Introduction

Security Analysis & Threat Models

Logistics

- Sessions
  - You can go to any sessions
- Project groups
  - You can switch groups for different projects
- Wait List

Evolving 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

- Advanced Persistent Threats (APT)
- Stuxnet, Flame, Gauss
  - Iranian nuclear infrastructure
  - Lebanese banking information

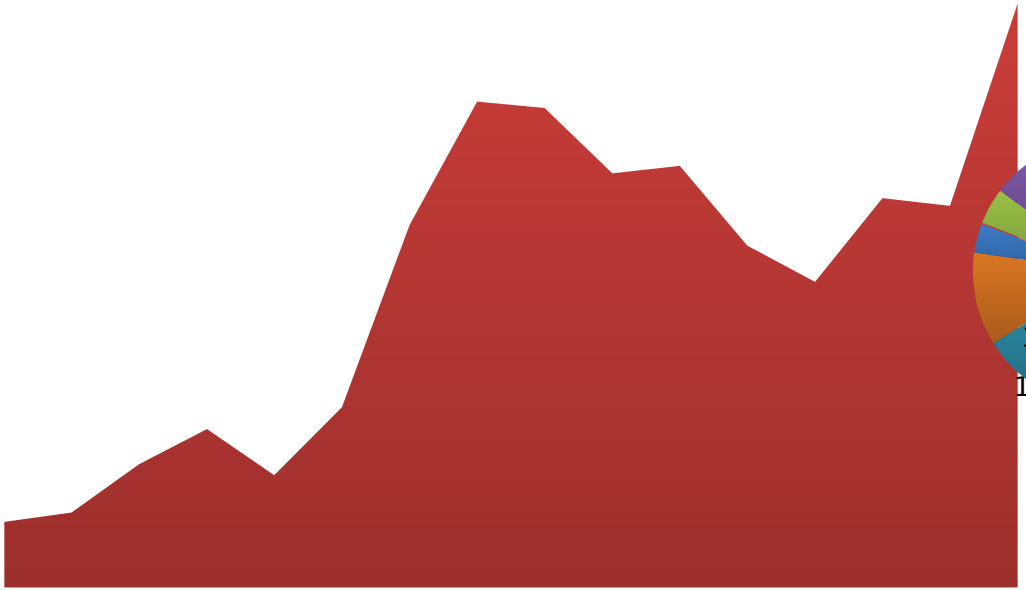
Politically Motivated

Other Motives?

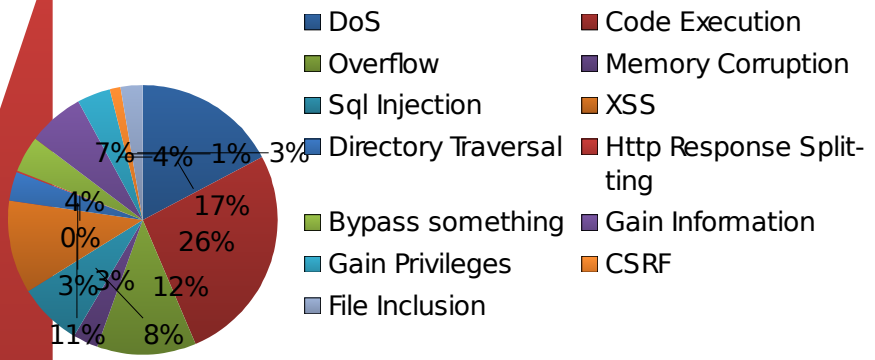
Threats Statistics

MITRE tracks vulnerability disclosures

of Vulnerabilities (CVE IDs)



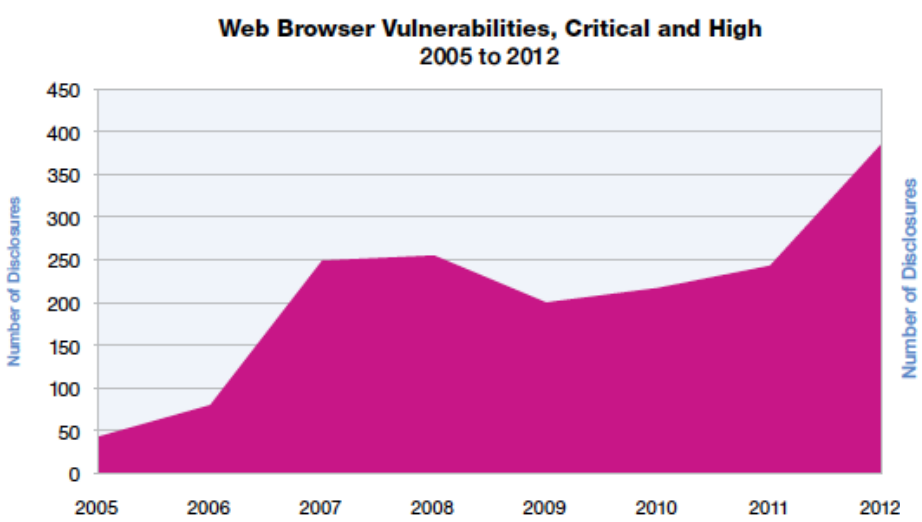
of CVEs by Type

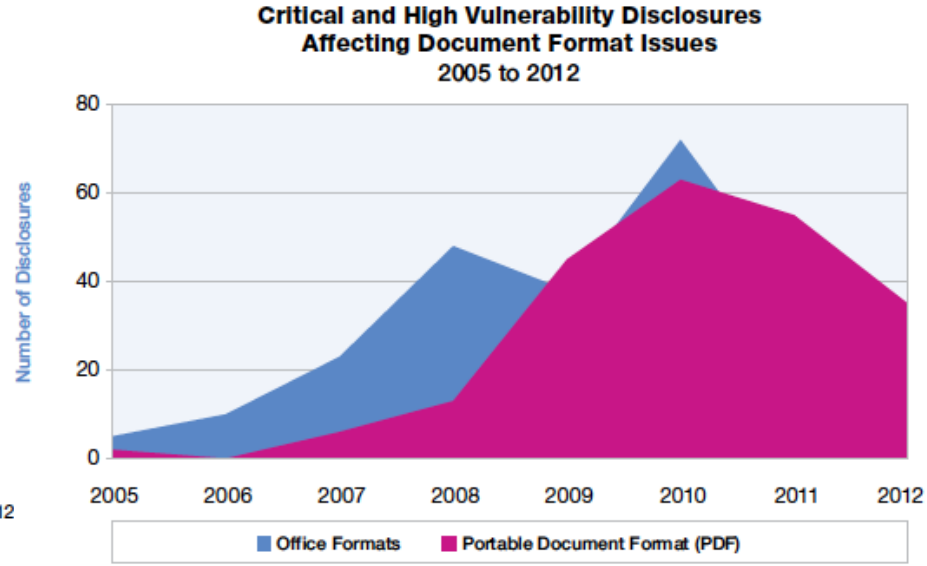


2010

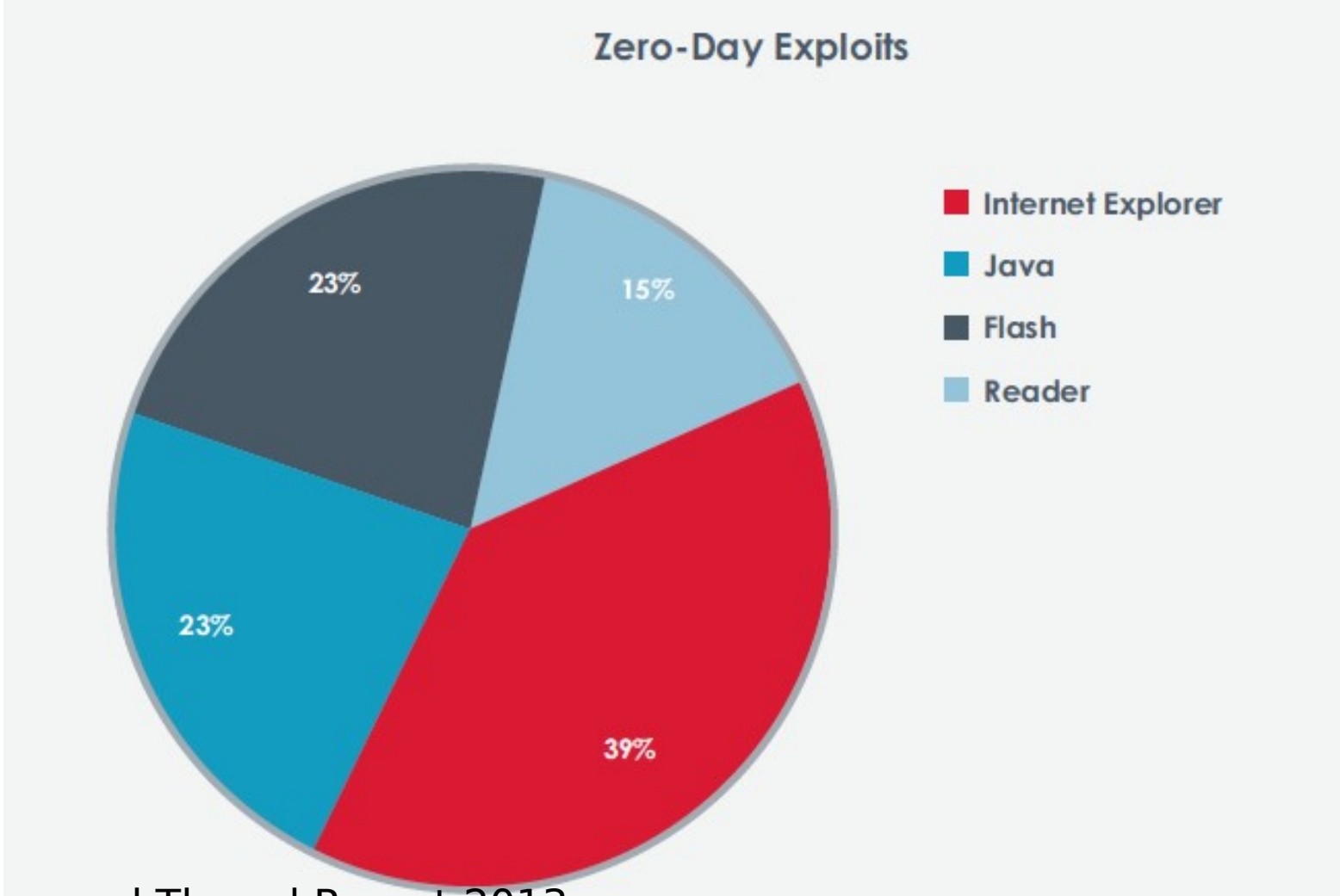
Data: http://www.cvedetails.com/browse-by-date.php

Trends in client-side vulnerabilities

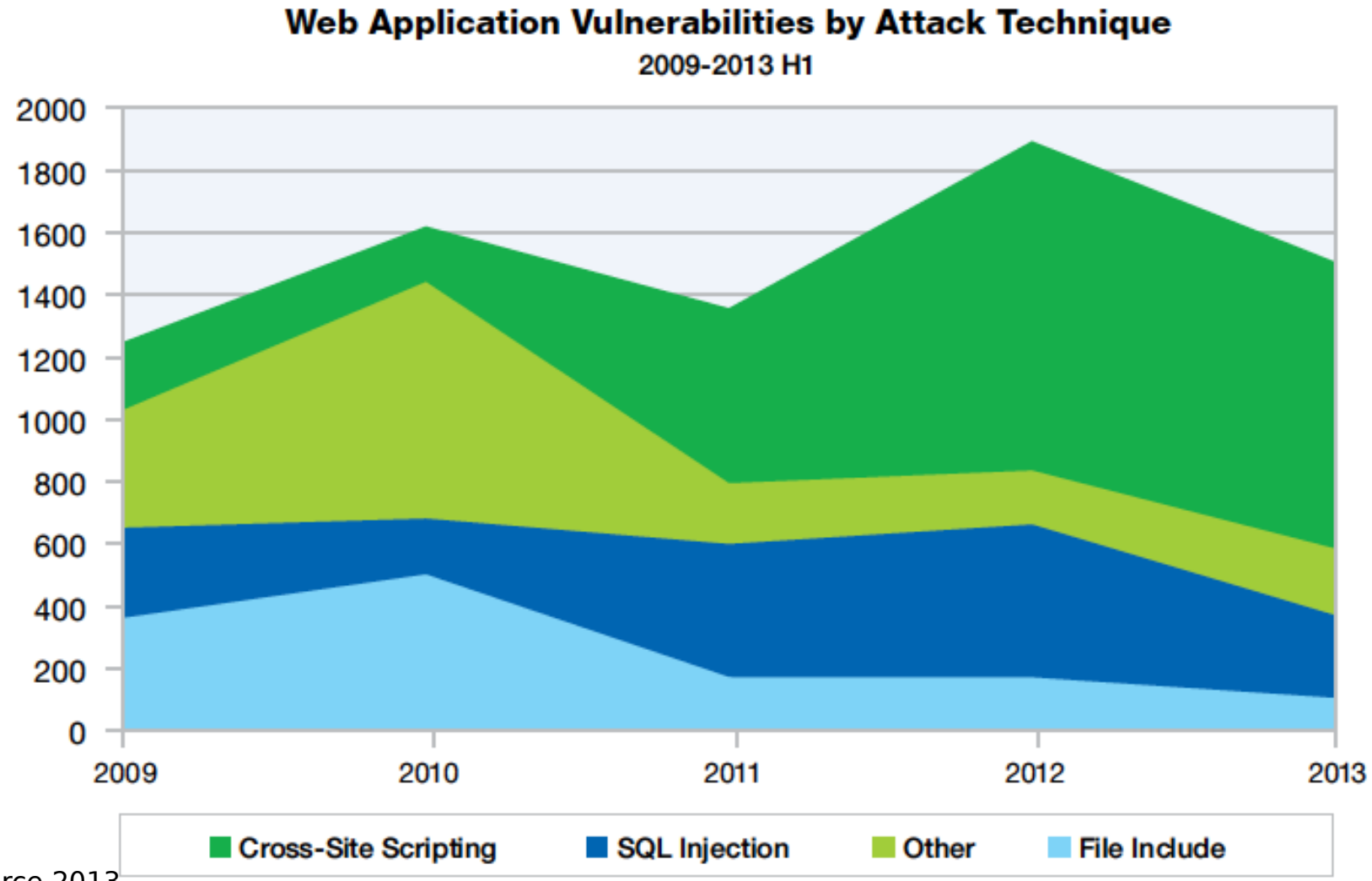




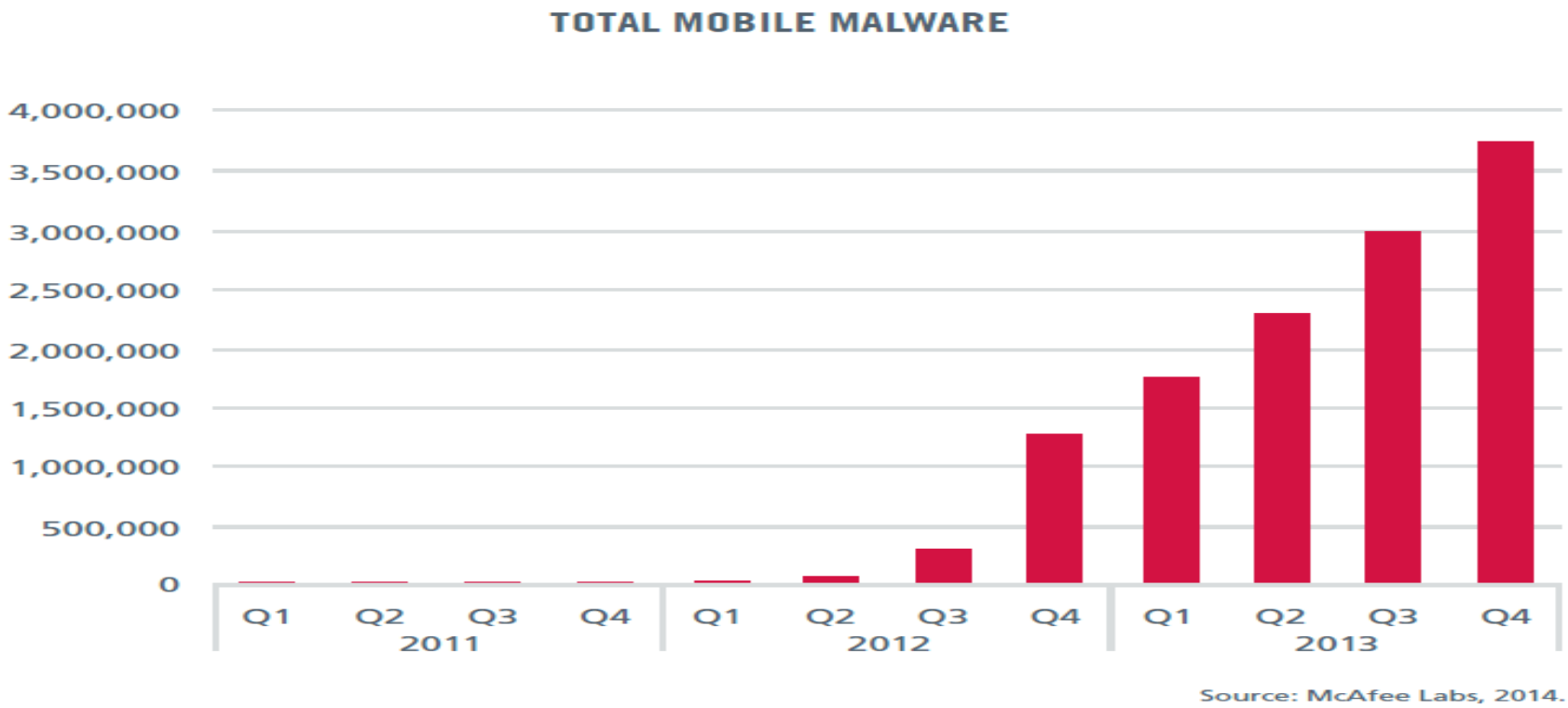
ource: IBM X-Force, Mar 2013



eEye Advanced Thread Report 2013


Web Application Vulnerabilities by Attack Technique
2009-2013 H1
2000
1800
1600
1400
1200
1000
800
600
400
200
0
2009
2010
2011
2012
2013
Cross-Site Scripting
SQL Injection
Other
File Include

Mobile Threats on the Rise



Payloads---Why Attackers Compromise Machines and What Do They Do?

I: IP address and bandwidth stealing

Attacker’s goal: look like a random Internet user

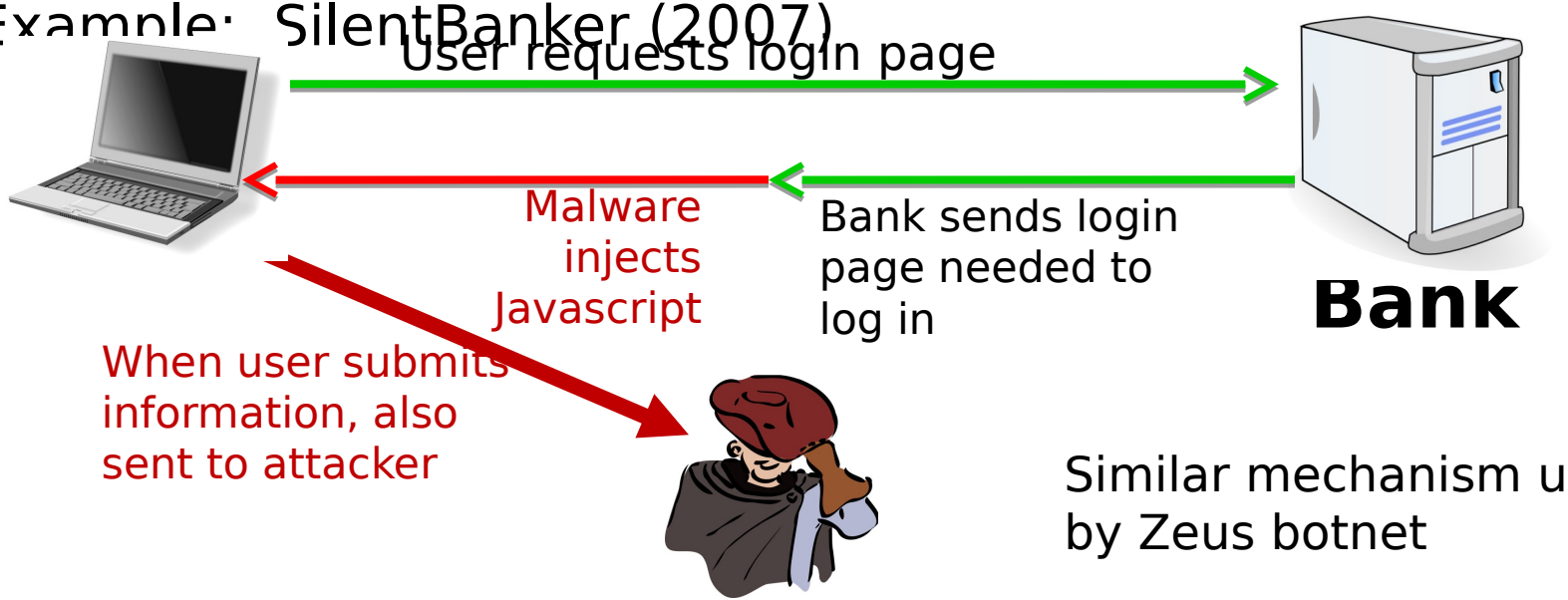
Use the infected machine’s IP address for:

- **Spam** (e.g. the storm botnet)
- **Denial of Service:**
- **Click fraud** (e.g. Clickbot.a)

II: Steal user credentials

keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (2007)



Similar mechanism used by Zeus botnet

III: 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: malicious software installed on servers of a
    single retailer stole 45M credit card (2007)
- Political motivation: The Sony Hack (2014), Aurora, Tunisia Facebook (Feb. 2011)
- Infect visiting users

Insider attacks: example

Hidden trap door in Linux (nov 2003)

- Allows attacker to take over a computer
- Really subtle change (uncovered via CVS logs)

Inserted a line in wait4()

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

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
- Insider logic bomb took down 2000 UBS servers

Monetization

Marketplace for Vulnerabilities

Option 1: bug bounty programs

- Google Vulnerability Reward Program: $100-20,000
- Mozilla Bug Bounty program: 3K$
- Pwn2Own competition: 15K $
- Github, HackerOne …

Option 2:

- ZDI, iDefense: 2K – 25K $

Marketplace for Vulnerabilities

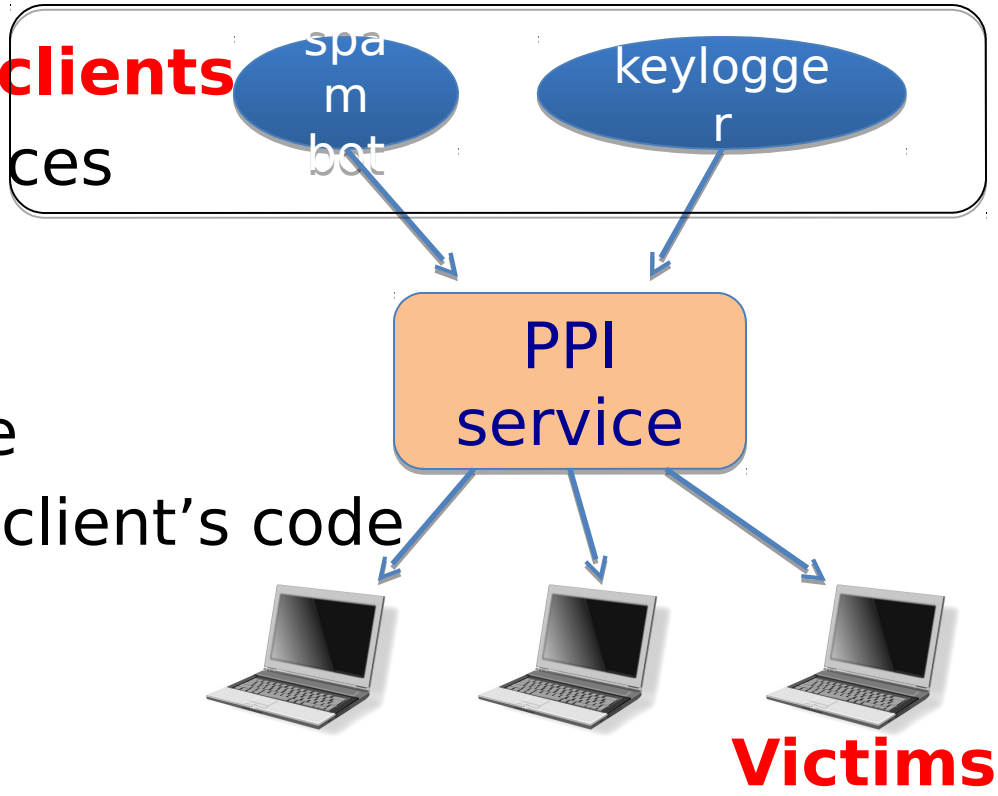
Option 3: black market

Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	A government official referring to what "some people" pay [9]
a "real good" exploit	over $100,000	Official from SNOsoft research team [10]

rce: Charlie Miller (securityevaluators.com/files/papers/0daymarket.pdf)

Marketplace for owned machines

Pay-per-install (PPI) services

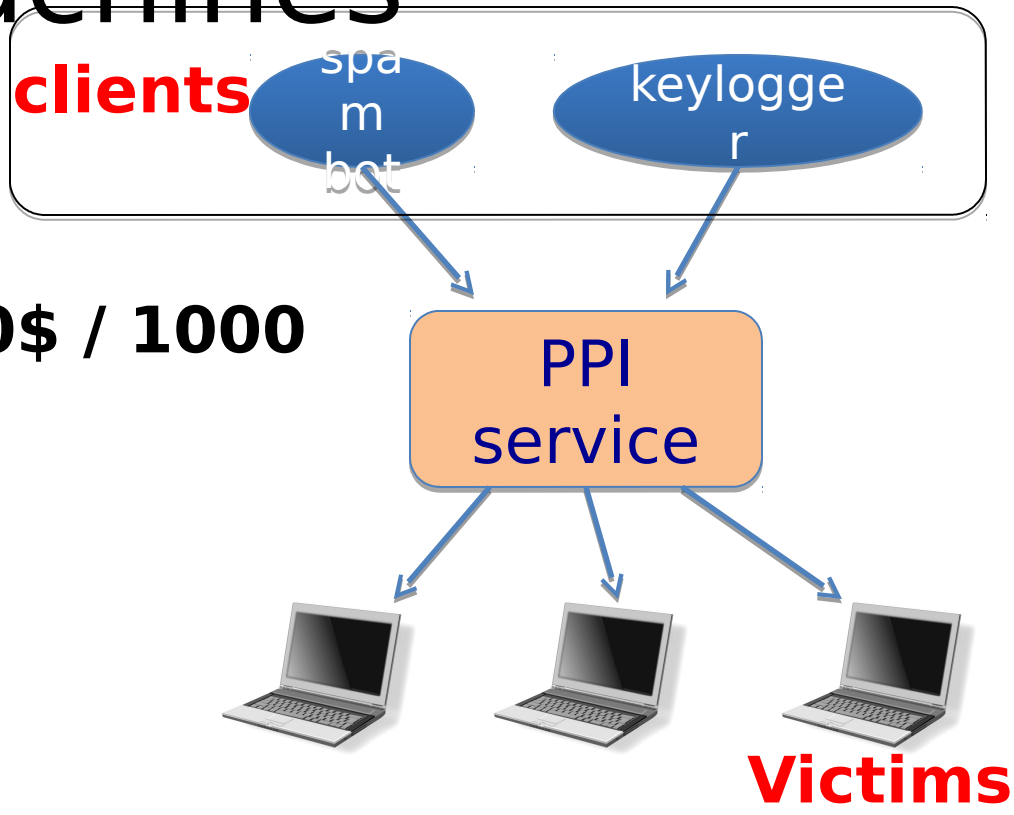


PPI operation:

1. Own victim's machine
2. Download and install client's code
3. Charge client

urce: 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

urce: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

Why Is Security Hard?

Two factors:

- **Lots of buggy software** (and gullible users)
- **Money can be made from finding and exploiting vulnerabilities**

1. Marketplace for vulnerabilities and exploits
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

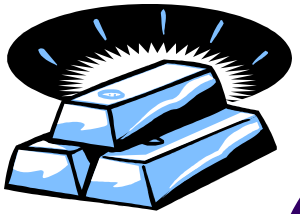
- Given a computer system, one may ask:

  Is the computer system secure?

Is the House Secure?

It Depends …

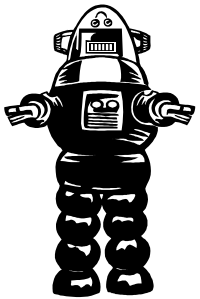
- What are the assets? What are the goals?



It Depends …

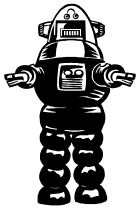
- Threat model
  - In SafeLand, you don’t need to lock the door
  - Attackers who pick locks
  - Attackers who drive a bull-dozer
  - Attackers who have super advanced technology
  - Attackers who may know you well



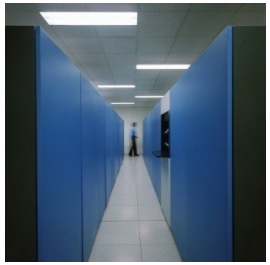




Is the House Secure?

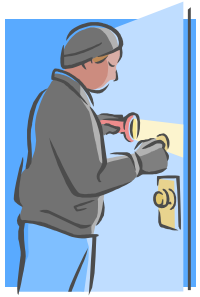
- Is the house's protection mechanism strong enough to protect the assets from attackers in a certain threat model?

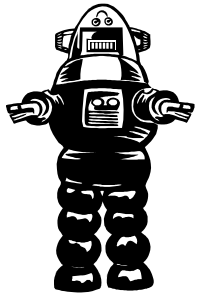


Which Threat Model Should You Choose?




?






Cost of Security

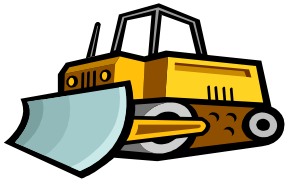
- Should you always build & evaluate a system secure against the strongest attacker?
  - A student may simply not be able to afford an alarm system
- Not about perfect security

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?

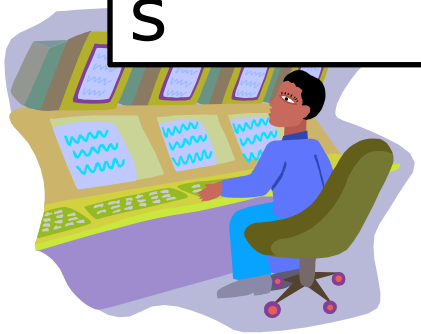






Key Elements to Security Analysis

Security properties



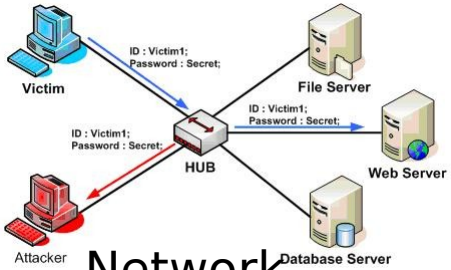
Threat Model

Security Analysis

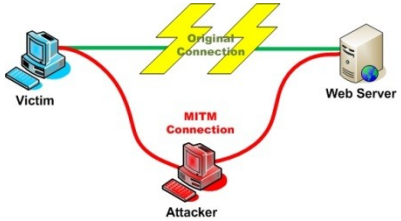
?

Threat Model

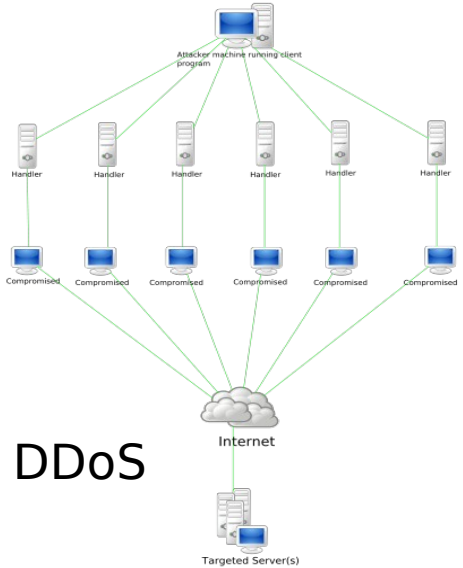
- Assumptions on attackers' abilities and



Network Eavesdropper

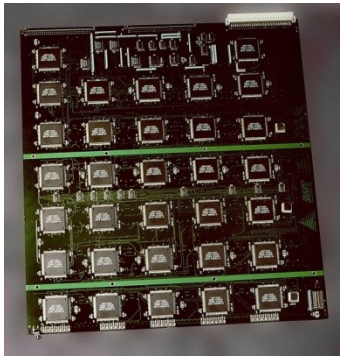


MITM Attack



DDoS

0Day



DES Cracker

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

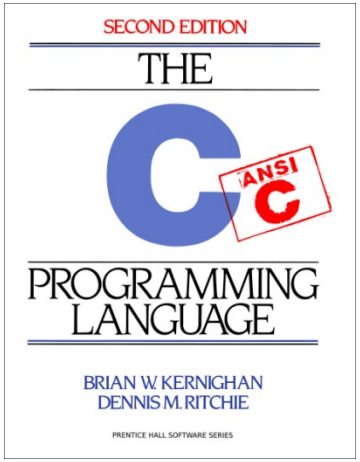
Over time….

New account, nothing of value;
No incentive for attackers

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

Browser	Known unpatched vulnerabilities					
	Secunia					SecurityFocus
	Extremely critical (number / oldest)	Highly critical (number / oldest)	Moderately critical (number / oldest)	Less critical (number / oldest)	Not critical (number / oldest)	Total (number / oldest)
Google Chrome 16	0	0	0	0	0	1 13 December 2011
Internet Explorer 6	0	0	4 17 November 2004	8 27 February 2004	12 5 June 2003	534 20 November 2000
Internet Explorer 7	0	0	1 30 October 2006	4 6 June 2006	9 5 June 2003	213 15 August 2006
Internet Explorer 8	0	0	0	1 26 February 2007	7 5 June 2003	123 14 January 2009
Internet Explorer 9	0	0	0	0	1 6 December 2011	26 5 March 2011
Firefox 3.6	0	0	0	0	0	1 20 December 2011

"Vulnerabilities." *SecurityFocus*. Web. 18 Jan. 2012. <http://www.securityfocus.com/>.