Security Compromised

Sherman Tan

08 May 11

Is there Secured Web Communication?

On 15 Mar 2011, the Comodo Group reported that one of its user accounts with an affiliate certificate registration authority had been compromised. This breach resulted in a new user account being created that issued nine certificate signing requests (CSR) for seven domains: mail.google.com, login.live.com, www.google.com, login.yahoo.com (three certificates), login.skype.com, addons.mozilla.org, and global trustee.

For the layperson, this intrusion may not be alarming but this incident clearly showed that the current systems of ensuring secured communication and commerce on the internet may not be as secured as previously thought. In the past when the internet was mainly used for publishing of static information, the lack of security was not an issue but with e-commerce such as purchases using the credit card over the internet, the need to create a secure channel over the insecure internet was apparent. The technology that was deployed is known as Hypertext Transfer Protocol Secure (HTTPS).

The main idea of HTTPS was to create a secure channel over an insecure network. HTTPS ensured reasonable protection from eavesdroppers and man-in-the-middle attacks provided the server certificate (typically at the merchant's end) was verified to be trusted by the Certificate Authority (CA) that issued the certificate. The trust inherent in HTTPS is based on major certificate authorities that come pre-installed in browser software. Simply put, the user trust the CA; e.g. VeriSign, Microsoft to tell the user whom he/she should trust.

Browser makers such as Microsoft, Apple, Mozilla and Google have authorised a large and growing number of entities around the world – both private organisations and government bodies – to create and manage certificates on their behalf. In turn, many private "certificate authorities" have worked with resellers or have deputized other companies to issue certificates in a "chain of trust". According to the Electronic Frontier Foundation, as at Dec 2010, a total of 676 organisations were signing certificates.

In the Comodo case, the hacker infiltrated an Italian computer reseller and used its access to Comodo's system to automatically create certificates for websites operated by Google, yahoo, Microsoft, Skype and Mozilla. With these certificates, the hacker could set up servers that appeared to work for those websites and then attempt to view millions of unscrambled messages and online transactions. Although Comodo had since suspended the Italian reseller and a second European reseller that the hacker had also infiltrated, the issue was far from over. Besides the Comodo case, there had been several major network system compromises in the recent months. See stories below.

Sony PlayStation Network Attack

According to a recent letter from Sony's Chairman to the US Congressional Committee, a group of attackers have exploited a software vulnerability in one of the applications in the network that support PlayStation Network, the online gaming site for Sony PlayStation customers. The network comprises 130 servers, 50 software programs and 77 million registered accounts. The letter further elaborated that personal data was compromised because it had found records of queries being made for it and large data transfers were being made out in response.

Responding to congress and public enquires, Sony explained that the intrusion was detected on 19 Apr 2011 but the company took a week for external expertise to conduct an investigation to determine the nature and scope of the incident. The investigation revealed the huge extent of the intrusion: names, addresses, birthdates, PSN passwords and credit card numbers for any of the network's 77 million customers who provided such information may have been acquired.

Sony is not alone

In mid-Mar 2011, security firm EMC notified its users that one of its companies, RSA, was the target of an "extremely sophisticated cyber attack" referring to it as an “Advanced Persistent Threat” (APT). The attack had the potential to compromise the security of RSA's two-factor authentication product, SecurID. In early Apr 2011, RSA begun to provide more details into the March attack but had required its customers to sign a Non-Disclosure Agreement (NDA) before they were prepared to share the details. While some companies signed, others didn’t but it was enough to provide various interested parties the information to piece together what had happened: the security breach involved an employee opening a malicious Excel document containing a zero day exploit of Adobe Flash*.

**The Adobe zero-day vulnerability, now patched by Adobe, allowed the attacker to control the victim's machine at RSA and use a variant of a long-known hacker tool called Poison Ivy to set up a command-and-control system aimed at extricating data.*

A couple of weeks later in end-Mar 2011, Epsilon, the world's largest permission-based e-mail marketer, suffered an attack that exposed names and e-mail addresses saved in the customer databases of many well known companies such as JPMorgan Chase, Capital One, Marriott Rewards, McKinsey Quarterly, US Bank, Citigroup, Ritz-Carlton Rewards, Brookstone, Walgreens, The College Board, and the Home Shopping Network (HSN). While some could dismissed the type of data (names and email addresses) harvested as a minor threat, the theft offered opportunity to targeted phishing attacks to customers that expect communication from these brands.

Next in line was the Oak Ridge National Laboratory that was hacked in late Apr 2011. The federal lab, funded by the U.S. Department of Energy, worked on a variety of projects including energy matters as well as computer security. Although the hackers were reported to have stolen only a "few megabytes" of data before the lab was shut down. The attack was the result of some employees of the federal lab opening an e-mail and clicking on a malicious link.

Some Common Sense Security Measures

As a user of the internet and online banking, there appeared to be little that we could do to prevent such infiltrations but at least, we could take some simple measures to minimise our exposures and avoid ending up being the victims:

- Although most banks issued their online banking users with a security token to generate one-time password, it is just as important to choose a strong password for the static password that go with the user ID.

- Avoid making online banking transactions or credit card transactions using public computers or at internet café where the security of such equipment could be compromised.

- Always remember to log-off from the online transaction and clear the browser cache after ending the session.

- Many compromised systems were due to phishing scams, i.e. emails that appeared to originate from your bank asking you to click on a certain link to re-enter all your account information. The end-Apr 2011 hack at Oak Ridge National Laboratory was due to its staff clicking on a malicious link. Always report such e-mails to your bank immediately when you received these emails.

- Before log into the bank website, examine the link carefully. When you have entered a secure site, the address of the site should start with https:// instead of http://. Learn to tell the difference between a secure site and an imitation.

Finally, if you find yourself the victim of fraud, report the matter to your bank immediately as you are not the first nor going to be the last.

The writer is the Principal Consultant & Director at Innovar Pte Ltd (www.innovar.com.sg). He can be contacted at office@innovar.com.sg.