Towards new cryptographic concepts 1/2

General Military Review No. 54

le chef de bataillon Mathieu MORALES

Published on 21/03/2019

Sciences & technologies

While a security gap often takes several years to close, the interconnection of systems continues to grow exponentially, paving the way for new threats. While today's computing power remains relatively limited, massive attacks with increasingly serious consequences are multiplying and highlighting the system's shortcomings. At the same time, the advent of quantum computers in the near future will call into question the very basis of our concepts for securing transmissions. Battalion Commander Morales considers that cryptographic research today is of strategic importance in order to face tomorrow's threats.

Since it became commonplace in the 1990s, the Internet has continued to evolve to adapt to the demands and needs of users.

As a result, an increasing proportion of systems find themselves connected when they were not intended to be. Systems are rarely reinvented, and modern IT development tends to add software bricks or interfaces to existing bricks. Security holes have existed since the origin of IT and continue to exist without any component escaping them. Sometimes it takes many years to fix them. Dirty cow[50] for example, took nine years to correct.

More recently, it is a flaw discovered in the WPA2 protocol (secure access to wifi networks) that is in the news. Beyond the flaw itself, it is the time it will take to abolish it that worries the National Commission for Information Technology and Civil Liberties (CNIL).[51].

Current Threats

In 2010, the STUXNET[52] had surprised the international community because it was the first recognized cyberweapon. Thus, without physical contact or deployed troops, the United

States had managed to stop the Iranian nuclear programme by taking advantage of the connections necessary to update its nuclear equipment.

But these techniques are no longer the prerogative of state actors today. 2017 was the scene of several large-scale actions. One of the most massive was WannaCry, which affected many companies around the world. This ransomware exploited the EternalBlue rift[53] of Windows systems prior to Window10. Once in place, the virus encrypted all data that could only be deciphered by paying a ransom. Windows XP, which is still running in many businesses (including many ATMs), was the most affected and allowed the virus to spread. At the same time, Adylkuzz relied on the same loophole to use the infected computers to produce crypto currency, with the gains for the hackers estimated at one million dollars. Finally, last summer, NotPeya affected large companies by disrupting part of their business; in France, the giant Saint-Gobain saw some of its subsidiaries (Lapeyre, Point P) completely paralyzed. 220 million, or 1.1% of revenue for the first six months of the year, and in France, the giant Saint-Gobain saw some of its subsidiaries (Lapeyre, Point P) come to a complete standstill.[54]. These attacks affect not only companies, but also sensitive and strategic infrastructures without collateral damage that cannot be controlled (hospitals, state institutions and nuclear power plants).

Our society has thus gradually allowed itself to be overwhelmed by the multiple network connections and is struggling to control, on the one hand, the quantity and, on the other hand, the flow of information circulating on the web. However, modern technologies and research are tending to further accentuate the circulation and dispersal of data.

Evolving threats

Web 2.0 and the invention of smartphones have revolutionized uses and value systems. We are now in the early stages of what many consider to be the third digital revolution with the emergence of the "internet of things". In addition to the smartphone and other connected watches, many other everyday objects are now being added to them (programmable light bulb, remote-controllable shutter, connected car, etc.). They constitute an increasingly dense network with its share of vulnerabilities because there is no security standard yet applied to these new technologies. The vulnerabilities are most often located at the level of the firmware that allows interaction with the hardware (firmware). These are difficult to secure because there is no antivirus software and because each component has its own specificities. Secondly, failure to comply with good security practices is too often observed (for example not changing default identifiers) and amplifies security problems.

It is true that the trade in connected objects began in the leisure and home automation fields, but it is in the medical field that progress is most expected. Combined with Big Data technologies, data sensors, embedded on patients, could make it possible to statistically predict the risk of recurrence of a serious illness or even alert a doctor of an incident. In order to keep these objects ergonomic, the measured information is transmitted to larger structures that store and process it. The amount of data is increasing and requires ever greater computing power.

Our armies are no exception. For several years now, the digitisation of the battle space has been a considerable challenge and the number of interacting systems has been growing steadily. Whether it is combat with the Félin system, communications with UAVs, or robotics, they all contribute to a multitude of data transmissions.

Thus, while system interconnections are already a source of threats, vulnerabilities and backdoors for accessing information will multiply and require new protocols to secure exchanges.

Securing information

At present, there are two types of encryption, one called symmetric, the other called asymmetric.

With symmetric encryption, a single key is used to both encrypt and decrypt the data. One of the best known is the "disposable mask" or Vigenère encryption, which is considered unbreakable by following precise key generation rules. The most commonly used are the triple DES and AES. While this type of encryption offers relatively satisfactory levels of security, it poses problems for key transmission.

To counter this, Whitfield Diffie and Martin Hellman introduced the concept of asymmetric encryption to the public at the National Computer Conference in 1976. Encryption is based on a pair of keys; the first, made public, is used to encrypt data; the other, kept secret, is used for decryption. This eliminates the need to exchange keys. Public-key encryption is widespread on the Internet and forms the basis for almost all secure transmissions. The best known is the RSA[55] used in SSL/TLS connections[56]s, online payments, electronic signatures and secure PGP messaging.[57].

Two mathematical principles surround the concept of asymmetric encryption: the discrete logarithm problem and the decomposition into prime numbers. In both cases, there is no efficient algorithm for solving the problem and it is necessary to try all combinations to find the one that gives the desired result. Thus, although it is possible to decrypt messages without the private key, this operation requires computing power that is not available. The principle is therefore to play on decryption times. This manipulation can take several years with classical algorithms and modern computing, but these times will be considerably reduced with the advent of quantum computers.

50 A flaw allowing to obtain privileges without leaving traces on the Linux system: http: //www.zdnet.fr/actualites/dirty-cow-une-faille-vieille-de-9-ans-corrigee-au-sein- du-noyau-linux-39843818 .htm

51 https://www.numerama.com/tech/298472-lanssi-salarme-la-faille-krack-va-we-do - livee-during-des-annees-avec-des-wi-fi-perces.html

52https://www.nouvelobs.com/rue89/rue89-internet/20120604.RUE0433/stuxnet-cow-the united states-and-israel-have-pirate-le-nucleaire-iranien.html

53 https://fr.wikipedia.org/wiki/EternalBlue

54 http://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.html

55 RSA encryption (named after the initials of its three inventors) is an asymmetric cryptographic algorithm widely used in electronic commerce, and more generally for exchanging confidential data over the Internet. This algorithm was described in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman.

56 SSL (Secure Socket Layer) / TLS (Transport Layer Security) is the most widely used security protocol that creates a secure channel between two machines communicating over the Internet or an internal network.

Title :	le chef de bataillon Mathieu MORALES
Author (s) :	le chef de bataillon Mathieu MORALES
Release date	14/03/2019