GLOBAL CYBER SECURITY CENTER

Newsletter

2017 October

Cyber Security is our mission

editorial

Robotic and Healthcare

Reading and talking about AI and robots and more, but there is a field where automation, digital transformation and robotic are very promising and represent a big opportunity in order to help a large number of people. New technology and robots can be used to enable people with cognitive, sensory, they may support people that are ill or injured, and last but not least aid the clinical workforce. Today we see robots everywhere in science fiction, but soon we will see them in hospital where they are going to change healthcare. From surgery routine task, they will have a big impact on the field of medicine. We know already some of this robots that today are monitoring patient vital data, alerting nurses in case we need assistance, many of these devices are also filling up electronic health record. In surgery, they are assisting doctors in complex task and in the latest years more and more we have machine used in surgery. In USA Food and Drug Administration approve the use of robot, where they are widely use it in surgeries as described above. Just to be clear they are not completely autonomous and a human mind is required. Robots here are used for minimally invasive surgery, where robotic arms are performing miniaturized cut instead of making large incision. Of course, they cannot operate today without a human assistance. But, you may probably be surprised that we may use this technology also in other areas like, for example, psychology. One of this example is available on-line as Woebot (https://woebot.io), the application is using AI algorithms and could function as your therapist. This chatbot was made by a group of scientists of the Stanford University starting from a therapeutic framework know as Cognitive Behavior Therapy and the results of this approach is available at https://mental.jmir.org/2017/2/e19/. Always in the therapy area PARO is a robot developed by a Japanese industry and is used for animal therapy in hospital and visiting their website we may see that many hospitals in US introduced this technology in therapy. The use of this robot has been found to reduce the stress factor experienced both by patients.
So, are we going to Skynet scenario? These and other questions are arising, like security and privacy. But what about life and death decision? The new scenario is really promising but is leaving many questions unanswered today, ethics, morality many border line issue that require human decision. As you may image security, cyber issue may only complicate this digital trend; a digital trend where promising technologies, like M2M, AI and robots, are entering, every day, in our life changing habits and lifestyle.

Nicola Sotira
General Manager GCSEC

events

FESTIVALFUTURO, La Rivoluzione delle Cose - Altroconsumo
Location: Milan, IT
Date: November 4-5, 2017
https://www.altroconsumo.it/festival-2017
Altroconsumo is projected in the future with the fifth edition of its Festival, which will be held this year at the Unicredit Pavilion in Milan on 4 and 5 November. The title of the event, "The Revolution of Things." The purpose is to understand how digital services will develop in the future. Poste Italiane will be present at the event with its Awareness Campaign that includes the Exhibition Social Media Victims Heroes, the CyberSecQuiz and the Awareness Videos about cyber security.

CSX 2017 EUROPE – AN ISACA CYBER EVENT
Location: London, UK
Date: October 30 - November 1, 2017
https://www.isaca.org/ecommerce/Pages/csx-europe.aspx
Interact with attendees from Europe and around the world. Experience unique opportunities to gain hands-on skills and invaluable knowledge in the dynamic fields of cyber security and information security. Cyber security doesn't go on holiday and it doesn't sleep. You need to be aware of the most effective tactics and tools to meet the ever-growing threat. CSX 2017 offers keynote speakers and sessions that dive deep into what you need to know now.

CSAW 2017
Location: Brooklyn, NY, USA
Date: November 9-11, 2017
http://cyber.nyu.edu/events/csaw-2017/
CSAW is the largest student-run cyber security event in the world, featuring international competitions, workshops, and industry events.

NATIONAL CYBERSECURITY CAREER AWARENESS WEEK
Location: Rockville, MD, USA
Date: November 13, 2017
https://www.nist.gov/news-

in this number

Fake News – What's going on?

by Gianluca Bocci - CERT e Cyber Security, Poste Italiane

Communication has been since the dawn of time in constantly changing. First communications were based on simple gestures, then came the words, and then, the first writing systems, where individual speech sounds were represented by a single sign. With the Egyptians and the Sumerians in the period from 12,000 to 4000 years BC, it's believed to have invented the "real" writing. Just writing was one of the first great revolution as part of the communication systems. Indeed, it is thanks to writing that it has been possible to guarantee that facts and thoughts were handed down through generations. Not entering into the details of how writing developed in the centuries, we come to the later revolution - the press - by which texts were not longer produced by the scribes but by the typographers. Through the exchange of the printed books, there was an acceleration in the spread of information and even more so with the advent of the telegraph, telephone, radio and television, especially the last, as a mass information dissemination tool and knowledge. In these evolutionary processes, politicians, "almost everywhere", has provided rules for the use of media, sometimes with the aim of preventing abuse and protecting citizens and businesses, sometimes to censor ideas and opinions. The latest major transformations based on digital technologies, has made available a new communication system, initially for military forces and scientific communities, then for large organizations and today practically for anyone, not just for the men, but even for so-called intelligent objects. Today, thanks to the Internet, with no space and time limits, we have the opportunity to enjoy a huge and heterogeneous number of services and informations; the latter by using chats, blogs, forums and social network[1], especially in democratic countries. In addition, the Internet has allowed in a "free" space to go beyond the classic communication models, allowing people to be always up-to-date and in real-time, but also to share their own experiences, opinions and feelings, becoming "contributors" of information. Unfortunately, however, in recent years the absolute lack of Internet controls has created a risk on the informations reliability which, through the alteration and/or manipulation, may generate misinformation, often useful for the most varied reasons such as for instance to influence public opinion, instigate hate, damage corporate image, offend and/or

[1] *Chats allow you to communicate with people in real time, forums are used to support discussions where not all participants are online at the same instant. The Social Network, exploiting a peculiar feature of the so-called Web 2.0, that is, the ability to interact with the Internet, is a real platform for aggregating people; as virtual squares facilitate the development of relationships through sharing of information, opinions, images, links, etc. The social networks, outpost of new communication tools, offer everyone the opportunity to participate in the "discussion" of any kind.*

events/events/2017/11/kick-national-cybersecurity-career-awareness-week
The National Initiative for Cybersecurity Education (NICE) will host an event at the National Cybersecurity Center of Excellence (NCCoE) to officially launch the first Annual National Cybersecurity Career Awareness Week to inspire and promote awareness and exploration of cybersecurity careers for children through adults. National Cybersecurity Career Awareness Week takes place during November's National Career Development Month (link is external), and each day of the week-long celebration will provide opportunities to learn about the contributions, innovations, and opportunities that can be found by exploring cybersecurity as a field of study or career choice.

CYBER SECURITY SUMMIT 360
Location: Rome, IT
Data: November 14, 2017
http://www.cybersecurity360summit.it/
The 2017 edition of Cyber Security Summit 360 take on the state of this underground war: new attacks on companies with "military" precision, differentiating the strategy according to the industry. How effectively is the new national strategy unfolding? What desirable improvements and what role will the various stakeholders?

news

KnockKnock campaign targets Office 365 corporate email accounts
https://www.helpnetsecurity.com/2017/10/05/knockknock-campaign/
Researchers uncovered KnockKnock, an attack on Office 365 Exchange Online email accounts, originating from 16 countries around the world and targeted organizations in manufacturing, financial services, healthcare, consumer products and US public sector. The attackers behind KnockKnock targeted automated corporate email accounts not tied to a human identity, which often lacked advanced security policies.
This campaign is based on a unique attack strategy of targeting administrative accounts commonly used to integrate corporate email systems with marketing and sales automation software. Since these accounts are not linked to a human identity and require automated use, they are less likely to have protection with security policies such as multi-factor authentication (MFA) and recurring password reset.

KRACK Attack Devastates Wi-Fi Security

threaten people, and much more. Adopting rules to have quality online information is therefore becoming an increasingly urgent need.

Initiatives to prevent and fight fake news

It doesn't take much for to figure out the size of the Fake News phenomenon. Through any search engine, if someone look for "*hoax on the net*", "*the biggest fake news on the net*" and similar keywords, find a lot of news about events that didn't never happen. No wonder that "La Stampa" tells with an online[2] article that the "2016 will go to history as well as the year we entered the post-truth era. The “hoax” is not a phenomenon born in the last 12 months, but in this period, more and more sites, blogs and accounts have begun to proliferate on the web in order to profit with the 'fake-news', to generate hate and discontent. Practically there's everything, from the seismologists who have said about the plot that the institutions would have designed in order not to pay damages to the citizens, to the fake and already dead Umberto Eco who would, through his statements, influenced the referendum of December 2016. There are also false statements by politicians, strange hypotheses about the origins of meningitis, and how it is transmitted in the world, microchips implanted under the skin of men in order to check their mind and lastly all fakes who have accompanied Trump and Clinton, uninterruptedly, for all the duration of their election campaign. On this last point came back shortly before the summer, Hillary Clinton in a her intervention at Wellesley College. Without reference to his opponent, who then won, Clinton made some interesting statements "You are graduating at a time when there is a full-fledged assault on truth and reason. Just log on to social media for ten seconds. It will hit you right in the face[3]" and still “In the years to come, there will be trolls galore online and in person. Eager to tell you that you don't have anything worthwhile to say or anything meaningful to contribute. They may even call you a nasty woman”. The issue of fake news should also be of interest to companies, especially those most exposed from a media point of view, since a false statement could have big impact on its reputation, as in the recent case involving Sturbucks[4]. This raises the question - what can be done to stem the fake news? The way some States are moving and how some large "big of Internet" are organizing, it seems that the room of manoeuvre

https://threatpost.com/krack-attack-devastates-wi-fi-security/128461/

A devastating weakness plagues the WPA2 protocol used to secure all modern Wi-Fi networks, and it can be abused to decrypt traffic from enterprise and consumer networks with varying degrees of difficulty. Not only can attackers peek at supposedly encrypted traffic to steal credentials and payment card data, for example, but in some setups, a third party could also inject malicious code or manipulate data on the wireless network.

Dangerous malware allows anyone to empty ATMs – and it’s on sale!

https://thehackernews.com/2017/10/atm-malware-hacking.html

Hacking ATM is now easier than ever before. Usually, hackers exploit hardware and software vulnerabilities to hack ATMs and force them to spit out cash, but now anyone can simply buy a malware to steal millions in cash from ATMs. Hackers are selling ready-made ATM malware on an underground hacking forum that anybody can simply buy for around $5000, researchers at Kaspersky Lab discovered after spotting a forum post advertising the malware, dubbed Cutlet Maker. The forum post provides a brief description and detailed manual for the malware toolkit designed to target various ATMs models with the help of a vendor API, without interacting with ATM users and their data. Therefore, this malware does not affect bank customers directly; instead, it is intended to trick the bank ATMs from a specific vendor to release cash without authorization.

Yahoo hack – All 3 Billion Yahoo accounts were hacked in 2013 attack

http://securityaffairs.co/wordpress/63813/cyber-crime/2013-yahoo-hack-3b-accounts.html

The Yahoo hack occurred in 2013, the biggest known data breach suffered by a tech company, is bigger than originally stated. Verizon Communications, which acquired Yahoo for $4.48 billion in June, announced on Tuesday that the 2013 Yahoo hack affected all three billion of company user accounts. Last year, Yahoo declared that the incident affected one billion accounts, and it wasn’t the unique incident suffered by the company. In 2014, hackers accessed 500 million accounts in a separate security breach. Attackers accessed names, birth dates, phone numbers, security questions, backup email addresses and passwords of Yahoo, a gift for hackers that could use the same data to access any other account owned by Yahoo users that share same credentials. Unfortunately, the hashed passwords were protected with a weak algorithm that was very easy to crack.

[2] http://www.lastampa.it/2016/12/31/societa/le-pi-grandi-bufale-del-X3Zin44VLpSL9mq9JBcmWP/pagina.html

[3] http://america24.com/news/hillary-clinton-contro-le-fake-news-paragona-trump-nixon

[4] http://www.businessinsider.com/fake-news-starbucks-free-coffee-to-undocumented-immigrants-2017-8?IR=T

pass through different types of measures, both legislative and technological. In France and Germany, initiatives were launched to verify the validity of the information with the aim of removing those fake; especially in Germany, recently came into force a Law, that will force social networks with more than two million users to remove hate speech, publish fake news and offensive pages, expose threats, etc.. The implementation of the Law will be guaranteed by fifty employees of the Ministry of Justice who will monitor the application of the rules. The Law, applied from January 2018, has a sanctioning facility that, assessed and enforced by the same ministry, in the worst cases provides for a fine of 50 million euros. France to protect his constituents during the recent election campaign to elect the new president of the Republic, commissioned a fact-checking company to point out fake news on Facebook. Even in Britain, after the Brexit referendum, the Media Commission had launched an investigation into the issue. In Italy, in February 2018, through a parliamentary initiative, was presented and announced by Senator Adele Gambaro[5] - Senate Act No. 2688 (XVII Legislature) - the first bill against fake news and incitement of hatred in Internet; the bill assigned to the Joint Committees 1 (Constitutional Affairs) and 2 (Justice) was intended by considering the guidelines set on January 25, 2017 by the Parliamentary Assembly of the Council of Europe with the approval of Resolution 2143 (2017) "Online media and journalism: challenges and responsibilities". The European Union, through new Digital Commissioner Mariya Gabriel, is taking a stand against the fake news, starting a public consultation in the coming weeks to find a balanced approach to the protection of everyone's freedom of expression. The “big of Internet” that handle the information are trying to figure out what their responsibilities are in managing the same information and especially the fake news. About it, an exercise was first made to try to understand the nature of the information with especially reference to its reliability. There is no doubt that some informations are clearly fake, and that, the only purpose is monetize them; in fact, through clamorous news and links that allow re-directing often on web pages that have nothing to do with the original information, the user may be led through the "click" on various advertisements, allowing the site manager to earn. Often the publication of this kind of informations goes against to the policy of the main social networks that remove them; similarly for all those information that are clearly in conflict with national and international Laws, such as those that are source of defamation. This is an area where social networks do not have great difficulty to act quickly. There is, however, a gray area in which it‘s difficult to act, since there may be a risk of limiting the freedom of others; it is enough to think of all the informations that, while distorting the truth, are the result of personal opinions that, expression of a freedom of thought, must be guaranteed to anyone. From this point of view, it is easy to create background noise; from this point of view, it is easy to create background noise; just to make an example, it is enough to think of a debate based on scientific studies which in turn are denied by other scientific studies.

For that reason it's very difficult to establish when and which informations must to be removed by a social network, especially when, in contrast to the obvious truth, lacks any objective evidence that justify its removal - could be it's just the product of democratic confrontation. With particular reference to Facebook, the basic idea to prevent and fight fake news phenomenon, is to involve media professionals and to develop appropriate tools to facilitate the task of the person in charge of control.

Based on these conditions, Facebook program to fight fake news is organised as following:

- involve actively those who are a media information professional (newspapers, press, etc.) to gather advice and suggestions on how to improve the social platform and make it more and more reliable;

[5] http://www.senato.it/leg/17/BGT/Schede/Ddliter/47680.htm

A New IoT Botnet Storm is Coming

https://blog.checkpoint.com/2017/10/19/new-iot-botnet-storm-coming/

A massive Botnet is forming to create a cyber-storm that could take down the internet.

An estimated million organizations have already been infected.

The Botnet is recruiting IoT devices such as IP Wireless Cameras to carry out the attack.

New cyber-storm clouds are gathering. Check Point Researchers have discovered of a brand new Botnet evolving and recruiting IoT devices at a far greater pace and with more potential damage than the Mirai botnet of 2016.

IoT Botnets are Internet connected smart devices which have been infected by the same malware and are controlled by a threat actor from a remote location. They have been behind some of the most damaging cyberattacks against organizations worldwide, including hospitals, national transport links, communication companies and political movements.

Bad Rabbit Linked to ExPetr/Not Petya Attacks

https://threatpost.com/bad-rabbit-linked-to-expetrnot-petya-attacks/128611/

A link has been confirmed between the Bad Rabbit ransomware outbreak detected yesterday in major organizations in Russia and Ukraine and this summer’s ExPetr/Not Petya attacks. Researchers at Kaspersky Lab said there are “clear ties” between the two attacks though one major piece of the puzzle is missing with Bad Rabbit. Like WannaCry before it, one of ExPetr’s propagation methods was the leaked NSA exploit EternalBlue, which triggered a SMBv1 vulnerability patched by Microsoft early this year and allowed it to worm out to the internet.

Kaspersky Lab researchers said they have found no evidence of EternalBlue—or EternalRomance, another NSA-developed attack that was publicly disclosed by the ShadowBrokers and used in the ExPetr attacks—in yesterday’s attack.

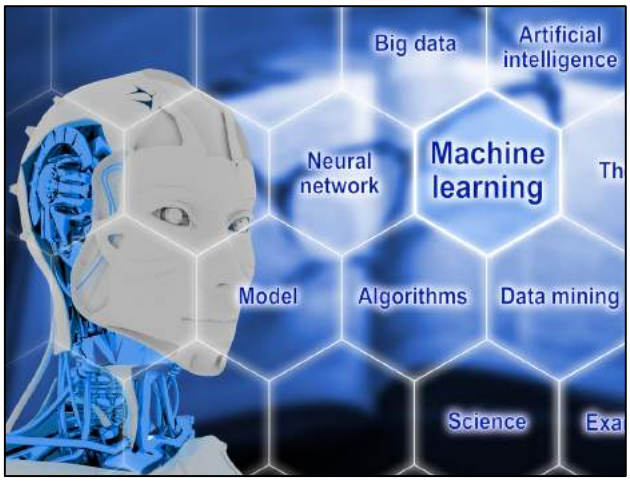
Hackers are attacking power companies, stealing critical data: Here's how they are doing it

http://www.zdnet.com/article/hackers-are-attacking-power-companies-stealing-critical-data-heres-how-they-are-doing-it/

Hackers are continuing to attempt to gain access to the networks of nuclear power companies and others involved with critical national infrastructure, raising concerns about cyber-espionage and sabotage.

A report compiled by the FBI and US Department of Homeland Security (DHS) has warned of an ongoing hacking campaign that has seen attackers infiltrate the networks of power companies and

- remove all fake information that, set out appropriately by users, includes links to websites that are far from the original post and have a lot of advertising content; about it, particular attention is paid to the development of new software tools that, based on Machine Learning techniques, shall facilitate identification of fake news, which are nevertheless manually verified before any removal; there is still a high risk of proposing false positives, at least until these techniques will not sufficiently mature;



- remove the fake accounts that are reported by users in order to create only real relationships between real people that, well-identified, are consequently responsible for what they publish. In this way, phenomena such as hate speech and cyberbullying are limited. Also in this case are being developed tools that using the Machine Learning; in addition strengthening the team that, in charge of the user's reports, checks and removes accounts;
- provide additional information to the user in order to put him in the conditions of developing a more critical sense and therefore realize if he has stumbled into fake news; in particular, at the end of 2016 France, Germany, United States and Holland, have begun a variety experiments based on collaboration with so-called “fact checking” organizations. About it, when a user thinks that a news is fake, he reports it to the social network, who immediately submits it to the fact checking organization (even more than one) and looks forward the outcome of the analysis. If the news is fake, it isn’t removed but marked as potentially "disputed". Since than, every user can see the mark and if he wants, he can deepen the reasons that have led social network to qualify the news it in this way. In addition, Facebook is upgrading the so-called “related articles”; related articles provide to the users link to webpages that deal the same subject and help to get more information to go into that.
- start awareness campaigns, for example through the involvement of schools, to provide useful tips to improve, once again, the critical meaning and therefore to identify fake news.

What definitely is perceived from the previous statements, is that there is a great excitement around this growing problem. In the future there will be a lot to be done, both at regulatory and technological level, increasingly exploiting Machine Learning techniques and also the big opportunities provided by the funding programs for the research and development.

others to steal details of their control systems, including information from control systems within energy-generation facilities.
Hackers are targeting the systems of government agencies and companies working in energy, nuclear, water, aviation, and critical manufacturing sectors, according to the report.
While it has long been known that state-backed hackers are keen to access critical infrastructure, the report provides one of the most detailed looks at how state-backed hackers are attempting to gather data on critical national infrastructure through a sophisticated and multi-stage project.

Exclusive – CSE ZLab experts spotted a new Wonder botnet in the wild
http://securityaffairs.co/wordpress/64633/malware/wonder-botnet-dark-web.html
The CSE CybSec Z-Lab Malware Lab spotted a new botnet, dubbed Wonder botnet, while it was investigating malicious code in the dark web.
While investigating the malicious code in the dark web, ZLab experts discovered a “NetflixAccountGenerator.exe” that promises to generate a premium account for Netflix services for free. Unfortunately, the software downloaded does not work as expected because it installs a BOT rather than create a desiderated account!
The malware researchers analyzed this “exe” file and discovered that the malware is not indexed yet: only one site on the Clearnet identified it as a threat after it was uploaded for the first time around September 20th, probably by the author in order to test its ability to remain stealth.
The analysis of the malware revealed it is a bot that belongs to an alive botnet dubbed by the experts Wonder botnet.

Firms Increasingly Turn to Machine Learning for Security Solutions
http://www.securityweek.com/firms-increasingly-turn-machine-learning-security-solutions
Forty-seven percent of organizations have already deployed machine learning (ML) solutions, with another 23% engaged in pilot projects, to help detect increasingly sophisticated incursions and lower the cost of response. A study (PDF) commissioned by Cylance and undertaken by Enterprise Strategy Group (ESG) surveyed 300 IT and security professionals from mid-market and large enterprises. The respondents are located in the United States (43%), Japan (21%), United Kingdom (13%), France (12%), and Germany (11%); and all are involved in the purchase process for endpoint security. The study sought to identify the 'top of mind' security threats, and the impact those threats have on endpoint security purchasing decisions. Phishing is the biggest concern for most respondents. In the last two years, 55% have experienced phishing with a malicious attachment, 54% have experienced phishing with a link to a malicious website.

A comprehensive approach to ECDSA

by Francesco Leccese, Francesco Peverini – GCSEC Internship

Introduction

Ever since ancient times, the pursuit of secrecy of information always played a primary role in human history. Simultaneously, a whole branch of math-ematics developed to optimize the encryption and decryption processes of a message: Cryptography. In the military, cryptography has always been crucial: an important example is Julius Caesar, who already used rudimen-tary cryptographic tools (Caesar cypher) to give orders to his lieutenants on the battle ground; another considerable example is World War II, and the key role played by the cypher machine ENIGMA for Hitler and Germany. With the advent of the digital era, cryptography played a more important role than it did before, because in the modern world whatever is on the net is encrypted (and also signed) with algorithms that use algebraic-geometric concepts. In an increasingly faster and interconnected world, Digital Signa-ture is of primary importance because it allows to uniquely identify and verify the author of a message. One of the current digital signatures standards is ECDSA (Elliptic Curves Digital Signature Algorithm), which exploits the Elliptic Curves over Finite Fields theory. The strength of ECDSA is given by the short-term intractability ECDLP (Elliptic Curves Discrete Logarithm Problem). Moreover, Elliptic curves cryptography offers significant benefits, such as the length of keys and memory costs, maintaining the same security level of other algorithms (for example RSA), as shown in the following table:

EC key bits	RSA key bits	Time to break	Memory	Arithm. Op.
110	428	5.5 sec	Trivial	$5.5*10^{17}$
160	1024	100 years	170 GB	$1.3*10^{26}$
224	2048	$\sim 10^{11}$ years	>200 GB	$1.5*10^{35}$

Table 1: Times to break with Sunway TaihuLight super-computer.

Elliptic Curves

In maths, elliptic curves are a specific kind of two variable plane curves. Given $a, b \in \mathbb{R}^2$ such that $4a^3+27b^2$ different from 0, we define as non-singular elliptic curve the set $E=\{(x,y)\in\mathbb{R}^2 t.c.\ y^2=x^3+ax+b\}$.

Given an elliptic curve E, it is possible to define an operation on its points, denoted as " + ": given P ,Q points of E, where P = (x1, y1) and Q = (x2, y2), we define P + Q as follows:

1. We draw the line r between P and Q.
2. We find T = (x3, y3) as the intersection point between the line r and the curve E.
3. Finally we obtain R = (x3,-y3) = P + Q as the symmetrical point of T through X.

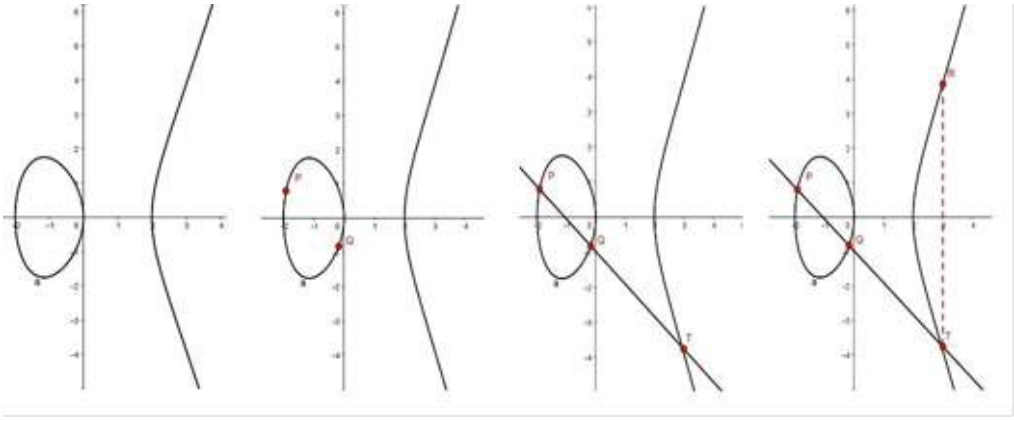


Figure 1: Graphical representation of P + Q

The previous operation has some important properties, for example it is closed on E (i.e. if P , Q are two random points of E, then P + Q belongs to E) and is commutative (P + Q = Q + P). It is also possible to show that (E,+) is an abelian group, i.e. E is a set with a closed operation on itself that is also commutative, associative and has the reciprocal of every element.

Fq and the modulus calculus

Elliptic curves over finite fields, denoted with Fq, are used in ECDSA. In these particular fields the common operations as sum, multiplication and exponentiation are performed; however, the arithmetic steps are much more different from those we usually use. For example, let us consider the finite field modulo 17 $F_q = \mathbb{Z}_{17} = \{\bar{0}, \bar{1}, \ldots, \bar{16}\}$, where every number is represented as the remainder of the division for 17 (e.g. 35 is represented as 1, because 35 = 2*17 + 1); assume that we want to calculate 10 + 28, 10*28 and 4^3 . In the real field, we obtain 10 + 28 = 38, 10*28 = 280 and 4^3 = 64; instead, in Z17 we obtain :

$$10 + 28 = 38 = 2*17 + 4 = 4 \text{ mod } 17;$$

$$10 *28 = 280 = 16*17 + 8 = 8 \text{ mod } 17;$$

and

$$4^3 = 64 = 3*17 + 13 = 13 \text{ mod } 17.$$

It is clearly more difficult to invert one of these operations in finite fields rather than in the real field (just consider solving the equation 7*x = 11 mod17). This aspect is basic in the ECDSA, and generally almost in the whole modern cryptography, because most algorithms base their security on the difficulty to invert modulus operation in short-time.

Elliptic Curves DSA Algorithm

We shall now see ECDSA in detail: let p be a big prime number ($p \sim 2^{256}$), E an elliptic curve over the finite field Fp, A a point belonging to E of order q (qA = A) (so as DLP is intractable in short time), and let $K = \{(p, q, E, A, m, B) t.c. B = mA\}$ be the set of all the possible keys. Finally, let us suppose we have a message M written in binary code. The public key will be the vector (p, q, E, A, B), while m will be the private key. We now have to choose a random (secret) number k (0 < k < q-1): we can then calculate the digital signature of M, $sig_K(M, k) = (r, s)$, as follows: first of all we calculate

$$kA = A + \ldots + A = (u, v)$$

and we define

$$r = u \, mod \, q \ ,$$

$$s = k^{(-1)}(SHA-1(M) + mr) \, mod \, q \ .$$

The verification process receives (M; (r; s)) as input, and we obtain

$$w = s^{-1} \, mod \, q \ ,$$

$$i = w \, SHA-1(M) \, mod \, q \ ,$$

$$j = wr \, mod \, q \ ,$$

$$(u, v) = iA + jB ,$$

finally, the digital signature will be accepted if and only if

$$u \bmod q = r .$$

The first idea that might come to mind when considering an attack the ECDSA is to somehow obtain k, because if an attacker knows k and knows that:

$$s = k^{(-1)}(SHA-1(M) + mr) \bmod q ,$$

then he can get m in a few simple steps, which require the calculation of the discrete logarithm logAB: given E an elliptic curve on the finite field Fq and A, B two points belonging to E, the attacker would have to find $k \in F_q$ such that

kA = B,

We shall now see an example of the difficulty of DLP: suppose we want to solve the equation

$$4^k = 13 \bmod 17 ;$$

one of the fastest algorithms to find k is brute force, i.e. to substitute to k all the possible numbers belonging to $\mathbb{Z}_{17}$. In this example, an attacker would need 17 tries to obtain the solution k = 3, but what if he uses brute force on a ECDSA key? On average, he would need 2^{80} operations and more or less 30 million years to run these. Some algorithms which improve the search of discrete logarithm (Pollard's Rho, Shank's Algorithm and others) already exist, although they need too much time for current computers. Despite the strength of ECDLP, there are some compulsory precautions to avoid an attack of the system by a hacker: for example, the value of q should not be factorizable in small prime numbers (Pohlig-Hellman Attack), and a same value for k should never be used in two different digital signatures; otherwise, it becomes easy to get k (as well as the private key m), just as happened to Sony in 2010.

The exhibition "Heroes and victims of social media" on display in Taranto

by Marianna Cicchiello - CERT e Cyber Security, Poste Italiane

In the framework of a specific national awareness-raising program on the conscious use of digital tools carried out by Poste Italiane, the exhibition "Heroes and Victims of Social Media" was set up in Taranto from October 17 to 20, organized by Adiconsum in collaboration with the company.

The event, which took place in a space dedicated to the “Citizen of Businesses” , was attended by many visitors: more than one thousand students from Ionian school institutions have been counted, all of them extremely involved and interested in the important themes that Poste Italiane is pursuing with its awareness campaign.

The exhibition is an important time to prevent the risks and dangers of internet with simple but explicit languages suitable for all age groups. Considering that the main content of the exhibition illustrates how social media has always existed throughout the millenniums and has always had the power to exalt or shadow the reputation of the people they focused on, in particular by talking about modern technologies, attention is drawn to the conscious use of these technologies so that they do not risk becoming "overwhelmed" by becoming a victim. An initiative aimed at young people and very young people, which increases their level of awareness and knowledge and allows them to take full advantage of internet benefit without taking risks.

During the exhibition, the video pills produced by Poste Italiane on cyber security, in particular "Correct use of e-mail", were screened in which these themes are illustrated with simple words, giving instructions and arrangements necessary for the protection of their data on the network, and In addition, visitors have been able to test their knowledge of computer security with the appropriate CyberSecQuiz application of Poste Italiane.

The next exhibition will be held in Milan on 4-5 November at FESTIVALFUTURO – La rivoluzione delle cose, UniCredit Pavillion.