SWCP Portal
March 2015

Like all fish stories, it just keeps getting bigger

Something Fishy Going On

What started last year with an annoying bit of adware has mushroomed into revelations of critical flaws in the basic software universally depended upon for secure communications – including buying and selling online. Moveover, the essential issues raised touch the core problem of trust on the Internet and the means to guarantee it, which affects everyone.

It began when the world's largest PC manufacturer, China-based **Lenovo**, quietly preinstalled some adware from a Palo Alto company called **Superfish**, specializing in "visual search", on some of its notebooks. When users would to pause to look at something while shopping, they'd be faced with a popup ad suggesting alternatives from elsewhere.

Users complained about this minor irritant but Lenovo **did little**. But the breach found in the browsers' supposedly safe shopping defenses by researchers was indeed alarming. Basically, the Superfish software acted like a virus that took over users' secure communications, leaving them extremely vulnerable to hostile outsiders. It was like they broke all the locks on a house so pushy salesmen could enter anytime.

The means by which transactions are kept safe, now called **TLS** (*Transport Layer Security*) but earlier, **SSL** (*Secure Sockets Layer*), are forbiddingly and arcanely complex. Like the rest of the Internet, it's a wonder the system works at all, and generally so well.

Users usually only notice TLS while shopping, if at all. When employed, addresses in the location bars of their browsers start with **`https:`** rather than **`http:`** and display a lock icon. ISPs, including SWCP, have always told users to be sure that was visible before entering *any* personal data, like credit card numbers, because TLS is their best gaurantee of privacy.

Trust but verify

To understand why, and what it means for all users, it may be easiest to imagine how it would apply to an actual situation. So we'll use something everyone does as an example, like buying a product on Amazon.com, although it should be noted that this problem is universal and has nothing to do with Amazon.

If you could order by phone, you could trust the phone company and the Yellow Pages that your call reaches the right company. But buying from Amazon is done entirely over the Web, and an Internet connection is not like an old-fashioned phone call. It's *not* a direct line between you and the store.

Instead, your information hops a number of times between servers and gateways before ever reaching Amazon's cloud. This means your private data could be spied upon, and Amazon's replies could be impersonated, too. Therefore it's crucial to ensure that you really are talking with Amazon and no one else.

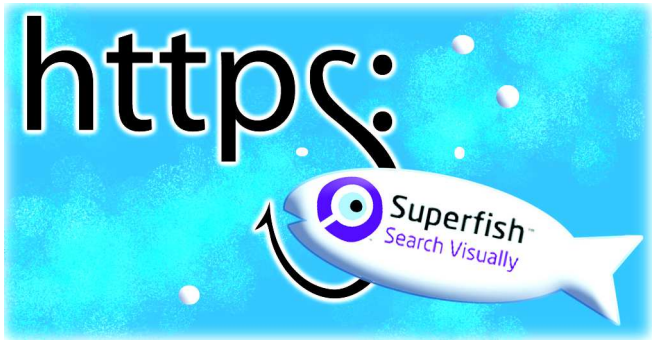
Sets of keys and secret handshakes

TLS and the digital certificate scheme's sole purpose is to make sure who's at the other end of the conversation. It all hinges upon a very complicated method based on some mathematical wizardry called **public-key cryptography**. This is how it basically works:

First, a trusted authority like **Symantec** verifies that Amazon is verily Amazon, and issues them a special document, a **digital certificate**, which says so. This Symantec signs using their *own* public key, authenticating it like a wax seal on a paper document. It matches the one in a **root certificate** *built into your browser*, so you can be sure it's really from them.

Symantec conjures up two related magic numbers for Amazon: a long **public key** which is published, and a shorter **private key** that Amazon keeps secret. The really clever **trick** is that the public key is used to encrypt messages to and from Amazon, but it requires their private key to unlock them.

Once you contact Amazon to begin a transaction, Amazon sends you their digital certificate that says yes, that's us, and includes their public key. You reply with a message encypted with that key which *only* Amazon should be able to read. And so you enter into a confidential conversation. More math tricks and secret "handshakes" further ensure your privacy from the very start of the exchanges.



Continued on back

Continued from front

The system works because any bad guy sitting in the middle could forge messages from Amazon to you but without their private key cannot read them nor your replies. However, what happened with Lenovo shows cracks in the whole Rube Goldberg scheme. The only obvious clue was that *all* certificates for every website visited were signed by Superfish.

Have you seen my fish?

What happened was that the adware **spoofed** the computer's root certificate with one of its own, using the *same* key for every site. A researcher **broke** the password in less than 3 hours to obtain Superfish's private key. This would allow anyone sitting between your infected computer and Amazon (or any other site) who wanted to impersonate them to easily do so. Like forging wax seals on paper documents, Superfish rendered the entire elaborate verification scheme totally and completely worthless.

Ominously, the malware has since been **found** elsewhere. The info it harvests is also disturbing. When a user hovers over a picture, Superfish gathers the metadata surrounding it to insert its own image. Though Lenovo **denied** it tracked users, it was potentially capable of building an extensive database. But the lackadaisical reaction by the manufacturer inspired the most outrage, for they first **defended** the dubious software as a feature.

Denying their reaction had been slow and ineffective, Lenovo first **claimed** the software was an attempt "to help customers potentially discover interesting products while shopping." Only lately have they admitted that they had been lied to and offered means of eliminating the infections, including half-heartedly offering **McAffee security scans**.

Yet meanwhile, the Department of Homeland Security has **recommended** its immediate removal. In any case, **certificates are only as good as the certifier**. But verification by the trusted authorities has gotten sketchier due to high demand; the system is now largely automatic. Root certificates can even be signed by parties on their own authority, as Superfish **did**. Another problem is the constantly-updated list of revoked certificates is not widely used. And finally, a single certificate, according to **Symantec**, can be used for up to a hundred different domains.

The numbers racket

But even more serious implications have arisen. Encryption of digital information is a mathematical game, and what must remain unknown for it to work are the **seed numbers** it starts with and the formula, or **algorithm**, it employs. That depends upon the generation of **psuedo-random numbers**. They're called "psuedo-random" because they're as close to truly random as can be made but they're not really. If they can be predicted, the whole scheme falls down.

A flaw was found in 2007 in the **RSA algorithm** allowing the numbers to be calculated. This amounts to a **backdoor** – a secret tunnel through the security wall. Moreover, it was deliberately placed there by the very **agency** that designed the algorithm, and later required it to be used in federal computers, which made RSA the default standard worldwide.

That agency was, of course, the **National Security Agency**, who naturally **wanted** strong defenses against everybody else but easy access for themselves. The NSA apparently **paid** RSA Security *$10 million* to use the flawed formula, too. The contradiction of the country's prime defender of privacy being also the world's chief hacker was not lost on the company's CEO Art Coviello, who recently **called** for the two-faced spy agency to be split apart and cyber-weapons to be renounced and treated much like atomic, chemical, and biological weapons.

Yet the RSA backdoor was not the only weakness found. The **Heartbleed security bug** scare last year woke the tech world up to problems lurking in the system long taken for granted. But in the Superfish fiasco, the layers of deception involved may be its most troubling aspect. Superfish lied to Lenovo, who lied to their customers, and the government lied to *everybody*. In the post-Snowden world, it is rapidly becoming clear that *all* Internet applications might have to be retooled, and trust will have to be earned.

What can online shoppers do?

First, *never* ignore alarms about certificate errors. Do not assume the website forgot to renew, but check the digital certificate and signature carefully. Secondly, remember that there still is one piece of data you can *always* rely on just like the phone number: *the Web address*. Every website has its own unique one, and despite a **few scares**, the Internet's root servers are still believed to be secure.

Criminals *cannot* hijack a legimate site's address, but they will try to disguise theirs. Be sure to examine the domain name in the URL before submitting credit card info. If you're ready to buy at Amazon and the location bar begins with anything at all *other* than `https://www.amazon.com/` you can be sure you're in the wrong place. For domain names and protocols, just like with passwords, spelling *always* counts.

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**

Click on blue terms in PDF file to open links.