Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 12
INTERNET LEGALITIES AND ETHICS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Francisco de Quinto, Piqué Abogados Asociados
Jordi Saldaña, Piqué Abogados Asociados
Jaume Abella, Enginyeria La Salle (URL) – ISECOM
Marta Barceló, ISECOM
Kim Truett, ISECOM
Pete Herzog, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

12.1. Introduction

New technologies, while building a new paradigm that invades every human activity, also influence the dark side of these activities: criminal behavior of individuals and of organized groups.

For this reason, we have reserved the last lesson of HHS to analyze some aspects related to Legality and Ethics, analyzing several behaviors that could end in crimes and the consequences of these crimes.

12.2. Foreign crimes versus local rights

As noted above, the introduction of new technologies can result in the creation of new dark sides of activities: criminal behavior of individuals or organized groups. There are two main characteristics through which Information Technology and Communications (TIC's) are related to crime:

1. Technologies can give the possibility of renewing traditional ways of breaking the law. These are illegal activities which traditionally appear in the penal codes, but are now being attempted in new ways. Examples include money laundering and illegal types of pornography.
2. In addition, because of their own innovation, TIC's are resulting in the appearance of new types of criminal activities, and because of their nature, these new crimes are in the process of being added to the legislation of several countries. Examples include the distribution of spam and virus attacks.

Another characteristic of the TICs which must be emphasized is their territorial displacement, which affects the general surroundings but without any doubt affects other countries as well. Previously, areas of 'law' always had a clear territory regarding the judicial authority judging (COMPETENT JURISDICTION) and also regarding the law to be applied in the judging (APPLICABLE LAW). Both concepts are still noticeably geographic.

In summary, we can say that the TICs are global and essentially multi-border, while the law and the courts are limited to a specific state or territory. In addition, this disorientation is even more confusing than it initially appears. Although we are not aware of it, a bidirectional online communication between a user in Barcelona and a Web site hosted in an ISP in California can pass through more than 10 ISPs, hosted in a variety of remote points around the world. Facing this diversity of addresses and nationalities, it becomes necessary to ask *What laws of which country will be applied in case of litigation? Which of the possible countries will be the suitable court to adjudicate the case?*

The relatively recent European Council's agreement on cyber-crime was signed in November 2001 in Budapest by almost 30 countries, including the 15 partners of the European Union, the United States, Canada, Japan and South Africa. This agreement intends to restore the TERRITORIAL PRINCIPLE to define competent jurisdiction. The signing of this agreement is the culmination of four years of work that have resulted in a document containing 48 articles that are organized into four categories:

1. Infractions against confidentiality
2. Falsification and computer science fraud
3. Infractions relative to contents
4. Violations of intellectual property

Once the especially complex regulations and sanctions on criminal activity on the Internet have been described, consensus must to reached on three main areas of concerns or difficulties:

1st DIFFICULTY: JURISDICTION CONFLICT. Election of the most competent court for judging multinational and multi-border crimes. This problem is not definitively solved by any of the known judicial systems.

2nd DIFFICULTY: CONFLICT OF LAWS. Once the court has been chosen, the first obstacle that the court will encounter is choosing the law applicable for the case to be judged. Again we are forced to conclude that traditional legal criteria are not designed for the virtual surroundings.

3rd DIFFICULTY: EXECUTION OF SENTENCE. Once the competent court has determined a sentence, the sentence must be carried out, possibly by a different country than the country which dictated the sentence. Therefore, it is necessary to have an international commitment to recognition and acceptance of any sentences imposed. This problematic issue is even more complicated to solve than the two previous ones.

These complications were clearly demonstrated in the recent case of a hacker in Russia, who had hacked several US systems, and was invited to a phony US company for an interview. During the interview, he demonstrated his skills by hacking into his own network in Russia. It turned out that the interview was actually conducted by the FBI, and he was arrested. The FBI used sniffers placed on the interview computer to raid the hacker's computer in Russia and download evidence that was used to convict him.

But there are many unresolved issues:

- Was it legal for the FBI to examine the contents of a computer in Russian, without obtaining permission from the Russian government?
- By inviting the hacker to the US, the FBI did not have to arrange for his extradition to the US. Was this legal?
- Could the US convict a person for crimes that were technically committed on Russian soil?

Finally, he was convicted in the US, because he had used a proxy server in the US to conduct some of the attacks. He served just under 4 years in prison and now lives and works in the US.

Exercise:

Conduct a modified white-hat / black-hat discussion of at least one of these questions (examination of a computer on foreign soil; invitation or entrapment(?) to avoid extradition; conviction for internet crimes committed against a country from foreign soil).

1. First, have students focus on and list reasons why the chosen topic was probably legal.
2. Then reverse and have them focus on and list why the chosen topic was probably illegal.
3. After these completely separate discussions, see if the class can reach a decision.

Note – these questions are interesting for discussion. There is no right answers, and governments are still working to come to a consensus on these and other issues related to the international nature of these crimes. This exercise is purely for critically examining and thinking about internet crimes, as well as formulating a logical argument for an opinion related to internet crimes.

12.3. Crimes related to the TICs

The classifications of the criminal behaviors is one of the essential principles in the penal systems. For this reason, several countries must think of changes to their penal codes, such as Spain, where the effective Penal Code was promulgated relatively recently. The well known Belloch Penal Code was approved on November 23rd 1995 (Organic Law from the Penal Code 10/1995) and it recognizes the need to adapt the penal criteria to the present social reality.

Among others, we can classify potential criminal actions into the following six sections.

1. Manipulation of data and information contained in files or on other computer devices.
2. Access to data or use of data without authorization.
3. Insertion of programs/routines in other computers to destroy or modify information, data or applications.
4. Use of other people's computers or applications without explicit authorization, with the purpose of obtaining benefits for oneself and/or harming others.
5. Use of the computer with fraudulent intentions.
6. Attacks on privacy, by means of the use and processing of personal data with a different purpose from the authorized one.

The technological crime is characterized by the difficulties involved in discovering it, proving it and prosecuting it. The victims prefer to undergo the consequences of the crime and to try to prevent it in the future rather than initiate a judicial procedure. This situation makes is very difficult to calculate the number of such crimes committed and to plan for preventive legal measures.

This is complicated by the constantly changing technologies. However, laws are changing to increasingly add legal tools of great value to judges, jurists and lawyers punish crimes related to the TICs.

Next we will analyze some specific crimes related to the TIC's.

1. Misrepresentation: The anonymity of the internet allows users to pretend to be anyone that they want to be. As a result, crimes can be committed when users pretend to be someone else to gain information, or to gain the trust of other individuals.
2. Interception of communications: Interceptions of secrets or private communications, such as emails, or cell phone transmissions, using listening devices, recording, or reproduction of sounds and or images.
3. Discovery and revelation of secrets: Discovering company secrets by illegally examining data, or electronic documents. In some cases, the legal sentences are extended if the secrets are disclosed to a third party.
4. Unauthorized access to computers: Illegal access to accounts and information, with the intent of profiting. This includes identify theft.
5. Damaging computer files: Destroying, altering, making unusable of in any other way, damaging electronic data, programs, or document on other computers, networks or systems.

6. Illegal copying: Illegal copying of copy-righted materials, literary, artistic, scientific works through any means without the authorization of the owners of the intellectual property or its assignees.

Exercise:

1. Choose one of the topics above, and conduct the following searches:
   - Find a legal case which can be classified as the chosen type of crime.
   - Was there a legal judgment, and if there was, what sentence was applied ?
   - Why did the authors commit this crime?
2. Regarding intellectual property: Are the following actions a crime?
   - Photocopy a book in its totality
   - To copy a music CD that we have not bought
   - To make a copy of a music CD you have bought
   - To download music MP3, or films in DIVX from Internet
   - What if it were your music or movie that you were not getting royalties for? What if it were your artwork, that others were copying and stating that they created it?

12.4. Prevention of Crimes and Technologies of double use

The only reliable way to be prepared for criminal aggression in the area of the TICs is to reasonably apply the safety measures that have been explained throughout the previous HHS lessons. Also it is extremely important for the application of these measures to be done in a way that it becomes practically impossible to commit any criminal or doubtful behaviors.

It is important to note that technologies can have multiple uses and the same technique used for security can, simultaneously, result in criminal activity. This is called TECHNOLOGIES OF DOUBLE USE, whose biggest components are cryptography and technologies used to intercept electronic communications. This section discusses the reality of this phenomenon and its alarming consequences at all levels of the human activity including policy, social, economic and research.

12.4.1. The global systems of monitoring: concept "COMINT"

The term COMINT was created recently as a result of the integration of the terms "COMmunications INTelligence" and refers to the interception of communications that has resulted from the development and the massive implementation of the TIC's. Nowadays, COMINT represents a lucrative economic activity providing clients, both private and public, with intelligent contents on demand, especially in the areas of diplomacy, economy and research. This has resulted in the displacement of the obsolete scheme of military espionage with the more or less open implementation of new technologies for the examination and collection of data.

The most representative examples of COMINT technologies are the systems "ECHELON" and "CARNIVORE" which are discussed next.

12.4.2. "ECHELON" System

The system has its origins in 1947, just after World War II, in an agreement between the UK and USA with clear military and security purposes. The details of this agreement are still not completely known. Later, countries like Canada, Australia and New Zealand joined the agreement, working as information providers and subordinates.

The system works by indiscriminately intercepting enormous amounts of communications, no matter what means is used for transport and storage, mainly emphasizing the following listening areas:

- Broadband transmissions (wideband and Internet)
- Facsimile and telephone communications by cable: interception of cables, and submarines by means of ships equipped for this
- Cell phone communications
- Voice Recognition Systems
- Biometric System Recognition such as facial recognition via anonymous filming

Later, the valuable information is selected according to the directives in the Echelon System, with the help of several methods of Artificial Intelligence (AI) to define and apply KEY WORDS.

Each one of the five member countries provides "KEY WORD DICTIONARIES" which are introduced in the communication interception devices and act as an "automatic filter". Logically, the "words" and the "dictionaries" change over time according to the particular interests of the member countries of the System. At first, ECHELON had clear military and security purposes. Later, it became a dual system officially working for the prevention of the international organized crime (terrorism, mobs, trafficking in arms and drugs, dictatorships, etc.) but with an influence reaching Global Economy and Commercial Policies in companies.

Lately, ECHELON has been operating with a five-point star structure around two main areas. Both are structures of the NSA (National Security Agency): one in the United States, coinciding with their headquarters in Fort Meade (Maryland), and another one in England, to the north of Yorkshire, known like Meanwith Hill.

The points of the star are occupied by the tracking stations of the collaborating partners:

- The USA (2): Sugar Grove and Yakima.
- New Zealand (1): Wai Pai.
- Australia (1): Geraldtown.
- UK (1): Morwenstow (Cornwell).
- There was another one in Hong Kong before the territory was returned to China.

12.4.3. The "CARNIVORE" system

The second great global systems of interception and espionage is the one sponsored by the US FBI and is known as CARNIVORE, with a stated purpose of fighting organized crime and reinforcing the security of the US. Because of its potent technology and its versatility to apply its listening and attention areas, CARNIVORE has caused the head-on collision between this state of the art system, political organizations (US Congress) and mass media.

CARNIVORE was developed in 2000, and is an automatic system, intercepting internet communications by taking advantage of one of the fundamental principles of the net: the dissemination of information in "packages" or groups of uniform data. CARNIVORE is able to detect and to identify these "packages of information". This is supposedly done in defense of national security and to reinforce the fight against organized and technological crime.

The American civil rights organizations immediately protested this as a new attack on privacy and confidentiality of electronic information transactions. One group, the Electronic Privacy Information Center (EPIC) has requested that a federal judge order the FBI to allow access by the ISP'S to the monitoring system – to ensure that this system is not going to be used beyond the limits of the law.

In the beginning of August 2000, the Appeals Court of the District of Columbia rejected a law allowing the FBI to intercept telecommunications (specifically cell phones) without the need to ask for previous judicial permission, through a Federal Commission of Telecommunications project that tried to force mobile telephone companies to install tracking devices in all phones and thus obtain the automatic location of the calls. It would have increased the cost of manufacturing equipment by 45%.

With these two examples, we see the intentions of the FBI to generate a domestic Echelon system, centering on the internet and cell phones, known as CARNIVORE. The project has been widely rejected by different judicial courts in the US and by Congress, as there is no doubt it means an aggression to American civil rights, at least in this initial version.

The project is being rethought, at least formally, including the previous judicial authorization (such as a search warrant) as a requirement for any data obtained to be accepted as evidence in a trial.

Exercise:

A joke related to these COMINT systems is found on the Internet. We include it here for class discussion of the ethical and legal implications:

An old Iraqi Muslim Arab, settled in Chicago for more than 40 years, has been wanting to plant potatoes in his garden, but to plow the ground is a very difficult work for him. His only son, Amhed, is studying in France. The old man sends an email to his son explaining the following problem:

"Amhed, I feel bad because I am not going to be able to have potatoes in my garden this year. I am too old to plow the soil. If you were here, all my problems would disappear. I know that you would plow the soil for me. Loves you, Papa. "

Few days later, he receives an email from his son:

"Father: For God's sake, do not touch the garden's soil. That is where I hid that . . . Loves you, Amhed. "

The next morning at 4:00, suddenly appears the local police, agents of the FBI, the CIA, S.W.A.T teams, the RANGERS, the MARINES, Steven Seagal, Sylvester Stallone and some more of elite representatives of the Pentagon who remove all the soil searching for any materials to construct pumps, anthrax, whatever. They do not find anything, so they go away.

That same day, the man receives another email from his son:

"Father: Surely, the soil is ready to plant potatoes. It is the best I could do given the circumstances. Loves you, Ahmed."

Exercise:

Search for information about the Echelon and Carnivore systems on the internet, as well as their application on networks and TICs systems in your country to answer the following question:

1. What does the term "ECHELON" mean?
2. What elements form the ECHELON system?
3. What elements form the CARNIVORE system?
4. Search for an example of controversy attributed to the ECHELON system and related to famous personalities.
5. Search for an example of the application of the CARNIVORE system related to a TERRORIST known worldwide.
6. What is your opinion about the "legality" of such systems?

12.5. Ethical Hacking

Besides talking about criminal behaviors, crimes, and their respective sanctions, we must make it very clear that being a hacker does not mean being a delinquent.

Nowadays, companies are hiring services from "Ethical Hackers" to detect vulnerabilities of their computer science systems and therefore, improve their defense measures.

Ethical Hackers, with their knowledge, help to define the parameters of defense. They do "controlled" attacks, previously authorized by the organization, to verify the system's defenses. They create groups to learn new attack techniques, exploitations and vulnerabilities, among others. They work as researchers for the security field.

Sun Tzu said in his book "The Art of War", "Attack is the secret of defense; defense is the planning of an attack".

The methodology of ethical hacking is divided in several phases:

1. Attack Planning
2. Internet Access
3. Test and execution of an attack
4. Gathering information
5. Analysis
6. Assessment and Diagnosis
7. Final Report

One helpful tool that Ethical Hackers use is the OSSTMM methodology - Open Source Security Testing Methodology Manual. This methodology is for the testing of any security system, from guards and doors to mobile and satellite communications and satellites. At the moment it is applied and used by important organizations such as:

- Spanish Financial institutions
- the US Treasury Department for testing financial institutions

- US Navy & Air Force

Exercise:

Find information about Ethical Hacking and its role in IT security companies.

Search for information about the OSSTMM and methodologies.

Search for information about "certifications" related to the Ethical Hacking.

12.6. The 10 most common internet frauds

Listed below is a summary from the US Federal Trade Commission of the most common crimes on the Internet as of 2005.

1. Internet Auctions: Shop in a "virtual marketplace" that offers a huge selection of products at great deals. After sending their money, consumers receive an item that is less valuable than promised, or, worse yet, nothing at all.
2. Internet Access Services: Free money, simply for cashing a check. Consumers are "trapped" into long-term contracts for Internet access or another web service, with substantial penalties for cancellation or early termination.
3. Credit Card Fraud: Surf the Internet and view adult images online for free, just for sharing your credit card number to prove you're over 18. Fraudulent promoters use their credit card numbers to run up charges on the cards.
4. International Modem Dialing: Get free access to adult material and pornography by downloading a "viewer" or "dialer" computer program. Consumers complained about exorbitant long-distance charges on their phone bill. Through the program, their modem is disconnected, then reconnected to the Internet through an international long-distance number.
5. Web Cramming: Get a free custom-designed website for a 30-day trial period, with no obligation to continue. Consumers are charged on their telephone bills or received a separate invoice, even if they never accepted the offer or agreed to continue the service after the trial period.
6. Multilevel Marketing Plans/ Pyramids: Make money through the products and services you sell as well as those sold by the people you recruit into the program. Consumers say that they've bought into plans and programs, but their customers are other distributors, not the general public.
7. Travel and Vacation: Get a luxurious trip with lots of "extras" at a bargain-basement price. Companies deliver lower-quality accommodations and services than they've advertised or no trip at all. Others impose hidden charges or additional requirements after consumers have paid.
8. Business Opportunities: Taken in by promises about potential earnings, many consumers have invested in a "biz op" that turned out to be a "biz flop." There was no evidence to back up the earnings claims.
9. Investments: Make an initial investment in a day trading system or service and you'll quickly realize huge returns. But big profits always mean big risk. Consumers have lost money to programs that claim to be able to predict the market with 100 percent accuracy.

10. Health Care Products/Services: Claims for "miracle" products and treatments convince consumers that their health problems can be cured. But people with serious illnesses who put their hopes in these offers might delay getting the health care they need.

Exercise:

Think about the following questions and discuss them with the rest of the class:

1. Do you think that you could have been a victim of some of the crimes mentioned throughout the lesson?
2. Here is a quote from an ISECOM board member: "In order to have the proper background to evaluate the security readiness of a computer system , or even an entire organization, one must possess a fundamental understanding of security mechanisms, and know how to measure the level of assurance to be placed in those security mechanisms. Discuss what is meant by this and how you could prepare to "evaluate the security readiness of a computer system". Have these lessons given you enough materials to get started?
3. [optional exercise for personal consideration (not general discussion)]: After analyzing the comments in this lesson, you may find that there are technological activities that you have heard about, or that you may have even done, that you never considered to be illegal, but now you are not sure. Some research on the internet may help clear up any questions or confusion that you have.

12.7. Recommended Reading

http://www.ftc.gov/bcp/menu-internet.htm

http://www.ic3.gov/

http://www.ccmostwanted.com/

http://www.scambusters.org/

http://compnetworking.about.com/od/networksecurityprivacy/l/aa071900a.htm

http://www.echelonwatch.org/

http://www.isecom.org/