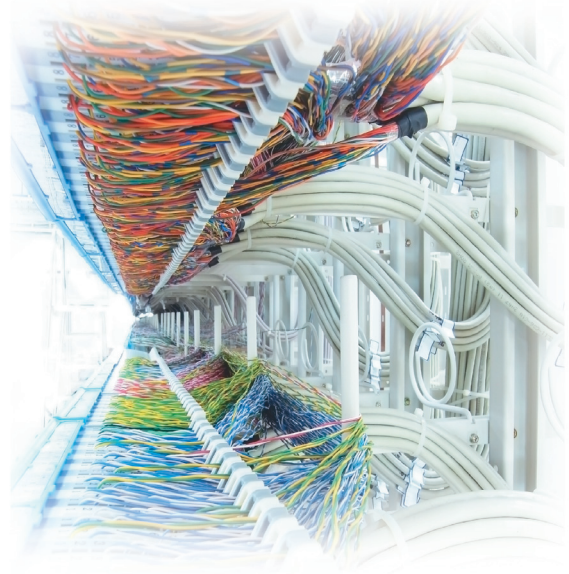


# Internet Security under Attack: The Undermining of Digital Certificates

Neal Leavitt



Several attacks this year against organizations issuing digital certificates are creating doubts about the system.

**F**or almost 20 years, digital certificates have been a key aspect of Internet security.

The certificates—detailed in the “The Digital Certificate” sidebar—are designed to establish the credentials of people doing business or otherwise communicating on the Web and to verify that they are who they say they are.

However, several attacks this year by a hacker against organizations issuing certificates are creating doubts about Internet communications’ safety in general and the digital-certificate model’s integrity in particular. The attacker tried to break into at least three certificate authorities’ systems and succeeded with two of the CAs.

The hacker then created fake certificates that looked as if they came from well-known, trusted companies, and utilized them to entice users to participate in communications. This made them vulnerable to attack or the theft of personal data.

“The capture of sensitive data such as account numbers and passwords can result in severe problems for users, the impersonated company, and the certificate authority,” said

Richard Martinez, network security research analyst for market-research firm Frost & Sullivan.

Carnegie Mellon University (CMU) computer science professor David Andersen observed, “The entire system is only as strong as the weakest CA.”

Moreover, noted Ed Moyle, principal analyst for market-research firm Security Curve, the devices used by CAs to approve and issue certificate requests are just computers and as such, can be attacked.

The attacks this year “were a warning sign for all players in this field,” said Eddy Nigg, chief operating officer and chief technology officer of StartCom, which is a CA.

## HACKING THE CERTIFICATE SYSTEM

At least three attacks were made during the past 12 months against CAs. Those against Comodo and DigiNotar were successful; the one against StartCom was not.

All were made by a hacker known as both Ich Sun and Comodohacker. Evidence indicates the attacks came from an Iranian IP address.

### Comodo

On 23 March, Ich Sun hacked into an Italian reseller of Comodo’s digital certificates. Determining exactly how this occurred is difficult, said Comodo vice president and principal scientist Phillip Halam-Baker.

The attacker used the reseller’s credentials to request digital certificates from Comodo. Ich Sun then made the certificates look as if they were those used by various high-profile websites.

Within hours, Comodo detected the problem, revoked the fake certificates, and notified its customers.

### DigiNotar

Security experts are unsure exactly how Ich Sun compromised DigiNotar’s system but have said that it had several important vulnerabilities.

For example, the company operated an external Windows network—unprotected by antivirus software or a system for detecting brute-force password-cracking attacks—that was connected to its secure servers, explained Simon Heron, a director and security analyst with Internet security firm Network Box UK.

## THE DIGITAL CERTIFICATE

**C**ryptographic researchers Martin Hellman and Whitfield Diffie first proposed a digital-signature procedure in 1976.

The following year, Massachusetts Institute of Technology researchers Ron Rivest, Adi Shamir, and Leonard Adleman created the first public-key algorithm, the RSA cryptosystem.

The first digital certificates were based on the X.509 standard, which the International Telecommunication Union's Telecommunication Standardization Sector adopted in 1988.

X.509 didn't become a key aspect of security, though, until it started being used with Secure Sockets Layer technology.

Netscape developed SSL in the mid-1990s. The Internet Engineering Task Force released SSL's successor, Transport Layer Security (TLS), in 1999.

### PKI

Using the public, unsecured Internet for secure transactions is a challenge.

The public-key infrastructure, including the use of digital certificates, is one approach to providing online security.

In PKI, senders apply to a certificate authority for a digital certificate. Upon verifying the sender's identity, the CA—which charges for its services—issues a certificate to be attached to their electronic communications.

It typically includes the sender's name; the certificate's serial number and expiration date; a copy of the certificate holder's publicly available, CA-signed encryption key; and the CA's digital signature.

A browser requesting a secure connection with a server first requests the server's digital certificate. The browser uses the public key included with the certificate to encrypt data it sends to the server.

"Only the private key generated with the public key can be used to decrypt the message," said Johannes Ullrich, chief technology officer of the Internet Storm Center, part of the SANS Institute, a security research and education organization. "The server decrypts the message and returns it to the browser as proof that it is in possession of the private key."

There are three types of digital certificates, each based on the degree of sender validation it provides.

*Domain-validated certificates* validate only the sender's name. This doesn't provide much security unless the recipient knows and trusts the domain-name owner.

*Organization-validated (OV) certificates* require validation of an organization's formal and DNS names. CAs validate the formal name by asking for copies of paperwork, such as articles of incorporation.

With *extended-validation certificates*, CAs must meet high minimum validation criteria as required by the Certification Authority Browser Forum, an organization of leading CAs, browser makers, and application vendors.

And with EV certificates, CAs have no discretion in implementing the standardized security policies, as they do with OV certificates.

CAs include Comodo, GlobalSign, StartCom, and VeriSign.

### Uses

Digital certificates are commonly used to secure communications between a browser and a webserver, noted Jessica Dash, spokesperson for the Microsoft Trustworthy Computing Group.

They are used with Hypertext Transfer Protocol Secure (HTTPS), which combines HTTP with SSL or TLS encryption and generates a lock icon in most browsers.

Recipients of messages can examine the accompanying SSL certificate and decide whether to trust the transaction.

Digital certificates are also sometimes used in lieu of passwords to authenticate a person or a device for accessing online services.

Computing devices can employ digital certificates to authenticate one another with little or no user interaction.

Also, he said, DigiNotar used a single master administrative account and it had a weak password.

After Ich Sun attacked DigiNotar's system and accessed 531 certificates, the company couldn't determine

which specific certificates were taken.

The CA's root certificate thus had to be marked as untrusted. This invalidated all certificates, legitimate and fraudulent, previously issued under the root.

Following this incident, DigiNotar declared bankruptcy.

Heron said Ich Sun probably used the stolen certificates to carry out man-in-the-middle attacks on 300,000 Iranian Google Gmail users.

### StartCom

Ich Sun attacked StartCom on 15 June. The company's Nigg said that a server was compromised but that the hacker didn't obtain certificates. Nigg wouldn't provide details about how StartCom thwarted the attack but said the company had planned for such an incident.

### THE BIG PICTURE

The recent attacks on CAs threaten the trust at the core of Internet security.

"Certificate authorities supplement validation and encryption to protect organizations and users. When that trust is compromised, [this process is] put into question," said Frost & Sullivan's Martinez.

Root CAs—such as DigiCert, Entrust, Equifax, GlobalSign, Go Daddy, and VeriSign—are considered trustworthy because they must pass audits by well-known professional-services firms.

However, they can appoint intermediate CAs to issue certificates under their authority. Problems can occur when the intermediate CAs don't conduct rigorous background checks of applicants before issuing certificates.

There currently are about 650 root and intermediate CAs. There are so many, said James Lyne, director of technology strategy at Internet security firm Sophos, that website visitors don't always know which are trustworthy.

## Concern about CAs

Because they store and issue digital certificates, CAs with weak security represent a glaring vulnerability for the system.

“DigiNotar’s servers ran out-of-date software and their network was poorly segmented, so problems would not be contained if they arose. Passwords used were simple and could have been found using brute force attacks, and server-side anti-virus protection was absent,” said Comodo’s Halam-Baker.

Strong competitive pressure to keep prices down discourages commercial CAs from adequately securing their systems, according to Security Curve’s Moyle.

Also, accounting for certificates that are stolen can be difficult for hacked CAs, said Network Box UK’s Heron. In this case, if a CA revokes the certificates they know about, users might fear that the hacker has others.

The alternative is to make the CA itself untrusted, Heron said. This can cause massive disruptions to users and damage the CA’s business, Lyne noted.

## Concern about browsers

While there are automated processes to revoke fraudulent certificates, Moyle noted, not every browser implementation checks an incoming certificate’s revocation status by default.

According to Lyne, CAs typically revoke stolen certificates fairly quickly after they find out about the theft. However, he added, even if hacked CAs revoke all their stolen certificates, browser makers might not update their products to reflect this right away.

“The risk gets compounded when they don’t do this in a timely manner,” said Moyle.

Another challenge, added Lyne, is that “many users still browse the Web on old browsers, which have varying cryptographic support and

sometimes shaky revocation and trust-management protocols.”

## Concern about users

Users, noted Heron, frequently ignore warnings about revoked certificates for numerous reasons, including ignorance about the risks involved.

And, he added, there are browser implementations that don’t recognize some CAs’ certificates at all, creating user confusion over whether rejection of a certificate really indicates a problem.

## Concern about fraudulent certificates

There are many malicious ways that hackers could employ stolen digital certificates.

## The attacks on CAs are now serving as a catalyst for rethinking Internet security.

For example, cybercriminals could utilize a fraudulent certificate to lure users—who think they are going to one website—to a hacker-controlled site.

The hacker could then relay messages between the victim and the site they intended to visit, thereby controlling the transaction via a man-in-the-middle attack and stealing transmitted information, explained Comodo’s Halam-Baker. This occurred in the Comodo and DigiNotar attacks.

Halam-Baker noted that hackers could also use fraudulent certificates to set up fake e-commerce sites, take orders, and thereby capture visitors’ names, addresses, credit card numbers, and other personal information.

## WHAT DO WE DO NOW?

“We should consider stronger regulation and audits on providers of trust and perhaps implement mul-

iple layers of redundant checking,” said Sophos’ Lyne.

The Electronic Frontier Foundation, a nonprofit digital-rights advocacy organization, is working on a framework that builds on the existing system but does away with depending on a large number of CAs that users don’t know or trust.

CMU researchers have devised Perspectives, a decentralized model that lets anyone run one or more *network notary servers*.

These Internet-connected servers monitor websites to build a history of the certificate each uses.

When a browser receives a certificate from a server, CMU’s Andersen said, it doesn’t seek confirmation that the certificate is linked to a root authority.

“Instead, [the browser] asks a notary whether it matches the certificate that the servers have been issuing,” he explained. “If so, that’s a good indication it’s a legitimate certificate for that site.”

However, noted Andersen, “It’s not a silver bullet. The model can be compromised.”

Mozilla has incorporated Perspectives into a freely downloadable extension for its Firefox browser.

Moxie Marlinspike, chief technology officer of security firm Whisper Systems, has designed Convergence, a beta project that replaces CAs with a browser add-on.

When a user visits a website, Convergence works with multiple notaries to evaluate the site’s certificate. Each notary independently checks the certificate, and if they all see the same one for the site, the system assumes it’s valid.

**T**he attacks on CAs are now serving as a catalyst for rethinking Internet security.

For example, Google has acted unilaterally to secure its Chrome browser by letting companies register their certificates directly with the

company, thereby bypassing the CA model.

CMU's Andersen said he would like to see fewer CAs "as people realize that [having] too many globally-entrusted CAs is horrible for security."

Comodo's Halam-Baker contended that CAs are doing their part to enhance security but that the rest of the industry now needs to respond.

Problems with the digital-certificate system are likely to continue because competitive market forces will still discourage CAs from

spending a lot of money on safety measures, noted Security Curve's Moyle.

Moreover, he argued, the digital-certificate system is so entrenched that there probably won't be many short-term changes.

According to Sophos' Lyne, hackers have so much to gain that they are likely to keep up their attacks.

He added, "All points of the infrastructure will come under challenge, so it's critical that we fix the process and trust issues in [future] technologies." **C**

*Neal Leavitt is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, China, France, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.*

**Editor: Lee Garber, Computer;**  
l.garber@computer.org

**cn** Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.



Enroll now.

**ON THIS BATTLEFIELD, EDUCATION IS YOUR BEST DEFENSE.**

Cyber attacks are being waged all over the world, creating an unprecedented demand for trained professionals to protect our country's data assets and develop cybersecurity policies. Help meet the demand with a bachelor's or master's degree in cybersecurity. Whether you plan to work for Cyber Command taking down cyber terrorists or for private industry battling hackers, UMUC can help you make it possible.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and DHS
- BS and MS in cybersecurity and MS in cybersecurity policy available
- Programs offered entirely online
- Interest-free monthly payment plan available, plus financial aid for those who qualify

**CYBERSECURITY**

800-888-UMUC • [umuc.edu/cyberwarrior](http://umuc.edu/cyberwarrior)

