Looking for undergrad research? Come see me!

http://crypto.stanford.edu/cs155

CS155

Computer Security
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

current state of computer security
MITRE tracks vulnerability disclosures

Cumulative Disclosures

Percentage from Web applications

Source: IBM X-Force, Mar 2011
Data: http://cve.mitre.org/
Vulnerable applications being exploited


The rise of mobile banking Trojans (Kaspersky Security Bulletin 2014)
Introduction

Sample attacks
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

Dan Boneh
Why own machines:

1. IP address and bandwidth stealing

Attacker’s goal: look like a random Internet user

Use the IP address of infected machine or phone 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 and inject ads

Keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (and many like it)

User requests login page

Malware injects Javascript

Bank sends login page needed to log in

When user submits information, also sent to attacker

Similar mechanism used by Zeus botnet
Why own machines:

3. Spread to isolated systems

Example: **Stuxtnet**

Windows infection ⇒

Siemens PCS 7 SCADA control software on Windows ⇒

Siemens device controller on isolated network

More on this later in course
Server-side attacks

• Financial data theft: often credit card numbers
  – Example: Target attack (2013), $\approx 140M$ CC numbers stolen
  – Many similar (smaller) attacks since 2000

• Political motivation:
  – Aurora, Tunisia Facebook (Feb. 2011), GitHub (Mar. 2015)

• Infect visiting users
Example: Mpack

- 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 $\Rightarrow$ Wikileaks
- SysAdmin for city of SF government. Changed passwords, locking out city from router access
- Inside logic bomb took down 2000 UBS servers

Can security technology help?
Introduction

The Marketplace for Vulnerabilities
Marketplace for Vulnerabilities

Option 1: bug bounty programs (many)
- Google Vulnerability Reward Program: up to 100K $
- Microsoft Bounty Program: up to 100K $
- Mozilla Bug Bounty program: 500$ - 3000$
- Pwn2Own competition: 15K $

Option 2:
- ZDI, iDefense: 2K – 25K $
**Marketplace for Vulnerabilities**

**Option 3:** black market

<table>
<thead>
<tr>
<th>Software</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE READER</td>
<td>$5,000–$30,000</td>
</tr>
<tr>
<td>MAC OSX</td>
<td>$20,000–$50,000</td>
</tr>
<tr>
<td>ANDROID</td>
<td>$30,000–$60,000</td>
</tr>
<tr>
<td>FLASH OR JAVA BROWSER PLUG-INS</td>
<td>$40,000–$100,000</td>
</tr>
<tr>
<td>MICROSOFT WORD</td>
<td>$50,000–$100,000</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>$60,000–$120,000</td>
</tr>
<tr>
<td>FIREFOX OR SAFARI</td>
<td>$60,000–$150,000</td>
</tr>
<tr>
<td>CHROME OR INTERNET EXPLORER</td>
<td>$80,000–$200,000</td>
</tr>
<tr>
<td>IOS</td>
<td>$100,000–$250,000</td>
</tr>
</tbody>
</table>

Source: Andy Greenberg  (Forbes, 3/23/2012)
Marketplace for owned machines

Pay-per-install (PPI) services

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

**Source:** Cabalerro 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)
This course

Goals:

• Be aware of exploit techniques

• Learn to defend and avoid common exploits

• Learn to architect secure systems
This course

Part 1: basics  (architecting for security)
• Securing apps, OS, and legacy code  
  Isolation, authentication, and access control

Part 2: Web security  (defending against a web attacker)
• Building robust web sites, understand the browser security model

Part 3: network security  (defending against a network attacker)
• Monitoring and architecting secure networks.

Part 4: securing mobile applications
Don’t try this at home!
Ken Thompson’s clever Trojan