Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

GEMALTO SIM CARD HEIST

HOW VULNERABLE ARE THE INDIAN MOBILE PHONE SUBSCRIBERS?

Dilipraj E
Associate Fellow, CAPS

Edward Snowden, the whistleblower, has once again shocked the cyber community with his recent revelations about the heist of encryption keys belonging to Gemalto, a digital security company. These keys were stolen by none other than Government Communications Headquarters (GCHQ) and NSA, the digital signal intelligence agencies of UK and US respectively. According to the revealed documents, the Gemalto episode is part of GCHQ's covert programme to gain access to core mobile networks. Before moving on to the actual heist, a brief profile of the company Gemalto would give us an idea of the seriousness of the issue.

Gemalto, in its official website, is claimed as the world leader in digital security manufacturing products like SIM Cards, Banking cards, Mobile payment systems, two-factor authentication devices used for online security, Identity & Access cards, hardware tokens for securing buildings and offices, electronic passports and chip inbuilt identification cards.[1] Their customers list includes almost all the leading mobile network providers and wireless operators across the world, government agencies of many countries, and big business ventures. Their Subscriber Identification Modules (SIM) are used by mobile network service provider companies in more than 40 countries which includes countries like US, UK, France, Germany, Netherlands, Russia, Iran, India, Canada, Singapore and many European and African countries. The company produces nearly 2 billion SIM cards in a year and has created revenue of $2.7 billion in 2013.[2]

The Heist

According to *The Intercept*, an online news website, the British and American intelligence agencies - GCHQ and NSA, respectively - have access to millions of encryption keys of the SIM card manufacturing company Gemalto. Using these keys the agencies have conducted surveillance on all the customers of various mobile companies which use Gemalto manufactured SIM cards for their service. By using the stolen keys, the intelligence agencies could decrypt all call details and text messages of the mobile subscribers which would give them humongous amount of information that can be processed later to acquire desired data.

The details of this revelation were touted to be passed on to *The Intercept* by 'Edward Snowden'. Few random revealed documents related to this Gemalto Heist focus more on this secret programme. The revealed document suggests that the main aim of the program is to gain "*CNE access to core mobile networks*" for which various methods are adopted. It is found that billing servers were breached to get access to SMS, authentication servers were also breached in order to obtain K's, Ki's and OTA (One Time Access) keys, machines belonging to the sales staff and network engineers of a company were also intruded to acquire customer information and network maps respectively and finally the computers of Gemalto were implanted with bugs and information was extracted. According to the document GCHQ believes that they have the entire network of Gemalto.

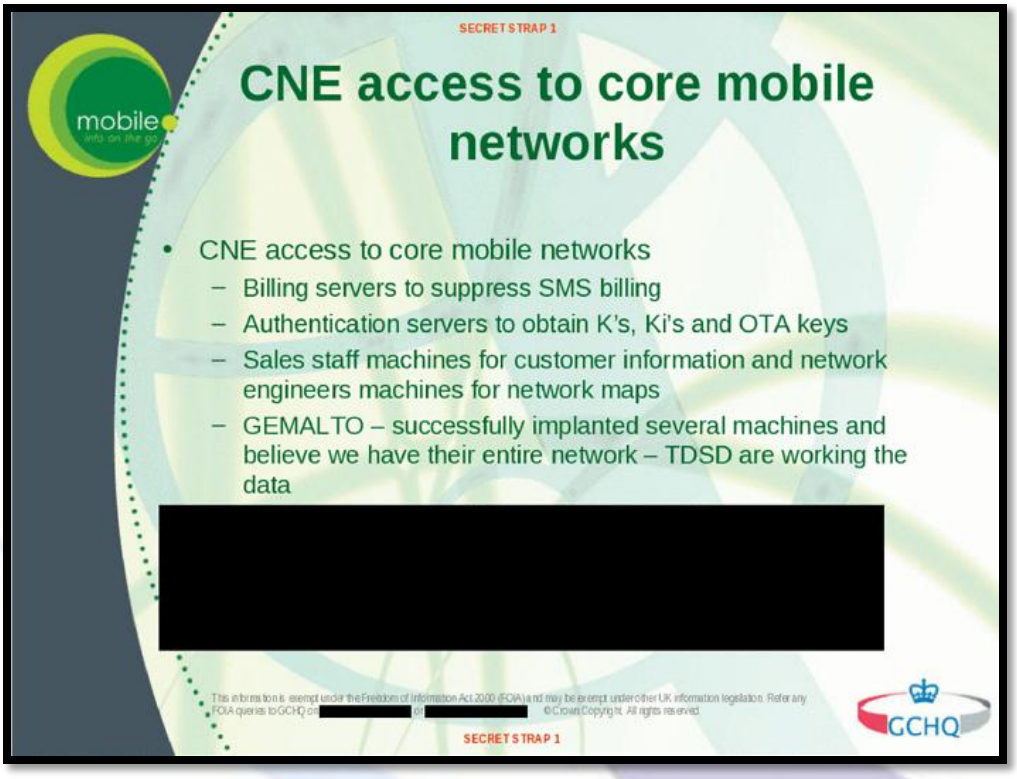

Image: Revealed Document explaining the GCHQ operation

The GCHQ and NSA's strategy of stealing the encryption keys of SIM cards is a master stroke in their ongoing surveillance program which would give them tremendous advantage in snooping into the mobile communication network of the world. In general, the mobile network providing companies do not manufacture SIM cards, instead it is outsourced to another company which manufactures the SIM cards and creates the secret encryption keys for each card. When the cards are shipped to the mobile network providing companies, the encryption keys are also shared either by physical mail services or through electronic transfer like email or other file transfer protocol methods with the companies. For a mobile phone to establish a connection to the wireless network, the SIM card uses its encryption key to authenticate itself with the network through a virtual 'handshake', for the mobile phone to connect to its intended network. Therefore, the encryption keys are important factors in mobile communication without which even if GCHQ and NSA agents manage to gather some communications they would not have been able to decrypt the communication without the possession of the keys. However, with the possession of millions of encryption keys with them, GCHQ and NSA agents could listen to

any subscriber's phone call or read anybody's text message in real time. Also, stealing of encryption keys has reduced the legal hassles for the intelligence agencies which otherwise would have to get legal approval from respective countries courts in order to conduct surveillance on foreign targets.

It has been revealed that the programme of stealing encryption keys from Gemalto started since 2010. The agencies achieved this task by cyber stalking on the company's employees in the virtual world. By gaining access to the email and social networking accounts of engineers and other employees of the company, the agencies have managed to collect information that leads them to gain access to millions of encryption keys.[3] In order to process their collected information about the employees and to find a prospective target, the agencies use the covert data processing programme of NSA - "Xkeyscore". The identified person is marked for follow up to acquire the encrypted keys. This is evident from the revealed document which states: *"(He) appears to be a Sales Manager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in XKEYSCORE. Again, if we ever become more interested in this area, he would certainly be a good place to start."*

In short, from the recent revelation about the Gemalto SIM card heist by GCHQ and NSA, it is clear that the agencies not only target prospective terrorists but their surveillance is on everybody who uses technology for everyday communication. It can also be stated that, it is not only the terrorists who become targets but anybody in the world can become a target if he/ she is found to be a potential information possessor that will be of help to the national security of UK and US.

How does this affect India?

For India, which has always been a target in all the covert cyber programmes of US and UK, it has once again occurred in this Gemalto encryption keys heist episode too. It can be inferred that Indian mobile subscribers have also been exposed to the mass surveillance conducted by US and UK because Gemalto was the supplier of SIM cards to Indian Mobile network providing companies like Bharti Airtel and TATA Docomo. In fact, Gemalto received "Value Partner of the Year" award from Airtel for the year 2009 for its service with the company[4] and TATA Docomo started its association with Gemalto on February 21,

2010.[5] In other terms, it means that all Indians who use Airtel and Docomo Networks as their mobile network are vulnerable to the covert operations as their calls and text messages could have been tapped by GCHQ and NSA.

Since there is a possibility that all of Gemalto's network could have been compromised by GCHQ and NSA as it is believed that they have Gamalto's whole network, makes the situation worse for other Indian customers. It has been found that four Indian companies are partners with Gemalto for their other products. These companies are

- Genesis Futuristic Technologies Limited - supplies unknown product to Indian Government fitted with Gemalto manufactured chip.
- K.D.K Softwares (India) Pvt. Ltd. – uses Identity & Access product from Gemalto
- Bay Datacom Solutions Pvt. Ltd. – uses Identity & Access product from Gemalto
- Agmatel India PTE Ltd. – Supplies unknown product to Indian Government fitted with Gemalto manufactured chip.[6]

Additionally, India is identified as one of the 'Target Personalisation Centres' in one of the revealed documents, along with other countries like Brazil, China, Japan, Malaysia, etc. It has been opined that Vodafone India Network might have also been compromised as it is a UK based firm and Vodafone also uses Gemalto SIM Cards for its network.

Conclusion

The information according to the revealed documents states that GCHQ has got automated systems for 'harvesting' encryption keys through various sources. This explains the amount of sophisticated technologies these intelligence agencies operate with in order to conduct mass surveillance on world citizens. This revelation has once again reiterated the vulnerability in the existing Information and Communication Technology (ICT) of the world and the way the virtual world is being governed. The question of individual's privacy and its impeachment by powerful countries are again in the forefront. The fact that Gemalto may not be the only company that might have been compromised by GCHQ and

NSA creates more panic in the minds of other chip manufacturing companies, cyber community and even the general public. While a viable solution may not be possible immediately to counter such covert programmes, long term solutions can be achieved only if the world community truly understands the nature of the virtual world, i.e. borderless, and frames universal policies to ably govern the activities in this world.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1] www.gemalto.com/company-info, accessed on February 23, 2015.

[2] Jeremy Scahill & Josh Begley , "The Great SIM Heist – How spies stole the keys to the encryption castle", *The Intercept*, February 20, 2015, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/, accessed on February 21, 2015.

[3] Ibid.

[4] "Gemalto Named "Value Partner of the Year" by Bharti Airtel in India", *Smart Card Alliance*, May 07, 2009, http://www.smartcardalliance.org/gemalto-named-value-partner-of-the-year-by-bharti-airtel-in-india/, accessed on February 22, 2015.

[5] "TATA Docomo Partners with Gemalto", Business Standard, February 22, 2010, http://www.business-standard.com/article/press-releases/tata-docomo-partners-with-gemalto-110022200097_1.html, accessed on February 22, 2015.

[6] Partner Locator, Gemalto, www.gemalto.com/companyinfo/partners/partners-list, Accessed on February 23, 2015.
