Findings of Gemalto's investigations into the alleged hacking of SIM card encryption

Following the release of a report by a news website in February 2015, Gemalto has conducted an investigation, based in particular, on two elements: the purported NSA and GCHQ documents which were made public by this website, and its internal monitoring tools and their past records of attempts of attacks.

Image: www.freedigitalphotos.net

All comments in this publication assume that the published documents are real and refer accurately to events that occurred during 2010 and 2011. Our publication here below does not aim at confirming partially or entirely nor at providing elements to refute partially or entirely the contents of those website published documents.

As a digital security company, people try to hack Gemalto on a regular basis. These intrusion attempts are more or less sophisticated and we are used to dealing with them. Most are not successful while only a few penetrate the outer level of our highly secure network architecture.

If we look back at the period covered by the documents from the NSA and GCHQ, we can confirm that we experienced many attacks. In particular, in 2010 and 2011, we detected two particularly sophisticated intrusions, which could be related to the operation. In June 2010, we noticed suspicious activity in one of our French sites where a third party was trying to spy on the office network. By office network we mean the one used by employees to communicate with each other and the outside world. Action was immediately taken to counter the threat.

Second incident

In July 2010, a second incident was identified by our security team. This involved fake emails sent to one of our mobile operator customers spoofing legitimate Gemalto email addresses. The fake emails contained an attachment that could download malicious code. We immediately informed the customer and also notified the relevant authorities both of the incident itself and the type of malware used. During the same period, we also detected

several attempts to access the PCs of Gemalto employees who had regular contact with customers.

At the time we were unable to identify the perpetrators, but we now think that they could be related to the NSA and GCHQ operation. These intrusions only affected the outer parts of our networks - our office networks - which are in contact with the outside world. The SIM encryption keys and other customer data in general, are not stored on these networks. It is important to understand that our network architecture is designed like a cross between an onion and an orange; it has multiple layers and segments, which help to cluster and isolate data.

While the intrusions described above were serious, sophisticated attacks, nothing was detected in other parts of our network. No breaches were found in the infrastructure running our SIM activity or in other parts of the secure network that manage our other products, such as banking cards, ID cards or electronic passports. Each of these networks is isolated from one another and they are not connected to external networks.

It is extremely difficult to remotely attack a large number of SIM cards on an individual basis. This fact, combined with the complex architecture of our networks explains why the intelligence services instead, chose to target the data as it was transmitted between suppliers and mobile operators as explained in the documents.

Reduced risk

The risk of the data being intercepted as it was shared with our customers was greatly reduced with the generalisation of highly secure exchange processes that we had put in place well before 2010. The report indicates that attacks were targeted at mobile operators in Afghanistan, Yemen, India, Serbia, Iran, Iceland, Somalia, Pakistan and Tajikistan. It also states that when operators used secure data exchange methods the interception technique did not work. In particular it, failed to produce results against Pakistani networks. We can confirm that the transmission of data between Pakistani operators and Gemalto used the highly secure exchange process at that time. In 2010, though, these data transmission methods were not universally used and certain operators and suppliers had opted not to use them. In Gemalto's case, the secure transfer system was standard practice and its non-use would only occur in exceptional circumstances.

The analysis of the documents shows that the NSA and GCHQ targeted numerous parties beyond Gemalto. As the leader in the market, Gemalto may have been the target of choice for the intelligence services in order to reach the highest number of mobile phones. However, we can see in the document that many aspects do not relate to Gemalto, for example:

- **Gemalto has never sold SIM cards to four of the 12 operators listed in the documents, in particular to the Somali carrier where a reported 300,000 keys were stolen;**
- **A list claiming to represent the locations of our personalisation centres shows SIM card personalisation centres in Japan, Colombia and Italy. However, we did not operate personalisation centres in these countries at the time;**
- **Table 2 indicates that only 2% of the exchanges of encryption keys (38/1719) came from SIM suppliers and states that the use of strong encryption methods by SIM suppliers means that the other groups (98%) are much more vulnerable to these types of attacks.**

In 2010-2011 most operators in the targeted countries were still using 2G networks. The security level of this second generation technology was initially developed in the 1980s and was already considered weak and outdated by 2010. If the 2G SIM card encryption keys were to be intercepted by the intelligence services, it would be technically possible for them to spy on communications when the SIM card was in use in a mobile phone. This is a known weakness of the old 2G technology and for many years we have recommended that operators deploy extra security mechanisms. However, even if the encryption keys were intercepted by the intelligence services they would have been of limited use. This is because most 2G SIMs in service at that time in these countries were prepaid cards which have a very short life cycle, typically between three and six months.

Weakness removed

This known weakness in the original 2G standards was removed with the introduction of proprietary algorithms, which are still used as an extra level of security by major network operators. The security level was further increased with the arrival of 3G and 4G technologies, which have additional encryption. If someone intercepted the encryption keys used in 3G or 4G SIMs they would not be able to connect to the networks and consequently would be unable to spy on communications.

Therefore, 3G and 4G cards could not be affected by the described attack. However, though backward compatible with 2G, these newer products are not used everywhere around the world as they are a bit more expensive and sometimes operators base their purchasing decision on price alone.

Digital security is not static. Today's state-of-the-art technologies lose their effectiveness over time as new research and increasing processing power make innovative attacks possible. All reputable security products must be redesigned and upgraded on a regular basis. SIM cards are no different and they have evolved over time. In particular, the technology was massively re-developed for 3G and 4G networks.

Security is even higher for mobile operators that work with Gemalto to embed custom algorithms in their SIM cards. The variety and fragmentation of algorithmic technologies used by our customers increases the complexity and cost to deploy massive global surveillance systems. This is one of the reasons why we are opposed to alternative technologies which would limit operators' ability to customise their security mechanisms. Such technology would make it much simpler to organise mass surveillance should the technology unfortunately be compromised or fail.

The best security levels

Gemalto would like to reiterate its commitment to providing the best security levels for civilian applications. Our security products, infrastructure and processes are designed to ensure the highest degree of security in a global, open, and commercial environment. These are regularly audited and certified by third-party private and public organisations.

Nevertheless, we are conscious that the most eminent state agencies, especially when they work together, have resources and legal support that go far beyond that of typical hackers and criminal organisations. And, we are concerned that they could be involved in such indiscriminate operations against private companies with no grounds for suspicion.

In light of the recent events our main focus is our customers. Our teams have particularly appreciated the support that they have shown us in the past few days. These events inspire our people to work even closer with our customers and the industry to build even more sophisticated solutions to serve the needs of end-users.

In today's world, any organisation could be subject to a cyber-attack. Therefore, it has never been more important to follow security best practices and adopt the most recent technologies. These include advanced data encryption, so that even if networks are breached, third parties cannot access any of the stolen information.

Gemalto will continue to monitor its networks and improve its processes. We do not plan to communicate further on this matter unless a significant development occurs.

For more, visit: https://www.bizcommunity.com