Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*

Christopher Soghoian and Sid Stamm†

"Cryptography is typically bypassed, not penetrated."
— Adi Shamir [1]

"Just because encryption is involved, that doesn't give you a talisman against a prosecutor. They can compel a service provider to cooperate."
— Phil Zimmerman [2]

Abstract

This paper introduces a new attack, the *compelled certificate creation attack*, in which government agencies compel a certificate authority to issue false SSL certificates that are then used by intelligence agencies to covertly intercept and hijack individuals' secure Web-based communications. We reveal alarming evidence that suggests that this attack is in active use. Finally, we introduce a lightweight browser add-on that detects and thwarts such attacks.

1 Introduction

A pro-democracy dissident in China connects to a secure web forum hosted on servers outside the country. Relying on the training she received from foreign human rights groups, she makes certain to look for the SSL encryption lock icon in her web browser, and only after determining that the connection is secure does she enter her login credentials and then begin to upload materials to be shared with her colleagues. However, unknown to the activist, the Chinese government is able to covertly intercept SSL encrypted connections. Agents from the state security apparatus soon arrive at her residence, leading to her arrest, detention and violent interrogation. While this scenario is fictitious, the vulnerability is not.

The security and confidentiality of millions of Internet transactions per day depend upon the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. At the core of this system are a number of *Certificate Authorities* (CAs), each of which is responsible for verifying the identity of the entities to whom they grant SSL certificates. It is because of the confidentiality and authenticity provided by the CA based *public key infrastructure* that users around the world can bank online, engage in electronic commerce and communicate with their friends and loved ones about the most sensitive of subjects without having to worry about malicious third parties intercepting and deciphering their communications.

While not known to most users, the CAs are one of the weakest links in the SSL public key infrastructure, a problem amplified by the fact that the major web browsers trust hundreds of different firms to issue certificates. Each of these firms can be compelled by their national government to issue a certificate for any particular website that all web browsers will trust without warning. Thus, users around the world are put in a position where their browser entrusts their private data, indirectly, to a large number of governments (both foreign and domestic) whom these individuals would never ordinarily trust.

In this paper, we introduces a new attack, the *compelled certificate creation attack*, in which government agencies compel (via a court order or some other legal process) a CA to issue false certificates that are then used by law enforcement and intelligence agencies to covertly intercept and hijack individuals' secure communications. As far as we are

†Both authors of this paper have written it in their personal capacities as academic researchers. All statements, opinions and potential mistakes are their own, and do not reflect the official positions of their respective employers.

aware, we are the first to formally introduce and analyze this attack in the academic literature.

We also reveal alarming evidence that suggests that this attack is more than a theoretical concern, but is in fact in active use. Furthermore, we reveal that at least one private company is supplying government customers with specialized covert network appliances specifically designed to intercept SSL communications using compelled certificates.

In order to protect users from these powerful government adversaries, we introduce a lightweight defensive browser add-on that detects and thwarts such attacks. Finally, we use reductive analysis of governments' legal capabilities to perform an adversarial threat model analysis of the attack and our proposed defensive technology. We believe that this form of legal threat model analysis is itself new to the computer security literature.

In section 2 we provide a brief introduction to CAs, web browsers and the man-in-the-middle attacks against them. In section 3 we discuss the presence of government CAs in the browsers. In 4, we introduce the compelled certificate creation attack and then in section 5, we present evidence that it is in fact being used. We also highlight in section 6 the close ties between some CAs and government agencies. In section 7 we introduce our browser based add-on, and in section 8, we analyze its effectiveness via a threat model based analysis. We conclude in section 10.

2 Certificate Authorities and the Browser Vendors

In this section, we provide a brief overview of the roles played by the Certificate Authorities in the public key infrastructure, the browser vendors in picking the certificate authorities that they include in the browsers, and existing man-in-the-middle-attack techniques that circumvent SSL based security.

2.1 Certificate Authorities

CAs play a vital role in the SSL *public key infrastructure* (PKI). Each CA's main responsibility is to verify the identity of the entity to which it issues a certificate.[1] Thus, when a user visits `https://www.bankofamerica.com`, her browser will inform her that the bank's certificate is valid, was issued by VeriSign, and that the website is run by Bank of America. It is because of the authenticity and confidentiality guaranteed by SSL that the user can continue with her transaction without having to worry that she is being phished by cyber-criminals.

CAs generally fall into one of three categories: Those trusted by the browsers ("root CAs"), those trusted by one of the root CAs ("intermediate CAs"), and those neither trusted by the browsers nor any intermediate CA ("untrusted CAs"). Furthermore, intermediate CAs do not necessarily have to be directly verified by a root CA — but can be verified by another intermediate CA, as long as the *chain of trust* eventually ends with a root CA.

From the end users' perspective, root CAs and intermediate CAs are functionally equivalent. A website that presents a certificate signed by either form of CA will cause the users' browser to display a lock icon and to change the color of the location bar. Whereas certificates verified by an untrusted CA and those self-signed by the website owner will result in the display of a security warning, which for many non-technical users can be scary [3], confusing, and difficult to bypass in order to continue navigating the site [4].

As the CA system was originally designed and is currently implemented, all root CAs are equally trusted by the browsers. That is, each of the 264 root CAs trusted by Microsoft, the 166 root CAs trusted by Apple, and the 144 root CAs trusted by Firefox are capable of issuing certificates for any website, in any country or top level domain [5]. For example, even though Bank of America obtained its current SSL certificate from VeriSign, there is no technical reason why another CA, such as GoDaddy, cannot issue another certificate for the same site to someone else. Should a malicious third party somehow obtain a certificate for Bank of America's site and then trick a user into visiting their fake web server (for example, by using DNS or ARP spoof-

[1] The level of verification performed by the CA depends upon the type of certificate purchased. A domain registration certificate can be obtained for less than $15, and will typically only require that the requester be able to reply to an email sent to the administrative address listed in the WHOIS database. Extended Validation (EV) certificates require a greater de of verification.

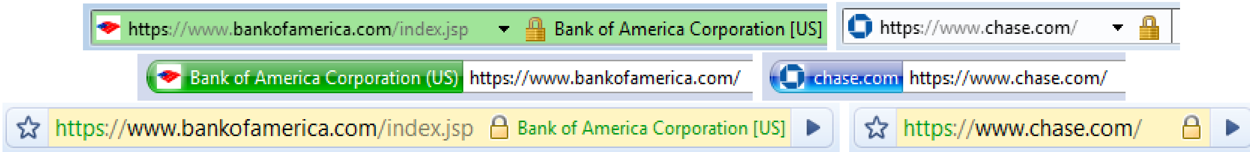


Figure 1: The browser location bars of Internet Explorer (top), Firefox (middle) and Chrome (bottom) when visiting an Extended Validation HTTPS site (Bank of America) and a site with a standard HTTPS certificate (Chase). Note that the country information ("US") presented by the browsers refers to the corporation that obtained the certificate (Bank of America), not the location of the Certificate Authority.

ing), there is no practical, easy way for the user to determine that something bad has happened, as the browser interface will signal that a valid SSL session has been established.[2]

Of course, GoDaddy is extremely unlikely to knowingly provide such a certificate to a malicious third party. Doing so would almost certainly lead to significant damage to its reputation, a number of lawsuits, as well as the ultimate threat of having its trusted status revoked by the major web browsers.[3] Therefore, it is in each CAs' self-interest to ensure that malicious parties are not able to obtain a certificate for a site not under their own control.

It is important to note that there are no technical restrictions in place that prohibit a CA from issuing a certificate to a malicious third party. Thus, both the integrity of the CA based public key infrastructure and the security users' communications depend upon hundreds of CAs around the world choosing to do the right thing. Unfortunately, as will soon be clear, any one of those CAs can become the weakest link in the chain.

[2]Even if the user examines the more complex security information listed in the browser's SSL interface, she will still lack the information necessary to make an informed trust decision. Since GoDaddy is a valid certificate authority and has issued millions of other valid certificates, there is no way for the user to determine that any one particular certificate was improperly issued to a malicious third party.

[3]The browser vendors wield considerable theoretical power over each CA. Any CA no longer trusted by the major browsers will have an impossible time attracting or retaining clients, as visitors to those clients' websites will be greeted by a scary browser warning each time they attempt to establish a secure connection. Nevertheless, the browser vendors appear loathe to actually drop CAs that engage in inappropriate behavior — a rather lengthy list of bad CA practices that have not resulted in the CAs being dropped by one browser vendor can be seen in [6].

2.2 Web Browsers

There is no technical standard that specifies how web browsers should select their list of trusted CAs. As a result, each browser vendor has created their own set of policies to evaluate and approve CAs [7, 8, 9]. Since there is no evidence to suggest that any browser has knowingly or incompetently approved a rogue CA, we do not discuss each particular vendors' policies in depth.

What does merit further attention is the method by which the browser vendors deliver and update their list of root CAs and the in-browser user interface provided to end-users to view and manage them.

The major browsers (Internet Explorer, Firefox, Chrome and Safari) have all adopted slightly different policies for managing and displaying the list of trusted CAs: Firefox is the only major browser to maintain its own database of trusted CAs, while the other three browsers instead rely upon a list of CAs provided by the operating system. However, since two of these three browser vendors are also major players in the computer operating system business, the line between browser and operating system tends to be rather blurry.

In years past, Microsoft, like the other vendors, included hundreds of CAs in its Windows operating system *Trusted Root Store*. Users who discovered the relevant user interface were able to view and manage the full list of CAs. However, in response to criticism from large enterprise customers, Microsoft reduced the number of certificates in the trusted store in subsequent OS versions down to just a handful.[4]

[4]The former product manager for Internet Explorer told us that "a very few enterprises who chose to control their own trust decisions raised concerns regarding a trusted store preloaded with 70-100 root CAs as a potential for abuse. For

It would be easy for a naive user (or security researcher) comparing the various CA databases through the user interfaces provided by Microsoft, Apple and Mozilla to conclude that Microsoft has adopted a far more cautious approach in trusting CAs than its competitors, since the user interface of a fresh installation of Windows Vista or Windows 7 will list less than 15 CAs in the operating system's Trusted Root Store. Unfortunately, this interface is extremely misleading as it does not reveal the fact that Microsoft has opted to trust 264 different CAs. The company's own documentation reveals that:

> "Root certificates are updated on Windows Vista [and Windows 7] automatically. When a user visits a secure Web site (by using HTTPS SSL) [. . .] and encounters a new root certificate, the Windows certificate chain verification software **checks the appropriate Microsoft Update location for the root certificate**. If it finds it, it downloads it to the system. To the user, the experience is seamless. **The user does not see any security dialog boxes or warnings. The download happens automatically, behind the scenes** [7]."

Thus, any web browser that depends upon Microsoft's Trusted Root Store (such as Internet Explorer, Chrome and Safari for Windows) ultimately trusts 264 different CAs to issue certificates without warning, although only a handful of them are listed in the operating system's user interface. While Microsoft clearly describes this in its online developer documentation [7], no mention of this rather important design decision is made in the browser or the operating system certificate management user interface, where interested users are most likely to look.

2.3 Man in The Middle

> "Any website secured using TLS can be impersonated using a rogue certificate issued by a rogue CA. This is irrespective of which CA issued the website's true certificate and of any property of that certificate."
> — Marc Stevens *et al* [11].

this and several other reason Microsoft has since reduced the number of root certificates in the trusted store [10]."

While an exhaustive explanation of man in the middle attacks against SSL is beyond the scope of this article, we at least provide a brief introduction to the subject. Over the past few years, the SSL protocol has been subject to a series of successful attacks by security researchers, some taking advantage of fundamental flaws in the protocol, and others focusing on social engineering and other deception based techniques [12, 13].

It is because SSL protected web connections flow over a number of other insecure protocols that it is possible for attackers to intercept and hijack a connection to a SSL protected server (these are known as *man in the middle attacks*). It is only once the browser has received and verified a site's SSL certificate that the user can be sure that her connection is safe.

However, this step alone is often not enough to protect users. Sites that supply self-signed certificates, or that exploit unpatched vulnerabilities in the certificate handling code in the browsers can still trigger the display of the SSL lock icon , yet without providing the user with the associated security protections that they would normally expect.

Security researcher Moxie Marlinspike has repeatedly attacked the SSL based chain of trust, revealing exploits that leverage both browser design flaws, as well as social engineering attacks against end-users. His *sslsniff* [14] and *sslstrip* [15] tools automate the task of performing a man-in-the-middle attacks, and when supplied with a valid SSL certificate (obtained via a rogue CA for example), can be used to intercept users' communications without triggering any browser warnings.

3 Big Brother in the Browser

Microsoft, Apple and Mozilla all include a number of national government CAs in their respective CA databases.[5] These government CAs are often included for legitimate reasons: Many governments embed cryptographic public keys in their national ID cards, or do not wish to outsource their own internal certificate issuing responsibilities to private

[5]For example, Microsoft's Root Certificate Program includes the governments of Austria, Brazil, Finland, France, Hong Kong, India, Japan, Korea, Latvia, Macao, Mexico, Portugal, Serbia, Slovenia, Spain, Switzerland, Taiwan, The Netherlands, Tunisia, Turkey, United States and Uruguay [16].

companies.

While it might be quite useful for Estonian users of Internet Explorer to trust their government's CA by default (thus enabling them to easily engage in secure online tasks that leverage their own national ID card), the average resident of Lebanon or Peru has far less to gain by trusting the Estonian government with the blanket power to issue SSL certificates for any website. Thus, users around the world are put in a position where their browser entrusts their private data, indirectly, to a number of foreign governments whom those individuals would never ordinarily trust.

As an example of what is currently possible, should it do so, the Korean Information Security Agency can create a valid SSL certificate for the Industrial and Commercial Bank of China (whose actual certificate is issued by VeriSign, USA), that can be used to perform an effective man-in-the-middle attack against users of Internet Explorer.

While this might at first seem like an extremely powerful attack, there are several reasons why governments are unlikely to use their own CAs to perform man in the middle attacks.

First, while *some* governments have convinced the browser vendors to include their CA certificates, not all governments have been able to do so. Thus, for example, the governments of Singapore, the United Kingdom and Israel (among many others) are not trusted by any of the major browsers. These governments are therefore unable to easily create their own fake certificates for use in intelligence and other law enforcement investigations where snooping on a SSL session might be useful.

Second, due to the fact that the SSL chain of trust is *non-repudiable*, any government using its own CA to issue fake certificates in order to try and spy on someone else's communications will leave behind absolute proof of its involvement. That is, if the Spanish government issues a fake certificate for Google Mail, and the surveillance is somehow discovered, anyone with a copy of the fake certificate and a web browser will be able to independently trace the botched operation back to the Spanish government.

4 Compelled Assistance

Many governments routinely compel companies to assist them with surveillance. Telecommunications carriers and Internet service providers are frequently required to violate their customers' privacy — providing the government with email communications, telephone calls, search engine records, financial transactions and geo-location information.

In the United States, the legal statutes defining the range of entities that can be compelled to assist in electronic surveillance by law enforcement[6] and foreign intelligence investigators[7] are remarkably broad.[8] Examples of compelled assistance using these statutes include a secure email provider that was required to place a covert back door in its product in order to steal users' encryption keys [2], and a consumer electronics company that was forced to remotely enable the microphones in a suspect's auto-mobile dashboard GPS navigation unit in order to covertly record their conversations [18].

Outside of the United States, and other democratic countries, specific statutory authority may be even less important. The Chinese government, for example, has repeatedly compelled the assistance of telecommunications and technology companies in assisting it with its surveillance efforts [19, 20].

Just as phone companies and email providers can be forced to assist governments in their surveillance efforts, so too can SSL certificate authorities. The *compelled certificate creation attack* is thus one in which a government agency requires a domestic certificate authority to provide it with false SSL certificates for use in surveillance.

The technical details of this attack are shockingly

[6] "An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall [...] direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted." See: 18 U.S.C. §2518(4).

[7] "An order approving an electronic surveillance under this section shall direct [...] a specified communication or other common carrier, landlord, custodian, or other specified person [...] furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance." See: 50 U.S.C. §1805(c)(2)(B).

[8] A thorough survey of the ways in which technology firms can and have been compelled to violate their customers' privacy can be found in [17].

simple, and do not require extensive explanation.[9] Each CA already has an infrastructure in place with which it is able to issue SSL certificates. In this compelled assistance scenario, the CA is merely required to skip the identity verification step in its own SSL certificate issuance process.

When compelling the assistance of a CA, the government agency can either require the CA to issue it a specific certificate for each website to be spoofed, or, more likely, the CA can be forced to issue a intermediate CA certificate that can then be re-used an infinite number of times by that government agency, without the knowledge or further assistance of the CA.

In one hypothetical example of this attack, the US National Security Agency (NSA) can compel VeriSign to produce a valid certificate for the Commercial Bank of Dubai (whose actual certificate is issued by Etisalat, UAE), that can be used to perform an effective man-in-the-middle attack against users of all modern browsers.

5 Evidence

In October 2009, one of the authors of this paper attended an invitation only conference for the surveillance and lawful interception industry in Washington, DC.[10] Among the many vendor booths on the trade show floor was Packet Forensics, an Arizona based company that sells extremely small, covert surveillance devices for networks.

The marketing materials (an excerpt of which is included in this paper as Appendix A) for the company's 5-series device reveal that it is a 4 square inch "turnkey intercept solution," designed for "defense and (counter) intelligence applications," capable of "packet modification, injection and replay capabilities" at Gb/sec throughput levels. The company proudly boasts that the surveillance device is perfect for the "Internet cafe problem." Most alarming is the device's ability to engage in active man-in-the-middle attacks:

> "Packet Forensics' devices are designed to be inserted-into and removed-from busy networks without causing any noticeable interruption [. . .] This allows you to conditionally intercept web, e-mail, VoIP and other traffic at-will, even while it remains protected inside an encrypted tunnel on the wire. Using 'man-in-the-middle' to intercept TLS or SSL is essentially an attack against the underlying Diffie-Hellman cryptographic key agreement protocol [. . .] To use our product in this scenario, [government] users have the ability to *import a copy of any legitimate key they obtain* ***(potentially by court order)*** or they can generate 'look-alike' keys designed to give the subject a false sense of confidence in its authenticity."

The company has essentially packaged *sslstrip* into a 4 square inch appliance,[11] ready for government customers to drop onto networks, at a price that is "so cost effective, they're disposable."

The company's CEO, Victor Oppelman confirmed, in a conversation with the author at the company's booth, the claims made in their marketing materials: That government customers have compelled CAs into issuing certificates for use in surveillance operations. While Mr Oppelman would not reveal which governments have purchased the 5-series device, he did confirm that it has been sold both domestically and to foreign customers.

Due to the fact that Packet Forensics' products contain encryption technology, anyone wishing to export the 5-series device to foreign countries other than Canada must submit semi-annual reports to both the US Department of Commerce, Bureau of Industry and Security and the National Security

[9] The legal issues relating to this kind of compelled assistance are far more complex. Any US government agencies compelling such CA assistance would almost certainly rely on the assistance provisions highlighted earlier. However, it is unclear if such compelled assistance would be lawful, due to the fact that it would interfere with the CA's ability to provide identity verification services. Such compelled assistance would also raise serious First Amendment concerns, due to to the fact that the government would be ordering the CA to affirmatively lie about the identity of a certificate recepient.

[10] The author caused national headlines in December of 2009, when he released an audio recording of one of the panel discussions at the same conference in which telecommunications company employees bragged about the extent of their cooperation with government agencies, including the extent to which they provide consumers' GPS location information [21, 22].

[11] It is quite possible that the company has created its own implementation of this attack, and is not using the actual sslstrip tool. We have no way of knowing what code it is shipping without a device to analyze.

Agency [23]. In late October 2009, we submitted a formal request to the Commerce Department to get a list of the foreign purchasers of Packet Forensics's 5-series device. That request has gone unanswered.

6 Some CAs Already Participate In Surveillance

Much of the power of the compelled certificate creation attack is due to the fact that it does not require the cooperation of a friendly CA. While no corporation can ultimately refuse to comply with a valid court order, firms with existing, profitable surveillance relationships with the government are perhaps less likely to vigorously fight those orders when they do come.

As such, we believe it is worthwhile to highlight the extremely close ties that several companies with CA product divisions already have to governments, and in particular, their regular involvement in and cooperation with other forms of surveillance.

6.1 VeriSign

VeriSign's certificates are used by more than one million Web servers worldwide, more than any other CA. The company claims that the world's 40 largest banks and over 95% of Fortune 500 companies choose SSL certificates from it or its subsidiaries [25]. Thus, of all the CAs, users are probably most likely to recognize VeriSign's brand name, and perhaps even associate it with secure electronic transactions.

Those few consumers who have heard of VeriSign are unlikely to know that the company is involved in a several other business areas other than its high profile sale of SSL certificates. Of particular relevance to this discussion is the VeriSign business unit used by many large telecommunications firms who have opted to outsource their own surveillance and government compliance responsibilities. VeriSign's own marketing materials describe its outsourced Communications Assistance for Law Enforcement Act (CALEA) compliance product offerings in some detail (See Figure 2), and further reveal that cable giant Cox Communications and VOIP leader Vonage are among its many satisfied corporate customers [26, 27]. A 2004 New York Times profile on the company's surveillance unit revealed that:

> "'All the costs carriers incur are ultimately going to be passed on to the consumer,' said Tom Kershaw, vice president for voice-over-Internet services at VeriSign, which provides surveillance support for Internet phone companies.
>
> To make wiretapping possible, Internet phone companies would have to buy equipment and software as well as hire technicians, or contract with VeriSign or one of its competitors. The costs could run into the millions of dollars, depending on the size of the Internet phone company and the number of government requests [28]."

We have no evidence to suggest that the CA unit within VeriSign has ever been compelled by the US government to produce a certificate for use by intelligence agencies. Likewise, we have no evidence to suggest that VeriSign has ever broken any laws, or improperly disclosed consumers' private data to government agencies.

Nevertheless, VeriSign, the largest provider of SSL certificates in the world, whose customers include many foreign banks, companies and governments from countries that do not have friendly relations with the United States, also happens to make significant sums of money by facilitating the disclosure of US consumers' private data to US government law enforcement and intelligence agencies. This fact alone may be sufficient to give some foreign organizations good reason to question their choice of CA.

6.2 Etisalat

Etisalat is the United Arab Emirates national telecommunications services provider, and operates in 17 countries across Asia, the Middle East and Africa. In addition to being the 13th largest mobile network operator in the world, the company is also an intermediate CA (trusted by the browsers via a certificate issued by root CA GTE CyberTrust).

In July 2009, approximately 100,000 UAE based BlackBerry subscribers of Etisalat received a mandatory "performance-enhancement patch" from the wireless carrier. The patch drew media attention after numerous users complained that it drained their handset battery and slowed performance [29]. After researchers examined the code,

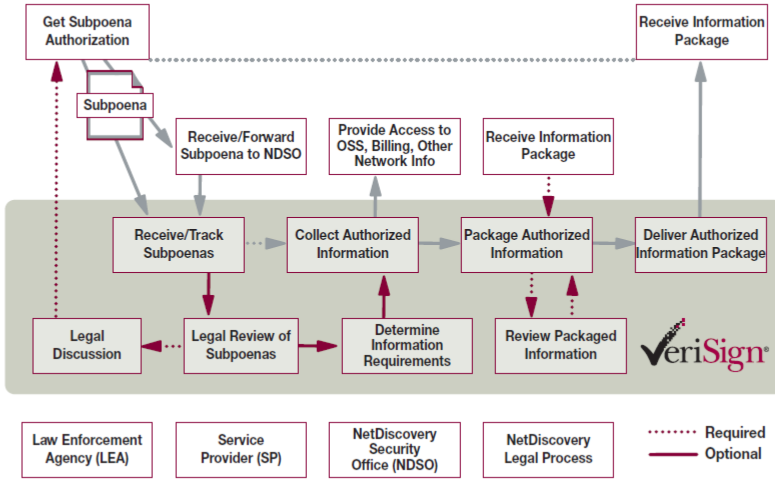


Figure 2: The process flow used by the VeriSign Security Office in handling outsourced subpoena requests (from the company's marketing materials) [24]

they discovered it actually contained surveillance software, which monitored outbound email messages and covertly sent copies of them back to a central server [30]. While Etisalat and SS8, the US based company that created and sells the surveillance software both refused to comment on the controversy, RIM (which manufacturers the Blackberry) confirmed that the software was being used to covertly monitor users and quickly released a patch to remove the spyware [31].

Again, just as with VeriSign, we have no evidence to suggest that Etisalat has ever issued an improper certificate in response to a government request. Likewise, we have no evidence to suggest that Etisalat has violated the laws of the UAE. It is quite likely that the company was compelled by the UAE authorities to deploy the surveillance software to its customers.

Nevertheless, hundreds of millions of people around the world, most of whom have never heard of Etisalat, unknowingly depend upon a company that has intentionally delivered spyware to its own paying customers, to protect their own communications security.

7 Protecting Users

The major web browsers are currently vulnerable to the compelled certificate creation attack, and we do not believe that any of the existing privacy enhancing browser add-ons can sufficiently protect users without significantly impacting browser usability. Certainly, none of the existing browser security add-ons have been designed to address this specific threat.

In an effort to significantly reduce the impact of this attack upon end-users, we have created *Certlock*, a lightweight add-on for the Firefox browser. Our solution employs a Trust-On-First-Use (TOFU) policy, reinforced with enforcement that the country of origin for certificate issuing does not change in the future. Specifically, our solution relies upon caching CA information, that is then used to empower users to leverage country-level information in order to make common-sense trust evaluations.

In this section, we will outline the motivations that impacted the design of our solution, discuss our belief in the potential for users to make wise country-level trust decisions, and then explore the technical implementation details of our prototype add-on.

7.1 Design Motivations

The compelled certificate creation attack is a classic example of a low probability, high impact event [32]. The vast majority of users are extremely unlikely to experience it, but for those who do, very bad things are afoot. As such, it is vital that any defensive technique have an extremely low false positive rate, yet be able to get the attention of users when an attempted SSL session hijacking is detected.

Most users are unlikely to know that this threat even exists, and so it is important that any protective system not require configuration, maintenance, nor introduce any noticeable latency to users' connections. Given the low likelihood of falling victim to this attack, most rational users will avoid any protective technology that requires configuration or slows down their Web browsing [33].

Furthermore, to achieve widespread adoption (even moreso if the browser vendors are to add similar functionality to their own products), any protective technology must not sacrifice user privacy for security. Information regarding users' web browsing habits should not be leaked to any third party, even if that party is 'trusted' or if it is done so anonymously. The solution must therefore be self-contained, and capable of protecting the user without contacting any remote servers.

We believe that most consumers have no idea how SSL functions, what a CA is, the role it performs, nor how many companies are trusted by their browser to issue certificates. Expecting consumers to learn about this process, or to spend their time evaluating the business practices and trustworthiness of these hundreds of firms is hopelessly unreasonable. Nevertheless, the security of the current system requires each user to make trust decisions that that they are ill equipped (nor willing) to perform.

We also believe that consumers do not directly trust CAs. Aside from the biggest CAs such as VeriSign and large telecommunications firms local to their country,[12] it is unlikely that consumers have ever heard of the vast majority of the hundreds of companies entrusted by their web browser to issue certificates. Thus, it is just as unreasonable to expect an American consumer to make a reasonable trust decision regarding a certificate issued by Polish technology firm Unizeto Technologies as it is to expect a Japanese consumer to evaluate a certificate issued by Bermuda based QuoVadis. However, both of these CAs are trusted by the major browsers, by default.

Consumers are simply told to look for the lock icon. What happens in the browser to produce that lock icon, is for all practical purposes magic. We believe that it is our responsibility as security technologists to make sure that what happens behind the scenes does in fact protect the average users' privacy and security.

This is not to say that we think that users are clueless — merely that browsers currently provide them with little to no useful contextual information without which such complex decisions are extremely difficult.

7.2 Country-Based Trust

We believe that many consumers are quite capable of making basic trust decisions based on country-level information.[13] That is, a US consumer whose banking sessions are normally encrypted by a server presenting a certificates signed by a US based CA might become suspicious if told that her US based bank is now using a certificate signed by a Tunisian, Latvian or Serbian CA.

To make this trust evaluation, she doesn't have to study the detailed business policies of the foreign CA, she can instead rely on common sense, and ask herself why her Iowa based bank is suddenly doing business in Eastern Europe. In order to empower users to make such country-level evaluations of trust, CertLock leverages the wealth of historical browsing data kept by the browser.

Individuals living in countries with laws that protect their privacy from unreasonable invasion have good reason to avoid trusting foreign governments (or foreign companies) to protect their private data. This is because individuals often receive the greatest legal protection from their own governments, and little to none from other countries. For example, US law strictly regulates the ability of the US government to collect information on US persons. However, the government can freely spy on foreigners around the world, as long as the surveillance is performed outside the US. Thus, Canadians, Swedes and Russians located outside the United States have absolutely no reason to trust the US government to protect their privacy.

Likewise, individuals located in countries with oppressive governments may wish to know if their communications with servers located in foreign democracies are suddenly being facilitated by a domestic

[12] For example, Verizon in the United States, Deutsche Telekom in Germany or Swisscom in Switzerland.

[13] However, the number of American fraud victims who continue to be tricked into sending money to scammers in Nigeria seems to suggest that not all consumers are equipped to evaluate trust based on country information.

(or state controlled) CA. Thus, for example, users in China told that their encrypted session to Google Mail is suddenly using a certificate provided by a Chinese CA are quite likely to realize that something is wrong.

7.3 Avoiding False Positives

A simplistic defensive add-on aimed at protecting users from compelled certificate creation attacks could simply cache all certificates encountered during browsing sessions, and then warn the user any time they encounter a certificate that has changed. In fact, such an add-on already exists [34].

The problem with such an approach is that it is likely to suffer from an extremely high false positive rate. Each time a website legitimately changes its certificate, the browser displays a warning that will needlessly scare and soon desensitize users. There are many legitimate scenarios where certificates change. For example: Old certificates expire; certificates are abandoned and or revoked after a data breach that exposed the server private key; and many large enterprises that have multiple SSL accelerator appliances serving content for the same domain use a different certificate for each device [35].

By adopting a Trust-On-First-Use policy, we assume that if a website starts using a different certificate issued by the same CA that issued its previous certificate, there is no reason to warn the user. This approach enables us to significantly reduce the false positive rate, while having little impact on our ability to protect users from a variety of threats.

We also believe that there is little reason to warn users if a website switches CAs within the same country. As our threat model is focused on a government adversary with the power to compel any domestic CA into issuing certificates at will, CAs within a country can essentially be seen as equals. That is, a government agency able to compel a new CA into issuing a certificate could just as easily compel the original CA into issuing a new certificate for the same site. Since we have already opted to not warn users in that scenario (described above), there is no need to warn users in the event of a same-country CA change.

By limiting the trigger of the warnings to country-level changes, we believe that we have struck a balance that will work in most situations.

7.4 Implementation Details

Our Certlock solution is currently implemented as an add-on to the Firefox browser.

The Firefox browser already retains history data for all visited websites. We have simply modified the browser to cause it to retain slightly more information. Thus, for each new SSL protected website that the user visits, a Certlock enabled browser also caches the following additional certificate information:

A hash of the certificate.
The country of the issuing CA.
The name of the CA.
The country of the website.
The name of the website.
The entire chain of trust up to the root CA.

When a user re-visits a SSL protected website, Certlock first calculates the hash of the site's certificate and compares it to the stored hash from previous visits. If it hasn't changed, the page is loaded without warning. If the certificate has changed, the CAs that issued the old and new certificates are compared. If the CAs are the same, or from the same country, the page is loaded without any warning. If, on the other hand, the CAs' countries differ, then the user will see a warning (See Figure 3).

At a high level, this algorithm is quite simple. However, there are a few subtle areas where some complexity is required.

Because governments can compel CAs to create both regular site certificates as well as intermediate CA certificates, any evaluation of a changed site certificate must consider the type of CA that issued it.

While the web browser vendors do not vouch for the trustworthiness of any of the root CAs that they include, we believe it is reasonable to assume that the browser vendors do at least verify the country information listed in each of their root CAs. Therefore, we are able to trust this information as we evaluate changed certificates.

When Certlock detects a changed certificate, it must also determine the type of CA that issued the new certificate. If the new certificate was issued by a root CA, then Certlock can easily compare the country of the old certificate's CA to the country of the new root CA. However, if the new certificate was issued by an intermediate CA, then we have

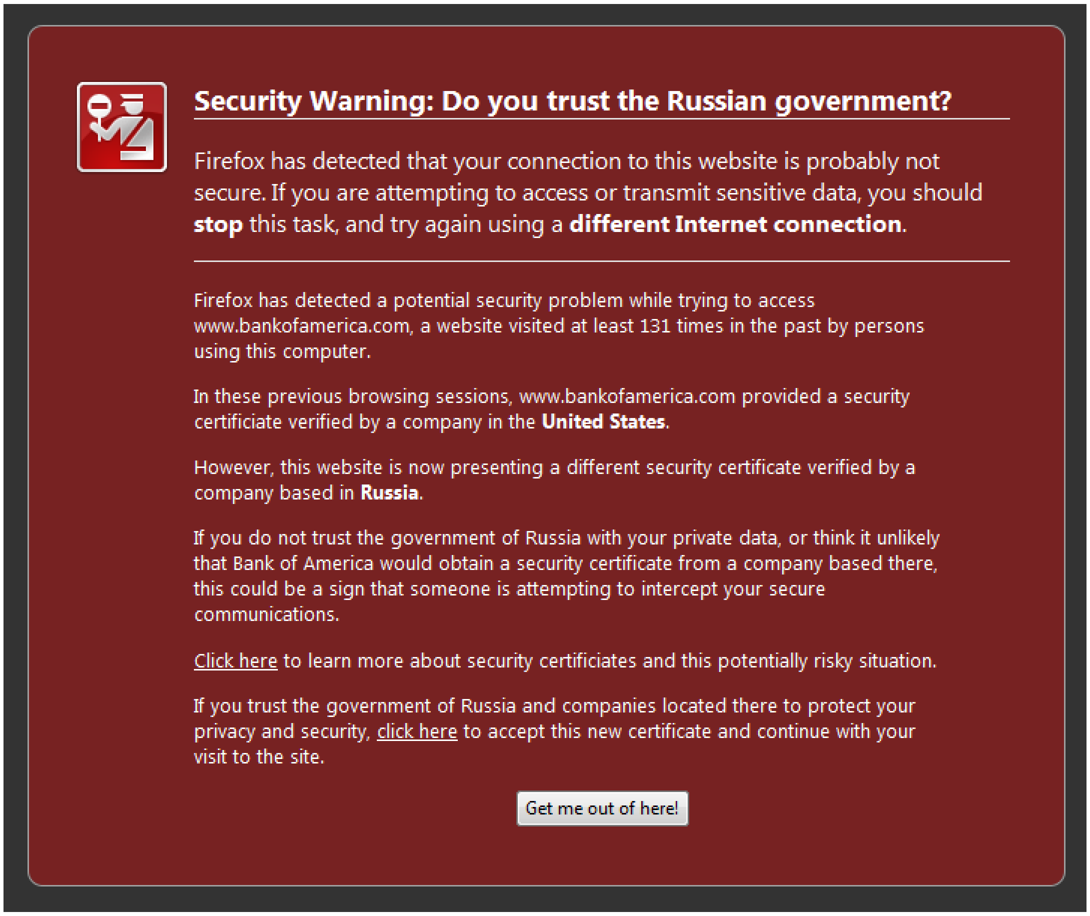


Figure 3: The warning displayed to users of Certlock.

no way of verifying that the issuing CA's country information is accurate.

As an example, the Israeli government could compel StartCom, an Israeli CA to issue an intermediate CA certificate that falsely listed the country of the intermediate CA as the United States. This rogue intermediate CA would then be used to issue site certificates for subsequent surveillance activities. In this hypothetical scenario, let us imagine that the rogue CA issued a certificate for Bank Of America, whose actual certificate was issued by VeriSign in the United States. Were CertLock to simply evaluate the issuing CA's country of the previously seen Bank of America certificate, and compare it to the issuing country of the rogue intermediate CA (falsely listed as the United States), CertLock would not detect the hijacking attempt. In order to detect such rogue intermediate CAs, a more thorough comparison must be conducted.

Thus, in the event that a new certificate has been issued by an intermediate CA, Certlock follows the chain of trust up to the root CA, noting the country of every CA along the path. If any one of these intermediate CAs (or the root CA itself) has a different country than the CA that issued the original certificate, then the user is warned.

8 Analysis

In this section, we outline several potential scenarios in which a government might wish to spy on a suspect's secure communications. In each example scenario, we examine the government's available surveillance options, consider the suitability of the compelled certificate creation attack, and evaluate the ability of CertLock to detect and thwart the attack.

8.0.1 Scenario A

Actual CA	VeriSign (USA)
Compelled CA	VeriSign (USA)
Website	Citibank (USA)
Location of Suspect	USA
Surveilling Government	USA

In this scenario, the United States government compels VeriSign to issue a certificate for use by a law enforcement agency wishing to spy on communications between a suspect located in the United States and Citibank, her United States based bank.

This attack is impossible for CertLock to detect, because the CA issuing the fake certificate is also the same that issued the legitimate certificate. However, we believe that this scenario is extremely unlikely to occur in the investigations of end users. This is because if a government adversary is able to obtain a court order compelling VeriSign's cooperation, it can just as easily obtain a court order compelling Citibank to disclose the suspect's account information.[14]

8.0.2 Scenario B

Actual CA	VeriSign (USA)
Compelled CA	GoDaddy (USA)
Website	Citibank (USA)
Location of Suspect	USA
Surveilling Government	USA

In this scenario, the United States government compels GoDaddy, a CA located in the United States to issue a certificate for an intelligence agency wishing to spy on communications between a suspect located in the United States and a bank also located in the United States (CitiBank), which obtained its legitimate SSL certificate from VeriSign.

Just as with Scenario A, this attack is extremely unlikely to occur. This is because any government agency able to compel GoDaddy is also capable of obtaining a court order to compel VeriSign or Bank of America. By simple reduction, any attacker capable of Scenario B is also capable of Scenario A. CertLock does not detect attacks of this type.

[14]While there are perhaps a couple volunteer run Internet providers that will do anything possible to avoid delivering user data to the government, including shutting down their servers, we believe that the vast majority of corporations will not refuse to comply. Our threat model specifically excludes this rare former category, and instead focuses on the corporations that provide services to most users.

8.0.3 Scenario C

Actual CA	VeriSign (USA)
Compelled CA	VeriSign (USA)
Website	*Poker.com* (USA)
Location of Suspect	USA
Surveilling Government	USA

In this scenario, US law enforcement agents are investigating a US-based online gambling website and the US-based users of the service. The agents wish to first obtain evidence that illegal activity is occuring, by monitoring the bets as they are placed via SSL encrypted sessions, before they later raid the offices of the company and seize their servers. In order to surveil the communications between users and the gambling website, law enforcement officials compel VeriSign to issue an additional certificate for the site, which is then used to intercept all communications to and from the website.

In this scenario, where both ends of the SSL connection are under investigation by the government, the compelled certificate attack is a highly effective method for covertly gathering evidence. However, because the issuing CA does not change, CertLock is unable to detect this attack and warn users.

In general, attack scenarios in which both the end-user and the website are under surveillance are beyond the scope of our threat model.

8.0.4 Scenario D

Actual CA	VeriSign (USA)
Compelled CA	CNNIC (China)
Website	CCB (China)
Location of Suspect	China
Surveilling Government	China

In this scenario, a resident of China is accessing her China Construction Bank online account, which obtained its legitimate SSL certificate from VeriSign, a US firm. The Chinese intelligence services are interested in getting access to the suspect's online transaction data, and thus seeks to compel the China Internet Network Information Center (CNNIC), a domestic CA to issue a certificate for the surveillance operation.

This scenario is not identical to scenario A, however it is quite similar. Again, if the Chinese government is able to compel a domestic CA into assisting it, we assume that it could just as easily compel the Chinese bank into providing the suspect's account details. While we believe that this attack scenario is unlikely, should it occur, CertLock will detect it.

8.0.5 Scenario E

Actual CA	VeriSign (USA)
Compelled CA	CNNIC (China)
Website	Google Mail (USA)
Location of Suspect	China
Surveilling Government	China

In this scenario, a US executive is travelling in China for business, and is attempting to access her secure, US-based webmail account using the Internet connection in her hotel room. Chinese authorities wish to intercept her communications, but due to Google's use of SSL by default for all webmail communications [36], the government must employ a man-in-the-middle attack. This scenario is thus an ideal candidate for a compelled certificate creation attack, since the Chinese authorities have no leverage to compel the assistance of Google or VeriSign. This scenario is also one that is easily detected by CertLock.

8.0.6 Scenario F

Actual CA	VeriSign (USA)
Compelled CA	VeriSign (USA)
Website	CCB (China)
Location of Suspect	USA
Surveilling Government	USA

In this scenario, a Chinese executive is travelling in the United States for business, and is attempting to acccess her China Construction Bank account using the Internet connection in her hotel room. US Government authorities wish to get access to her financial records, but are unwilling to let the Chinese government know that one of their citizens is under investigation, and so have not requested her records via official law enforcement channels.

This scenario is almost identical to scenario E, however, there is one key difference: The legitimate certificate used by the Chinese bank was issued by a CA located in the United States and the US government has turned to the same US based CA to supply it with a false certificate. Thus, while this scenario is an ideal candidate for a compelled certificate creation attack, it is not one that can easily be detected by looking for country-level CA changes. As such, CertLock is not able to detect attacks of this type.

8.1 America's Surveillance Advantage

As described above, there is one scenario in which users are not protected by our country-notification based system. When organizations obtain SSL certificates from a foreign CA, they expose their users to highly effective surveillance performed by government agencies in that same foreign country. Unfortunately, this scenario is far from hypothetical — since American CAs totally dominate the certificate market, and are used by many foreign organizations.

As just one example — a number of the big banks in Pakistan, Lebanon and Saudi Arabia (countries in which the US has a strong intelligence interest) all use VeriSign issued certificates for their online banking servers.

As long as foreign websites continue to rely on SSL certificates issued by CAs located in the United States, the US government will maintain the ability to perform man in the middle attacks that are practically impossible to detect. Fixing this flaw is beyond the scope of this paper, but luckily, organizations can easily address it themselves — by switching to a domestic CA (or at least one located in a country whose government they trust).

9 Related Work

Kai Engert created Conspiracy, a Firefox add-on that provides country-level CA information to end-users in order to protect them from compelled certificate creation attacks. The Conspiracy tool displays the flag of the country of each CA in the chain of trust in the browser's status bar [37]. Thus, users must themselves remember the country of the CAs that issue each certificate, and detect when the countries have changed. We believe that this is an unreasonable burden to place upon end-users, particularly given how rarely the compelled certificate creation attack is likely to occur.

Wendlandt *et al.* created the Perspectives, a Firefox add-on that improves the Trust-On-First-Use model used for websites that supply self-signed SSL certificates [38]. In their system, the user's browser securely contacts one of several notary servers, who in turn independently contact the webserver and obtain its certificate. In the event that an attacker is attempting to perform a man in the middle attack upon the user, the fact that the attacker-supplied SSL certificate, and those supplied by the Perspectives notary servers differ will be a strong indicator that something bad has happened.

Unfortunately, the Perspectives system requires that users provide the Perspectives notaries with a real-time list of the secure sites they visit.[15] Although the scheme's designers state that "all servers adhere to a strict policy of never recording client IP addresses, period," we still don't think it is a good idea to provide users' private web browsing data to a third party, merely based on the fact that they promise not to log it.

Alicherry and Keromytis have improved upon the Perspectives design with their DoubleCheck system [39], substituting Tor exit nodes for special notary servers. Because the Tor network anonymizes the individual user's IP address, there is no way for the Tor exit nodes to know who is requesting the certificate for a particular SSL website. While the authors solved the major privacy issues that plague the Perspectives scheme, their choice of Tor carries its own cost: Latency. Their system adds an additional second of latency to every new SSL connection, and up to 15 seconds for visits to new self-signed servers. We believe that this additional latency is too much to ask most users to bear, particularly if the chance of them encountering a rogue CA is so low.

In May 2008, a security researcher discovered that the OpenSSL library used by several popular Linux distributions was generating weak cryptographic keys. While the two-year old flaw was soon fixed, SSL certificates created on computers running the flawed code were themselves open to attack [40, 41]. Responding to this flaw, German technology magazine Heise released the Heise SSL Guardian for the Windows operating system, which warns users of Internet Explorer and Chrome when they encounter a weak SSL certificate [42].

In December 2008, Stevens *et al* demonstrated that flaws in the MD5 algorithm could be used to create rogue SSL certificates (without the knowledge or assistance of the CA). In response, CAs soon accelerated their planned transition to certificates using the SHA family of hash functions [11]. As an additional protective measure, Márton Anka developed an add-on for the Firefox browser to detect and warn users about certificate chains that use the MD5 algorithm for RSA signatures [43].

[15] Modern browsers already leak information about the secure web sites that users visit, as they automatically contact CAs in order to verify that the certificates have not been revoked (using the OCSP protocol). While this is currently unavoidable, we wish to avoid providing private user web browsing data to any additional parties.

10 Conclusion and Future Work

In this paper, we introduced the compelled certificate creation attack and revealed alarming evidence that suggests that governments are actually subverting the CA based public key infrastructure. In an effort to protect users from these powerful adversaries, we introduced a lightweight defensive browser based add-on that detects and thwarts such attacks. Finally, we use reductive analysis of governments' legal capabilities to perform an adversarial threat model analysis of the attack and our proposed defensive technology.

Our browser add-on is currently just a prototype, and we plan to improve it in the future. First, our currently used warning dialog text is far from ideal, and could be greatly improved with the help of usability and user experience experts. We also plan to explore the possibility of expanding the country-level trust model to regions, such as the European Union, where, for example, residents of France may be willing to trust Spanish CAs. Finally, We are considering adding a feature that will enable users to voluntarily submit potentially suspect certificates to a central server, so that they can be studied by experts. Such a feature, as long as it is opt-in, does not collect any identifiable data on the user, and only occurs when potentially rogue certificates are discovered, would have few if any privacy issues.

Ultimately, the threats posed by the compelled certificate creation attack cannot be completely eliminated via our simple browser add-on. The CA system is fundamentally broken, and must be overhauled. DNSSEC may play a significant role in solving this problem, or at least reducing the number of entities who can be compelled to violate users' trust. No matter what system eventually replaces the current one, the security community must consider compelled government assistance as a realistic threat, and ensure that any solution be resistant to such attacks.

11 Acknowledgements

Thanks to Kevin Bankston, Matt Blaze, Jon Callas, Allan Friedman, Jennifer Granick, Markus Jakobsson, Dan Kaminsky, Moxie Marlinspike, Adam Shostack for their useful feedback.

References

[1] Adi Shamir. Cryptography: State of the science. *ACM A. M. Turing Award Lecture*, June 8 2003. awards.acm.org/images/awards/140/vstream/2002/S/s-pp/shamir_1files_files/800x600/Slide8.html.

[2] Ryan Singel. PGP Creator Defends Hushmail. *Wired News Threat Level Blog*, November 19 2007. www.wired.com/threatlevel/2007/11/pgp-creator-def.

[3] Johnathan Nightingale. SSL Question Corner. *meandering wildly (blog)*, August 5 2008. blog.johnath.com/2008/08/05/ssl-question-corner/.

[4] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the 18th Usenix Security Symposium*, August 2009.

[5] Ed Felten. Web Certification Fail: Bad Assumptions Lead to Bad Technology. *Freedom To Tinker*, February 23 2010. www.freedom-to-tinker.com/blog/felten/web-certification-fail-bad-assumptions-lead-bad-technology.

[6] Mozilla. Potentially problematic CA practices , 2010. wiki.mozilla.org/CA:Problematic_Practices.

[7] Microsoft Root Certificate Program, January 15 2009. technet.microsoft.com/en-us/library/cc751157.aspx.

[8] Mozilla CA Certificate Policy (Version 1.2). www.mozilla.org/projects/security/certs/policy/.

[9] Apple Root Certificate Program. www.apple.com/certificateauthority/ca_program.html.

[10] Craig Spiezle. Email conversation with author, February 15 2010.

[11] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne Weger. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, pages 55–69, Berlin, Heidelberg, 2009. Springer-Verlag.

[12] Marsh Ray and Steve Dispensa. Renegotiating tls, November 4 2009. extendedsubset.com/wp-uploads/2009/11/renegotiating_tls_20091104_pub.zip.

[13] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 51–65, Washington, DC, USA, 2007. IEEE Computer Society.

[14] Moxie Marlinspike. sslsniff, July 3 2009. www.thoughtcrime.org/software/sslsniff/.

[15] Moxie Marlinspike. sslsniff, December 18 2009. www.thoughtcrime.org/software/sslstrip/.

[16] Windows Root Certificate Program Members, November 24 2009. download.microsoft.com/download/1/4/f/14f7067b-69d3-473a-ba5e-70d04aea5929/windows\%20root\%20certificate\%20program\%20members.pdf.

[17] Christopher Soghoian. Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era. In *Journal on Telecommunications and High Technology Law*, Forthcoming.

[18] Declan McCullagh. Court to FBI: No spying on in-car computers. *CNET News*, November 19 2003. news.cnet.com/2100-1029_3-5109435.html.

[19] John Markoff. Surveillance of skype messages found in china. *The New York Times*, October 1 2008. www.nytimes.com/2008/10/02/technology/internet/02skype.html.

[20] Andrew Jacobs. China requires censorship software on new pcs. *The New York Times*, June 8 2009. www.nytimes.com/2009/06/09/world/asia/09china.html.

[21] Christopher Soghoian. 8 Million Reasons for Real Surveillance Oversight. *Slight Paranoia blog*, December 1 2009. paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html.

[22] Kim Zetter. Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year. *Wired News Threat Level Blog*, December 1 2009. www.wired.com/threatlevel/2009/12/gps-data/.

[23] Packet Forensics. Export and Re-Export Requirements, 2009. www.packetforensics.com/export.safe.

[24] VeriSign. Netdiscovery service subpoena processing and handling, 2004. www.verisign.com/stellent/groups/public/documents/data_sheet/001928.pdf.

[25] Why VeriSign. www.verisign.com/ssl/why-verisign/index.html.

[26] VeriSign Case Study. VeriSign helps an innovative broadband telephony provider focus on core business goals, October 16 2006. www.verisign.com/static/039933.pdf.

[27] VeriSign. Cox communications: Complying with CALEA regulations in a cost-effective manner, while expanding services, 2004. www.verisign.com/stellent/groups/public/documents/success_stories/002378.pdf.

[28] Ken Belson. The call is cheap. the wiretap is extra.; enlisting internet phones in the battle against crime. *The New York Times*, August 23 2004. www.nytimes.com/2004/08/23/business/call-cheap-wiretap-extra-enlisting-internet-phones-battle-against-crime.html.

[29] Kim Zetter. Researcher: Middle East Blackberry Update Spies on Users. *Wired News Threat Level Blog*, July 14 2009. www.wired.com/threatlevel/2009/07/blackberry-spies/.

[30] Chris Eng. BlackBerry Spyware Dissected. *Veracode: Zero in a bit*, July 15 2009. www.veracode.com/blog/2009/07/blackberry-spyware-dissected/.

[31] RIM. RIM Customer Statement Regarding Etisalat / SS8 Software, July 19 2009. www.securityprivacyandthelaw.com/uploads/file/RIM%20Statement.pdf.

[32] Matthieu Bussiere and Marcel Fratzscher. Low probability, high impact: Policy making and extreme events. *Journal of Policy Modeling*, 30(1):111–121, 2008.

[33] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW '09: Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, September 2009.

[34] Certificate patrol, 2010. patrol.psyced.org/.

[35] Dan Kaminsky. Email conversation with author, February 28 2010.

[36] Sam Schillace. Default https access for Gmail. *The Official Gmail Blog*, January 12 2010. gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html.

[37] Kai Engert. Conspiracy — A Mozilla Firefox Extension, March 18 2010. kuix.de/conspiracy/.

[38] Dan Wendlandt, David G. Andersen, and Adrian Perrig. Perspectives: improving ssh-style host authentication with multi-path probing. In *ATC'08: USENIX 2008 Annual Technical Conference on Annual Technical Conference*, pages 321–334, Berkeley, CA, USA, 2008. USENIX Association.

[39] Mansoor Alicherry and Angelos D. Keromytis. Doublecheck: Multi-path verification against man-in-the-middle attacks. In *ISCC 2009: IEEE Symposium on Computers and Communications*, pages 557–563, Piscataway, NJ, USA, 2009. IEEE.

[40] David Ahmad. Two Years of Broken Crypto: Debian's Dress Rehearsal for a Global PKI Compromise. *IEEE Security and Privacy*, 6:70–73, September 2008.

[41] Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage. When private keys are public: results from the 2008 Debian OpenSSL vulnerability. In *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, pages 15–27, New York, NY, USA, 2009. ACM.

[42] The H Security. heise SSL Guardian: Protection against unsafe SSL certificates, July 4 2008. `www.h-online.com/security/features/Heise-SSL-Guardian-746213.html`.

[43] Márton Anka. SSL Blacklist 4.0, January 31 2010. `www.codefromthe70s.org/sslblacklist.aspx`.

A Appendix

The following two scanned pages are a limited portion of Packet Forensics' marketing materials, sufficient to document the product's features and the company's statements. We believe that our inclusion of this content for scholarly purposes is solidly protected by fair use.

Technical Details

Man-in-the-Middle Capabilities

Intercept any communication within Secure Socket Layer (SSL) or Transport Layer Security (TLS) sessions

All Packet Forensics targeting and policy capabilities can operate within the encrypted tunnel

Operational Configurations

In-line with hardware bypass / failsafe

Import any certificate / public key or generate your own for presentation

Availability

Available in firmware releases after August 31st, 2009 for all Packet Forensics platforms

Available under customization program

Contacts

Offices in Virginia and Arizona, USA

Headquarters

420 S Smith Rd

Tempe, AZ 85281

United States of America

Telephone & E-mail

Domestic US +1 (800) 807 6140

International +1 (757) 320 2002

salesteam@packetforensics.com

PACKET FORENSICS

HOW DOES IT WORK?

Deployment and Capabilities

Just as it sounds, engaging in a man-in-the-middle attack requires the interception device to be placed in-line between the parties to be intercepted at some point in the network. This could be at the subscribers' telecom operator or even on-premises, close to the subject. Packet Forensics' devices are designed to be inserted-into and removed-from busy networks without causing any noticeable interruption. Even the failure of a device due to power loss or other factors is mitigated by our hardware bypass fail-safe system. Once in place, devices have the capability to become a go-between for any TLS or SSL connections in addition to having access to all unprotected traffic. This allows you to conditionally intercept web, e-mail, VoIP and other traffic at-will, even while it remains protected inside an encrypted tunnel on the wire. All the same capabilities as other Packet Forensics products are still available, including the ability to extract pen/trap details only.

Technical Considerations: PKI

Using "man-in-the-middle" to intercept TLS or SSL is essentially an attack against the underlying Diffie-Hellman cryptographic key agreement protocol. To protect against such attacks, public key infrastructure ("PKI") is often used to authenticate one or more sides of the tunnel by exchanging certain keys in advance, usually out-of-band. This is meant to provide assurance that no one is acting as an intermediary. Secure web access (HTTP-S) is the best example of this, because when an unexpected key is encountered, a web browser can warn the subject and give them an opportunity to *accept* the key or *decline* the connection.

To use our product in this scenario, users have the ability to import a copy of any legitimate key they obtain (potentially by court order) or they can generate "look-alike" keys designed to give the subject a false sense of confidence in its authenticity.

Of course, this is only a concern for communications incorporating PKI. For most other protocols riding inside TLS or SSL tunnels—where no PKI is employed—interception happens seamlessly without any subscriber knowledge or involvement.

HOW CAN YOU USE IT?

Government Security

IP communications adoption dictates the need to examine encrypted traffic at-will, especially transiting government networks.

Investigations

Your investigative staff will likely collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VoIP encryption.

Product Testing and Evaluation

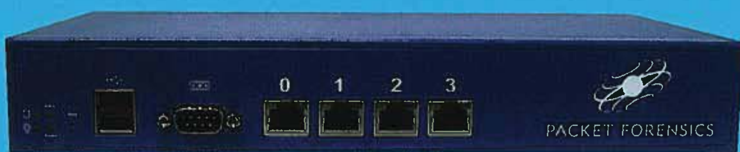
All network products should be tested diligently for phone-home capabilities with encryption.

PACKET FORENSICS

SMALL DEVICES. BIG OPPORTUNITIES.

INTRODUCING THE 5-SERIES

Packet Forensics 5-Series are the most flexible tactical surveillance devices in the world of IP networks. Designed for defense and (counter) intelligence applications, they are fully-embedded without moving parts and available in a variety of sizes, shapes and power footprints, all customized for the client. In under five minutes, they can be configured and installed in-line without knowledge of existing network topology. **Capabilities include:** Keyword, RADIUS, DHCP and **behavior-based** session identification; filtering, modification and injection of packets; compatibility with existing collection systems. With this modular platform, Packet Forensics creates **mission packages** based on customer requirements. Best of all, they're so cost effective, they're disposable--that means less risk to personnel.



Introduction

The 5-Series is a turnkey intercept solution in an appliance platform. Offering the most flexible approach to network surveillance and novel approaches to rapid deployment and stealthy reporting of captured data, the 5-Series devices are unmatched in the industry.

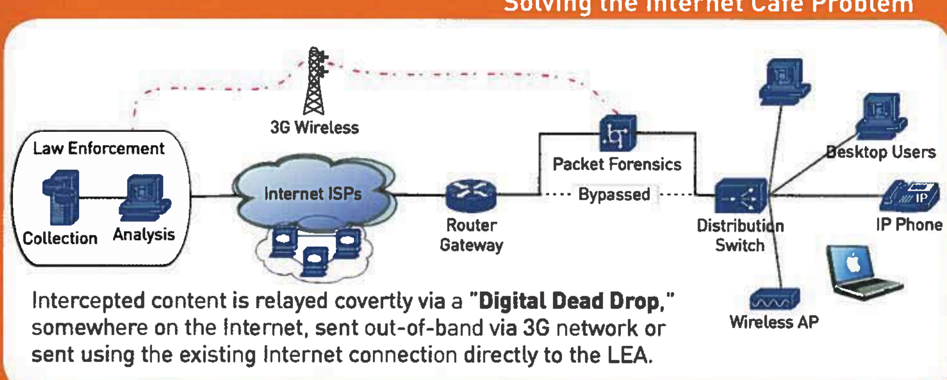
An attractive feature of the 5-Series is its ability to passively discover network toplogy--this allows an individual to deploy it with no prior knowledge of the target network. The device can be placed in-line and immediately act as a passive bridge while performing its mission. As intelligence is being gathered and the device has an understanding of the network, it uses its stealth reporting techniques to return captured information or accomplish a variety of other missions.

The 5-Series has no MAC address or IP address; it dynamically masquerades as the most appropriate host that sits topologically behind it. The 5-Series can be used to intercept and record matching sessions to internal flash-memory, or report them upstream using a variety of protocols. In the most hostile environments, this upstream reporting can be accomplished using a technique that makes the 5-Series' presence undetectable using standard network security methods.

The Internet Cafe

The 5-Series is an ideal solution to the "Internet Cafe Problem." Quick deployment and remote control minimize personnel risk and maximize collection capabilities. Small footprint and minimal power requirements make installation easy.

Solving the Internet Cafe Problem



Intercepted content is relayed covertly via a **"Digital Dead Drop,"** somewhere on the Internet, sent out-of-band via 3G network or sent using the existing Internet connection directly to the LEA.

Key Advantages

- **Customized** mission packages
- Small form-factor, solid-state (as small as 4 square inches)
- No moving parts, highly reliable
- Battery, PoE or wired power
- Hardware bypass, fail-safe
- Tamper detection, fail-secure
- Up to Gb/sec throughput
- Deployable with **no knowledge of target network topology**
- Supports **stealth upstream reporting** (practically **undetectable**)
- **"Digital Dead Drop"** delivery
- Triggers intercepts based on **keywords, RADIUS, DHCP, behavior** or other subject criteria
- **Probe** and **Mediation** capabilities
- Performs **dialed digit extraction**
- Packet **modification, injection** and **replay** capabilities
- Packet Forensics software stack and PeerTalk™ technology
- Advanced firmware-update keeps software up-to-date