Sorveglianza digitale, un primo accenno

Riccardo Dal Fiume

IMOLUG

Imola & Faenza Linux User Group

Secret court orders allow NSA to sweep up Americans' phone records

Secret court orders allow NSA to sweep up Americans' phone records metadata.

They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.

They know you called a gynecologist, spoke for a half hour, and then searched online for the local abortion clinic’s number later that day. But nobody knows what you spoke about.

PRISM

NSA doesn't have direct access to the servers, but can request user data from the companies, which are compelled by law to comply.

A national security letter (NSL) is an administrative subpoena issued by the United States federal government to gather information for national security purposes. NSLs do not require prior approval from a judge. The Stored Communications Act, Fair Credit Reporting Act, and Right to Financial Privacy Act authorize the United States federal government to seek such information that is "relevant" to authorized national security investigations

Britain's version of the NSA taps fiber optic cables around the world

The British spy agency, the Government Communications Headquarters (GCHQ), works closely with the NSA, sharing data and intelligence in a program that's codenamed Tempora.

Tempora is one of the key NSA/GCHQ programs, allowing the spy agencies to collect vast troves of data. Some companies that collaborate with the GCHQ in the Tempora program: Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute.

NSA spies on foreign countries and world leaders

The German newsweekly Der Spiegel revealed that the NSA targets at least 122 world leaders.

Other stories over the past years have named specific targets like German Chancellor Angela Merkel, Brazil's President Dilma Roussef, and Mexico's former President Felipe Calderon, the French Foreign Ministry, as well as leaders at the 2010 G8 and G20 summits in Toronto.

XKeyscore, the program that sees everything

Makes available everything you've ever done on the Internet — browsing history, searches, content of your emails, online chats, even your metadata — all at the tap of the keyboard.

The program gives analysts the ability to search without any prior authorization — no warrant, no court clearance, no signature on a dotted line. An analyst must simply complete a simple onscreen form, and seconds later, your online history is no longer private.

NSA efforts to crack encryption and undermine Internet security

What's the point of tapping fiber optic cables if the data flowing through them is unreadable?

NSA, isn't able to compromise the encryption algorithms underlying these technologies. Instead, it circumvents or undermines them, forcing companies to install backdoors, hacking into servers and computers, or promoting the use weaker algorithms.

NSA elite hacking team techniques revealed

The NSA has at its disposal an elite hacker team codenamed "Tailored Access Operations" (TAO) that hacks into computers worldwide, infects them with malware and does the dirty job when other surveillance tactics fail.

Fun Fact: In 2012 TAO tried to remotely install an exploit in one of the core routers at a major Internet service provider in Syria, instead they bricked the router, causing Syria to suddenly lose all connection to the Internet.

That’s what Snowden calls an “oh shit” moment.

NSA cracks Google and Yahoo data center links

When bulk collection or PRISM fails, the NSA had other tricks up its sleeve: It could infiltrate links connecting Yahoo and Google data centers, behind the companies' backs.

Google and Yahoo announced plans to strengthen and encrypt those links to avoid this kind of surveillance, and a Google security employee even said on his Google+ account what many others must have thought privately: "Fuck these guys."

NSA collects text messages

It's not just about Internet data though. The NSA, following its unofficial motto of "collecting it all," intercepts 200 million text messages every day worldwide through a program called Dishfire.

In leaked documents, the agency described the collected messages as a "goldmine to exploit" for all kinds of personal data.

NSA intercepts all phone calls in two countries

The NSA intercepts and stores all phone calls made in the Bahamas and Afghanistan through a program called MYSTIC, which has its own snazzy logo.

The NSA also collects all phone calls' metadata in Mexico, Kenya and the Philippines.

LOVEINT, love in the time of NSA

A riff on HUMINT (human intelligence) or SIGINT (signals intelligence).

In 2005, a National Security Agency employee was given his first day of access to the United States' SIGINT capability. So what did he do with his vast powers?

According to a newly published letter by the NSA Office of the Inspector General (OIG), "he queried six email addresses belonging to a former girlfriend, a U.S. person, without authorization."

NSA employees routinely pass around intercepted nude photos

Then Alan Rusbridger, The Guardian’s editor-in-chief, asked: “You saw instances of that happening?”
“Yeah,” Snowden responded.
“Numerous?”
“It's routine enough, depending on the company that you keep, it could be more or less frequent. These are seen as the fringe benefits of surveillance positions."

Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

— Edward Snowden, answering questions live on the Guardian's website

https://savecrypto.org/

References

http://mashable.com/2014/06/05/edward-snowden-revelations/
http://www.wired.com/2014/08/edward-snowden/
http://arstechnica.com/tech-policy/2013/07/new-snowden-leak-details-widest-reaching-nsa-digital-surveillance-program/
http://arstechnica.com/tech-policy/2013/09/loveint-on-his-first-day-of-work-nsa-employee-spied-on-ex-girlfriend/
http://arstechnica.com/tech-policy/2014/07/snowden-nsa-employees-routinely-pass-around-intercepted-nude-photos/
http://arstechnica.com/tech-policy/2014/08/snowden-the-nsa-not-assad-took-syria-off-the-internet-in-2012/
https://www.eff.org/nsa-spying
https://www.eff.org/nsa-spying/timeline
https://ssd.eff.org/es/module/why-metadata-matters

https://freedom.press/blog/2013/06/encryption-works-how-protect-your-privacy-age-nsa-surveillance
https://ssd.eff.org/en/module/communicating-others
https://whispersystems.org/

https://savecrypto.org/