Applied informatics

Secure access to data, security analysis, legislative restrictions.

ZEMÁNEK, Z. – PLUSKAL,D. – SMETANA, B.

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Secure access to data, security analysis, legislative restrictions.

1. Secure access to data - Solution
2. Analysis of data security
3. Legislative measures
4. Assignments

Aims of the lecture

1. Provide students with basic information about secure access to the data.
2. Clarify the importance of analyzing data security; diversity of manifestations of malware.
3. To characterize the diversity of legislative legal restrictions.

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Secure access to data

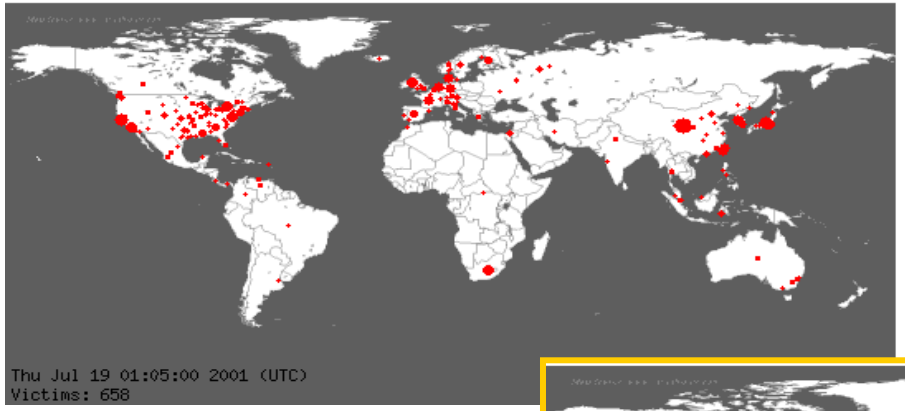
- Implementing update of the operating system itself (Microsoft Windows) or Microsoft Office is not so much the problem (updates are downloaded automatically, or can be easily searched through Windows Update).
- What updates for other applications?
- A great risk may be, for example unpatched third-party applications that are associated with different browsers in the form of plug-ins (PDF viewer such as Adobe Acrobat Reader, players of "flash" animations - Adobe Flash Player ...).
- If there is a security hole and the attacker exploits it (gets into a computer without the user's knowledge, for example, a malicious program steals sensitive data ...).
- Information security issues are still a priority, as the environment becomes increasingly sophisticated malicious software. [1]

Secure access to data

- Do you have sensitive data, financial data, contact lists and other things that you do not want to see anyone else in your computer?
- Computer security is often discussed topic. You do not necessarily suffer paranoia when you want to secure access to sensitive data.
- Secure your access to the operating system as well as data.
- This can be achieved by several different methods with various software helpers.
- It is also important to identify the possible threats and risks of malware. [2]

Malware

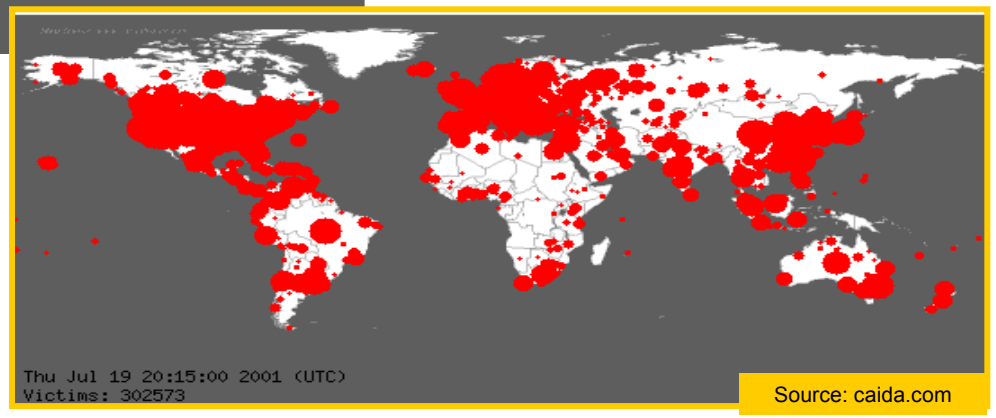
Malicious code is a special program code, whose task is to damage the device, data programs, exhaust system resources, dispose of information, etc.



Speed of spreading of malware - Code Red - 2001

Infection starts…

... 19 hours later



Source: caida.com

Malware

Malware – unwanted, malicious software.

Malware classification:

- Viruses
- Worms
- Trojans (Trojan horses)
- Spam
- Alarm messages (hoax)
- spyware
- Other parasitic programs - Backdoor, Rootkit, ...

[3]

Malware

Viruses

- A computer virus is a computer program, usually malicious, that can create copies of Itself and spread without the user's knowledge.
- Viruses can perform any malicious activity and are divided into many different groups.

Worms

- Viruses which use programs communicating in computer networks (local and global) to spread.

[3]

Malware

Trojan (horses)

- It is a program that secretly installs with any other program, in which it is "hidden".
- Concealed then performing malicious activities.
- It is not a virus as it does not create a copy and spread.
- Often tries to get into the computer when opening unsafe websites.

[3]

Malware

SPAM

- It is an unsolicited e-mail, mostly advertising content.
- Some viruses spread via spam, and are attached in a form of an executable file.
- In many countries sending spam is punishable.

Hoax

- It's kind of spam with a false e-mail message - not based on truth.
- It may, for example, warn against a dangerous virus that does not exist, attracts money from people etc.

[3]

Malware

Phishing

- It is a fraudulent technique used on the Internet for obtaining sensitive data (passwords, credit card numbers, etc.).
- Its principle is sending e-mail messages that are disguised as official request of banks or other similar institutions and invite the recipient to enter their data on the linked page.
- This page may imitate online banking login to ask for their username and password.
- These data can be revealed to the attackers, who are then able to steal money from the account.

Malware

Spyware

- It is a tracking program.
- You can capture typed text, stealing data, passwords, monitor network traffic and the like.
- Often installed in companies to monitor employees' work!

Adware

- It is a program that is disturbing work using an application that displays advertisements.
- Often changes the home page of an internet browser.

[3]

Malware

Backdoor

- a method that allows you to bypass normal authentication, which normally prevents the user from unauthorized use of a computer system.
- Backdoors are included with the software and can be used for serious purposes (e.g. for service access), but they are often misused, so they are classified as a security risk or vulnerability.
- Exploit is a special program in computer science, data, or sequence of commands that make use of programmer error, which causes the originally unintended operation and software enabling you to get any benefit.
- Most of the exploits used to gain directly administrator rights (root or administrator), but there are also those where the attacker first obtains lower rights and using other exploits leverages rights to the administrator.

[3]

Malware

Rootkit

- It is a malicious program changing behavior and security of operating system.

- Rootkit technology masks the presence of malicious programs, hiding directories and files.

[3]

Data security

- Update your operating system and other programs.
- Install anti-virus program and regularly update the program and the virus database.
- Regularly check (scan) data on the computer.
- Install firewall.
- Regularly back up your data (weekly, monthly). For example, use an external hard drive.
- Never open suspicious e-mails, such as e-mails from unknown persons (with attached files).
- Data transfer should use encryption.

[5]

Antivirus

The antivirus program monitors all the essential entry / exit points, which would viruses to penetrate into the computer system.

[3]

Data security - firewall

Firewall is a network device that is used to control security and network traffic between networks with different levels of trust and security.

To simplify, we can say that it serves as a control point, which defines the rules for communication between networks, which it separates.

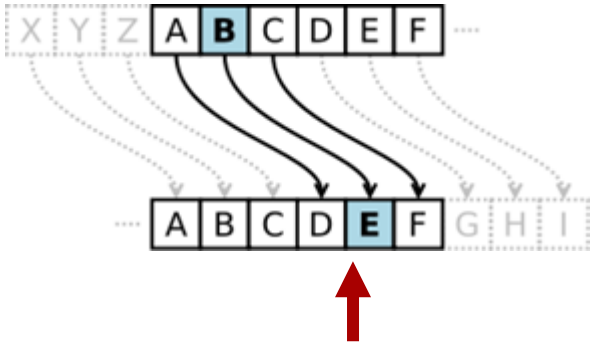
These rules historically always included the source and target data (source and destination IP address), and source and destination ports.

Modern firewalls include also information on the connection status, knowledge of the protocols and possibly elements of IDS (intrusion detection system).

[5]

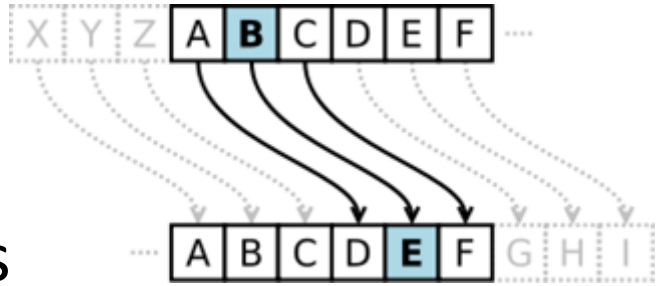
Data security

Cryptography



- Cryptography literally means the study of secret writing, is known from ancient times, through the Caesar cipher (100 BC - 44 BC), Enigma ...
- means the ability to maintain confidential report secret
- cryptanalysis is the art to decipher the code, and thus reveal the secret message

Cryptography



- Cryptology is mathematics for cryptography and cryptanalysis
- encryption algorithm is a mathematical function which performs encryption and decryption of the data
- cipher - encryption key can be compared to a password

Symmetric encryption

- Advantages
  - Speed (1000x faster than asymmetric encryption).
- Disadvantages
  - The key is secret
  - A separate key is need for each party we communicate with
  - *Key must be pre-shared!*

Asymmetric encryption

- Advantages
  - Public key is public
- Disadvantages
  - Speed (slow)

[5]

Electronic signatures

Electronic signatures provides for:

- authenticity - can verify the authenticity of data (identity of the sender of the message)
- Integrity - the file has not been changed/damaged intentionally or unintentionally,
- Non-repudiation - the author can not claim that he/she did not sign the electronic document
- may contain a time stamp that shows the date and time the document was signed.

Possible problems:

- electronic signature verification after a long time since its creation (e.g. after expiration date of certificates)
- long-term archiving of electronically signed documents

[5]

Assignments

- Provide students with basic information about the secure access to the data.
- Clarify the importance of analyzing data security, diversity of manifestations of malware.
- To characterize the diversity of legislative legal restrictions.

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Resources:

1. *Záplatování bezpečnostních děr* [online]. 2012-10-17. [cit. 2013-12-27]. Dostupné z: *http://viry.cz/?s=Bezpečnost+dat*
2. KRAUS, Josef. *Nejlepší program pro zabezpečení přístupu do počítače [online]. 2012-06-10.* [cit. 2013-12-18]. Dostupné z: http:// www.zive.cz/clanky/nejlepsi-program-pro-zabezpeceni-pristupu-do-pocitace/sc-3-a-164090/default.aspx
3. *Počítače - počítačové viry* [online]. [cit. 2013-11-23]. Dostupné z: *www.zskomslavkov.cz/pages/download/.../zapis_pocitacove_viry.ppt*
4. *Policie ČR zdražuje!* 2013-01-11. [cit. 2013-12-23]. Dostupné z: *http:// www.viry.cz/policie-cr-zdrazuje/*
5. ČEKAN, Lukáš. *Podniková informatika přednáška 08* [online]. 2013-04-07. [cit. 2013-12-25]. Studijní materiály z FEI UPCE, obor Informační technologie. Dostupné z: http://fei.pepiczech.cz/?p=136
6. *Pozor na to, co instalujete!* [online]. 2013-04-07.[cit. 2013-12-25]. Dostupné z: *http://viry.cz/?s=Bezpečnost+dat*