Run! The Fukushima of the Security World is coming!

David Holmes, 2011-03-04

The world is transfixed by the cascade of disasters in Japan this month. As if the biggest earthquake of the modern era wasn't enough the country is hit by a Tsunami and a nuclear meltdown; just when you think it can't get any worse it always seems to.

A similar series of catastrophes is happening in the online security world this year: an **ultimate hack** of the world's premier security company's crypto data and the improper issuance of "false" certificates from a certificate authority.

Honestly, **I never thought it would get this bad**. But it has.

RSA SecurID Pwnd

F5 is a Security Company. It's taking people a little time to come around to the idea but it is happening. When people think about a security company they often think of **the mother of all Security Companies**, **RSA Incorporated**. It would be difficult to overstate RSA's current and historical significance to the three worlds of academia, e-commerce, and enterprise security.

Enter Next Token: PWND11

RSA's multi-factor authentication product, **SecurID**, has historically funded the majority of RSA's revenues. If you have a high-security environment (or even an E-Trade account) there's a good chance that you own, or are using, an RSA hardware token. As RSA's cash cow, SecurID generates revenue that pays for all their other research and influence in the community (the annual security conference is called RSA).

By now you might have heard that attackers hacked the servers at RSA and stole information that "is specifically related to RSA's SecurID two-factor authentication products." RSA hasn't said anything more than this but the security community is assuming that it is the seed data for all the tokens that was stolen.

Here's a threat model analysis of how this incident could affect the 40 million SecurID users. And another one - even juicier.

There's a very real possibility that RSA is right now revving all their SecurID tokens for a massive, 40-million unit replacement. As one of our architects says, "*Distribution of Replacement Units is a Military Prioritization Issue*" (caps mine). This is to say that the ultimate class warfare may erupt when RSA has to decide which customers to upgrade first. And second. And Last. Where is your organization on their list? Do you know?

Not a real Comodo Image

Certificate Authority Issues Google Certificate to Hacker

If the RSA SecurID breach is an earthquake, then the Comodo issue can be the breached reactor vessel. Okay, maybe this analogy is starting to break down, especially because the breaches are totally unrelated except in the proximity of time.

I've been saying this for 15 years; the **Achilles Heel of Public Key Crypto is the certificate management**. The Comodo breach is the perfect example of this. The attacker first tried to crack the RSA keys but found he could get nowhere. So instead he attacked the certificate management system, found an embedded password in a root certificate authority's *Italian reseller,* and then used that vulnerability to issue himself several certificates, including his own **Google, Skype** and **Yahoo** certificates. Comodo closed the barn door after the attacker left by revoking the certificates and then having the Mozilla browser and its kin rev their certificate lists.

Is certificate revocation at the root certificate authority level an acceptable fix? Browsers are supposed to check the status of a server certificate, using a protocol called OCSP (Online Certificate Status Protocol) but not all of them do. Specifically, 30% of the browsers out there are IE 6 or IE 7 running on XP, which has no OCSP support. Those browsers have no way of knowing which of the Google.com certificates are real, and which are not. **That's just downright scary: millions and millions of users cannot truly rely on the global PKI.**

Browser	OCSP Support	Market Share (Mar 2011)
Firefox 3+	Yes, Default = Yes	26%
IE 7+ [Vista/Win7]	Yes, Default = Yes, buts fails open	16%
IE 6 / IE 7 [XP]	None	30%
Opera	Yes, but fails open	3%
Chrome	Yes, Default = Yes	10%
Safari	Yes, Default = No	4%

Stats from gs.StatCounter.com, w3schoools.com, netmarketshare

You know what makes this even worse? Many of the browsers, IE7 and Opera among them, will "fail open" if there's a problem reaching the OCSP server. In my experience, OCSP servers are NOT the strongest link in the chain, which is probably why the browsers just silently continue when the servers don't respond. So the situation is probably worse than the table above shows.

What to make of this debacle in the long term? We are all, especially the Comodo CA, going to learn our lesson about doing proper due diligence before issuing certificates, right?

Apparently not, because THIS ALREADY HAPPENED IN 2008. Same Certificate Authority (Comodo). Same reseller problem.

Maybe the third time will be the charm!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com