POLITECNICO DI BARI
Dipartimento di Elettrotecnica ed Elettronica
Via Orabona, 4 – Bari (Italy)

5th IT STAR WS on
Electronic Business

12 November 2010, Zagreb, Croatia

Legal Framework and Security Issues

Giuseppe MASTRONARDI
Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari, Italy
mastrona@poliba.it

INTRODUCTION

- Privacy on the Internet remains a burning issue, which could affect not just the success of the net economy.
- I present a closer look to the Italian law on privacy issues and related security technologies.
- A communication tool as Internet, where information can move at high speed and on a global scale, generates many problems and questions on the privacy protection.

“There is no privacy without security"

The current technology that supports the Internet is completely in contrast with the law on privacy.

The problem is: after the first generation of software/services on the Internet, who does not stand up to expand the range with recommended suppliers or products of specific interest to the customer (obtained from the digital information left by the same customer)?

As for our legal system, the right to privacy is protected by Legislative Decree n. 196/2003 (defined "Code on personal data protection”)

Privacy Law

- It is defined personal any information relating to the natural person, legal person, association or society or can be identified, directly or indirectly by reference to any other information, including a personal identification number.
- The processing of sensitive data is possible, but only with the written consent and approval of the Privacy Authority (National Guarantor).
- Personal data must still be processed lawfully and fairly collected and recorded for specific, explicit and legitimate means.

e-Commerce Operators

The law of privacy, for example, applies to all operators in the area of e-commerce:

- the internet-provider
- the supplier or the owner of the web-site
- the certification authority
- the holder of the private key.

The Provider

Data Log files are of particular importance, because store all users movements, while browsing on Intemet.

The providers shall be recorded on the log each access to the system, with the date, the time of link beginning and end, the network addresses, the subscriber identifier codes in the case of anonymous or pseudonyms use.

This practice naturally responds to the needs of quality control services, access timing to the exact billing, and any verification of crime commissions, at the request of the court.

The site owner

If the site provide products or services in Internet, as site owner and as manager of the treatment of data relating to site visitors, will be required, for its part, to respect the formalities under privacy law.

Therefore, the on-line commercial offers should contain the information and be prepared to allow the user, whether professional or consumer, to agree or deny its consent, as required. Only after reading the note, the site visitor will be able to give its consent, as a condition for the order.

The certifier

The observance of the security measures is a fundamental obligation of Certification Authority (CA).

The regulation on digital signatures expressly declares that is required to take all appropriate technical and organizational measures to prevent harm to others and must, in particular, to comply with the minimum security for the processing of personal data.

In fact, the certifier, as owner of the data on the holders of the keys, is always required to take all safety measures under Law No 196/2003.

POLITECNICO DI BARI
Dipartimento di Elettrotecnica ed Elettronica
Via Orabona, 4 – Bari (Italy)

The owner of the private key

The owner of the private key, as owner of data processing, has the obligation to comply with the requirements relating to privacy and provide the necessary security measures and prescribed, at the same way as certifiers.

The attacks on Internet

The Internet allows even groped attacks to remote computers without having to spend capital calls or having to fool the systems in the telephone company.

It allows you to hide messages posing as if they originated from other computers (spoofing) to exploit and snatched bits of information from messages in transit (sniffing).

Unauthorized access, Viruses, Illegal software, ...

For transmission of sensitive data, some solutions available today on the Internet are:

- Accept no privacy
- The end-user level encryption
- The SSL protocol
- The SET protocol

Cyber Security and Critical Infrastructure Protection (July 15, 2010)

The Parliamentary Committee for Security of the Republic (Copasir) published July 15, 2010 the "Report on the possible implications and threats to national security resulting from the use of cyberspace"describing the scenario of international and national security in the near future and are as follows:

- introduction of new synthesis of strategic issues related to the tasks of the Committee;
- a description of the activity;
- illustration of the characteristics of the phenomenon at a global level;
- analysis of the consequences for our country;
- presentation of the main findings of the intelligence;
- proposed measures to strengthen the analytical capacity of our security apparatus and to strengthen activities to prevent and combat cyber threats.

POLITECNICO DI BARI
Dipartimento di Elettrotecnica ed Elettronica
Via Orabona, 4 – Bari (Italy)

Operative tasks

- to define completely the threat and prepare a national security document dedicated to the protection of critical infrastructure and equipment;
- to prepare an action plan that defines the perimeter of the Italian cyber security by defining the roles and responsibilities of all those responsible for national security;
- to prepare, in close coordination with the institutional partners and individuals, starting with our intelligence apparatus, the strategic policies of protection, cyber security and resilience - developing public-private collaboration to improve the action of preventing and combating the cyber-crime;
- to promote plans for specialist training common among the various stakeholders at national and international level, including promoting information campaigns targeted towards subjects of strategic importance, to raise the level of awareness of risks in cyberspace;
- to prepare disaster recovery plans for data of strategic value for the security of the Republic;
- to coordinate the participation of delegations to the Italian tables of international cooperation in bilateral and multilateral, EU and NATO.

POLITECNICO DI BARI
Dipartimento di Elettrotecnica ed Elettronica
Via Orabona, 4 – Bari (Italy)

New Rules of Conduct for the Wi.Fi. (November 5, 2010)

There is no denying that the ICT are changing our lives.

The relations between people are changing:

- Social Networks can now build relationships quantitatively and qualitatively very different from the past.
- The newspapers today provide information easily accessible via Internet, or via phone, and are constantly updated.
- Our way of having fun is changing: no longer queues to video rentals, just download (legally or not) movies to your PC or PDA.
- The way to care is changing: telemedicine allows remote diagnostic tests and to undergo surgery a patient admitted to hundreds of kilometers from the doctor.

So, from 1st January 2011 there will be more tolerant and less bureaucracy for those who choose to share their Wi-Fi connection.

To protect your Wi-Fi network, is now recommended to use WPA2 Personal (for home or small business) who changed the encryption algorithm AES by the previous RC4, making it much safer. But each card has its own Mac Address, so you can restrict access to your wireless network to only authorized Mac Addresses.

But there are also the following measures:

- DHCP disabled
- Class IP changed
- Reduction of signal strength (if allowed)
- Hidden SSID with different name than the default

In addition, the Privacy Authority introduces new rules of conduct for Google Cars. Cars must be recognizable and Google will provide citizens with detailed information on the Italian passage of vehicles used for the service Street View.

Citizens will be able to decide freely, whether or not to accept being taken, with their homes themselves, and then appear on the overview maps online.

POLITECNICO DI BARI
Dipartimento di Elettrotecnica ed Elettronica
Via Orabona, 4 – Bari (Italy)

New Rules for Video-Surveillance (September 14, 2010)

In view of the massive video-surveillance systems for different purposes (investigation, prevention and suppression of crime, public safety, protection of private property, traffic control, etc.), the Privacy Authority introduced new rules for installation and use of cameras and video-surveillance systems in public and private places:

- Citizens in transit in areas supervised must be informed with signs clearly visible in the dark too
- Video-surveillance systems connected to the police require a special warning notices
- Cameras installed in order to protect public order and security, always respecting the work rules, can not be indicated
- Recorded images can be stored for a limited period (usually up to a maximum of 24 hours, for banks and risk assets up to a maximum of one week). The restrictions do not apply in relation to the investigation activities, but still with preliminary verification of the Guarantor.

CONCLUSIONS

Technological innovations trigger the invasion of privacy and sensitive legal issues.

Sometimes the pace of change is so urgent that the same technologies and the right seem unable to keep pace.

But I trust the informatics techniques are now able of countering the attacks which has made it possible.

This is the new business of the software house.

Thank You

for Attention