The evolution of IT Security from Network Security to Identity Access Management and Zero Trust

Abstract

IT security has much developed in the last years, but the security scenario today is such that the IT systems cannot be trusted and IT security incidents must be considered as inevitable. The "perimeter defence" approach is not able to cope with the current IT security threats, and to protect the IT systems it is necessary to implement strong and agile IT Security Threats and Risk management programs based on a Zero Trust approach.

In the last 15 years, IT security has developed enormously, probably even more than IT itself. Notwithstanding this, we cannot surely affirm that our digital life and all our digital information and data are safer today than 15 years ago. It is useful to look at what has happened and what is happening to understand what we achieved, what we are trying to do to improve IT security and what we are still not addressing.

Obviously it will not be possible in this short essay to address all areas and all aspects of IT security, but we hope to cover at least some of the significant issues.

IT evolution

If we look back, a lot has changed in the pervasiveness and use of IT in the last years: 15 years ago the Personal Computer was a <u>work</u> instrument that was becoming also a household tool, families started to have one PC at home for <u>family</u> use, from keeping in touch with friends and relatives to booking vacations. Now we have <u>personal</u> devices, typically smartphones, that follow and dictate almost every minute of our life: we keep friends, relations and the entire world up to date on what we are doing, we search all possible kind of information, we get an infinite number of suggestions, we buy many different kind of goods, we manage our bank accounts, credit cards etc.

There are multiple dimensions to the IT evolution, some of them are:

- the technology: the type of devices evolved in time and purpose, from the large mainframes (still running) to the smallest “smart” devices (not only phones but also watches, glasses etc.)
- the users: to the initial research community have been added business, family, individuals and in the future, the “Things” (see below)
- the type of information managed: this has scaled following the users of IT but extending much more than those, by now most information related to individuals is managed by IT systems both private and work related.

Indeed it seems that the near future will bring us the Internet of Things (IoT) where all kind of devices, from televisions to refrigerators, washing machines, cars, light bulbs and whatever else, will connect to us digitally.

The meaning of “IT Security”

IT security goes back at least to the '70s and '80s [1,2]. In those years IT security meant military security that started from the principle of controlling who is accessing which information. This required to classify and label (like “Secret”, “Top Secret” etc.) each data and to implement rules so that only those who have the appropriate security clearance can access each data.

In the '80s and early '90s networking and internet were born, IT became widespread first in universities and research centres, then in businesses. Classifying and labelling information did not make much sense in this contest since the vast majority of information was public at least to all those having access to the networks.

So a new approach to IT security emerged which was focused on avoiding misuse and consequences from vulnerabilities and bugs.

From the mid-90s internet, web, business and private use of IT started to grow exponentially. Some data managed by today's IT systems can be considered public, but other data, for example for economical transactions or sensitive private or business information, must be protected and must be accessible only to those authorized.

Unfortunately since then, also for commercial and economical reasons, IT security has been mostly considered as an add-on to an IT product or service, and not built-in from the beginning.

It is possible to classify in two main kinds the IT security features so developed:

1. Defensive features: IT security features introduced or added to IT systems, networks and applications to prevent unauthorized access or exploitation of vulnerabilities and bugs;
2. Confidentiality (and also availability and integrity) features: IT security features that provide security services, like authentication and authorization.

The following are simple and basic examples of these two kinds of IT security features.

The first example is the advent of the Firewall and the concept of Perimeter (or Network) Security. In the late '90s and early 2000s it was considered good practice to divide the IT network world in "Inside" and "Outside" and to position a Firewall at the connection between these two worlds with the purpose of allowing the income of only "trusted" connections. Usually the outgoing traffic was unrestricted.

The "Inside" IT systems were trusted, whereas the "Outside" systems were untrusted by default. So all traffic, connections, activities were allowed if originated from the "Inside" IT systems or from trusted "Outside" IT systems.

Filtering outside connections has the purpose of avoiding abuse of the internal IT systems, and of preventing unauthorized access or exploitation of vulnerabilities and bugs.

But very soon it was realized that not all internal users and systems could be trusted in the same way, so that typically internal networks were also divided in three or more "zones": a Demilitarized zone (DMZ) facing the outside world, an internal Local Area Network (LAN) and a secure LAN with restricted access also for internal users.

The main example of IT application security features is just the well known "username+password" mechanism and in general the processes of Authentication, Authorization and Accounting (AAA). The defensive IT security features discussed previously are mostly built outside or on-top of IT applications and services, whereas IT application security features have to be built within the applications and services and must function within their business and application logics. Indeed each IT application and service must be aware of each user, and must manage data and functionalities for the individual user.

In this case the role of security can be perceived differently by different people. Indeed if all the internal users (or all the users of one internal security zone) are trusted, do we need to have "password" or using just "usernames" is enough? Since our Firewalls prevent untrusted connections to the internal zone, purely following logic (and costs) we could say that "passwords" are not needed and that we can do well enough just with "usernames". But if we look at it from a security risk perspective, we conclude that the trust in the Firewalls and in the users is most likely overrated. We surely do need "passwords"! And better if they are not default nor trivial.

The end of the first IT security achievements

For more than 10 years we built security in IT systems mostly as described above, sometimes better, even much better, but most often we just merely managed.

What we realized in the mid-2000s was that the security of our IT systems was working more or less as in this famous image [4]:

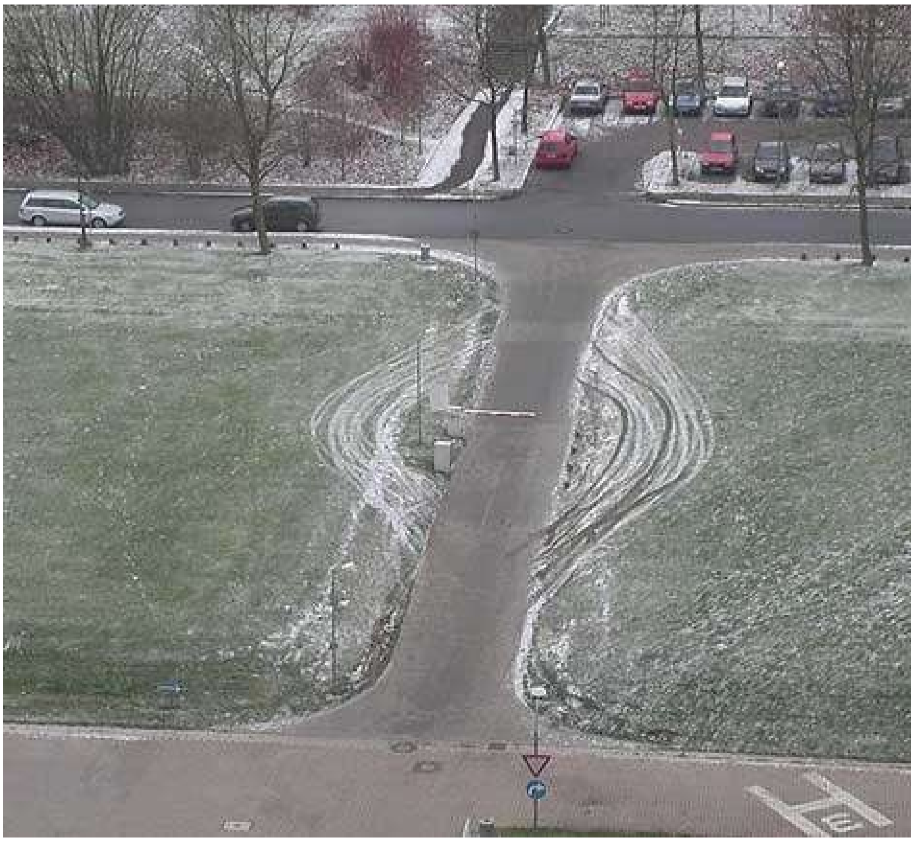

Fig. 1. Security avoided

the bar in the middle should represent our Firewalls and related security tools, and the tracks of the cars, the paths of the real transactions.

The evolution of IT Security

Already in 2007 [3] there was the claim that the IT Perimeter Security was “dead”, at least in part. In 10 years the security threat scenario had changed dramatically, from a research environment where attacks where almost pranks or at most isolated crime attempts, to a business environment where organized crime had started exploiting the presence of companies on internet and the connection to internet of their IT systems. Dividing the world in trusted and untrusted users by setting a firewall in between, was definitively not enough. The approach to IT security was then extended by including new security features like the following:

- improving the security of the users' endpoint devices mostly by using anti-virus tools and configuration management
- further segmentation of internal networks
- more network and perimeter defences, like Intrusion Detection and Prevention Systems (IDS/IPS), Web Proxy Filtering and Web Application Firewalls, Network Access Control / Protection (NAC / NAP) etc.
- adoption of encryption for critical internal data, backups etc., for external communications, like Virtual Private Networks (VPN), for authentication and confidentiality of web services (web certificates and encrypted web sessions), etc.

Another important point was the realization of the importance of fixing security software vulnerabilities and bugs in operating systems, server applications and user applications. Notable on this has been Bill Gates' “Trustworthy Computing” initiative [5].

Security advances cannot “break” IT

Still the development must be by gradual evolution and cannot be by revolution. In other words, we cannot change IT from one day to another to introduce a higher level of security and trust. Indeed this often would require a complete overhaul not only of all IT systems all over the world, but also of all businesses all over the world which by now all rely in one way or another on IT,[1] and would have dire implications for the every day life of most people on our planet.

IT protocols must be modified gradually over the span of many years, giving everybody the time of upgrading before retiring old, insecure versions. The same is true for major upgrades in operating systems, server applications and user applications, whereas updates and bug-fixing have by now become periodic common practice.

A primary example of this practical problem is the management of the introduction of new cryptographic protocols and algorithms and of the withdrawal of cryptographic protocols and algorithms which have been broken or are considered too weak or insecure. Very often cryptographic protocols and algorithms are built-in in applications and operating systems, and it is not possible to change them without re-writing, sometimes even in an extensive way, part of the applications and operating systems themselves. This takes time and exposes the users and the IT systems to the risk of using broken cryptographic protocols and algorithms which instead of providing security features, are a vulnerability and create a risk of attacks, intrusions and economical or personal loss.

A simple scenario and attack vector

Before proceeding, it is convenient to explore a simple scenario of an attack vector, described in Figure 2, which will be useful to clarify one class of threats to which our IT systems are subjected daily.

[1] Think about all financial and economical business transactions which, as of today, are all done through some IT systems, from banks, to credit cards and digital only currencies.

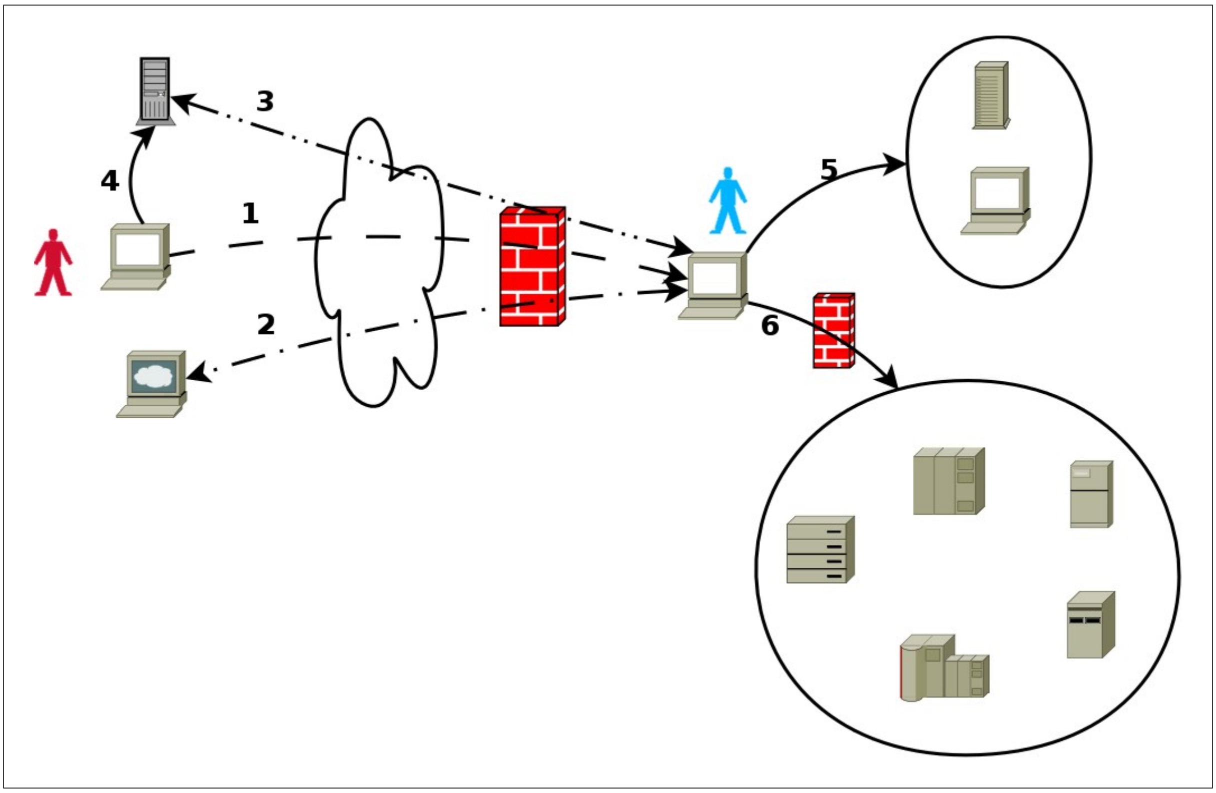

Fig. 2. A simple attack vector

We assume that an attacker (the red man in Figure 2) is interested to access the IT systems of a company. Quite often the purpose of the attack is to find and extract some sensitive company's information which can be for financial gain (eg. credit card information), or to obtain personal information, trade secrets or military information.

In the first step, the attacker identifies an employee of the company (the blue man in Figure 2) and sends to him some "Spear Phishing" emails[2] (see phase 1 in Figure 2). The fake sender and the content of the email should trick the employee to an action which will allow the attacker to obtain access to the employee's IT device. Typical examples of this phase are (see phase 2 in Figure 2) :

- if the employee is using a mobile device, like a smartphone or a tablet, the attacker can lure him to download and install on the device an "App" which, besides the advertised functionalities, contains also some hidden and malicious code;
- if the employee is using a Personal Computer (PC), the attacker can lure him to visit a web-site where some malicious code has been installed: by visiting the web-site, the malicious

[2] A "Spear Phishing" attack is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.

code is downloaded and installed on the employee's PC without the employee noticing it (usually the malware exploits some vulnerabilities or bugs of the software installed on the PC).

Notice that it is not needed that the attacker gains access as administrator of the employee's device, even if this happens quite often. For our purposes, it is enough that the attacker gains access to the employee's device with the same privileges as the employee, that is as the employee himself.

The third phase of the attack (see phase 3 in Figure 2) establishes the connection that allows the attacker to access the employee's device. The malware installed on the employee's device establishes a connection to the attacker's Command and Control (C&C) server. This connection is usually masqueraded as a normal web connection to a website so that the company firewall allows it. Notice that this connection goes from employee's device to the attacker C&C, so it is easier to masquerade.

Now, as long as the malware on the employee's device is active, the connection with the attacker C&C is established from the employee's device. The attacker also connects to the C&C (see phase 4 in Figure 2) and from there, using the established connection, has access to the employee's device.

At this point the attacker has full control of the employee's device either as the employee himself or as the administrator of the device.[3]

As an internal user, the attacker can then access other internal systems like email services, file-shares, databases, Intranet applications etc. (see phase 5 in Figure 2), or higher security internal systems (see phase 6 in Figure 2) by either using the credentials of the abused users or exploiting some vulnerabilities or security weaknesses of the internal systems.

Security risks

Once an attacker has access to one internal system, there is a high risk that he will be able to access most or all the other internal IT systems. The attacker usually tries to make his access Persistent, and in general this kind of attacks are called “Advanced Persistent Threats” (APT) [6]. This implies that the attacker activities are often hidden and last a long time. In this time a lot of data can be extracted and many copies and variations of malware can be installed for extortion, sabotage, ransom or theft.

[3] Notice that the attacker now is a “trusted” user according to the definition of the previous sections.

For this type of attacks to be successful, it is very important to remain hidden and active for a long time, so that it is expected that the evolution of this kind of threats will be to add “Stealth” features to the malware and to the techniques adopted by the attackers (see eg. [7]).

As we read in the news, many incidents of this kind have been reported in the last few years, and in some cases the breach has been discovered months after it happened, giving the attacker all the time needed to pursue the crime.

The “Zero Trust” defensive security approach

From the previous example scenario it follows that no internal IT system can be trusted and that the approach to IT security should start from the assumption that any internal IT system can be breached and abused by an attacker. This approach goes often under the name of “Zero Trust” [8,9] which originally referred only to a network design security approach.

Indeed the first defence against this risks is to further compartmentalize the internal network, dividing it in many very small areas, if possible down to the single machine, and to monitor and filter the traffic to each area.[4] The main difficulties in implementing such a compartmentalization of the internal network are that it becomes extremely complex and difficult to manage the networking filtering rules, and that the monitoring of all these very small areas produces a huge amount of information that should be collected, matched, analysed and stored.

So the network design becomes very important from a security point of view, but by far it is not enough. As of today, a secure network design is only one of the pillars on which IT Security is built.

Indeed the Zero Trust approach must be extended to all IT components, from applications, to data and users.

Incident Management

If we do not trust our users, applications and networks, it means that we expect some IT security incidents to happen. We know that IT security will never be perfect, and that something sooner or later will slip through our defences.

[4] Filters should be implemented both at layer 2 (eg. Ethernet), layer 3 (eg. TCP/IP) and at the application layer (eg. Proxy filters).

So we must be ready for it.

To be ready, we need to implement an IT Security Incident Management system which in summary:

- monitors the IT systems;
- detects attacks and intrusions;
- reacts to attacks and intrusions, limiting damages;
- recovers from attacks and intrusions, restoring the IT systems to a normal status.

As it is easy to write these four bulleted items, as it is really difficult to implement them. Indeed it is already a quite difficult task to understand what has to be “monitored” and how to do it, or how to “detect” an attack or intrusion.

Defence in Depth without Trust

Besides to be ready for an IT Security Incident, we need to improve our defences. This requires to somehow go back to the old military approach to IT Security of data classification and access authorization. We have just seen the reasons for this: not all information is public, actually s lot of information managed today by IT systems is at least of sensitive nature, both personal / private information and business information. If information and data are not public, we need to authorize users, applications and systems to access it, and to be able to authorize someone, we need to know who he/she/it is, that is we need to identify and authenticate him, her or it.

Information and Data Classification

Somehow in line with the military approach to IT Security, we need to label the data which represents the information managed by the IT systems. Indeed we need to know what we are defending to implement the appropriate defence measures. As of today this is a very hard problem both in practice and in theory, first of all because the amount of data / information generated and managed by the IT systems is enormous and it keeps growing extremely fast. Only for very few and very sensitive systems we can label all data following the military approach of the 80's [1,2].

Instead what we can do [10] is to identify the information of particular relevance that must be protected, like for example credit cards' numbers, and classify consequently all information and data that has the same security requirements.

The next step is to know which systems manage which data so to be able to apply a security classification also to all systems based on the classification of the data they manage.

The Triple A

Authentication, Authorization and Accounting (AAA) are the purpose of Identity Access Management (IAM) systems. An IAM system is another pillar of the IT Security defences since its purpose, as the name indicate, is

- to identify who or what is accessing a resource, system, application, or data;
- to provide the authorization for the access;
- to trace the access.

Referring back to our simple attack scenario, see Figure 2, it is obviously very important to have a IAM system with a good security configuration to allow the internal user to access only the resources strictly necessary for his/her work and only with the privileges needed. These resources will be available to the attacker who has taken control of the user device, but they will be strictly limited to the minimum. Even the administrative account of the user's device should be limited and should not permit to access as administrator other devices on the network.

Due to its role, an IAM system is a principal target for attacks. Indeed once an attacker has access to an IAM system itself, he has access to all the networks, systems, applications and data managed by it. An IAM system is usually attacked by exploiting software vulnerabilities and/or a low level of security configuration. For example, the IAM policies must not allow administrative users to have blank or very simple password, like '1234', which can be easily guessed. Actually for administrative and sensitive users, multiple-factor authentication methods should be adopted.

Availability is also a crucial factor for IAM systems: since no access to a resource must be allowed without the authorization of the IAM system, in case of failure of the IAM, even due to a Denial of Service (DoS) attack, all the IT systems managed by it become non accessible.

Vulnerabilities and Security Tools

Once an attacker has gained access to an IT device inside the company perimeter, he will try to exploit vulnerabilities and weak security configurations to access other systems and finally the whole company IT. To defend against this, it is necessary to keep all software updated with all security bugfixes, to adopt applications developed with secure coding practices which minimize the possibility of vulnerabilities and their consequences, and to introduce security tools to protect particularly sensitive resources, as for example by encrypting them, masquerading, adding extra access procedures and filters, monitoring etc.

Summing Up and Looking Forward

IT Security has changed vastly in the last years. Today we cannot sufficiently trust the security of our IT systems and we should assume that an intrusion will happen, if it has not already happened. This implies that we should:

- manage IT Security incidents;
- design and manage the IT network, applications, systems and users with a Zero Trust security approach;
- classify the information and data managed by the IT systems;
- implement Secure IAM services;
- adopt security tools and procedures to protect the IT systems, detect attacks and minimize damages.

Obviously this is a long journey which will never end, it is a continuous program which will improve constantly and adapt to the new technologies, the new features and components of our IT systems, to the new threats and attacks. At any given moment we can only implement some basic security features plus the best security measures for the current main threats.

All this can be done only within a strong and agile IT Security Threats and Risk management program, able to quickly identify new trends and the areas where to intervene so to maximize the effects of the investments in IT Security and the security of the IT systems.

References

[1] The Orange Book, DoDD 5200.28-STD, issued in 1983 and updated in 1985 by the National Computer Security Center (NCSC), an arm of the National Security Agency (NSA), http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

[2] “Common Criteria for Information Technology Security Evaluation” (abbreviated as “Common Criteria” or CC), ISO/IEC 15408, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341

[3] see for example: http://www.techrepublic.com/blog/tech-sanity-check/is-perimeter-security-dead-and-is-protecting-the-data-all-that-matters/ and http://www.ucci.it/docs/CFS-200705.pdf

[4] This famous picture was circulating on internet in 2005, the copyright holder is not known, for references see:
https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices ,
https://www.securecoding.cert.org/confluence/download/attachments/2426/kurios119.jpg ,
http://www.syslog.com/~jwilson/pics-i-like/kurios119.jpg

[5] See eg. http://www.wired.com/2002/01/bill-gates-trustworthy-computing/,
http://www.cnet.com/news/gates-security-is-top-priority/

[6] see eg. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat", SANS Technology Institute, 2011/5/22

[7] “2016 Predictions: it's the end of the world for APTs as we know them”, Kaspersky Security Bulletin 2015

[8] “Developing a Framework to Improve Critical Infrastructure Cybersecurity”, NIST The National Institute of Science and Technology & Forrester Research, Inc. , 04/08/2013,
http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf

[9] “Zero Trust Approach To Network Segmentation”, Palo Alto Networks,
https://www.paloaltonetworks.com/solutions/initiative/network-segmentation.html

[10] See for example NIST.SP.800-60

Andrea Pasquinucci (PhD CISA CISSP)