Security & Privacy

How secure is your data?

Sabrina Schmitzer

27.05.2015

Introduction

In the realm of Security and Privacy a lot depends on a reliable encryption. That's why it's a area in which there is a constant development, because the "bad guys" of the business never stop either to crack the code or get into the system.

To represent the power game which is always present, I am going to represent important individuals from both sides . At first I will introduce Arthur Scherbius, the inventor of the enigma. After that I will concentrate on Marian Adam Rejewski, who was heavily involved in deciphering the enigma. Making a small time leap I will then continue with a more modern thread, the hackers. In this area, I will would like to introduce two individuals, Kevin Mitnick and Tsutomu Schimomura. The first is one of the most famous hacker in the world, and the other was the one who stopped the other.

1 Arthur Scherbius

Arthur Scherbius is the inventor of the encoding machine enigma, but how did he come to invent such a devices? He was born in Frankfurt am Main in 1878, studied engineering and founded his own company in 1918 called Scherbius&Ritter with his close friend Richard Ritter.

He was very interested to replace the old chiffre systems of the first world war with new ones. For this he wanted to use the technical possibilities of the 20th century. That is how the enigma, which is based on cipher disk and a rotating mill, came to be.

At first Arthur was of the opinion, that because of the level of the security, the enigma would be in great demand. He tried to sell the machine to the

privet enterprises and the army, for which he had a more advanced version, but neither of them were very interested at first. The army because at the point they were still very wary because of the failure in encoding they had during World War One and the privates because they were imitated by the huge price, 50000 Mark.

He was not the only one trying to sell his machine, three others, from different countries, tried it as well , but Arthur was the only one of them who did not stay unsuccessful. 1928 the army began to use the enigma for their uses. Even if he witnessed the beginning of the military use of his machine, he never got to see what a success his invention brought the German army in World War Two, or it's defeat that helped in ending the war. That is, because he died in 1929 in an accident.

2   Marian Adam Rejewski

Marian Adam Rejewski was born in Bydgoszcz, Poland. He studied mathematics in Poland and after that he attended a cryptology course instructed by the Cipher Bureau. After that he began a two year long statistic course in Germany, but he never finished it, because after he took a break from it, he was offered a teaching position at the Poznan university. He also worked part-time at the Poznan Bureau of the cipher bureau, because he was the most gifted of a group of twenty candidates in a new recruiting strategy of the polish. They switched from specialising on linguists to scientists. 1932 he started working fulltime in the Bureau in Warsaw. There he was joined by Jerzy Rozyeki and Henryk Zagalski, two polish mathematicians.

His methods allowed them to decipher most messages encoded by the enigma, but in 1936 the Germans complicated the encoding procedure. In 1938 they were again able to decipher three quarter of the messages, at which there was added a further complexity added to the enigma.
When Poland was invaded by the Germans, Rejewski and others from the Bureau were evacuated to Romania, before the troops reached Warsaw. The three mathematicians avoided the refugee camp, were able to contact the French embassy and were evacuated to Paris. There they joined the Château des Fouzes intelligence unit and by the end of the year they were again managing to decode the messages from the enigma.
Over the time they had to flee multiple times. From France to Algeria, back to France, then to Spain, only to be put into prison there. After they were set free they went to Portugal and from there to Britain where they stayed

for the rest of the war. When he got back home there were enquiries carried out by the Polish Security Service, but they did not find out about his role in deciphering the enigma.

In 1973 his involvement in the deciphering of the enigma emerged, from which he became famous. He later died from a heart attack.

3   Kevin Mitnick

Kevin Mitnick was born 1963 in America and works as a computer security consultant, but that is not what he is most well known for.

Kevin Mitnick is probably one of the most famous hackers in the whole world. He even landed on the FBI most wanted list.In 1979 Kevin hacked the first computer and copied secured software.

He hacked into not less than forty major corporations just for the challenge. That is also how he was caught. He hacked into to the company of one Tsutomu Shimomura, whom i will talk about later. This attack was not random, he always prided himself with being able to hack large companies, without being caught, and if he was caught and sentenced to prison, he did not stop, he continued after he had set his sentence. The attack itself was also very well planed out, he even picked the 25th of December to have a lesser chance of being disturbed or caught. Two and a half year later he was arrested and was sent to prison to be released five years later. That was his last arrest in 1995.

Now he owns his own security company and is also very highly in demand in checking security systems to help them protect their data more securely. Even the media has a great interest in him and he has been in multiple shows to talk about security.

4   Tsutomu Shimomura

Tsutomu Shimomura is a japanese citizen, but was raised in Princton, New Jersey. In 1984 he became a staff physicist at the Los Alamos National Laboratory and was one of the most architects of an advanced parallel computer. 1989 he came to the University of California. Now he is a senior fellow at the San Diego Supercomputer Center.

Tsutomu Shimomura shows that not all hackers are bad. He was one of the many hacking victims of Kevin Mitnick. Kevin had robbed him ninety-four personal files, but Tsutomu was able to trace him back and so helped the FBI in getting the Kevin Mitnick arrested.

Summary

Privacy and Security is a topic that neither is a new topic, as it has been around for hundreds of years, or will stop being an important aspect of our world for a long time neither.

Just the way how it is managed within a society has changed, and will most likely also change in the future. There will always be new individuals who will threaten the security of a person, a company or a country. That also means that there will be others who will try protect those.

Petzold, Hartmut, "Scherbius, Arthur" in: Neue Deutsche Biographie 22 (2005), S. 685-686 [Onlinefassung]; URL: http://www.deutsche-biographie.de/ppn127822089.html

http://www.history.co.uk/study-topics/history-of-ww2/code-breaking

http://cs-exhibitions.uni-klu.ac.at/index.php?id=282

http://www-history.mcs.st-and.ac.uk/Biographies/Rejewski.html

http://www.gizmodo.de/2011/09/25/hacker-geschichte.html

https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography

http://takedown.com/bio/

http://www.takedown.com/bio/tsutomu.html

http://www.tomshardware.com/reviews/fifteen-greatest-hacking-exploits,1790-11.html