates.

The legal requirements attached to the issuance of government certificates are more stringent than for other 'qualified' certificates. The program of requirements, which guides the regulatory scheme of the certificates and its issuance process, states how CAs must be certified in order to issue *PKIOverheid* certificates. Such certification of the company must be carried out by an external party. And a yearly audit is mandatory.[17] In 2004, DigiNotar entered the quite exclusive market of *PKIOverheid* certificates.[18]

The market to issue qualified certificates, on the other hand, is easily accessible for CAs, since it merely requires registration as opposed to certification.[19] CAs can either provide their own declaration accompanied by a supporting information file describing their compliance or they can obtain a Trusted Third Party.nl (TTP.nl) declaration. To obtain such a declaration, an accredited auditor must audit the CA. This concerns merely a management audit. The auditor investigates whether the systems of the management comply with the European Telecommunications Standards Institute (ETSI)-norm TS 101 456, which outlines policy

[13] See OVV, *Het Diginotar-incident*; Logica, *Evaluatie PKI: rapportage*, 2012. For an overview see *Kamerstukken II*, 2011 – 2012, 26 643, nr. 222.
[14] European Parliament, Council, "Directive 99/93/EC, OJ L 13/12 of 19 January 2000," *EUR-Lex*, January 19, 2000, available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:NOT*.
[15] *Kamerstukken II* 2000/01 27.743, Statute Book 2003, 199 (Electronic Signatures Act) in art, 18.15 (security requirements) and art, 18.16 (auditing obligations) of the Dutch Telecommunications Act.
[16] OVV, Het Diginotar-incident, 36.
[17] *PKIOverheid Programma van Eisen*, Appendix Evaluatie Crisis Rijksoverheid, 2012.
[18] Only 6 CAs provide *PKIoverheid* certificates.
[19] OVV, Het DigiNotar incident, 57.

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

requirements for CAs issuing qualified certificates, and all legal requirements for vendors of qualified certificates.[20]

Moreover, the CA must demonstrably possess trustworthy systems. And the CA is subject to periodic audits to determine if it complies with the ETSI norm. For the former, when CAs issue their own declarations, the OPTA engages in a marginal test to determine eligibility and for the latter, a TTP.nl declaration, the OPTA allows the company to register without any (further) investigation.

Besides this registration requirement, CAs are also subject to periodic audits carried out by a third party. For DigiNotar, the last one, before the arrival of the disaster, took place in November 2010. On paper then, inspection occurs. Even so, neither the auditors nor the Dutch Telecom Authority recognized the inadequacies of the information security practices of DigiNotar, which is an important indication of a systemic failure.

The main power rests with the corporation carrying out the audit. In the case of DigiNotar it was PricewaterhouseCoopers LLP. Unless the auditor finds reason to suspect the CA is not compliant, the OPTA remains uninvolved. As long as the CA is compliant, the company receives the TTP.nl declaration and is trusted without question by the OPTA. Yet, the issuance of such a declaration depends on open norms, since the government wanted to stimulate self-regulation in the CA market.

The main focus on self-regulation and the power granted to the TTP.nl declaration are fundamental aspects of an underlying 'weakness' with respect to inadequate oversight. The Dutch Safety Board (DSB) concludes that the parties in the system, in particular Logius and the OPTA, grant too much value and power to the TTP.nl declaration.[21] Both organizations seemingly assume, according to the DSB, that based on the declaration CAs are completely compliant with the ETSI norm and all relevant regulatory requirements. As noted by the DSB, this is not necessarily the case. The actual compliance with such requirements is only subject to a marginal test by an external auditor. The auditor merely checks whether the management system of the CA offers "justified confidence" that it is compliant with the rules. Even so, both organizations, Logius and OPTA, base their conclusions on these external audit reports. This means there is a discrepancy between the expectations of government agencies and the reality of the work carried out by external auditors.

As previously noted, much, arguably too much, value is attached to the possession of a TTP.nl declaration. The Dutch Telecommunications Act basically grants the opportunity to assume CAs are compliant with regulatory requirements based on the mere possession of the declaration. This has, according to the DSB, delegated the interpretation of and compliance with the open norms to the CA itself. Hence, the government trusts the CAs, which has led many to directly conclude there is a lack of oversight. A more accurate conclusion is that the oversight system in place is inadequate, especially considering the pivotal role played by CAs. The near blind trust placed in CAs is unjustified, even though they are information security companies. According to the DSB, considering the critical function of CAs in the overall chain of digital security, the current set-up of oversight is irresponsible.

[20] "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates," *ESTI*, May 2007, available at: *http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf.*
[21] OVV, Het DigiNotar incident, 42.

The national government audit service, *Rijksauditdienst* (RAD), also reflects on the problems with the oversight system and highlights several aspects which were missing from a more standard oversight perspective. These included the absence of a risk assessment of the different parties involved, insufficient insight into the number and types of certificates in circulation, and lack of clarity about the oversight criteria.[22] Especially the first two aspects potentially complicate the treatment of a digital disaster, since considerable time and energy must be devoted to determine who is involved and where the certificates issued by DigiNotar are located, i.e. on what sites, for what purpose. Lack of such insight made the ability to oversee and subsequently limit the damage more complex. This becomes evident in the next section.

Lack of security attention and risk awareness

Besides a lack of oversight, there was also a lack of awareness for those responsible for digital certificates. This lack of awareness is largely caused by the ongoing tension between both the possibilities of digitalization and the risks associated with increased usage, especially for government purposes. The implementation and oversight of digital certificates and overall e-government developments is largely in hands of the Ministry of the Interior and Kingdom Relations. Their priority is efficiency and convenience. Little attention is devoted to the security aspect.[23]

The DSB describes how there was little to no insight into the risks associated with a potential compromise of the reliability of digital certificates. None of the responsible parties had engaged in scenario studies to determine how digital certificates could potentially be endangered and what type of consequences this could have for the remainder of the infrastructure. The DSB specifically refers to Logius, OPTA, the Minister of the Interior and Kingdom Relations, and the Minister of Economic Affairs. Any attention they did pay to risks primarily concerned their internal operations. This leads DSB to conclude how the DigiNotar incident managed to escalate into a crisis in part due to fragmentation. The system as a whole was not kept in mind by any of the parties.

This risk awareness was present in the Dutch government, but at another organization. GOVCERT.NL, the Dutch Government Computer Emergency Response Team, was the first government party to be notified in the Netherlands. Since GOVCERT.NL's core business is security, the agency was quite well aware of risks associated with digital certificates. The lack of integration of GOVCERT.NL's knowledge and experience is particularly painful since the agency was an affiliate of Logius, before moving to the Ministry of Security & Justice when the organization evolved into the National Cyber Security Centre (NCSC) at the start of 2012. This, however, did not occur until after the DigiNotar disaster. Indeed, provider and protector were sufficiently linked as to incorporate security aspects into its service provision.

At the municipal level, similar concerns are present. Municipalities are the gateway to government services for citizens in the Netherlands. They therefore form a crucial link in the overall communication and information exchange between the government and its citizens.

---

[22] RijksAuditDienst (RAD), "De zaak 'DigiNotar': handelde de overheid adequaat? Onderzoek naar alertheid en adequaatheid van handelen van de overheid ten tijde van de 'DigiNotar'-problematiek," Rijksauditdienst Ministerie van Financien, March 8, 2012, available at: *http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/03/16/rapport-rad-onderzoek-diginotar.html.*

[23] For a more extensive and general reflection on this problem see van der Meulen, Nicole, Financial Identity Theft: Context, Challenges and Countermeasures (The Hague: TMC Asser Press, 2011), 158 – 159.

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

Interestingly, the DSB mentions in its findings how the lack of connection or integration between security and primary business processes was not noted as a risk by those interviewed.[24] The DSB itself does recognize this risk, since business processes and security yet again operate in isolation of each other. The compromise of digital certificates in this context can have considerable consequences for Dutch citizens as their confidential information can be intercepted, since they interact with local government via the electronic highway. Since Dutch users were most likely not the primary target of the attack, the odds of their confidential information having been intercepted is unlikely. Even so, the risk remains when little attention is afforded to such security since e-government transactions generally include the usage of confidential information, which can subsequently be abused for purposes of identity theft.

Lack of risk awareness and security attention return in another area as well. There is a common trend, at least in the Netherlands, for the government, either local or national, to outsource the provision of its own services. The government auditors question whether such outsourcing to private parties is desirable in all cases or whether the maintenance of services under its own wing could be preferable, especially considering the accountability from the government toward the general public.[25] The impression, according to the auditors, is that too much trust is placed in reputation and good names whilst quality received little to no attention.

Security becomes the orphan when involved parties exclusively focus on their formal role in the process and neglect to take responsibility for the security aspect of their tasks.[26] The absence of risk awareness and attention to security led to the facilitation of the DigiNotar incident and also hindered the ability to respond rapidly based on insight into the risks of CA compromises. This closely connects to the next challenge, which is the lack of an effective mitigation strategy.

Lack of mitigation strategy

Prevention is only half of the story; mitigation completes the existence of a disaster management plan. Besides a lack of oversight, security attention and risk awareness, another underlying weakness worthy to note is the lack of an existing and effective mitigation strategy. This absence is in part connected to the previous point, since a lack of risk awareness also leads to a lack of realization that a sound mitigation strategy is needed once something does go wrong in the certification process. For CAs, there was a plan in place, but one which demonstrated significant lack of insight into the potential consequences of such a plan.

The idea maintained by Logius, the responsible party, was to simply revoke its trust in all certificates issued by a compromised CA. Basically, if a CA finds itself compromised, Logius would pull the plug.[27] The consequences of such an action, however, are considerable in terms of economic damage and societal imbalance. Nearly all digital communication relies on certificates, for electronic signatures, website authenticity, etc. This was unforeseen by Logius, due to a lack of knowledge and understanding about where the certificates are located, what they are used for and how pulling the plug would maintain both economic and societal consequences. A prominent example used during the disaster management was the

[24] OVV, Het DigiNotar incident.
[25] RAD, "De zaak 'DigiNotar.'"
[26] OVV, Het DigiNotar incident, 8.
[27] Ibid.

inability to accept the delivery of imported goods in the Rotterdam Harbor. The visual of mangos rotting away was used to illustrate the point of how revoking certificates did have a physical impact. The digitalization of society implies that revoking trust in digital means leads to physical consequences, including potential damage to critical infrastructures.

The revocation of trust in certificates issued by DigiNotar allowed the incident to evolve into a disaster. The overnight conference was scheduled to report such revocation and to alert citizens who would receive a message that government websites could no longer be trusted. OPTA who perhaps sensed a considerable responsibility as a result of its poor oversight which facilitated the successful character of the intrusion, withdrew the permission of DigiNotar to issue qualified certificates. As a result of this decision, all services facilitated through DigiNotar certificates were no longer able to take place. This has led to several legal civil claims against OPTA, even by other government parties. Even the government auditor states how, whilst the OPTA decision is justifiable seen through their perspective, they should have had more attention for the continuity of service provision.[28] With better mitigation strategies and contingency planning, this part could have been better kept under control.

An alternative solution such as maintaining back-up certificates which could immediately replace the certificates which need to be revoked, was not part of the plan. This could have guaranteed a greater sense of business continuity, and still have removed a source of potential insecurity. The main problem remains that an actual compromise of a CA appeared to be largely unexpected and unanticipated. Any description of the potential of such a compromise remained restricted to theoretical vulnerabilities. The unlikeliness of an attack against an information security company has finally been removed.

Analysis: The Broader Context

The DigiNotar disaster was a painful wake-up call for the world, not just for the Dutch government. They provided the stage on which this disaster could unfold. The breach maintained considerable repercussions for various parties around the globe, especially the affected Gmail users in Iran. This demonstrates how, through the internet, fallacies in one country can lead to dire consequences somewhere else in the world. The global nature of the problem, however, is also the result of similar incidents taking place at other companies.

For anyone following the news, it is clear DigiNotar is unfortunately not an isolated incident. In the same year, the media also reported on other attacks against RSA[29] and an affiliate of Comodo, another CA.[30] Both are information security companies and they are not alone. Other examples include multiple breaches against Verisign, another CA, in 2010, which did not come into the public eye until 2012.[31] These breaches are signs of a (potential) trend. And these attacks are worrisome considering the fundamental role played by these companies in the overall cyber security landscape. The main objective in all cases was to either generate falsified certificates or to gather the necessary confidential information, as in the case of

[28] RAD, "De zaak 'DigiNotar'," 13.
[29] Elinor Mills, "RSA: Cyberattack could put customers at risk." *CNET*, March 17, 2011, available at: *http://news.cnet.com/8301-27080_3-20044455-245.html.*
[30] Phillip Hallam-Baker, "The Changing Threat Model," Comodo Blogs, March 25, 2011, available at: http://blogs.comodo.com/it-security/data-security/the-changing-threat-model/.
[31] Kim Zetter, "VeriSign Hit by Hackers in 2010," *Wired*, February 2, 2012, available at: *http://www.wired.com/threatlevel/2012/02/verisign-hacked-in-2010/.*

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

RSA, to infiltrate into the security measure and use it as a means of attack.[32] As noted in the first Cyber Security Assessment of the Netherlands, "[w]ith this in mind, security products are no longer merely a means of defense but have now become a means of attack. Because of the very fact that these products are used to secure confidential information, the impact can be major."[33] The attacks on information security companies have introduced, what I have labeled, a 'metavulnerability.' Due to the dependency of various actors, ranging from ordinary citizens to government agencies to businesses, on the products delivered by information security companies an attack on them occurs on a higher level of abstraction. It is an overarching vulnerability, where those who trust and rely on the security 'product' maintain no control. In essence, these attacks have shaken the core of digital security.

The nature of these companies is the most distinguishing feature. Often the focus of information security is on the clients of these companies, rather than the companies themselves. The general sentiment was that as long as individuals and business implemented information security tools, they maintained a sense of invincibility. Yet, these attacks force a closer inspection of the security practices maintained by information security companies, but also puts pressure on their clients, including governments, to improve parts of their operations, including oversight and disaster preparation.

Despite the crucial role played by certificates, especially with respect to communication and information exchange between various parties, including governments, citizens and corporations, these are not categorized, at least in the Netherlands, as 'critical infrastructure.' This is problematic since many other areas of society, which do receive the label of critical infrastructure, depend on certificates. As a result, the certificate infrastructure is a fundamental backbone and as such critical in its own right. This is precisely why attacks on information security companies are a worrisome development, especially for critical infrastructure protection. If the instruments used to protect our information cannot be trusted, then what alternatives exist? The answer is: Few, if any. In its final report, Fox-IT specifically notes this. The authors write, "[a]verage users and businesses will have a very limited capacity to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure."[34]

The DigiNotar incident has demonstrated how digital disasters require a different approach and significant in-depth technological knowledge in order to understand the implications. Even politicians seemingly struggled when they had to explain how serious the situation was and why the incident had been elevated to the level of a crisis. Lack of visibility enlarges the need to be aware of the risks and to devote sufficient attention to security, through the development of scenario studies and comprehensive disaster management plans. At least, through the execution of a scenario study the entire communication chain is evaluated. This means that the consequences of revocation can be tested to determine the amount and type of damage. This is subsequently vital input for the development of a disaster management plan.

[32] A connection has been drawn between the breach against RSA and the subsequent attacks against US Defense Contractor Lockheed Martin. See for example Christopher Drew and John Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed," *New York Times*, May 27, 2011, available at: *http://www.nytimes.com/2011/05/28/business/28hack.html?_r=0.*

[33] Ministry of Security & Justice, "Cyber Security Assessment Netherlands," National Coordinator for Security and Counterterrorism, September 19, 2012, available at: *http://english.nctv.nl/current_topics/Cyber_Security_Assessment_Netherlands/.*

[34] Fox-IT, Black Tulip Report, 68.

The question is not if another digital breach will occur, but rather when and who will be the next target? This demonstrates how neither the Netherlands nor DigiNotar are 'unique.'

Among the most important findings generated through the research conducted by, in particular the DSB, was the lack of administrative or executive attention for the pressing issue of digital security. Somehow security becomes only the primary object of attention for those directly involved. As such, we can speak of 'security in isolation' rather than 'security of.' The aim ought to be to move toward the latter, which forces the integration of security into ordinary business practices, which ought to assist the level of risk awareness and security attention.

Moving Forward

The DigiNotar incident has laid bare many weaknesses which must be addressed in order to reduce the probability of future scenarios and to install better coping mechanisms, through improved mitigation strategies. To improve the resilience against future intrusion, the relation between the government as protector and the government as provider must be better coordinated. The Dutch government has made such an attempt through the introduction of an awareness task force in the Ministry of the Interior and Kingdom Relations. This Ministry is traditionally known for its role as provider, especially considering the focus on e-government. Such an awareness task force aims to increase the feeling of necessity and urgency to devote as much attention to protection as it does to provision of services and reducing administrative burdens. Since the DigiNotar incident, Logius has also autonomously altered its operations. The organization, for example, now visits CAs periodically at its own initiative.[35] Still, the complexity remains of the separation of protection on the one hand, at the Ministry of Security & Justice, and provision on the other, at the Ministry of the Interior. As noted by the audit service from the national government, after DigiNotar cooperation among different government parties has received a crucial impetus. Other countries can use the experience in the Netherlands as a source of critical reflection to determine how the issue of security, in particular with respect to e-government services, is situated within their respective ministries and departments.

Closely connected is the necessity for better supervision of Trusted Third Parties. This is in large part due to the high dependency on such parties. The lack of effective oversight combined with the insufficient attention paid to security at the companies themselves has led to the introduction of a significant vulnerability. Even before the DigiNotar incident occurred, Lemos wrote "[a]s attacks on the security infrastructure increase, we must ask if the firms responsible for our safety can protect themselves, much less us."[36] This is a justified question and deserves to be asked in the context of the various successful breaches against different information security companies.

Changes in the system on a global level are also called for. ENISA even notes how there are fundamental weaknesses in the design of the Hypertext Transfer Protocol Secure (HTTPS) system. As the agency writes, "[i]n the current setup, browsers and operating systems (e.g. Microsoft's certificate store) place trust by default in a large number of CAs (hundreds) by

[35] OVV, Het DigiNotar incident.
[36] Robert Lemos, "Hackers step up attacks on security firms," March 25, 2011, available at: *http://www.infoworld.com/t/security-management/hackers-step-attacks-security-firms-803.*

http://scholarcommons.usf.edu/jss/vol6/iss2/4
DOI: http://dx.doi.org/10.5038/1944-0472.6.2.4

default, so a failure with one of them creates a risk for all users and all websites. The security of HTTPS equates to the security of the weakest CA."[37]

More focus on mitigation is also of essential value. In general, prevention is a far more popular topic in political and policy discourse than mitigation. Especially with respect to security in the counterterrorism age, prevention prevails. This exclusive focus on prevention, however, introduces problems of its own. For one, absolute security simply does not exist. As such, there are no guarantees that a compromise cannot occur. Alternative plans must therefore be in place in order to mitigate an incident and limit damages. The DSB underscores how damage reduction and recovery must also be included in whatever action plan evolves.[38]

Conclusion

DigiNotar became the first digital disaster in the Netherlands and is widely recognized as a valuable wake-up call. The forensic investigation of the breach demonstrates how DigiNotar, despite being an information security company, proved quite negligent with respect to standard security practices. As a CA responsible for the delivery of digital certificates, including certificates for the Dutch government, its compromise caused considerable damage. As a landmark case, DigiNotar has played a pivotal role in developing a greater sense of urgency surrounding digital security not only in the Netherlands, but also in other parts of the world where stakeholders are confronted with similar challenges. Moreover, the disaster has also forced the government to take a closer look at the regulatory framework of CAs and its own preparedness for digital disasters. Based on the research, the DigiNotar incident managed to evolve into a disaster in large part due to a lack of attention to risk and security awareness as well as the absence of a mitigation strategy. From a broader perspective, DigiNotar fits within a 'trend' of attacks on information security companies which has introduced the notion of a 'metavulnerability.' Where the security system in place is no longer secure, due to the insecure nature of information security companies. As Clapper notes, "[t]he compromise of U.S. and Dutch digital certificate issuers in 2011 represents a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions."[39]

As a result, considerable investments must be made to better prepare ourselves against future digital disasters, but also to consider how to deal with the aftermath. As Stewart Baker illustratively stated during a congressional hearing, "[w]e are all living in a digital New Orleans. No one really wants to spend money reinforcing the levees. But the alternative is worse."[40] While this article provides a case study of DigiNotar as a digital disaster, its experiences are of broader value for potential future scenarios in which similar disasters seem to be on the horizon. DigiNotar demonstrated how digital disasters, just as physical disasters, require better preparedness, response capacity and resilience.

[37] ENISA, Operation Black Tulip.
[38] OVV, Het DigiNotar incident.
[39] James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," January 31, 2012, available at: *http://www.fas.org/irp/congress/2012_hr/013112clapper.pdf.*
[40] Stewart Baker, "Security America's Future: The Cybersecurity Act of 2012," Testimony before the Homeland Security and Governmental Affairs Committee, *United States Senate,* February 16, 2012, 8, available at*: http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012*.