Gemalto hack shows how far we are from deciding acceptable 'security norms'

March 2 2015, by Keith Martin

Credit: AI-generated image (disclaimer)

Is it true spies hack technology companies? Can governments really listen to your phone calls? Should we care? The latest details of NSA and GCHQ intelligence agency activities to come from files leaked by Edward Snowden are of the apparently massive theft of mobile phone SIM card encryption keys from the Dutch firm Gemalto.

This "great SIM heist" targeted Gemalto because it produces billions of mobile phone SIM cards for 450 telecoms providers worldwide, and acquiring copies of encryption keys would make it possible to eavesdrop on cell phone calls with comparative ease. While press reports state these attempts were successful, after a brief internal audit – far too brief, some experts say – Gemalto has stated that nothing was stolen.

> Gemalto, a company that operates in 85 countries, has figured out how to do a thorough security audit of their systems in 6 days. Remarkable
>
> — Christopher Soghoian (@csoghoian) February 25, 2015

Who is right? Whether this is resolved or not, in this particular case the handbags will no doubt fly. But the fact of the matter is that there are bigger issues we should all be considering.

Putting walls around data

In the physical world we do a fairly good job of keeping ourselves secure. I assume, for example, that you locked your front door when you left your house this morning. In the digital world we tend to be a lot more careless. We tend to leave doors wide open. In many cases we don't even put doors between the outside world and our data. For intelligence agencies this is very fortunate since our emails, social media posts, and browsing habits are usually conveniently just lying around.

Encryption, on the other hand, provides a secure place with a front door behind which data is inaccessible. That is, unless you have the front door key. Encrypted data is meaningless and of little use to an intelligence agency – to make sense of it the keys to decrypt it are needed.

Mobile phones encrypt calls between the phone and the nearest mobile

phone mast, preventing anyone who intercepts the call as it travels through the air from making any sense of it. The encryption key used is derived from the phone's SIM key, which is a personal key that comes pre-installed on your SIM card. Anyone who knows the SIM key – normally only your phone and your mobile operator – can decrypt the call if they listen in.

Gemalto's business is putting SIM keys into SIM cards; if someone breaks into Gemalto's systems then it is certainly possible that they could make off with SIM encryption keys. This isn't great news for the security of whatever mobile phones they later end up in.

Sidestepping the locks

Bad though this sounds, it's really just the latest of many revelations of this type that have leaked out of the Snowden files. The picture that has emerged is of intelligence agencies clearly frustrated by the increasing use of encryption in our everyday technology. As the encryption is (mostly) too good to break, so the intelligence agencies have been using every technique imaginable to find a way around it.

Broadly speaking, there are really only two ways to get around good encryption. Option one is to try to access data either before it is encrypted or after it is decrypted – Snowden's files suggest the intelligence agencies have been doing plenty of that. Option two is to try to get hold of the keys needed to decrypt the data. The Great SIM Heist seems to be the latest example of attempts at this second strategy.

What do we want for the future?

In one sense this is not a new development. As encryption has been deployed more widely, its use has created tension between the rights of

the individual to privacy and the duties of the state to protect society. Over the last few decades governments have made several attempts to mediate between these, attempts which appeared to have concluded in favour of strong encryption and individual privacy.

Prior to Snowden it was publicly believed that the "crypto wars" had largely been lost by the intelligence agencies; instead, leaked files such as these reveal that the wars have just become bloodier than any of us really imagined.

Many people are outraged by the many Snowden revelations. Others take the view that this is the intelligence agencies' job and they ought to be left to get on with it. There are good arguments supporting both of these viewpoints.

So, should you care? If you do, then there has never been a better time to stand up and make your feelings known. We as a society really ought to form an opinion on what "security norms" we wish to see developing around our increasing use of the internet as a place where we, partially, live our lives. If we don't, then clearly others, with perhaps very different agendas, will decide them for us.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Gemalto hack shows how far we are from deciding acceptable 'security norms' (2015, March 2) retrieved 28 June 2024 from https://phys.org/news/2015-03-gemalto-hack-norms.html