TNN Al-Tahrir News Network

Technology

Cryptography in a post-Snowden era

By: Lewis Sanders · June 26, 2014

SHARE

How important is it to protect your online presence? (graphic: Information Age)

Related Posts

Julian Assange: Ask Me Anything on Reddit recap

Germany to launch investigations over NSA spying

Snowden may seek asylum in Brazil

Germany may accept testimony from Snowden over NSA phone tap on Chanc. Angela Merkel

Germany kicks out Verizon phone company over US spying

Latest

Russia announce delivery of first warplane batch to Iraq
10:07:32 pm
Alexander Lukashevich, Russian Fore-more...

In the wake of Edward Snowden's release of classified documents concerning US National

Security Agency’s (NSA) espionage programmes, cryptography has witnessed a massive upsurge in interest from the average web surfer.

Did you know that you can track the geographic location of practically every email you receive? Go into the last personal email you received, click the button “show all information”, copy the IP address, and paste it into an IP tracker. There you go, now you know exactly where your friend, family member, or client sent that email. Now think of who has access to your email and how that information could be used.

In the wake of Snowden’s release of classified documents concerning the NSA’s espionage program, which revealed to the public its strategies to intercept data and store them, everything from Angela Merkel’s emails to Afghanis’ phone calls, cryptography, or the study, development, and implementation of secret codes to hide information from third-parties, has never been as important as it is now.

Undermining Security for Security’s Sake

For all that could be said concerning the NSA’s ability to access and store private data, nothing is more alarming than its collaborative efforts in implementing security protocols for the internet. One of the most notable cases concerning their involvement in undermining security protocols and cryptographic norms goes back to a leaked NSA report provided by Snowden in 2013.

“Recent news reports about leaked classified documents have caused concern from the cryptographic community about the security of NIST [National Institute of Standards and Technologies] cryptographic standards and guidelines,” wrote chief of the Computer Security Division at the NIST, Donna Dodson, following the release of a report which spelled out the NSA’s policy of implementing backdoor access within the US institute’s crypto algorithms.

The NIST is known for developing crypto algorithms used to encrypt private data (specifically, passwords, bank account information, etc.) on websites.

The issue with the NSA becoming “the sole editor” of the crypto algorithm developed by the NIST is that they were able to implement certain backdoors which would circumvent the security measures put in place, as Snowden’s leaks suggest. Though shortly after the reports surfaced, the NIST asked users of its crypto algorithms to discontinue use in fear that they had been compromised, it nonetheless puts into the question the relationship between institutions such as the NIST, who are responsible for developing cryptographic norms, in partnering with the NSA to create the next generation of widely used encryption protocols.

It is no longer current news that Google, Microsoft, Yahoo, and Facebook have willingly offered the NSA their users’ data, though most of the companies have escaped with minimum backlash after citing legal procedures when referencing the instances. One of the most important revelations to be divulged from their relationship regards PRISM, the NSA codename for a clandestine mass electronic-surveillance-data-mining programme, to which the aforementioned companies had

Pakistani Army launches major campaign against militants

10:02:01 pm

The Pakistani army began on Monday,-more...

Israel finds bodies of kidnapped teens

09:59:33 pm

The Israeli army has announced that-more...

Al-Sisi vows to avenge Monday's bomb attacks

09:56:56 pm

Egyptian President Abdel-Fattah Al--more...

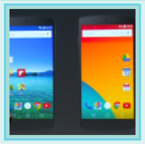
Hong Kong braces for rallies following pro-democracy vote

08:17:52 pm

Hong Kong is preparing for what is -more...

TNN Bulletin

Technology



All you need to know about Android L, Google’s latest OS

Posted on: Jun 29th, 2014

Cryptography in a post-Snowden era

Posted on: Jun 26th, 2014

History & Culture

Antiquities Minister demands action

reportedly complied with.

Beyond the NSA

The need for better and more accessible cryptographic technologies is not solely due to the NSA's practices. The fact that precedents are currently being made with regards to how governments may use laws to access user data outside of their jurisdiction suggests that the need for accessible cryptographic technologies is paramount. A pertinent example is that of Microsoft's appeal against a Federal search warrant to seize emails stored outside the US, namely Ireland.

Microsoft appealed the Federal court ordered search warrant that would force them to provide emails stored on servers in Ireland to the court. Microsoft's corporate vice president and deputy general counsel David Howard wrote in a blog post on the tech giant's website, "The US government doesn't have the power to search a home in another country, nor should it have the power to search the content of email stored overseas."

"The US has entered into many bilateral agreements establishing specific procedures for obtaining evidence in another country. We think the same rules should apply in the online world, but the government disagrees," Howard added.

Despite Microsoft's attempts to appeal the search warrant for electronic information, US magistrate Judge James Francis noted in a court document, "Even when applied to information that is stored in servers abroad, an SCA [Stored Communications Act] warrant does not violate the presumption against extraterritorial application of American law."

Though Microsoft is still appealing the Federal court search warrant issued by Francis, it also shows how persistent US institutions are at retrieving data outside their territorial boundaries. Even more so alarming is that national borders are no longer being considered when the US seeks out data, as we have witnessed with the leaked classified documents concerning the NSA's espionage programme. The implications of such seemingly legal processes are frightening as we continue to witness more users accessing and storing data online. The US court case concerning Microsoft serves as an example of how information stored outside the country could also be accessed even without the help of the NSA.

But as governments continue to grow more so bold in their attempts to access private data even at the cost of breaking the laws they have put in place, one thing is for sure: Cryptography is entering a new age.

Protecting Who You Were, Are, Will Be

One of the most unnerving ambitions of an ordinary web surfer is trying to understand the tools that are available to secure online privacy and create some form of anonymity on the internet. Maybe anonymity is not the end goal but, instead, a form of security in knowing that one's private information (i.e. chats, emails, browsing history, etc.) will not be compromised or even snooped on by third parties. Though there are many options for all varying degrees of expertise, there are also many

developing Old Cairo

Posted on: Jun 29th, 2014

Ramadan: A tale of mosques and lanterns

Posted on: Jun 28th, 2014

CAIRO

23 C

mist
humidity: 78%
wind: 3km/h NNW
H 23 • L 23

32 C	31 C	31 C	30 C	33 C
WED	THU	FRI	SAT	SUN

easy-to-use tools for the ordinary web surfer, most notably developed by the free and open source software group Tor Project.

The Tor Project has developed many of their products with the average internet user in mind. Though not 100% fool-proof (nothing is when it comes to the internet), the project offers some of the most nuanced and accessible technology for serving the privacy needs of a wide-array of web surfers at no cost. Here are a few questions Tor Project's Executive Director Andrew Lewman answered for us at TNN.

> **In the wake of Snowden's release of classified documents exposing the NSA's tactics at undermining people's privacy globally, do you see the future of online privacy as being much more exposed or potentially more secure?**
>
> *Lewman:* The Internet has never been anonymous or private. There are technologies to improve the economics of privacy and lower risks for users, such as encryption, tor, and other privacy enhancing technologies. The general public is now becoming aware of this fact. The fix is likely a mix of policy, technology, and consumer economics. I can't predict the future, but I think once knowledge is gained, many will make their own choices, some will want more privacy, some assume they never had any and continue on apace, others are dropping out and not using the Internet.
>
> **In your opinion, how important is it for web surfers to protect their online presence?**
>
> *Lewman*: This is a question of risk and threat modeling. For many Tor users, they trust Google, Facebook, Twitter, Microsoft, etc, but not all of the 3rd party advertising networks and people and devices between them and their destination. For others, taking a minority opinion can be life threatening, and they need to take more precautions. It's all a matter of learning enough facts and helping people think through their concerns and threats and then helping them choose which technology may work best to protect them. In general, we hope that the answer is Tor.
>
> **How easy are Tor Project's tools to use for ordinary web surfers? Do they require a certain level of knowledge?**
>
> *Lewman*: We design our products for the average user. We try to educate them on modeling their privacy and anonymity so they can maintain it. However, it's up to the user to understand the nuances and implications of their online behaviours when using Tor. For example, on the download page, we have a warning message to try to catch the users attention, http://torproject.is/download/download-easy.html.en#warning
>
> **What does the future look like for Tor Project?**
>
> *Lewman*: We're working on tools and technologies to keep Internet freedom and privacy alive. Generally, improving censorship circumvention, strengthening our privacy technology,

Find us on Facebook

TNN Al-Tahrir News Network
Like

45,448 people like Al-Tahrir News Network.

Facebook social plugin

Tweets Follow

TNN @altahrirenglish 10h
How to treat heat exhaustion - Al-Tahrir News Network fb.me/2VffaaR0x

TNN @altahrirenglish 10h
Al-Sisi vows to avenge Monday's bomb attacks - Al-Tahrir News Network fb.me/2BMPQQ6JO

TNN @altahrirenglish 15h
Russian journalist Anatoly Klyan was shot and killed by Kiev forces in eastern Ukraine. He is the 6th journalist... fb.me/3qs2ptPmR

> and doing all of this in an easy to use product is our future.
>
> **If you could give one piece of advice to future generations, what would it be?**
>
> *Lewman*: The Internet is your ‘permanent record’, act accordingly.

While the Tor Project is not the only facilitator of anonymity in the web, they do provide some of the most easily accessible technology for securing your online presence and private data. An honourable mention goes to Google’s upcoming End-to-End extension for Chrome which would allow Gmail users to encrypt their email given that the receiver also has the extension installed.

Why it matters

While some have suggested that we are gradually moving into an era wherein all data will be publicly accessible, others are drastically concerned with protecting their private information. Though there are still leaps to made within the domain of cryptography and usability, many tools exist to assist online users in encrypting their information, from web browsers to email services to more advanced operating systems.

But there is still a question that has been left unanswered. If governments are able to spy on our private communications and tap into our private data, why are we, as web surfers, not able to tap into theirs? Of course, the logic goes that they have information that should not be accessed and typically follows a discussion regarding national security or some other sycophantic argument of the sort. At the very least, implementing basic security practices to protect your private data is the first step to eventually resolving this question and promoting a more secure internet.

For more information concerning online data rights and privacy, check out the Electronic Frontier Foundation, an organisation that specialises in protecting digital rights.

Tags: Cryptography Edward Snowden NSA

0 Comments www.tnnegypt.com Login

Sort by Best Share Favorite ★

Start the discussion…

Be the first to comment.

ALSO ON **WWW.TNNEGYPT.COM** WHAT'S THIS?

In Moses' footsteps

1 comment • 2 months ago

AvatarDee Salah — Perfect :)

Fighting bubbles

1 comment • 9 days ago

AvatarMido Hassan — Bubble football Egypt

Meet Abdel-Fattah Al-Sisi

1 comment • 2 months ago

AvatarMohamed Kamel — Dr. Mohamed Morsy announced a presidential low – mid December 2012- protecting any of his decisions from being rejected or reviewed by the Highest Corte. All key oppositions and political activators …

Neck-and-neck presidential race in Colombia: Will FARC deal break the tie?

1 comment • a month ago

AvatarHassan Lotfy — Very informative

Subscribe Add Disqus to your site DISQUS