We are vulnerable

Waking up reading, as usual, on line newspaper; checking Schneier security blog and discover that NYT home page and security specialized blog have the same news. We are getting used to read about cyber-attacks and unfortunately read about security incidents. ATM machine in Kiev stops working and, at the same time, technician starts to monitor Chernobyl radiation while a chocolate big factory in Australia was infected and fighting against the new threat. In two months, we have to cope with a global ransomware attack. Ransomwares are kind of malware that are blocking the access to computers demanding money for release it. They are encrypting documents and file and the victim, in order to regain the access, have to pay a ransom typically in Bitcoin. Based on preliminary information seems that the malware sample is a clone of the GoldenEye ransomware family. This variant has two encryption layers, one is encrypting the target files and the others is cyphering the NTFS structure. In this way, they are preventing the victims to boot up in a live OS and recalling stored information. The exploit used is similar to Wannacry, including the EternalBlue which originated from a cyber tool developed by NSA and leaked by a hacker group called shadowbrokers, see Bruce Schneier blog. The results are that in a matter of hours the attack was global affecting Russia, Ukraine, Romania, EU, US and so on. The source is still not clear and Europol is announcing that are monitoring and investigating this massive attack. As usual, computers that are running the latest Microsoft update should be safe, and again backup is another very important measure that must present and implemented; least but not last users need to be advised to control if they have the latest and updated version of Windows and do not have to click on suspicious link. Pay the ransom is something to avoid because you are encouraging the attackers and there is no guarantee that the documents will be restored. In order to be more effective on these kinds of attacks we need to increase the cyber resilience of the national infrastructure, monitor the digital transformation in order to have a good IT implementation that may increase the security. Information sharing needs to be formalized and be part of the company process internally and externally. We are vulnerable, modified version of these malware created by cybercriminal may affect our digital domain and we need to increase also security culture in the organization filling the today’s gap. Very often people are unaware of the use of digital tools and are using them inappropriately. Cybercriminal are sharing info and knowledge something to learn from them, our security people need to share more and open also to imitative like the Coordinated Vulnerability Disclosure Manifesto. Something that we are promoting with initiative and research, so stay tuned...

Nicola Sotira
General Manager GCSEC

Cyber Security Summit
Location: London
Date: 2017 July 4
http://www.cybersecurityconference.co.uk

With the recently published Cyber Security Strategy, the launch of the National Cyber Security Centre, Government investment of £1.9bn in cybersecurity capabilities and weekly reports of mass cyberattacks, cybersecurity remains a key focus for government, as well as, businesses and individuals alike. Join 250+ cyber security and ICT professionals from across central government, local government, law enforcement, the NHS and wider public sector, to tackle key issues at the heart of UK public sector cyber security at the 4th Annual Cyber Security Summit. Discover, determine and deliberate the latest developments, strategies and technologies available to successfully defend your organisation online. Keep up to pace with the scale, complexity and ever-changing threat we face.

From PCI to PI: the tipping point in payments security?
Location: London
Date: 2017 July 5
http://wwwpci-portal.com/event/pcilondon

While many large companies, and even entire sectors – such as tertiary education – are struggling to achieve an acceptable level of PCI DSS compliance for their card payment processes, innovation in the payment industry threatens to overtake current security programmes. For example, in the UK alone it is estimated that there are now over 2,500 payment service providers in the UK, offering new payment products and services. So rapid have been these developments that industry insiders believe that 2017 will see a tipping point in payment industry security. The explosion in the number and type of payment providers, and the willingness of end-customers to embrace new payment methods is driving a convergence of PCI DSS, ISO27001 and GDPR programmes and putting PCI at the
Yes. However, if I go ahead and enforce that she can't have "cyber" in his time? Yeah, he would have guessed "captain" in a heartbeat. Could a kiddie have guessed her password as "captain" on an account of Kirk. Now can a script kiddie have guessed this? Yes. Could Russia have guessed this? Yes. However, if I go ahead and enforce that she can't have the password of heart of business-oriented cyber-security. And PCI professionals are in a great position to benefit.

**Data breach: allarme cybersecurity e privacy a rischio per le aziende**
Location: Milan  
Date: 2017 July 5 - 6  

The workshop is aimed at companies in all sectors, with specific reference to legal and corporate affairs, compliance, internal audit, organization, ICT, as well as business professionals and consultants. During the workshop, extensive sessions will be dedicated to the question time to encourage participants' interactivity.

The topics discussed during the workshop will be: Big Data and Cyber Security: between Privacy and Consumer Protection; Data Economy; Big data & analytics; Privacy protection; Prevention of cyber-risk; False practices and competition.

**Applicazioni pratiche del GDPR**
Location: Rome  
Date: 2017 July 12  

With the new European Privacy Regulation, European organizations and all companies providing services or products to Union citizens, regardless of their geographic location, will have to face a revolution in the management of personal data. In fact, these organizations will have to respect new rights, principles and approaches to managing personal data and complete compliance activities and achieve regulatory compliance by May 2018. What practical tips? How to be prepared? The workshop will be a time for discussion on some concrete and operational aspects such as changes to privacy information and data retention period; identification of critical information and implementation of the PIA; consent to the processing of personal information, data portability in the banking sector.

**Ira Winkler**

Ira Winkler, CISSP, is President of Secure Mentem and Co-Host of the Irari Report. He is considered one of the world’s most influential security professionals and has been named a “Modern Day James Bond” by the media. He won the Hall of Fame award from ISSA, and most recently, CSO magazine named him a CSO Compass Award winner as “The Awareness Crusader.” Winkler has designed, implemented, maintained and assessed awareness programs for decades, in organizations throughout most industries. He performed empirical research on the success of awareness efforts. His espionage simulations examine the success of security programs in general, and also provide a base of knowledge in responded to incidents, many involving human exploitation.

**Christopher P. Skroupa**

To introduce some of these ideas covered in your book, *Advanced Persistent Security*, let’s start off with your recounting your time at NSA, when you came across an obvious cyber vulnerability and how that spoke to the importance of detection in prevention.

**Ira Winkler**

Right. So when I worked at NSA, I worked with a woman whose last name was Kirk. I was training her how to use the system and I told her, “Ok, log on to the system. Now log on to the database. Ok, the database ID is going to be your last name: Kirk. Now enter your password, Captain, C-A-P-T-A-I-N.” She looked at me in horror and said, “How do you know what my password is?” And I’m like, “You’ve got to be kidding me.”

With that in mind, the issue is that there is a system at NSA that allowed her to have a password as “captain” on an account of Kirk. Now can a script kiddie have guessed her password? A teenager with nothing better to do with his time? Yeah, he would have guessed “captain” in a heartbeat. Could a cyber-terrorist have guessed this? Yes. Could Russia have guessed this? Yes. However, if I go ahead and enforce that she can’t have the password of A new wave of cyber attacks is shocking the IT industry, a massive attack leveraging the Petwrap ransomware has infected systems across the world  

A new wave of cyber attacks is shocking the IT industry, a few weeks after the WannaCry massive attack, security experts are facing a new threat that is rapidly spreading. Once again it is a ransomware that is infecting computers worldwide making chaos, systems at banks, power
"captain," it doesn't matter who the threat is—I have taken away the vulnerability for them to attempt to exploit it. So in that case, that's the key—if you can mitigate the underlying vulnerabilities, you can stop the bad guys from potentially getting in. So now, we have to assume failure is going to happen—protection will fail. Once protection fails, you need to ensure that you've put detection in place, and when you put detection in place, you look for where your protection has been breached. When you find it, you implement a reaction plan. That's how good security programs should be designed. They should always be looking for failure in protection, and too many people don't look for failure in protection. There have been some studies, and this is not the exact number, but it was along the lines of 80% of security money was spent on protection and not on detection and reaction. Detection and reaction were just afterthoughts. Initially, [detection] was just a side issue. Security was always bolted on, not built in, which meant it was just kind of like, "I don't know what I'm going to secure, I'll just figure that out after the system is built." Now, people have started to build security into things, because security is recognized as a problem, but what they're building-in is protection. Then they'll be like, "Ok, let's bolt on a detection tool after the fact. I'll put a network monitoring tool or a log tool on." Again, if they're building detection on after the fact, it's usually unacceptable because they're not looking in the right places. They're just buying a tool that looks broadly, not looking for specific targets. Here's a key factor: If you have the right detection in place, you can save a lot of money on protection as well. Security does not fail until the bad guy gets out with the targeted information. It's ok if they get in, as long as you stop them from achieving their ultimate goals; whether their goal is stealing information, deleting information, or modifying information. But if you can detect them when they get in, and detect them when they're sitting through the information, you can stop them from achieving their goals, and it might be much cheaper. It might be both more effective and less expensive than to implement detection as opposed to unlimited protection.

Skroupa: So, it's a "one without the other" kind of thing.

Winkler: Right. Though, this is just a hypothetical example, but there are a lot of security managers, and I was talking to one guy who said, "I have more than a million computers. How am I supposed to protect all of them?" And I replied, "You're not." Not all computers are created equal. Some computers have minimal value, and some computers-like the CEO's computer—would obviously have a lot of value. Email servers have a lot of value. Looking at SONY, the movie databases clearly had a lot of value that they weren't adequately protecting. So, if you have an immense system such as in an organization like SONY, you can't stop everybody from getting in—it would be impossible. But you could have implemented intrusion detection systems on the movie storage system, and you could have stopped a lot of the problem—you know that's where the bad guys want to go. Again, you're trying to protect value and detect when it is inevitably being compromised. Same thing with Target. Obviously, with all of the aspects of Target's infrastructure, some are more valuable than others. Detection should have been on the point of sales systems to see if they were modified wrongly or if there was malware on the system. Or, likewise, the Target backend servers were a clear target for the hacker/criminal. If they would have put detection there, that would have enabled Target to stop the activity. You want to implement enough detection. There's also the 80/20 rule where you solve 80% of your problem with 20% of the effort, though with most protection, you can solve 95% of the problem with 5% of the effort. For example, the most devastating attacks lately have been attributed to phishing messages. The SONY hack was attributed to phishing messages against the administrators. The OPM hack, where 22 million federal employees' records were hacked, was attributed to phishing. The DNC hack has been attributed to phishing. Phishing is a nice, simple, really low-tech way of getting in. Clearly, once the bad guys had their foot in the door, they were able to completely get in. But what if I were to tell you that there is inexpensive and frequently free protection that would have protected people's credentials? Multifactor authentication would have prevented the initial compromises of SONY, the OPM, and DNC, and might have stopped the attacks in their entirety.

Skroupa: In your book, Advanced Persistent Security, do you cite any solid statistics on how many companies on average have these security measures suppliers and businesses in Europe, Russia, Ukraine, and India have been targeted by Petwrap. The Petwrap ransomware is a variant of the notorious Petya ransomware that encrypts files demanding $300 in bitcoins to open victims. Like WannaCry, also Petwrap exploits the Windows SMBv1 vulnerability and the effects appear to be serious on a large scale highlighting the poor level of security of computers worldwide. According to the security researchers Matt Suiche, founder of cyber security firm Comae Technologies, the malware use the same attack vector exploited by EternalBlue and the accompanying DoublePulsar rootkit.

Android Marcher Trojan Masquerades as Flash Update

Researchers are warning of a new iteration of the sophisticated Marcher banking trojan, capable of targeting over 40 financial applications. Zscaler explained in a blog post that the malware is disguised as an Adobe Flash player update: Adobe_Flash_2016.apk. The malware will also use social engineering to trick users into disabling security on their Android device and allowing third-party apps to install. Once installed, the malware will hide itself from view and remove any icons on the main menu, before registering the victim's device and any relevant metadata to its C&C server. "After a few sleep cycles, the malware waits for the user to open an app from its targeted list. We found that this variant is capable of targeting over 40 financial apps. When the user opens any of the targeted apps, the malware will quickly overlay a fake login page, which lures the victim into supplying user credentials," explained Zscaler.

The Google Project Zero expert Tavis Ormandy has found a flaw in Windows Defender that allow attackers to bypass the Microsoft anti-virus tool http://securityaffairs.co/wordpress/60434/hacking/microsoft-windows-defender-flaw.html

The popular Google Project Zero hacker Tavis Ormandy has discovered a new bug in Windows Defender that allow attackers to circumvent the Microsoft anti-virus tool. Ormandy publicly disclosed the news of the vulnerability in Windows Defender on Friday after Microsoft released a for its software. Ormandy reported the vulnerability to Microsoft on June 9th. The vulnerability resides is in the non-sandboxed x86 emulator Windows Defender uses. The expert explained that “apicall” instruction can invoke internal emulator APIs running them with system privilege, unfortunately, it is exposed to remote attacks by default. The hacker discovered a heap corruption issue in the KERNEL32.DLL!VFS_Write API. “I discussed Microsoft’s “apicall” instruction that can invoke a large number of internal
in place already, or have this type of digital risk management in place?

Winkler: Down to the level of a specific protection tool, the answer is no—it's hard to know. That was not one of the things we included in the book. But again the previous example of something available for free, that you just have to turn on, could have stopped some of the most notorious attacks. If they would have implemented multi-factor authentication, not to say that it would have been impossible, but it would have been exponentially more difficult to start the attacks. Another thing we talk about in the book is how to create a culture of security. Companies don’t understand their culture. There's also a problem in believing that younger generations know how to secure themselves better. There's also a distinction between knowing how to secure yourself better and actually doing it—that's a very important distinction. Despite the fact that younger people have been exposed to the technology longer, they don't know how to secure it any better. They're more comfortable using it, but it doesn't mean they've looked at the right things to know how to secure it better. One of my friends, a former CIA operative who went on to teach information sciences at the University of Texas, conducted a study. He asked his students what they thought the definition of privacy is, and they said they believed privacy is defined as controlling what you “put out there.” He assigned his students a term project where he wanted them to put together an intelligence dossier on themselves—in other words, how much information they could find through open sources. He told me, “I can tell you exactly when the people started the term project, because the day after they started, they came to class early and asked me, ‘How do I get this stuff off the internet?’” This was even though they thought they were all protecting their privacy. And remember, they were all graduate students studying information sciences. There’s another concept: Just because people know something, it doesn't mean they behave in the way they know they should. For example, if I tell you what a good password is, you repeat back, “Yeah, I know what a good password is: numbers, letters, at least eight characters, do not reuse your password on multiple accounts and all that sort of stuff.” And a lot of people know that, but the reality is that even when people know that, they don’t always use a good password.

Skroupa: Exactly—you can have the knowledge, but you're not always going to implement it in an effective way, because you don't understand exactly the risk.

Winkler: Exactly. It's like being healthy. Everybody knows to be healthy—you need to eat right and exercise. But you look at the average person, even though they know what it takes to be healthy and know they should do it, they don't. The first thing we recommend in our protection section is proper governance of security. Governance as a whole is not just security related, it's financially related—it's how you run the business. If you do not have proper specification as to what is important to protect, and then details on how it is to be protected, your security program is an accident. Sometimes it is accidentally good, but usually, it's accidentally bad. For example, I could accidentally have a CEO who values security and properly funds security, and they find a chief security officer who knows what they're doing, and that chief security officer uses his budget in a proper way. That's great. But that's a complete accident. Governance acknowledges that security is important, determines how it should be budgeted, explains the behaviors to implement, and how to protect the technology. There should be guidelines and procedures that say how computers should be secured, how information should be released, how people should be trained for awareness, and so on. Security should be driven by proper governance. It has nothing to do with people being aware individually, and it has nothing to do with industry. Either an enterprise has proper governance or it doesn't. If they don’t have proper governance and are still secure, that's awesome to a certain extent, but if the security manager leaves or you get a new CEO in who doesn't think he wants to spend the money on security anymore, the whole security can be blown away, unless of course it's documented and made a part of the corporate DNA, and governance is what makes it a part of the corporate DNA.

Skroupa: So it's really governance training. And then I imagine you go over the details of that in the book as well.
Winkler: Yes. It's even said that the governance chapter is the most important chapter in the book. Think about it this way—how you handle money, that's documented. Orders come in and are verified, money is processed, money is logged, and all that sort of stuff. They have all the important business processes and procedures properly documented. It is the same with security: Employees should be told step-by-step how they should behave. The technology people should provide specific guidance on how the technology is to be implemented. Security guards should be told exactly what they look for and how to look for it, and so on. And if it's not written down, your security is an accident, and usually it is a bad accident.

Skroupa: I think the governance section seems to be where all of this can be implemented on a grand scale. We all have the tools, but we don't all have the implementation plan, and so that'll be the next step before anyone can really create a formidable advanced persistent security (APS) infrastructure.

Winkler: Professionally, my primary purpose is to implement awareness programs, which is valuable to my clients. However without proper governance, awareness is basically just telling people what best practices are. We like to work with companies and define their governance, and use the awareness to promote the established governance. It is infinitely better to tell people how to behave, instead of what they should be afraid of and how not to behave.

Skroupa: And that's why these things exist, so we can bring it to a public conversation, which is not only why you wrote the book, but why we're hoping to cover it.

Winkler: I appreciate that.

Skroupa: So this has all been really interesting. Do you feel like there is anything we haven't touched on that is really relevant to the thesis?

Winkler: Proper governance should be the key driver of your security program. Governance essentially makes a should into a must, because most people think they should be secure, but proper governance says specifically how they must be secure, and if something is a should they basically should all over themselves, and that's a problem. So that's number one. The second concept is a good APS program should have detection and reaction as a comprehensive security protocol. Most security programs fail because they are not security programs—they are just protection programs. Another thing, I think security doesn't fail when the bad guy gets in, security fails when the bad guy gets out and achieves their goal. If the book has a mantra, it is, “Protection, detection, reaction.” These principles come from information warfare, and security is not about security—security is about risk management. In risk management, failure is acceptable—the goal is to ensure you plan for those failures, which, again, is part of governance. What losses are you willing to accept? Security seems to be the only discipline in business where people think any failure is unacceptable. Clearly it's embarrassing, but it is usually minimal compared to the amount of money they lose elsewhere, such as in credit card transactions. Billions are lost each year. People can shoplift and that's accepted. They call it shrinkage—they have a term for it to make it sound like a business element. But for some reason a hacker breaks in and hacks, and they think, “That's bad, so let's fire the security people.” Again, unless you give an unlimited budget to security people, there will be security failures, unless you let the security person do it intelligently.

Google removes two ZTORG trojans from play marketplace

Google, for the second time this month, has removed malicious apps from Google Play that could have laid the groundwork for an attacker to root infected devices. A researcher with Kaspersky Lab on Tuesday described how attackers managed to evade settings set in place by Google Play's VerifyApps malware scanner in order to sneak malware onto unsuspecting users' devices. Earlier this month Google removed a rooting Trojan, Dvmap, from Google Play that was disguised as a puzzle game. If downloaded, the app could have rooted Android devices and injected malicious code into an infected device's system. The two apps that Google removed more recently, Magic Browser, and Noise Detector, were vehicles for the Ztorg Trojan, Kaspersky claims. The more successful of the two apps, Magic Browser, mimicked the Google's Chrome browser. It was installed 50,000 times after it was uploaded on May 15, but never was updated according to Roman Unuchek, a senior malware analyst with Kaspersky Lab an Android malware specialist who discovered the apps.
With Rodotà's death, an "adult democrat" disappear, not just a great jurist and an acute philosopher of law, perpetually struggling to defend the values of justice and equality. There have been many areas that have been the protagonists of this tireless scholar, who was born in a region of Magna Greece (Cosenza in 1933), surely not by chance, to judge the great speculative capacity that has marked the superb intellectual production but had Found in the Capital the main theater of its commitment. At Sapienza University, a professor emerging from civil law, was able to entertain students, researchers but also many managers during frequent seminars he organized, focused on the great challenges of contemporaneity: freedom, security, evolution of European constitutions, bioethics, biological will, regulation f civil unions, fate of common goods, a profuse agenda of issues that reflected the vastness of the interests of an omnivorous intelligence, expressed even through politics (he was parliamentary in the independent left and candidate for the presidency of the Republic by Grillo Movement in Recent years). But what I would like to recall, in a country often spoiled by prejudices and ideological rage, is the institution's man, the president of the Lelio Foundation and Lisl Basso, but above all the Guarantor of Privacy, held by Rodotà from 1997 to 2005. In this Role his legacy will remain indelible. Some central passages such as the definition and the achievement of the unique text of Privacy, to the latest provisions such as the definition of the European Regulation with the introduction of new functions (the DPO only to mention one) have their first source of vision in open innovation that Rodotà first conceived and promoted in dealing with themes designed to mark the development of society, but also the rules of coexistence. He was a forerunner in many fields. He has always seen in advance social phenomena, lifestyles, language changes, learning and communication, "said President Emeritus of Italian Repubblic Giorgio Napolitano in the outline of Rodotà's profile, with which he also had had many reasons for dissent.

**Democracy and Internet**

What strikes is the modernity of his thinking, a lawyer open to the phenomenology of change; the Jurist was fully aware that the Net was not a simple communication tool, but a complex infrastructure that would transform individuals, as well as society and the right. His expressed, at the Internet Global Forum a few years ago, conferring a Nobel to Internet, which could show provocative, now becomes prophetic in light of the many contradictions and new fears that push many countries to raise the censorship wall, denying fundamental rights and freedoms. "It is being created - this was his thought I collected in a recent interview - thanks to technologies, a planetary dimension of rights capable of developing a new path. We must, therefore, set aside simplified projections and be aware that tools we have, offer positive prospects for representative democracy, or how I prefer to define it as a continuing democracy. What has already happened in China, but also in Iran and South Korean workers, shows that today theme of rights is the point of universal convergence, the primary need that passes through the world, the great narrative of the 21st century, after the collapse of great ideologies. "Hence the Nobel proposal, which is going to argue for a long time: "Reasons and motivations can be many," she explained, "but I think the most reliable is the fact that the Internet is the largest public space that humanity has known, where time and boundaries are challenged, where sovereignty is in trouble, where knowledge takes on the appearance of a common good, where individualism and sociality discover new dimensions, where creativity expands, where one can see important promises for Democracy ".

This is the focal point of a loose search: the strength of Constitution that is translated into the health of democracies, in which the new dimension of the network should not be mortified, rather exalted. "We know very well what are the inequalities that manifest themselves in that space, and even strengthen themselves; what are the risks associated with the so-called electronic democracy, in which it is not dangerous to even see the most congenial form of political populism; new powers without control materialize; hate languages can encounter planetary platitudes. However, the opportunities of knowledge and dialogue, learning of the fundamental freedoms of liberty out of any authoritarian imposition, common action of people of good will, talk about preconditions neither diplomats nor military, of any culture of peace. Without the Internet, the largest peace movement so far known, appeared on the world scene with demonstrations against the intervention in Iraq would not have been possible. "

**Towards digital citizenship**

Certainly fascinating Rodotà's writings dedicated to development of the Information Society and particularly to the definition of a digital citizenship that is opening up a new generation of human rights. "We must first wonder whether digital citizens actually add something to equality and participation in public life. Is it a driving force towards greater equality? The answer - he wrote in Democracy and the new communication technologies- can not be absolute. Today's challenge is to affirm an inclusive dimension of citizenship. From the time of the Edict of Caracalla, citizenship
conferred a superiority, linked to being *civis romanus*. The prevailing logic was of an exclusive nature, supported by the close correlation between citizenship and territory. This scheme holds up to the time of the modern state. With the affirmation of social rights, a new season opens. The idea of a citizenship of the person begins to get in the way of an international scenario that overcomes the traditional concept of the Hobbesian state. Digital citizenship, which recognizes Netizen (the person who actively participates in Internet life, contributing to the strengthening of freedom of speech n.d.r.), can only be an extension of the original historical heritage linked to the general evolution of society. It is no coincidence that this conceptual framework should be analyzed in the light of a re-reading of universal rights."

Another crucial aspect for security concerns is anonymity, now emphasized by the web 2.0 paradigm and the pervasiveness of the IOT. This is also worth recalling his thoughts directly: "We can assume multiple identities on the net. The digital "person" has more faces. When it is addressed to the accountant, the doctor, the friend may exhibit a pseudonym. It happens that we all live in a universe where shreds of each other's identity are scattered in different databases. Those multiple identities that articulate on the world scene with different representations of themselves, know different degrees of public persistence, which vary according to the intensity with which the right to oblivion is recognized. In fact, we need to add that the technological tools put us under constant control, none of us can be anonymous even when we want to. We are constantly with an on-board video surveillance camera, with a mobile operator recording all the activities we have. The evolved context therefore generates a need for privacy and confidentiality. The anonymity, which seemed to disappear in the dimension of technological society, then re-emerged as an individual's right to enjoy an area of freedom."

**Right, Security and Privacy in the Network Company**

In this viewpoint, the concept of Privacy is also intended to flex in new important enunciations that Rodotà sums up with an original and effective image: the protection of the "electronic body". "We can no longer speak of privacy as a simple need for confidentiality, the concept extends to the protection of the information system that concerns the citizen and often follows uncontrollable paths. Collecting information for commercial purposes, so-called user profiling is "building identity" activities that can not be done without the agreement of the person concerned. By profiling a company, or any other subject that operates on the market, traces an "erroneous destiny" that may have effects on individuals' lives, with the consequences we can imagine. " One point remains firmly expressed in one of the latest theses (*The right to have rights*): In the new global space of digital networks, without an adequate evolution of law, there can be no democracy or peace among peoples: "New ways of acquiring consensus are being determined, which do not always correspond to a new distribution of power. But the dimension of electronic democracy must not be confused with the possibility of being called to say yes or no at the end of a decision-making process all run by others. The power of individuals and groups must be exercised in a transparent manner, allowing access to all the information necessary to exercise widespread control, to participate in the public debate, to design and suggest and to intervene in decision-making processes, integrating the Representative democracy with participatory democracy."

This lucid vision of democracy is accompanied by a concern that shakes the mind of this great laic man thinker: the most striking cases of violated rights that lead into the world today to the escalation of violence and the overthrow that also invests the most sacred "fence" of family affections. This had been his answer: it is difficult to believe that there are serious or less serious violence, since anyone who is subjected to violence, even though small, is denied in his humanity. Of course, we must remember the Shoah, a truly unique violence, along with the war, indiscriminate violence. Violence is fought with education, with the knowledge of others by promoting in assessment spaces, and therefore primarily in public school. Only by going out of any ghetto - cultural or religious, locality or privileged - one learns to recognize one another in the other, to accept it. If you do not go in this direction, if fear and violence take hold of society, it is not worth thinking that there are shelters "from a heartless world," like the family, who takes part in the climate in which we lives. " It is certainly the clearest message that can help us to go the way to progress, which is still unfortunately very long.
**The aim:** The Master program aims to train experts able to identify, prevent and counter the main types of cyber attack that can be perpetrated at the expense of public and private organizations. The Students will learn to use attack techniques in a responsible manner and analyze security aspects from the hacker’s point of view in order to increase the level of protection and security of organizations. They will experience, in specially designed virtual environments, techniques of attacking to infrastructures, authentication systems, mobile devices, and hardware.

**Requirement:** Master’s degree or specialist in Computer engineering or Science and Information technology or Cyber Security, Electronic Engineering, Telecommunication Engineering, Automation Engineering, Management Engineering, Security Engineering, Computer Science statistics.

**Training objectives:** The Master program intends to create professionals able to:

- Become expert in attack techniques and the same tools used by hackers and the main tools of cyber threat intelligence.
- Test the network and systems with the same methods and techniques used by hackers to test for vulnerabilities and security flaws.
- Identify the best security measures to be implemented to prevent, intercept and prevent quickly cyber attacks.

---

**REGISTRATION FEE**
Master registration fee is 2000 €

**DURATION OF THE COURSE**
12 months

**CREDITS**
63CFU

**ADMISSION DEADLINE**
Publication and admission September 2017

**BEGINNING LESSONS**
November 2017

**TEACHING ACTIVITY**
Friday (2-8pm) and Saturday (8-14am)

**INFORMATIONS**
Head of the Master Program, Prof. Andrea Pugliese
andrea.pugliese@unical.it
https://www.dimes.unical.it/