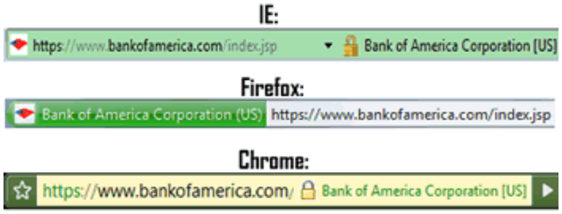
Certified Lies: Big Brother In Your Browser

Government capable of wiretapping millions of encrypted sessions, including those secured by IE, Microsoft's SSL, others.

By Ms. Smith on Fri, 07/23/10 - 12:04pm.

Share Tweet This Email this page Comments (8) Print Newsletter Sign-Up

You probably feel safe when you see the padlock on your browser window indicating secure communication with your bank or e-mail account. You probably think your users are safe if they are accessing your network over your SSL VPN. What if instead of worrying about man-in-the-middle attacks, it became government-spy-in-the middle eavesdropping? Is Big Brother spying on you? Before I'm done showing you these surveillance products, you will probably be ticked for both security and privacy reasons.



IE:

https://www.bankofamerica.com/index.jsp Bank of America Corporation [US]

Firefox:

Bank of America Corporation (US) https://www.bankofamerica.com/index.jsp

Chrome:

https://www.bankofamerica.com/ Bank of America Corporation [US]

*Note and *hint* that the country information ("US") shown by the browsers refers to the corporation that obtained the certificate (Bank of America), not the location of the Certificate Authority (CA).

368 diggs 368 diggs

The Extended Validation Certificates (EV) produces the green bar in most modern browsers. In a purely hypothetical example, the U.S. government can force a Public Key Infrastructure (PKI) to give them a publicly trusted certification for www.amazon.com. They then poison your DNS and route your traffic for www.amazon.com to a site they own that has the fake certification installed. Your browser then gives you that pretty green bar or little lock and you think everything is cool, safe and secure. Or... they can put a device between you and your target and then perform SSL interception.

Two researchers, Chris Soghoian and Sid Stamm reported on an industry claim that governments could get "court orders" giving them access to falsified cryptographic credentials (spy certs). If National Strategy for Trusted Identities in Cyberspace (NSTIC) is implemented, the threat seems to intensify if the government itself is running the PKI.

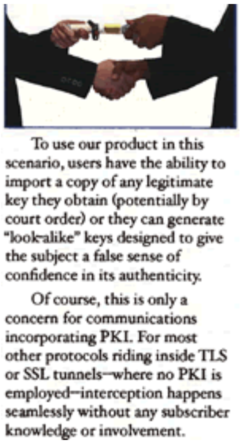
What this means is that an eavesdropper who can obtain fake certificates from *any* CA can successfully impersonate *every* encrypted website you might visit. And you have no way of knowing that you haven’t landed on the authentic, actual site. Most browsers silently accept new certificates from any valid authority, even sites for which certificates have already been obtained. An eavesdropper with fake certificates and access to a target's net connection can quietly negotiate a "man-in-the-middle" (MITM) attack, observing and recording all encrypted web traffic while the user is clueless that it's happening.

Are there really eavesdroppers out there -- spies or law enforcement agencies using spy certificates to intercept encrypted web traffic? Are there really wiretapping conventions for eavesdroppers? Oh yes, the next is in October 2010, but IIS World Americas is open only to "law enforcement, intelligence, homeland security analysts and telecom operators responsible for lawful interception, electronic investigations and network intelligence." There are many vendors of products that assist the government in spying, but the HACKING TEAM and Packet Forensics are two that should send an eerie eavesdropping chill up your spine.

Here's an FYI about the HACKING TEAM:

> Remote Control System V6 (RCS) is a premier, integrated, multi-OS platform for remotely attacking, infecting and controlling target computers and mobile phones. RCS FULLY SUPPORTS XP, Vista, 7, MacOS, iPhone and Symbian - It is INVISIBLE to most protection systems available in the market - It is a PROVEN technology: it is being used by Agencies worldwide since 2003 - Target monitoring includes Skype, chat, mail, web, removable media, encrypted communications, PGP, GSM-cell GEO-tracking, GPS GEO-tracking, voice calls, etc.

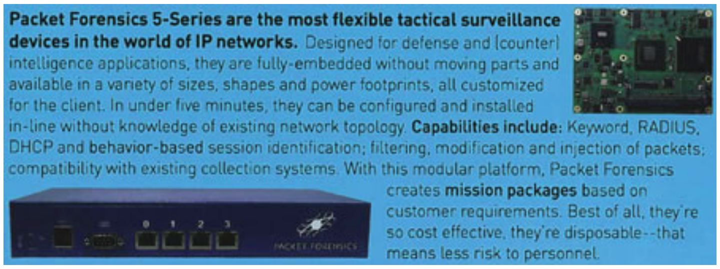
Let's focus on Packet Forensics for now. Packet Forensics offers a 5-series device that is a 4 square inch "turnkey intercept solution" surveillance product, “using `man-in-the-middle' to intercept TLS or SSL.” It's marketed and sold to law enforcement and intelligence agencies in the US and foreign countries, designed to collect encrypted SSL traffic based on forged "look-alike" certificates obtained from cooperative CA. In the image, please note the parenthesis around (potentially by court order) as if it is not entirely important...



To use our product in this scenario, users have the ability to import a copy of any legitimate key they obtain (potentially by court order) or they can generate "look-alike" keys designed to give the subject a false sense of confidence in its authenticity.

Of course, this is only a concern for communications incorporating PKI. For most other protocols riding inside TLS or SSL tunnels—where no PKI is employed—interception happens seamlessly without any subscriber knowledge or involvement.

According to the Packet Forensics flyer: "Packet Forensics' devices are designed to be inserted-into and removed-from busy networks without causing any noticeable interruption [. . .] This allows you to conditionally intercept web, e-mail, VoIP and other traffic at-will, even while it remains protected inside an encrypted tunnel on the wire [. . .] To use our product in this scenario, [government] users have the ability to import a copy of any legitimate key they obtain (potentially by court order) or they can generate `look-alike' keys designed to give the subject a false sense of confidence in its authenticity [. . .] Your investigative staff will collect its best evidence while users are lulled into a false sense of security afforded by web, e-mail or VOIP encryption [. . .] In under five minutes, they can be configured and installed [. . .] they're disposable -- that means less risk to [government] personnel."



Packet Forensics 5-Series are the most flexible tactical surveillance devices in the world of IP networks. Designed for defense and [counter] intelligence applications, they are fully-embedded without moving parts and available in a variety of sizes, shapes and power footprints, all customized for the client. In under five minutes, they can be configured and installed in-line without knowledge of existing network topology. **Capabilities include:** Keyword, RADIUS, DHCP and **behavior-based** session identification; filtering, modification and injection of packets; compatibility with existing collection systems. With this modular platform, Packet Forensics creates **mission packages** based on customer requirements. Best of all, they're so cost effective, they're disposable--that means less risk to personnel.

Microsoft's documentation shows that it has adopted a more cautious approach in trusting CAs than its competitors; a fresh installation of Windows 7 will list 15 CAs in the operating system's Trusted Root Store. Sadly, however, this interface is terribly misleading as it doesn't reveal the fact that Microsoft has opted to trust 264 different CAs. This means any web browser that depends upon Microsoft's Trusted Root Store (such as Internet Explorer, Chrome and Safari for Windows) ultimately trusts 264 different CAs to issue certificates without warning. Firefox is the only major browser to maintain its own database of trusted CAs. Each of the 264 root CAs trusted by Microsoft, the 166 root CAs trusted by Apple, and the 144 root CAs trusted by Firefox are capable of issuing certificates for any website, in any country or top level domain. You don't think the government will use their own CA which could be tracked back to them if discovered, do you?

About Privacy and Security Fanatic

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues. Smith has a diverse background in information technology, programming, web development, IT consulting, and information security. She focuses on the unique challenges of maintaining privacy and security, both for individuals and enterprises. She has worked as a journalist and has also penned many technical papers and guides covering various technologies. Smith is herself a self-described privacy and security freak.

Smith is an independent contractor and is not affiliated with any vendor that makes or sells information technology.

RSS Contact Requires Login

Archives

July 2010
June 2010

On The Web

Follow all Microsoft Subnet bloggers on Twitter

To be fair, however, all encrypted streams that travel over the Internet are susceptible to government spying, not just those that use Microsoft technology.

How does this affect you? Many information-hungry governments routinely compel companies to assist them with surveillance. ISPs and telecommunications carriers are frequently required to violate their customers' privacy by providing the government with email communications, telephone calls, search engine records, financial transactions and geo-location information. A few examples of this electronic surveillance by law enforcement include: a consumer electronics company that was forced to remotely enable the microphones in a suspect's auto-mobile dashboard GPS navigation unit in order to covertly record their conversations, as well as a secure email provider that was required to place a covert back door in its product in order to steal users' encryption keys. And who can forget the NSA's wiretapping?

In regard to Packet Forensics and Big Brother in your browser, EFF's Senior Staff Technologist Seth Schoen advises, “HTTPS Everywhere does not address this threat. We have been doing other research to try to investigate this concern. There are several Firefox plugins that try to use information other than CA-issued certificates to validate web sites' keys -- for instance, Perspectives, Monkeysphere, CertPatrol, and Petnames. The general problem is that right now these approaches sometimes call for considerably more effort on the part of the user. Under certain assumptions, this might be unavoidable."

Schoen has written more about these issues, including, Behind the Padlock Icon: Certificate Authorities' Mysterious Role in Internet Security.

Researchers, Chris Soghoian and Sid Stamm, are working on a Firefox plugin. Until then, I'm using Certificate Patrol to help detect a MITM attack.

Electronic surveillance is happening all around you, all the time, and perhaps *to* you. If surveillance devices like Packet Forensics is around for law enforcement and national intelligence agencies, then you can be sure that cyber-criminals are using them too. I would have said these devices are used by bad guys and good guys, but if The Law is spying on you then it's hard for me to call them "the good guys."

According to Cisco, there are 35 billion devices connected to the Internet. How many of those are being eavesdropped upon? Next time you see the padlock on your browser, will you still feel like your important communications are secure? Do you feel like your privacy is truly private?

Tags
Microsoft
Security
Big Brother
electronic surveillance
fake CA
man-in-the-middle
Packet Forensics
security
wiretapping

DMCA Ramifications

By Steve (not verified) on Fri, 07/23/2010 - 8:00pm.

Technically, I can see the uncertainly and possibility for such an 'attack'. However, the content on a site such as Amazon is copywritten and therefore the content should fall under the guidelines of the Digital Millennium Copyright Act (DMCA), which makes it a federal offense to circumvent encryption of content.
It makes you wonder whether or not the government would break it's own laws in order to achieve this goal, and if so, whether bringing up the DMCA in court could have such evidence thrown out.

DMCA

By kevin (not verified) on Fri, 07/23/2010 - 8:08pm.

@Steve
One word will answer your questions:
COINTELPRO
Wikipedia, or Google, read it. and throw out any notion that it will be 'thrown out.' Those laws are for you, not for them.

> ### Countering Counter-Intelligence Pros
>
> By amanfromMars (not verified) on Sat, 07/24/2010 - 10:21am.
>
> > Those laws are for you, not for them.
>
> For some, are those laws for you and them, and not us, kevin.

Yes I feel safe.

By Anon (not verified) on Fri, 07/23/2010 - 8:15pm.

Yes I feel safe.

So basically the CA's aren't trusted...

By Anon (not verified) on Fri, 07/23/2010 - 9:10pm.

The EFF should declare itself a CA, and then people could manually add it to their browsers.
Also the EFF could ask every CA to swear that they have not been compromised by the NSA. Those which decline can be removed from the CA list on users browsers.
Another thought... Doesn't the US Government have certs for .COM, .ORG, .NET and .EDU and .GOV anyway?
I'm guessing there are NSA moles in most of the CA's anyway, so the government has all the SSL secret keys. Any important keys they didn't have could be brute forced anyway, since they actually DO have the computing power.

R U KIDDING ME?

By Anon (not verified) on Sat, 07/24/2010 - 12:52am.

Anyone out there that thinks ANY of their commo (email, cell - Analog or Digital, LL, iNet, mail, and radio) is secure from interception just simply has no business turning on the switch.

> ### No not really..
>
> By KooperStone on Sat, 07/24/2010 - 9:43am.
>
> All it requires is a wiretapping warrant or bill to start tracking - so it's not really inconceivable as you suggest
> internet tv

Welcome to 1984

By Anon (not verified) on Sat, 07/24/2010 - 7:28am.

Unfortunately this is a two edge sword. The positive is that the law enforcement will have tools to catch law breakers. The negative is that the people will have to have faith that their law enforcement as well as the government is not corrupt and would use this technology in a way that would not violate our freedoms and rights according to the Constitution. Do we know of any type of oversight on law enforcement to prevent such abuses? Do we know if law enforcement must get a search warrant prior to starting this and what would allow a judge to grant such a search warrant? We have already seen bureaucrat abuses in the State Department where they were leaking Passport information on celebrities and politicians to the media. Is there any type of recourse for a party who believes that their Internet traffic was intercepted and used for the wrong purposes? i.e. a bureaucrat leaking or selling this information for personal gain.
This article brings up more questions than answers.

Your name: Anon

Subject:

Comment: *

CAPTCHA
This question is for testing whether you are a human visitor and to prevent automated spam submissions.

What is the third word in the phrase "sekika opulep ginoyu ora irupo"?: *

Post comment

Quick Poll Results - The Anxiety Behind Security and Compliance- Intel

Quick Poll Results: The Planned Refresh-Simplifying IT Management- Intel

Quick Poll Results - Security: Everyone's Challenge- Intel

Save now with the best deals from CDW. - CDW

Get down to business with colleagues around the globe-anytime, anywhere-in unmatched detail with Logitech® HD Webcams. - Logitech

Download Gartner report: Identity & Context Virtualization Key to IdM- Radiant Logic, Inc

Learn how to reinvent network security with next-generation firewalls. - Palo Alto Networks

Get overheating under control with the Liebert CRV. Learn more.- Emerson

Network World, Inc
The Connected Enterprise

About Us
Jobs @ NWW
Contact Us
Newsletter Subscriptions
Advertise
Reprints & Links
Partnerships

Other IDG Sites

CIO
Computerworld
CSO
DEMO
GamePro
Games.net
IDG Connect
IDG Knowledge Hub
IDG TechNetwork
IDG Ventures
InfoWorld
ITworld
JavaWorld
LinuxWorld
MacWorld
Network World
PC World