CSCI 1800 Cybersecurity and International Relations

Attacks on Hardware & Software

John E. Savage

Brown University

Outline

- State of malicious software, i.e. malware
- Types of cyber attacks
- Computer viruses
- NotPetya – most devastating cyberattack
- Phishing and browser attacks.
- SQL injection attacks

General Observation

There are only two types of companies: those that know they have been compromised and those that don't know!

Dmitri Alperovitch

McAfee, 2011

(Now at Crowdstrike)

The Cost of Cybercrime

Breaches & Intellectual Property (IP) Loss

- In 2018 Ponemon Institute study†
  - Average cost a breach to an org. of was $3.86 M
  - Average cost per lost or stolen record $148
  - Average of 197 days needed to discover a breach, often by outsiders, and 69 days to contain it.
  - Causes: Criminals (48%), Glitches (25%), Error (27%)

* https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

† https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

2019 – Cyber Attacks Changing*

- Intellectual property theft remains expensive
- Industrial controls are now under assault!
- Data altered to breed distrust!
- Human layer attacked more often
  - Weakest link in cyber defense
  - Ransomware, phishing, & social engineering rising
- Merck lost $1.3B due to 2017 NotPetya† attack. Insurance cos. won't pay – It's an "act of war!"

* https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

† https://www.inquirer.com/wires/bloomberg/merck-cyberattack-20191203.html

2019 – Cyberspace Is Changing*

- Supply chains now under attack!
  - 3rd & 4th-party supply chain partners attacked!
- New regulations
  - GDPR - General Data Protection Regulation 5/25/19
    - Fines up to €20 M or 4% of annual global revenues
    - French data regulator has already issued fine of €50 M!
  - California Consumer Privacy Act (CCPA) now in force
    - Fines will be $7,500 per violation
- 100% companies rely on Internet – 25% 10 yrs ago

* https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

† https://www.inquirer.com/wires/bloomberg/merck-cyberattack-20191203.html

Types of Cyberattack

Types of Cyberattacks

- Logic bomb
- Computer virus
- Computer worm
- Trojan
- Email phishing and spear phishing
- Browser attacks via active media
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- SQL injection
- Malware-free intrusion

Insider Attacks

- Insider (programmer) can leave backdoors providing unauthorized access:
  - Backdoor typically has secret login id and password.
  - Backdoors may have been innocent, e.g. for maintenance
- A backdoor now often inserted by malware (Trojan)
  - A buffer overflow often used to inject malware code.
  - It occurs when more entries written into an array than expected but did not prevent!

Logic Bombs

- A logic bomb is malware that is activated when a logical condition is met.
  - Soviets sought to steal Western technology in 70s and 80s. CIA inserted logic bomb in pipeline pumps.
  - In ‘82 “bomb” reportedly led to biggest non-nuclear explosion ever seen in Siberian natural gas pipeline
  - In 2008 logic bomb found in Fannie Mae network software. It was discovered 3 months before it was to erase memory on ~4,000 Fannie Mae servers!

Defending Against Insiders

- Avoid single points of failure.
  - Have multiple programmers study critical code
- Limit authority & permissions
  - Practice principle of least privilege, just enough to do the job
  - Require need-to-know
  - Require approval from two individuals to activate critical functions
- Critical systems require good physical security.
- Check for anomalous employee behavior.
- Control the installation of software.
  - Only allow software on a “whitelist” to be installed
  - Keep all software up to date
  - Segment systems, protect each subsystem – defense in depth

Defending with Digital Signatures

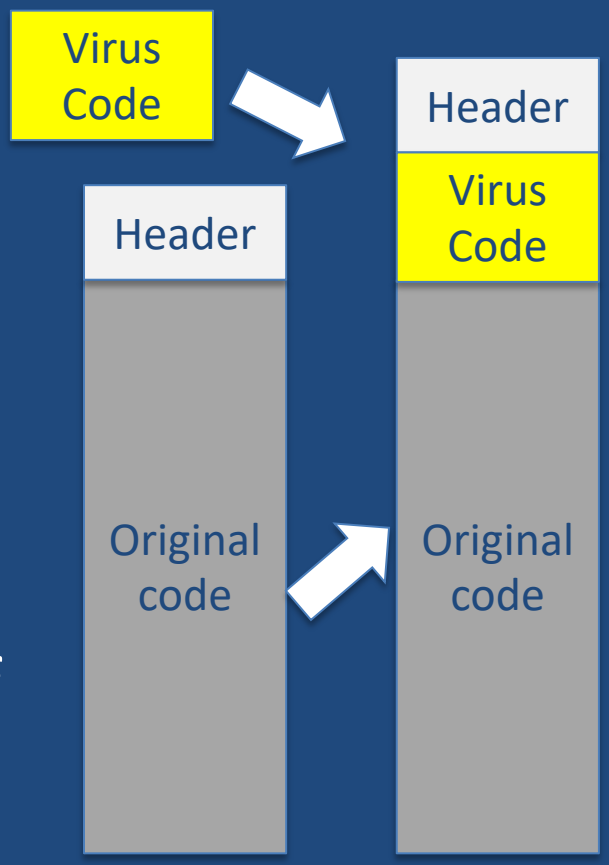
- A digital signature is a hash* of a string (code).
  - Example: Replace characters with their 8-bit codes
    - XOR the bits - e.g. 01011001 $\oplus$ 11100001 = 10111001
  - Hash functions are very hard to invert
  - Code and its hash are supplied together
- Signatures can protect against malware:
  - Compute hash locally & compare to vendor's
  - If they differ, don't run the code – bug detected!

* A hash function produces a compressed string from its input string.

Computer Viruses

Computer Viruses

- A virus is software that inserts itself into a program P that, when run, replicates itself. It infects another computer only when P is run!
- Types of viruses
  - File virus – resides in a file
  - Macro virus – e.g. an Excel macro
  - (Disk) Boot sector virus – read when disk is inserted into drive and run
- A virus can be put into any type of executable code.



Old Example of a Virus

- Mellissa – emerged in 1999
  - First virus to spread itself via mass emailing. Infected Microsoft Word 97 & Word 2000.
  - Gave access to 80 pornographic sites.
  - Created an overload that shut down email systems.
  - It mailed copies to 40 or 50 addresses in victim's address book when infected document was opened

Defending Against Malware

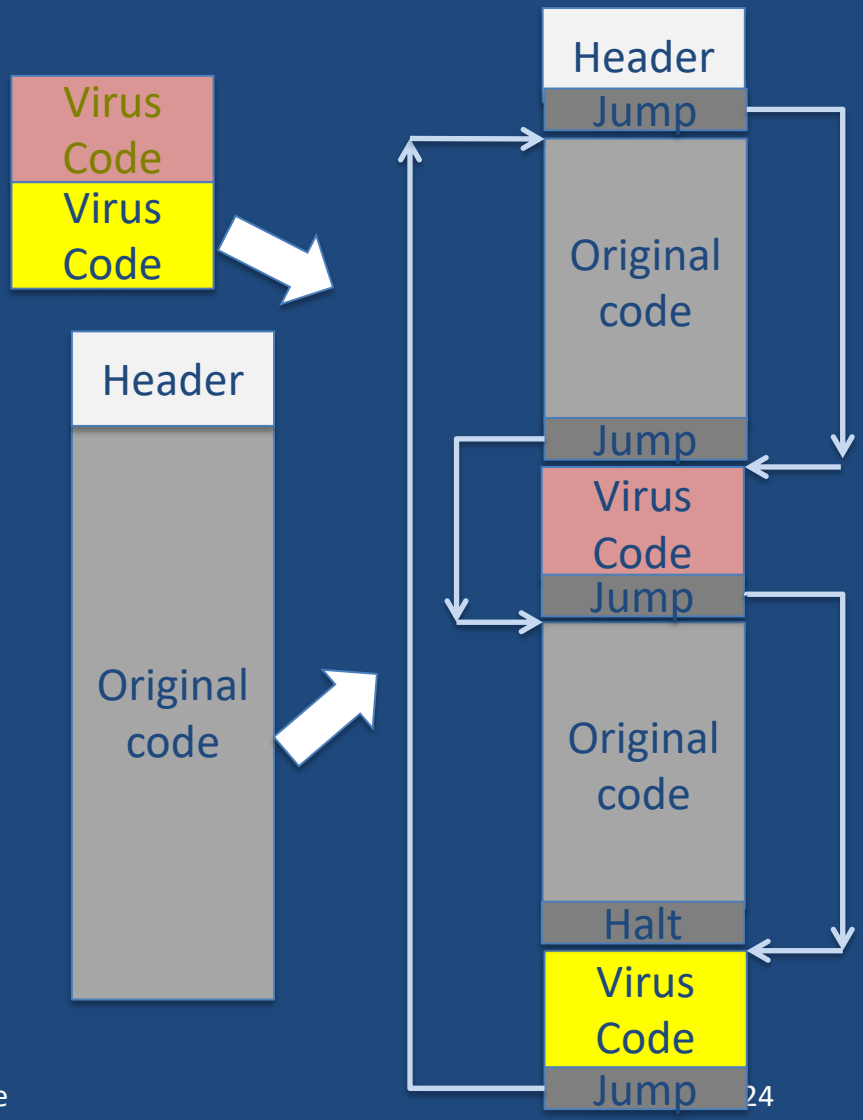
- Malware has signatures, character strings that distinguish malware from code.
- Antivirus (AV) software:
  - Looks for virus signatures – fails if virus is new/morphed
  - Heuristic – makes approximate match of signatures
  - Sandbox – a program is run in a virtual machine to reveal suspicious behavior
    - But, some malware can tell it is in sandbox and not turn on
- AV software will remove or quarantine some viruses

Polymorphic Viruses

- Virus contains malware as well as encryption and decryption code
- On activation, malware is decrypted & executed
- Before propagating, malware re-encrypted with new key
- Can be discovered by scanning for decryption engine or by running code in sandbox and scanning decrypted code

Metamorphic Virus Injection

- Viruses can morph or change shape.
- Injected deep into code using jumps
- Makes it harder to find!
- It runs before execution of infected program.



Worms and NotPetya

Trojans and Worms

- Over time malware has become very sophisticated.
- Trojan horse –backdoor built into product
  - In 2008 Mocmex virus was discovered in Chinese-made digital photo frame. When connected to Windows it started transmitting passwords to Chinese site.
- Worm – self-propagating malware - exploits OS bugs
  - Morris worm (1988). Not malicious but overwhelmed about 10% of computers on Internet. Cost ~$10million.
  - Robert Morris convicted under new 1986 Computer Fraud & Abuse Act (CFAA). Now MIT faculty member.

NotPetya Ransomware

- 2017 – ransomware NotPetya embedded in software needed to file taxes in Ukraine.
- It propagated around the world rapidly.
- Most destructive cyber attack ever, $10Billion*
  - It affected Ukrainian organizations, WPP, Merck, Maersk, Rosneft, British National Health Service, etc
- It used an NSA exploit, Eternal Blue, that compromised Microsoft's Server Message Block

* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Phishing and Browser Attacks

Phishing Attacks

- A form of social engineering – method to persuade humans to give secret data; via email, texting, etc.
  - Goal: get users to click a link or visit phony website
  - Attackers masquerade as a trustworthy source, e.g.
    - Federal employees phished before international meeting
    - Snow removal emails sent just before storm arrival
- At times URLs are slight misspellings of real URLs
- Vishing is phishing via telephone
  - Kevin Mitnick was famous for vishing
  - He is now a security consultant!

Actual Phishing Email Sent to Me!

Savage, John <john_savage@brown.edu>

CSCI 1800: OCRA Reserve Approval Required

Brown University Library <ocra@dl.lib.brown.edu> Sun, Jan 29, 2012 at 2:00 PM
To: jes@cs.brown.edu

Greetings,

Timothy Dylan Peacock has started the process of reserving books for CSCI 1800 (Cybersecurity and International Relations). As the instructor of record, your approval is required before any further action is taken.

The following books have been requested:

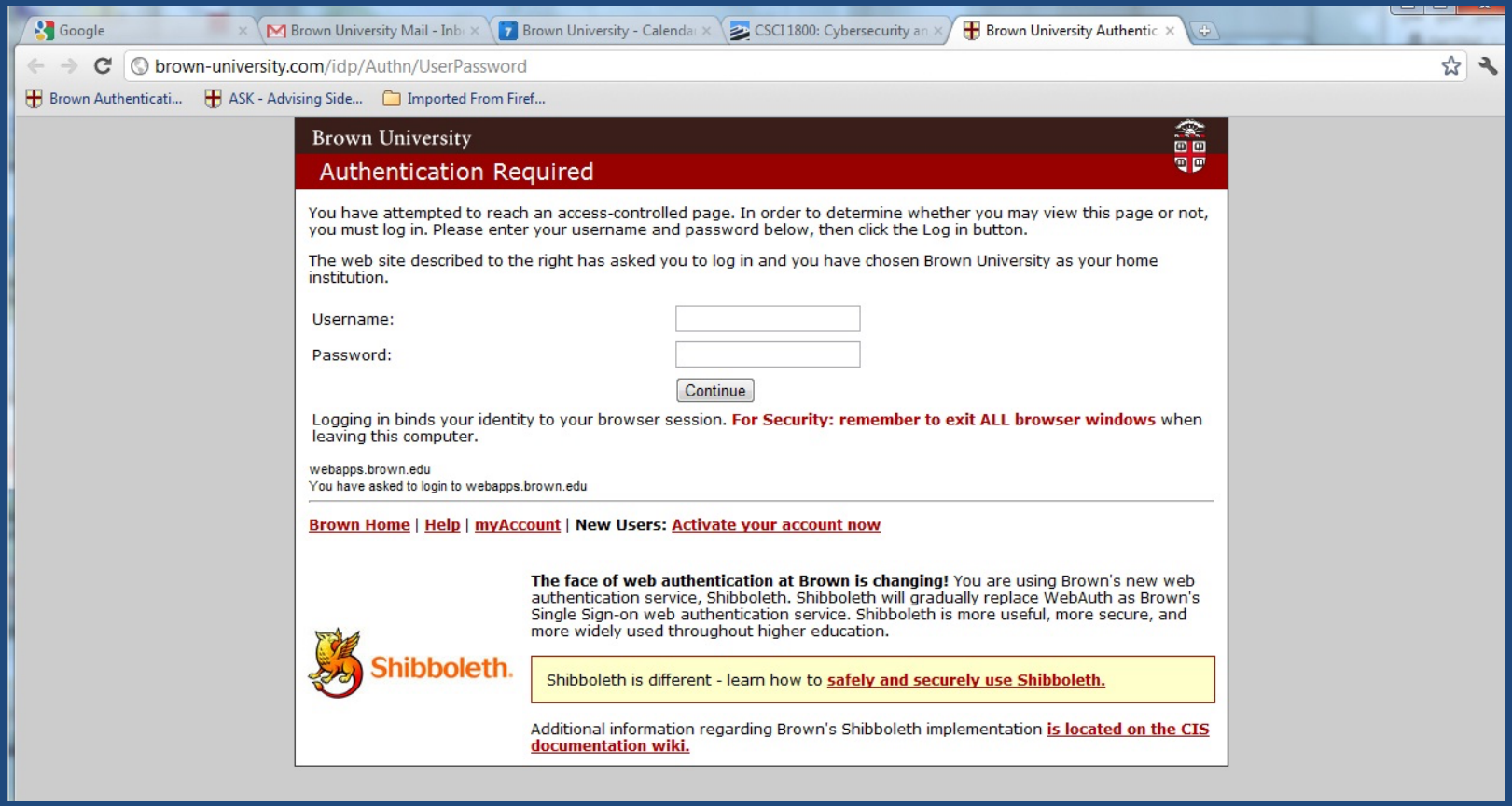
1. Introduction to Computer Security, Michael T. Goodrich and Roberto Tamassia, Addison-Wesley, 2011, ISBN 0321512944

Please log in to review the request.

Sincerely,
The Brown University Library Staff

It Looks Real

- The link took me to http://brown-university.com/idp/Authn/UserPassword



But I’m Embarrassed by the Response

Hello

This site was constructed to demonstrate the effectiveness of spear-phishing attacks against users, even knowledgeable ones.

Please refrain from "warning" people about the link: it reduces the overall effectiveness of the test.

Your password has not been recorded as a part of this experiment.

For more information, contact Tim Peacock or Neal Poole.

HTML for Email Reveals the Trap

```
Return-Path: <nbpoole@cs.brown.edu>
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on
        sourpatch.cs.brown.edu
X-Spam-Level: *
X-Spam-Status: No, score=1.7 required=5.0 tests=HTML_MESSAGE,MIME_HTML_ONLY
        shortcircuit=no autolearn=disabled version=3.2.5
X-Original-To: jes@cs.brown.edu
Delivered-To: jes@cs.brown.edu
Received: from cslab2f.cs.brown.edu (cslab2f.cs.brown.edu [10.116.72.149])
        by sourpatch.cs.brown.edu (Postfix) with ESMTP id 4BA6E7A8078
        for <jes@cs.brown.edu>; Sun, 29 Jan 2012 14:00:17 -0500 (EST)
Received: by cslab2f.cs.brown.edu (Postfix, from userid 33865)
        id 413C2120107; Sun, 29 Jan 2012 14:00:17 -0500 (EST)
To: jes@cs.brown.edu
Subject: CSCI 1800: OCRA Reserve Approval Required
X-PHP-Originating-Script: 33865:jes-email.php
MIME-Version: 1.0
Content-type: text/html; charset=iso-8859-1
From: Brown University Library <ocra@dl.lib.brown.edu>
X-README: This is a phishing email designed for CSCI 1800. If you are reading this header, congrats on (hopefully) not falling for it.
Message-Id: <20120129190017.413C2120107@cslab2f.cs.brown.edu>
Date: Sun, 29 Jan 2012 14:00:17 -0500 (EST)

<html>
<body>
<p>Greetings,</p>

<p>Timothy Dylan Peacock has started the process of reserving books for CSCI 1800 (Cybersecurity and International Relations).
As the instructor of record, your approval is required before any further action is taken.</p>

<p>The following books have been requested:</p>
<ol>
   <li><u>Introduction to Computer Security</u>, Michael T. Goodrich and Roberto Tamassia, Addison-Wesley, 2011, ISBN 0321512944</li>
</ol>

<p>Please <a href="http://brown-university.com/idp/Authn/UserPassword">log in</a> to review the request.</p>

<p>Sincerely,<br />
The Brown University Library Staff</p>
</body>
</html>
```

Browser Attacks

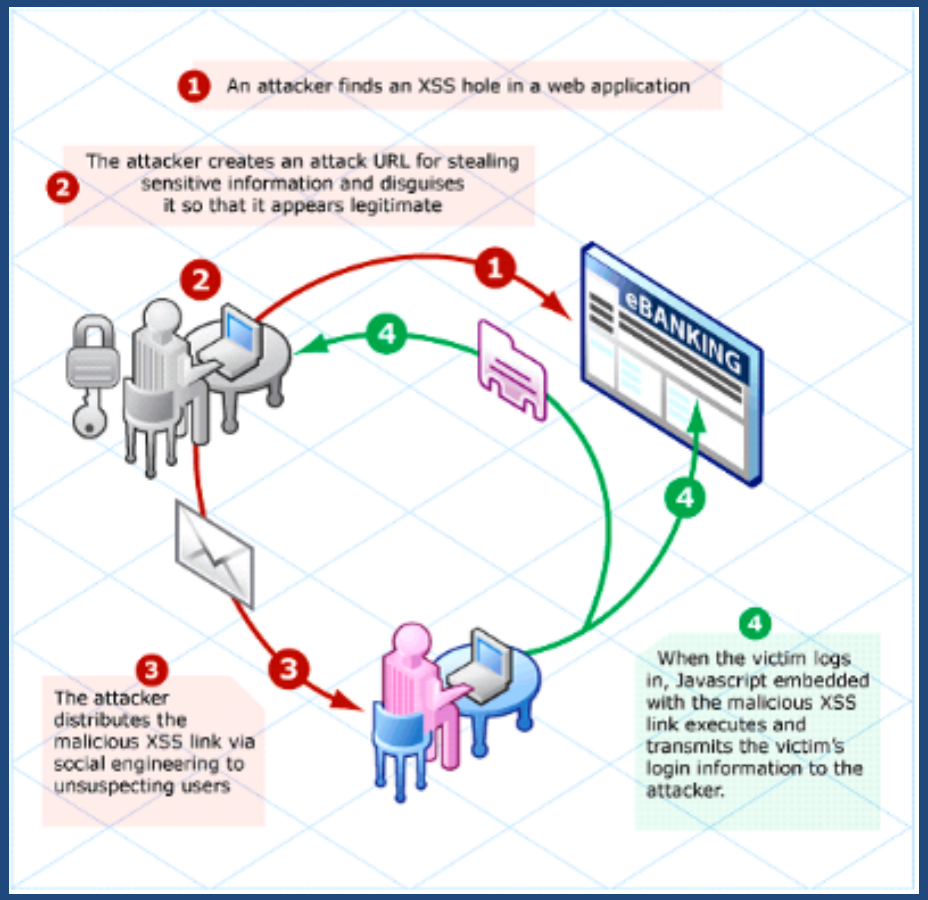
- Cookies are small files put on client by server
  - They retain client state on client site between visits
  - They are unprotected but may have confidential info, e.g. banking login information
  - Cookies can be used without authorization.
  - Third-party cookies may let advertisers track users.
    - E. g. Are you surprised by the ads you are delivered?
- An attacker can hijack a browser session by "sniffing" a cookie shared by client and a server

Attacks via Web Media Content

- Web media types: HTML, text, PDF files, Word, images
- A browser determines file type from suffix, e.g. html, txt, pdf, doc, jpg, & selects an interpreter to run on the file.
  - If the file contains malicious code, it may exploit a flaw in the interpreter and take control of the computer.
- If an html file has an attachment, it may contain code. If you click on it, you will run the code.
  - This could give attacker control of your machine!
  - This is a malware-free intrusion.
- Don't let others run their software on your machine!

Cross-Site Scripting (XSS)

- In XSS a malicious "script" is placed on a trusted site. Users visit. They get infected!
- XSS top web attack vector in 2017, 31% of all web attacks.
- Attacker takes control of a user's computer.



Defending Against XSS

- XSS is a client-side vulnerability. Occurs when server did not prevent users from inserting code
  - Quotes and brackets <, > may be used to specify scripts to a database on server.
- Some browsers prevent XSS by stripping such chars. But even that can be defeated.
- Browsers often warn users that html contains scripts and ask if scripts are allowed to be run.

Cross-Site Request Forgery (CSRF)

- This is an extension of XSS:
  - Attacker does an XSS that causes user's browser to contact a trusted third party, e.g. a bank, and execute a command.
- Example:
  - Eve visits Alice's website which returns this html code:

    Hello Alice. Look here:

    <img src="http://bank.boston.com/withdraw?account=Alice&amount=1000&for=Eve">
  - This looks like a request to display an image (<img src = …) but instead it contacts Eve's bank using her cookie and authorizes a transfer of $1,000 to Alice's account.
  - Alice has tricked Eve with a forged request!

Top 10 Web Vulnerabilities* (OWASP)

1. Injection, e.g. SQL injection
2. Broken Authentication, e.g. weak passwords
3. Sensitive Data Exposure, e.g. weak data protection
4. XML External Entities (XXE), e.g. malicious use of XML
5. Broken Access Control, e.g. bypass authorization step
6. Security Misconfigurations, e.g. segmentation helps
7. Cross-Site Scripting, e.g. trick users to click on link
8. Insecure Deserialization, e.g. too hard to explain
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

* https://sectigostore.com/blog/what-is-owasp-what-are-the-owasp-top-10-vulnerabilities/

SQL Injection Attacks

SQL Database Queries

- Structured Query Language (SQL) used to access relational databases. Data is stored in tables.

id	title	author	body
1	Computers	John	Message1
2	Databases	Joe	Message2
3	Technology	Jane	Message3
4	Security	Julia	Message4

- This is code to select all rows in table where the id has value 2 (here * means “all”):
  - SELECT * FROM table WHERE id = 2

id	title	author	body
2	Databases	Joe	Message2

  - SELECT author FROM table WHERE title = Security
    - Julia

SQL Injection Attack in Words

- A website designer may expect a user to provide text as input.
- If the designer doesn't check that the user supplied just text, the user can provide commands as well as text.
- When the user input is given to a database management system (DBM), the commands will be executed, taking action not expected by the designer.

SQL Injection Attack Illustrated

- $title = ‘Security’;
  - Here is a typical command executed by server:
  - exec_sql(‘SELECT author FROM record_table WHERE title = $title’); No problem when $title = ‘Security’;
- If $title = ‘Security; DROP TABLE record_table’;
  - exec_sql(‘SELECT author FROM record_table WHERE title = $title’);

After the SELECT command is run, the DROP TABLE command is run and TABLE is erased. VERY BAD!

Outline

- State of malicious software, i.e. malware
- Types of cyber attacks
- Computer viruses
- NotPetya – most devastating cyberattack
- Phishing and browser attacks.
- SQL injection attacks

Guest Speaker on Wednesday

- Role of Intelligence and Information Sharing
  - Mike Steinmetz, College Hill Ventures
  - Former RI Cyber Security Officer
  - Navy pilot
  - 20 Years with Department of Defense
  - Worked for NSA and Cyber Command
- Mike will run a simulation to demonstrate how to respond to a cyber threat