GlobalResearch
Center for Research on Globalization

Stealing the Keys: The SIM Card Hacking Case

By Dr. Binoy Kampmark
Global Research, February 23, 2015
Region: Europe, USA
Theme: Intelligence

"Security to be Free." – Motto of Gemalto, producer of SIM cards

It is hard to muster enthusiasm for events that have become so frequent in their pummelling effect, they are as expected as the sun's clockwork appearance in the morning. It would, however, be dangerous to yawn at the latest Edward Snowden treat, one transmitted via Glen Greenwald's *The Intercept*.

The suggestions came out on Thursday that the US National Security Agency and fellow darling the UK Government Communications Headquarters went about the business of hacking the Franco-Dutch company Gemalto, one of the largest SIM card makers, for reasons of pilfering keys to the encryption codes held in the manufactured chips. These chips also have other uses – credit cards, passports and the like. (Life here falls into grand irony: the US government has a deal with Gemalto to make such chips for passports in the first place.)

Gemalto, obviously feeling that their security was either immune, or not interesting enough, to warrant a good hack, yielded the encryption keys in bulk as they were sent to carriers.[1] In what seemed like adolescent practice, the company resorted to sending the master key files via email or File Transfer Protocol (FTP), a sort of pinch me if you can statement. The hackers can hardly have been too impressed with their skills.

Gemalto have, instead, orchestrated something of a tactical retreat. No, they were not specifically targeted because of their vulnerability, the ease of obtaining the encryption keys, and because of their general shoddiness. The operation "was an attempt to try and cast the widest net possible to reach as many mobile phones as possible, with the aim to monitor mobile communications without mobile network operators and users consent."[2]

According to *The Intercept*, "In one two-week period, the team accessed the emails of 130 people associated with wireless network providers or SIM card manufacturing and personalization. This operation produced nearly 8,000 keys matched to specific phones in 10 countries." Another two-week period produced an even richer bounty: 85,000 keys.[3]

The agencies have had their expansive ears, in other words, to the majority of cell phone communications since 2010 without even needing to go through the pretence of seeking approval from telecom companies or foreign governments, though what, exactly, those ears have actually obtained is highly questionable. The agencies of the "Five Eyes" alliance have shown a good degree of deafness and blindness over time, and there is little reason to assume that such habits have changed.

Greg Nojeim, Senior Counsel of the Center for Technology & Democracy, was predictably gloomy about the shredding of privacy – as if there was much left to shred.[4] "Almost

everyone in the world carries cell phones and this is an unprecedented mass attack on the privacy of citizens worldwide. While there is certainly value in targeted surveillance of cell phone communications, this coordinated subversion of the trusted technical security infrastructure of cell pones means the US and British governments now have easy access to our mobile communications."

Then, there has to be the idea of result: what, exactly, did this vastly intrusive mission accomplish? Cell phone communication, for one, has minimal protections – the incentive to bolster the technological barriers to hacking were never there. End-to-end encryption simply does not take place, as it only covers discussions between the phone and the relevant tower.

Russell Brandon, writing in *The Verge*, suggested a good degree of futility arose from the effort. "The Gemalto attack is unique not just for its aggressive scope, but for how little it seems to have actually accomplished."[5] The point being made here is that intelligence services were already able to engage in stingray attacks, targeted exploits, and carrier requests via court order. And researchers were already full of the stock of woe for SIM-level attacks around such systems as the GSM (2G), which was plagued by no small measure to authenticate cell towers and poor encryption algorithms.

European legislators are also doing the rounds of manufactured outrage, though they can hardly be any more disturbed than what had already transpired from Snowden's revelations spectacular in 2013.[6] The European Parliament's chief negotiator on the European Union's data protection law, Jan Philipp Albrecht claimed that the hack was "obviously based on some illegal activities." The United Kingdom was doing more than just upsetting the applecart as a member of the European community in "not respecting the law of the] Netherlands and partner states".

Behind such activities lies the stench of collusion and complicity – governments in bed with others, filled with concessions and selective blindness; companies taking up with certain agencies in the hope of being left, essentially, alone. Privacy might be killed off, but business must go on.

Brandon is wrong to assume that this heist has achieved nothing. There are serious consequences that fly in the face of the Anglo-American obsession with corporate mercantilism. It is exactly such revelations that do wonders to puncture market confidence in communications security. (Just to prove a point, Gemalto's shares fell by 7.5 per cent on Friday.)

Such acts of stealthy plunder cut both ways, and while it looks dandily much like an assault on Gemalto, it was more correctly seen as a global assault on communications. For Matthew Green, cryptography specialist at Johns Hopkins Information Security Institute, this was "bad news for phone security. Really bad news" (*The Intercept*, Feb 19).

Not just for that side of the communications aisle, either. Visa, MasterCard, American Express, Chase, Barclays and JP Morgan will be having vexed boardroom meetings about customer suspicions and concerns. While the NSA-GCHQ collective may have gotten access in the name of excess at the price of privacy, they have also managed, in such conduct, to give the corporate sector a cold.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He

lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes:

[1] http://www.digitaltrends.com/mobile/nsa-gchq-sim-card-hack--snowden-leak-news/3/#how

[2] http://www.gemalto.com/press/Pages/Information-regarding-a--report-mentioning-a-hacking-of-SIM-card-encryption-keys.aspx

[3] https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

[4] https://cdt.org/press/us-and-uk-government-sim-card-hack-threat-to-privacy--infrastructure-security/

[5] http://www.theverge.com/2015/2/20/8079083/gemalto-sim-card-gchq-surveillance

[6] https://firstlook.org/theintercept/2015/02/20/gemalto-heist-shocks-europe/

Articles by: Dr. Binoy Kampmark