CSC 482/582: Computer Security

Threats, Attacks, and Vulnerabilities
Topics

1. Threats
2. Cybercrimes
3. Attacks, Attack Surface, and Exploits
4. Malware
5. Vulnerabilities
6. Mitigations and Patches
Definitions

**Threats** are people who are able to take advantage of security vulnerabilities to attack systems.
- Vandals, hacktivists, criminals, spies, disgruntled employees, etc.

**Vulnerabilities** are weaknesses in a system that allow a threat to obtain access to information assets in violation of a system’s security policy.

(2719662) Vulnerabilities in Gadgets Could Allow Remote Code Execution

**Attacks** are actions taken by threats to obtain assets from systems in violation of the security policy.
Who are the Threats?

Hacktivists  Vandals  Criminals

Spies
Hacktivists

Hacktivists attack systems for political goals.

- Deface websites to spread their message (defacement of avg.com shown)
- Take down sites in retribution for actions.
[!] Struck by 1337

Google Malaysia STAMPED by PAKISTANI LEETS

We are TeaM MADLEETS

H4x0r HuSY - KhantastiC HaXor - H4x0rL1f3 - Inveetu8 - Shadow008 - r00x - Don - MindCracker - Dr.Z0mbie - phpBuGz - MaD GirL
MaDCoDe - Sn1p3r_GS - DeXter - Neo Haxor - Darksniper - Pain006 - b0x - R3DL0F - Sahrawi - 3thiaah00b - Hme17 - MakMan - Sniffer - AL MaX HaCkEr - Ch3m0by1

-----------------------------
www.MaDLeeTs.com
| LeeTHaXor@Y7mail.com |
-----------------------------

Pakistan Zindabad
Cybercriminals

Focus on monetizing information via:

- Identity theft (phishing)
- Credit card or bank account fraud (phishing)
- Extortion (via ransomware or DDoS)
- Clickjacking
- Fraud (auction fraud, 419 scams, etc.)

Specialists who sell services to other criminals

- Distribute malware
- Rent botnet computing services
Cyberspies

Threats that work for a nation state or corp:

- Obtain classified information
- Install backdoors for later access
- Distract enemies from other operations
- Destroy physical devices (Stuxnet)

Terms: Cyberespionage and cyberwarfare
Insider Problem

**Insiders** are threats who are members of the organization that they are attacking.

Insiders are dangerous because they:

- Are inside the security perimeter, so cannot be blocked by perimeter defenses like firewalls and locked doors.
- Have some level of legitimate access to systems.
- May have physical access to systems and information.
A **cybercrime** is a crime that uses a computer to commit a crime or that targets a computer in the commission of the crime.

Examples of cybercrime include:

- Spam
- Phishing
- Fraud
- Harassment (cyberstalking, cyberbullying)
Spam

Spam is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.

- Types: E-mail, IM, wiki, comment spam.

Used to deliver other attacks

- Malware
- Phishing and other fraud enticements
Over 90% of e-mail is spam!

<table>
<thead>
<tr>
<th>Subject</th>
<th>Sender</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>check this out man...</td>
<td>Nelda Romano</td>
<td>Thursday 14:59:37</td>
</tr>
<tr>
<td>Help me!</td>
<td>Osvaldo MANNING</td>
<td>Thursday 12:47:59</td>
</tr>
<tr>
<td>Have Arthritis pains? There is help for you.</td>
<td>Orsa</td>
<td>Thursday 03:45:36</td>
</tr>
<tr>
<td>down on her, and</td>
<td>Reginald Stubbs</td>
<td>Wednesday 06:02:05</td>
</tr>
<tr>
<td>natural enlargement</td>
<td>diane george</td>
<td>Tuesday 16:37:15</td>
</tr>
<tr>
<td>No Subject</td>
<td>fabian dickhaut</td>
<td>Monday 10:38:59</td>
</tr>
<tr>
<td>only Youngest have Shocking sexuality other</td>
<td>Kristie Sapp</td>
<td>Monday 01:07:32</td>
</tr>
<tr>
<td>Reduces stress</td>
<td>frankie kim</td>
<td>06.02.2005 16:27</td>
</tr>
<tr>
<td>PERSONAL</td>
<td>esno12005</td>
<td>06.02.2005 04:56</td>
</tr>
<tr>
<td>We need to render the delight of having the finest</td>
<td>Clotilda Gadnunq</td>
<td>06.02.2005 02:10</td>
</tr>
<tr>
<td>Find more savings online</td>
<td>kennith draper</td>
<td>05.02.2005 22:30</td>
</tr>
<tr>
<td>faster cheaper meds</td>
<td>Lidia White</td>
<td>05.02.2005 16:37</td>
</tr>
<tr>
<td>Breaking News</td>
<td>Dee H. Edwardsd</td>
<td>05.02.2005 14:40</td>
</tr>
<tr>
<td>We have your wanted meds at low prices only.</td>
<td>lucien hyatt</td>
<td>04.02.2005 06:59</td>
</tr>
<tr>
<td>100% zum einladen_1679438</td>
<td>Isel Rios</td>
<td>03.02.2005 03:34</td>
</tr>
<tr>
<td>Enjoy your wanted meds.</td>
<td>tracey uliano</td>
<td>03.02.2005 02:28</td>
</tr>
<tr>
<td>Confirm Your Washington Mutual Online Banking</td>
<td>Washington Mutual On</td>
<td>02.02.2005 22:03</td>
</tr>
<tr>
<td>out P1NNACCLE SYSTEM, MACR00MEDIA, SYMANTEEC, PC GAMES, ...</td>
<td>Valerie Ileen</td>
<td>02.02.2005 19:11</td>
</tr>
<tr>
<td>Finished</td>
<td>Cecilia Fuller</td>
<td>02.02.2005 05:57</td>
</tr>
<tr>
<td>You can save more thru ordering meds on our site.</td>
<td>mel sevick</td>
<td>02.02.2005 01:21</td>
</tr>
<tr>
<td>The most insane action</td>
<td>Katrina Souza</td>
<td>31.01.2005 08:19</td>
</tr>
<tr>
<td>You don’t have to be fat Noel</td>
<td>Kristin</td>
<td>28.01.2005 03:22</td>
</tr>
</tbody>
</table>
Dear Sky Bank customer,

We recently reviewed your account and suspect that your Sky Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Sky Financial network is our primary concern. Therefore, as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your Sky Internet Banking account. In case you are not enrolled for Internet Banking, you will have to fill in all the required information, including your name and your account number.

2. Review your account history for any unauthorized withdrawals or deposits, and check your account profile to make sure no changes have been made. If any unauthorized activity has taken place on your account, report this to Sky Financial Group staff immediately.

To get started, please click the link below:

[SIGN-ON]

©2005 Sky Bank Financial Group. All rights reserved.
Phishing Site

Sky Online Banking Users - Microsoft Internet Explorer


Sky Connect Online Banking Services
Online Banking

Sky Online Banking Users, please enter your User ID and Password below.

User ID: 
Password: 
Sign-On

Fraud Alert! Help Protect Your Accounts. Remember, always access Sky Online Banking by going to www.skyfi.com directly and not through links from other sites or sent in an e-mail message. NEVER click on a link in an e-mail message, open an attachment, or reply to any e-mail message that warns you that an account of yours will be closed unless you confirm your billing information or asks you to verify personal information to activate a feature. If you think your Sky Bank account information has been compromised, contact Sky at 1-866-SKY-BANK (1-866-759-2265). Report any suspicious activity to the FTC and send the actual e-mail message to uce@ftc.gov. Sky does not contact clients via e-mail, phone or mail to request or verify security information about passwords or PINs. In addition, for your protection, when you call our financial center or the Sky Client Call Center, our representatives use special "know your caller" procedures to prevent unauthorized distribution of your personal account information. Find out more about how to protect yourself from identity theft. Do you need help signing on? Click here for instructions. If you need additional assistance, send e-mail to personal@skyfi.com or call our Client Service Center at 1-866-SKY-BANK (1-866-759-2265) Monday through Friday 7 a.m. to 7 p.m. or Saturday 8:30 a.m. to 1:00 p.m.

If you need to sign up for Personal Online Banking, you can apply for it by filling out and sending in this personal online banking application form.
Cybercrime Organization

Sponsors
- Governments, corporations, activist groups, organized crime, individuals.

Cybercrime Boss
- Works for sponsor or may be sponsor himself.
- Plans crime, recruits tech providers and money mules.

Technology Providers
- Deployment providers
- Malware authors
- Botnet masters

Money Mules
A threat model describes which threats exist to a system, their capabilities, resources, motivations, and risk tolerance. Also known as an adversary model.

- Four quadrant model: skill and targeting.
- Resources and capabilities.
- Do you keep enough data about historical incidents to know capabilities and motivations?
Four Quadrant Threat Modeling

Attacker Types and Techniques 2012

Off-the-Shelf tools and techniques
- Motivations:
  - Cyber Crime
  - Vandalism
  - Existing exploit and malware kits
  - Botnet builders
  - Spam and DoS

Sophisticated
- Motivations:
  - Cyber Espionage
  - Cyberwar

Broad

Targeted
- Motivations:
  - Cyber Crime
  - Hactivism
  - Financially motivated targeted hacks
  - DDoS attacks

Motivations:
- Cyber Crime
- Cyber Espionage
- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulnerabilities

IBM X-Force 2012 Trend and Risk Report
Resources

- Skilled personnel
- Money
- Computational power
- Technology
- Infrastructure
Capabilities

Computational
- Can try $X$ keys/second or $X$ passwords/second.

Informational
- Has access to \{past, current, future\} encrypted data.
- Has access to $X$ GB of data.

Access
- Physical access.
- User access: none, authenticated, admin.
- Can read network data.
- Can inject packets into network.
Advanced Persistent Threat

Advanced persistent threat (APT) refers to a group that has the ability to maintain a constant presence inside a target’s network.

- Sophisticated
- Targeted.
- Skilled personnel.
- May be backed with considerable budget.
Threat Information Sources

- Computer Emergency Response Team (CERT)
- Krebs On Security
- SANS Internet Storm Center (ISC)
- Symantec Internet Threat Reports
- ThreatPost

See resources page on class site for more.
Attacks

An **attack** is an action taken by a threat to gain unauthorized access to information or resources or to make unauthorized modifications to information or computing systems.

- Spoofing (pretending to be another entity)
- Packet sniffing (intercepting network traffic)
- Man in the middle (active interception of traffic)
- Injection Attacks (buffer overflows, sql injection, etc.)
- Denial of Service (resource depletion)
- Defacement (vandalism)
- Social Engineering, etc.
How are Digital Attacks Different?

Automation
- Salami Attack from *Office Space*.

Action at a Distance
- Volodya Levin, from St. Petersburg, Russia, stole over $10\text{million} from US Citibank. Arrested in London.

Technique Propagation
- Criminals share attacks rapidly and globally.
A **spoofing** attack is when a threat masquerades as another entity on a telecommunications network. Examples of spoofing include:

- E-mail spoofing
- ARP spoofing (MAC to IP address map spoofing)
- IP address spoofing
- Caller ID spoofing
- GPS spoofing
Packet sniffing is when a program records wired or wireless network packets destined for other hosts.

- Wireless traffic is available to everyone nearby.
- Antennas can extend range to miles.
- Wired traffic is accessible depending on network location.
- If network location unsatisfactory, ARP spoofing can redirect traffic to sniffing machine.

Sniffing used to

- Obtain passwords (ftp, imap, etc.)
- Obtain other confidential information
Man in the Middle

A man-in-the-middle attack is an active eavesdropping attack, in which the attacker connects to both parties and relays messages between them.
Injection Attacks

Injection attacks send code to a program instead of the data it was expected, then exploit a vulnerability in the software to execute the code.

- Buffer overflows inject machine code into a process.
- Cross-site scripting injects JavaScript code into a web page seen by another user.
- SQL injection injects SQL code into a database query run by an application.
Denial of Service

A denial of service (DoS) attack attempts to make computer or network resources unavailable to its intended users.
Social Engineering

Social engineering is the psychological manipulation of people to reveal confidential information or perform actions to violate security policy.
**Attack Surface**

*Attack surface*: the set of ways an application can be attacked.

Used to measure attackability of app.

- The larger the attack surface of a system, the more likely an attacker is to exploit its vulnerabilities and the more damage is likely to result from attack.
- Compare to measuring vulnerability by counting number of reported security bugs.
- Both are useful measures of security, but have very different meanings.
Exploits

An exploit is a technique or tool that takes advantage of a vulnerability to violate an implicit or explicit security policy.

Exploits can be categorized by

1. The type of vulnerability they exploit.
2. Local (runs on vulnerable host) or remote.
3. Result of exploit (elevation of privilege, DoS, spoofing, remote access, etc.)
Exploitation Frameworks
Malware, short for malicious software, is software designed to gain access to confidential information, disrupt computer operations, and/or gain access to private computer systems. Malware can be classified by how it infects systems:

- Trojan Horses
- Viruses
- Worms

Or by what assets it targets:

- Ransomware
- Spyware and adware
- Backdoors
- Rootkits
- Botnets

Malware by categories
How much malware is out there?

New unique samples added to AV-TEST's malware repository (2000-2012)
Trojan Horses
Trojan Horse Examples

- If you double-click the file, iTunes plays it and...
- At the same time the malicious code hidden inside the ID3 tag of the mp3 file executes itself.

XP Antispyware 2009 - Unregistered version

- WARNING! XP Antispyware 2009 has found 28 useless and UNWANTED files on your computer!
- 18 of those items are considered critical privacy compromising content
- 7 of those items are considered medium privacy threats
- 3 of those items are considered to be junk content of low privacy threats
- Personal data at the reach of anyone’s hand
- Internet history records available
- Compromising and adult material stored on your system
- Chat sessions’ logs and personal emails easily reachable

You need to register XP Antispyware 2009 to clean the unwanted files found. Click “Register now” button below to obtain the license key and remove useless or compromising material from your PC.
Viruses

A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other files. This process is called infecting.
A **worm** is a type of malware that spreads itself to other computers.
Ransomware

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Information Stealers

Information stealers target specific types of information, such as passwords, financial credentials, private information, etc.

- Keyloggers (can be hardware too)
- Desktop recorders
- Memory scrapers
Spyware and Adware
Backdoors
Backdoor Example: Dark Comet
Rootkits

- Execution Redirection
- File Hiding
- Process Hiding
- Network Hiding
- Backdoor
Covert Channels

*Covert channels* enable communication using techniques not meant for information exchange.

- Malware could increase CPU usage to 100% to communicate a 1, regular usage is a 0.
- Malware could fill a storage device to 100% to communicate a 1, non-full device is a 0.
- Malware could send 2 packets/second to indicate a 1, 1 packet/second to indicate a 0.
Vulnerabilities can be found in any software:

- **PC**: Office, Adobe Reader, web browsers
- **Server**: Databases, DNS, mail server software, web servers, web applications, etc.
- **Mobile**: Mobile phone OS, mobile applications
- **Embedded**: printers, routers, switches, VoIP phones, cars, medical devices, TVs, etc.
- **Third party software**: Web browser plugins, Ad affiliate network JavaScript include files, Mobile ad libraries
Document Format Vulnerabilities

IBM X-Force 2012 Trend and Risk Report
Web Browser Vulnerabilities

IBM X-Force 2012 Trend and Risk Report
Embedded Vulnerabilities

Wireless Car Hacking Demonstrated in New Video

Security Hole in Samsung Smart TVs Could Allow Remote Spying

The company that made headlines in October for publicizing zero day holes in SCADA products says it has uncovered a remotely exploitable security hole in Samsung Smart TVs. If left unpatched, the vulnerability could allow hackers to make off with owners' social media credentials and even spy on those watching the TV using compatible video cameras and microphones.

In an e-mail exchange with Security Ledger, Malta-based firm said that the previous unknown ("zero day") hole affects Samsung Smart TVs running the latest version of the company's Linux-based firmware. It could allow an attacker the ability to access any file available on the remote device, as well as external devices (such as USB drives) connected to the TV. And, in an Orwellian twist, the hole could be used to access cameras and

There really is no need to present the worst-case scenario, when it comes to the hacking of modern cars, because everybody's familiar with its implications. The more systems are controlled by software, the more vulnerable to "cyber attacks" the vehicle is.
Mitigations

A **mitigation** is a process, technique, tool, or software modification that can prevent or limit exploits against vulnerabilities.

- A password length policy is a process mitigation to protect against password guessing attacks.
- A firewall is a tool mitigation that limits exploits by blocking certain types of network traffic.
- Checking for the lock icon in the location bar of your browser is a technique mitigation for verifying that web connections are encrypted.
A security patch is a software modification designed to prevent or limit a vulnerability. A patch is a type of mitigation.

- Administrator may have to apply manually.
- Some vendors specify certain days to patch, such as “Patch Tuesday,” the 2nd Tuesday of the month when MS releases updates.
- Increasingly software auto updates itself with current patches.
Vulnerability Timeline

- Vulnerability introduced
- Exploit released in the wild
- Vulnerability discovered by the vendor
- Anti-virus signatures released
- Patch released
- Patch deployment completed

Zero day attack
Follow-on attacks
Window of exposure
Zero Day

A **zero day** vulnerability, attack, or exploit is a newly discovered one for which no patch currently exists.

- Once a patch is released, the vulnerability, attack, or exploit is no longer a zero day.

Google’s Project Zero focuses on finding zero day vulnerabilities in open source and commercial software before attackers do.
Vulnerability Markets

Box Score: Vulnerability Pricing

Ballpark pricing of individual exploits, provided by Tripwire's Dwayne Melancon:

- Adobe Reader: $5,000–$30,000
- Adobe Flash: $5,000–$100,000
- Java browser plugins: $5,000–$100,000
- Mac OS X: $20,000–$50,000
- Android: $30,000–$60,000
- Microsoft Word: $50,000–$100,000
- iOS: $100,000–$250,000
- Firefox: $60,000–$150,000
- Safari: $60,000–$150,000
- Microsoft Windows: $60,000–$120,000
Vulnerability Databases

**National Vulnerability Database**

- **Mission and Overview**
  - NVD is the U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g., FISMA).
  - NVD contains content (and associated systems) implementing the Security Content Automation Protocol (SCAP). This enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, SCAP-related software flaws, misconfigurations, product names, and impact metrics.

**OSVDB**

- **78117: Jetty Hash Collision Form Parameter Parsing Remote DoS**
  - Views This Week: 15
  - Views All Time: 597
  - Added to OSVDB: 10 months ago
  - Last Modified: about 1 month ago
  - Modified (since 2008): 5 times
  - Percent Complete: 70%

**Timeline**

- Vendor Informed Date: 2011-10-18
- Disclosure Date: 2011-12-28

**Description**

Jetty contains a flaw that may allow a remote denial of service. The issue is triggered when an attacker sends multiple crafted parameters which trigger hash collisions, and will result in a loss of availability for the program via CPU consumption.

**Classification**

- Location: Remote / Network Access
- Attack Type: Denial of Service
- Impact: Loss of Availability
- Solution: Solution Unknown
- Exploit: Exploit Public
- Disclosure: Uncordinated Disclosure
- OSVDB: Web Related

**Solution**

OSVDB is not aware of a solution for this vulnerability.

**Products**

- Unknown or Incomplete
Time to Attack after Deployment

Jan 1 2005 – Jan 1 2014

https://isc.sans.edu/survivalt ime.html
Key Points

1. Definitions
   - threat, threat model, APT, attack, attack surface, exploit, vulnerability, mitigation, patch, zero day, malware

2. Four Quadrant Threat Model
   - Expertise: off-the-shelf tool users up to sophisticated built your own
   - Focus: broad attack anyone to targeted attacks on high value victims

3. Attack types: spam, phish, spoof, sniff, MITM, DoS

4. Malware types: Trojan, virus, worm

5. Vulnerability lifecycle
   - Introduction, zero-day, patch, window of exposure

6. You can improve the security of a system by
   - Mitigating vulnerabilities
   - Reducing attack surface
References


Released under CC BY-SA 3.0

- This presentation is released under the Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) license

- You are free:
  - to Share — to copy and redistribute the material in any medium
  - to Adapt — to remix, build, and transform upon the material
  - to use part or all of this presentation in your own classes

- Under the following conditions:
  - Attribution — You must attribute the work to James Walden, but cannot do so in a way that suggests that he endorses you or your use of these materials.
  - Share Alike — If you remix, transform, or build upon this material, you must distribute the resulting work under this or a similar open license.

- Details and full text of the license can be found at https://creativecommons.org/licenses/by-nc-sa/3.0/