Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Who do you trust?

Imagine this scenario: a woman is enjoying a cup of coffee at her favorite Wi-Fi hotspot, and uses her iPad to check her email. As she starts to login to Gmail, she doesn't realize that the man sitting a few tables over, apparently working on his laptop, has intercepted her login and is pretending to be Gmail in an effort to capture her user name and password.

Copyright SANS Institute
Author Retains Full Rights

AD
observe it
MANAGE THE RISK OF YOUR USERS
FREE USER
ACTIVITY MONITORING
TRY IT NOW

Who do you trust?

By Matthew Luallen

While certificates have their uses in a security regimen, they are not a bullet-proof method to ensure the authenticity of software, a person, or communications.

Imagine this scenario: a woman is enjoying a cup of coffee at her favorite Wi-Fi hotspot, and uses her iPad to check her email. As she starts to login to Gmail, she doesn't realize that the man sitting a few tables over, apparently working on his laptop, has intercepted her login and is pretending to be Gmail in an effort to capture her user name and password. Since he is on the same network, he is able to answer faster than Google and preempt the genuine response. Her computer believes that he really is Gmail because he has presented a certificate that her computer has accepted as authentic. Once the criminal has that information, he can try that name and password on other applications because people routinely use the same names and passwords for multiple accounts. If you think this sort of thing couldn't happen, it already has. A hacker in Iran stole or created working certificates for a group of applications, including Gmail, eBay, PayPal, and others.

The attack vector works because all her browser needs to see is a legitimate certificate for the Website from a trusted authority. It may be stolen or forged, but it's enough to do the job. Certificates are useful to show that Websites and software are trustworthy. It's hard to imagine what Web surfing would be like if we had to stop at every site and manually give permission for it to load. However, they are not bullet-proof. There are many ways in which cyber criminals can circumvent the process.

It was just about 10 years ago that Microsoft had an embarrassing time when it farmed-out its certificate authority management. Microsoft hired Verisign to administer its program, which was to include maintaining a certificate revocation list. Verisign received a request for a certificate from what was apparently an internal Microsoft user, but it was actually a stolen user account. Verisign generated the requested certificates which were then used repeatedly to cover bogus software. Eventually Verisign revoked the certificates, but they continued to work. The online certificate status protocol at the time called for applications to check the list for

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

revocations, however this went almost entirely unheeded. It wouldn't have helped anyway because Verisign did not compile the list - there was nothing to check. Solving that problem involved Microsoft issuing a software patch, setting up its own certificate authority, and enforcing use of the online certificate status protocol. That protocol is now a standard element within Web browsers to identify revoked certificates.

There are more subtle ways in which the system can fail. More recently, part of Stuxnet's success depended on using compromised certificates from JMI and Realtek. These convinced the Iranian systems that the malware was trusted.

One of the main problems with certificates is that your system has to have its own reference of trusted certificate authorities. This is normally embedded into operating systems and browsers with a default list of sources, but most users are probably unaware of its existence and therefore don't know what is on the list. Most users have no practical way to evaluate what's there and decide if they agree with the evaluations of whoever compiled that database. The list cannot be static because new certificates will need to be added and compromised certificates that have been revoked or expired must be removed, otherwise they will continue to be effective.

This very process of updating and correcting lists of trusted certificates has served as an attack vector. The Zeus botnet, for one, has the ability to go into a system and download certificate stores. It can also make its own additions to the list so your OS will accept a certificate it presents at a later date.

Certificate authorities are companies and not, at least so far, government bodies. As we have seen over the last several years, companies can fail or change ownership under difficult conditions. Imagine if a trusted certificate authority was purchased by cyber criminals or fell under their influence. Just like the mafia buying its own bank to launder money, such a group could create powerful resources for those criminals. While such a thing has not happened yet, at least to my knowledge, there is little to prevent it. Government participation in the process is probably not far off, for better or worse, but we can only speculate what form it might take.

International standards organizations now require certificates under certain circumstances. ICSJWG 2009 provided a great presentation by ABB discussing the challenges of certificate authorities, certificate management, and the immaturity of integration within the control system space. So far, relatively few require their integration. Examples include IEC 62351, Secure DNP3/TCP, and OPC-UA. If you ask the nearest traditional IT web administrators when the last time was that they had any difficulties

© 2011 SANS Institute, Author retains full rights.

managing certificates, they'll probably mention a time when they initially expire unnoticed.

So if the certification system has so many flaws, how should a user organization use it? Does it provide any practical value? The answer is yes, but only if the environment is appropriately managed. It will not work by itself. Here are some suggested steps:

- Find out what is in the databases attached to your operating systems, applications, and browsers. With some persistence, you can find the lists in systems provided by Microsoft, Apple, etc.

- Understand who the certificate authorities are and which are most trustworthy. This is easier said than done, because as of this writing, there are few if any resources available, so you're basically on your own. At least for control system environments it is much simpler as most of the certificate authorities would be removed. You will need to work with your control system vendor to discern which certificates are necessary in your environment.

- Enforce internal procedures regarding issuing, revoking, and re-issuing certificates already in place. You do not want to use self-signed certificates and then simply instruct your users to "accept the new certificate authority." This is a common practice that can lead to disastrous consequences.

Ultimately you need to understand whom you trust both personally and electronically. Certificate authorities are the validating entity that has a process to associate an entity with an electronic identifier, the digital certificate. If you do not trust the authoritative body or how the receiver of the identity manages it, then remove it from your electronic devices. Once again, ensure that you are not required by your systems to have the trust before removal.

© 2011 The SANS Institute Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced