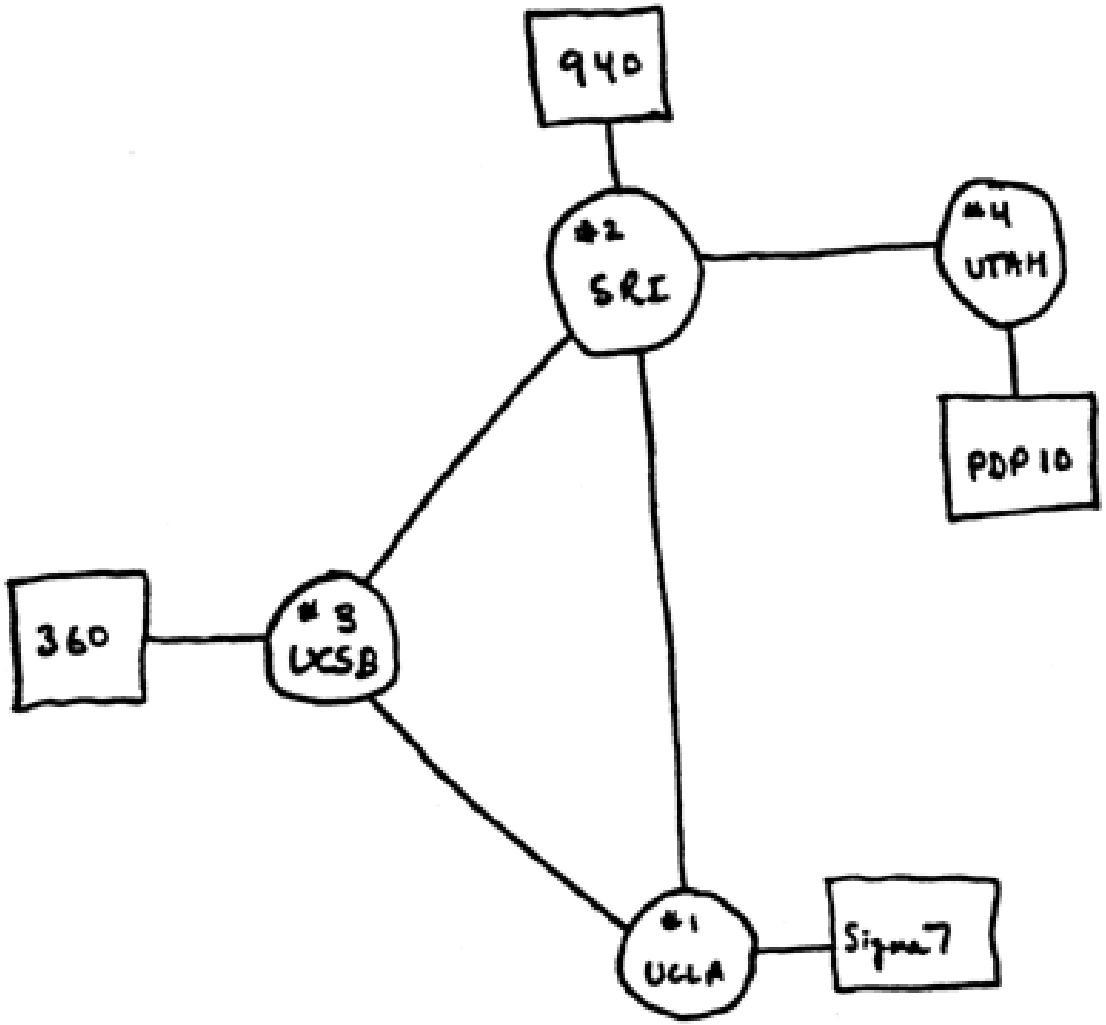
CSE508 Network Security (PhD Section)

1/29/2015 **Basic Concepts and Threat Landscape**

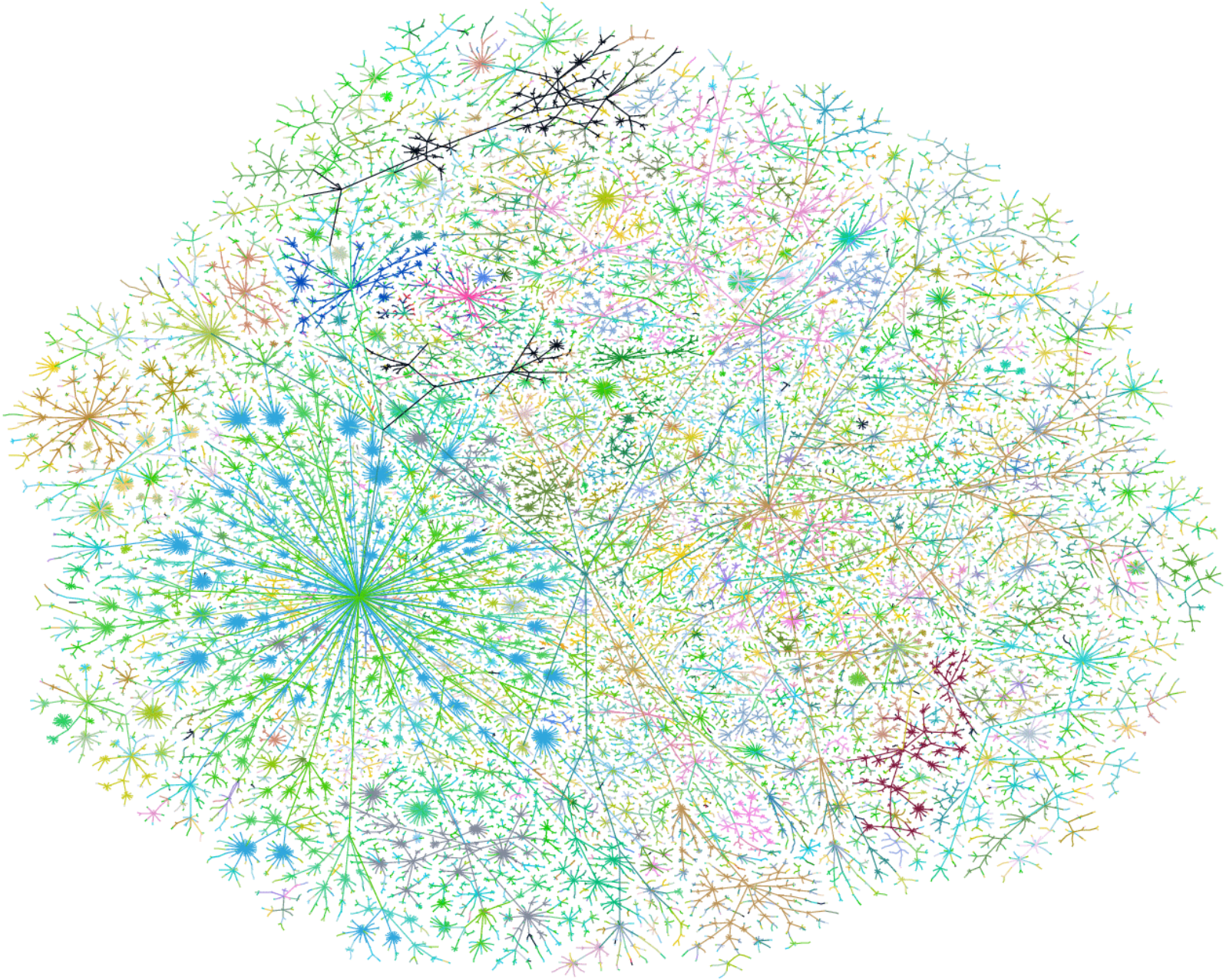
Michalis Polychronakis

Stony Brook University

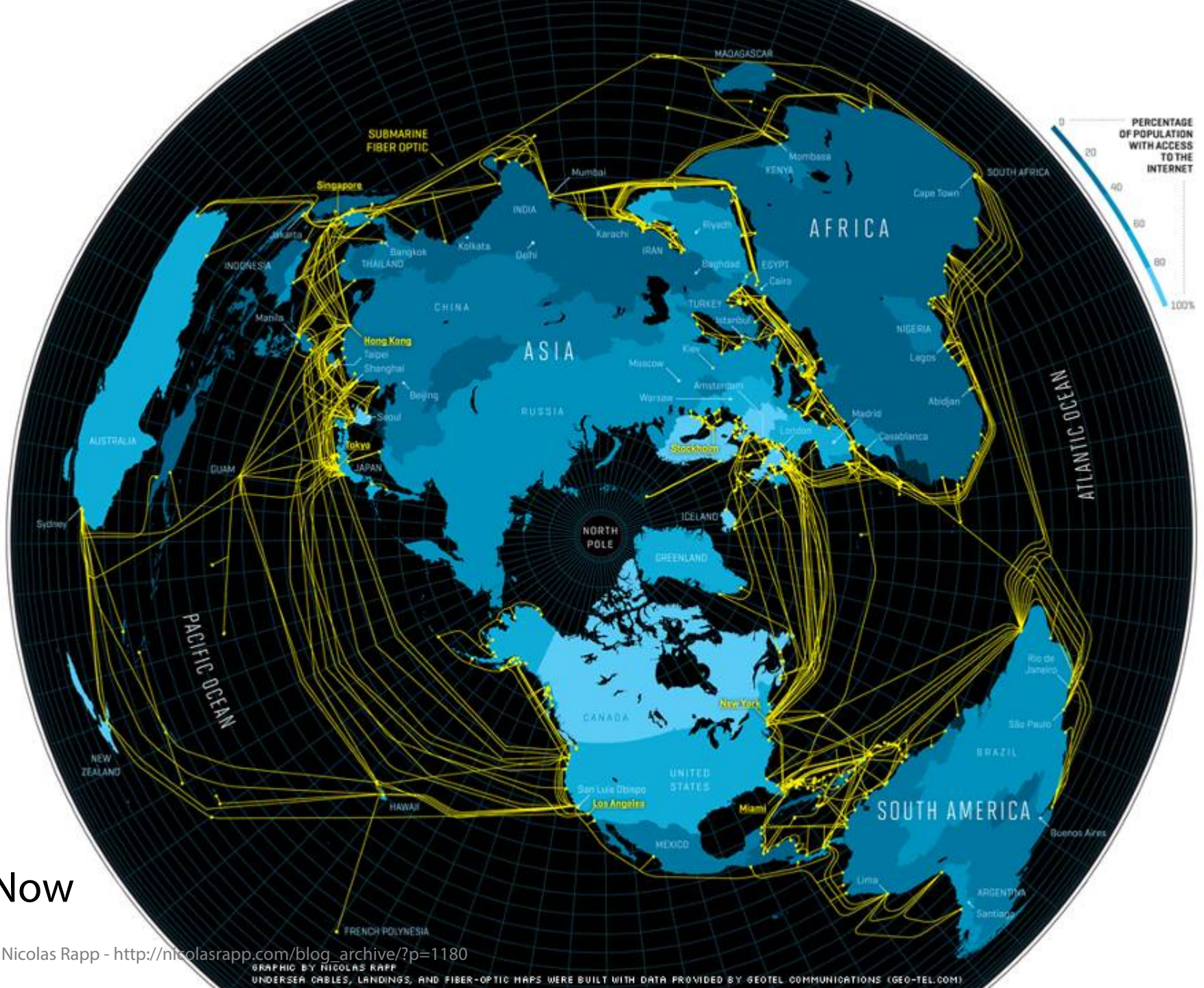
Why care about network security?



1969



1998



Now

An increasing part of our business, social, and personal life involves the internet

- Web, email/IM, cloud, social networks, …
- Mobile computing
- Cyber-physical systems
- Internet of things

Protecting the security and privacy of our digital interactions is critical

- Most of them involve *networked systems and applications*

UPDATE 2-Home Depot breach bigger than Target at 56 mln cards

Thu Sep 18, 2014 7:12pm EDT

RELATED NEWS

CORRECTED-Tim Hortons reports strong Q3 same-store sales growth so far

ANALYSIS & OPINION

Pakistani woman embraced by Islamic State seeks to drop U.S. legal appeal

RELATED TOPICS

Stocks »
Markets »
Earnings »
Cyclical Consumer Goods »
Financials »
Technology »

(Recasts, adds details about costs of breach and likelihood of costs rising, comment from computer security experts, background)

By Jim Finkle and Nandita Bose

(Reuters) - Home Depot Inc Thursday said some 56 million payment cards were likely compromised in a cyberattack at its stores, suggesting the hacking attack at the home improvement chain was larger than last year's unprecedented breach at Target Corp.

Home Depot, in providing the first clues to how much the breach would cost, said that so far it has estimated costs of $62 million. But it indicated that costs could reach much higher.

It will take months to determine the full scope of the fraud, which affected Home Depot stores in both the United States and Canada

TRENDING ON REUTERS

1 Greek PM Tsipras freezes privatisations, markets tumble | VIDEO
2 Two Israeli soldiers, U.N. peacekeeper killed in Israel-Hezbollah violence | VIDEO
3 Wall Street ends lower after Fed statement, oil drop
4 Flooding leaves mess in oceanfront Massachusetts after storm | VIDEO
5 Litvinenko autopsy was world's most dangerous, UK inquiry hears

Follow Reuters

Facebook Twitter RSS YouTube

RECOMMENDED VIDEO


Maggie McGrath Forbes Staff

Got one eye on the markets, the other on Gen Y's pressing $$ issues

FOLLOW

INVESTING 10/02/2014 @ 5:51PM | 7,054 views

JP Morgan Says 76 Million Households Affected By Data Breach

+ Comment Now + Follow Comments

JPMorgan Chase JPM -2.58%, the nation's largest bank by assets, has revealed the scope of the cyber-attack that compromised its data in mid-August. And while the number of households affected doesn't surpass the 110 million accounts that were compromised in the Target TGT -0.67% data breach in late 2013, it does comprise more than half of all U.S. households.

JPMorgan said in an SEC filing Thursday afternoon that information from 76 million households — the equivalent of 65% of all U.S. households — and 7 million small businesses was compromised in the August cyber-security attack

Share
Next Post
CONFERENCES AND MORE

National Security

Hackers breach some White House computers

Malware

International Space Station attacked by 'virus epidemics'

Malware spread from infected devices in orbit, proving not even computers in space are safe from viruses

Featured comment

In space, no one can see your blue screen.

alanredangel
12 Nov 2013

See more comments

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

MOST RECENT WIRED POSTS

Facebook Just Had Another Record Quarter, and It Has Apple to Thank

Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable


A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online

Amazon Challenges Google and Microsoft With Its Own Email Service


These Are the Hottest New Open Source Projects Right Now


Canada Joins World Powers in

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

But the deeper aspects of your personality remain hard to detect.

MORE IN TECHNOLOGY

Introducing the Supertweet
IAN BOGOST

My Parents' Facebook Will
JAKE SWEARINGEN

Computing

US police force pay bitcoin ransom in Cryptolocker malware scam

Unprepared officials blindsided by sophisticated virus call experience 'an education'


New Rules in China Upset Western Tech Companies

STATE OF THE ART
Uber's Business Model Could Change Your Work


ECONOMIC SCENE
Job Licenses in Spotlight as Uber Rises


DEALBOOK
After Alibaba Spinoff, Yahoo May Become a Takeover Target

Bits

Search Bits SEARCH

SECURITY

Apple Says It Will Add New iCloud Security Measures After Celebrity Hack

By BRIAN X. CHEN SEPTEMBER 4, 2014 11:32 PM 21 Comments

PREVIOUS POST
Microsoft Introduces Three New Smartphones

NEXT POST
Daily Report: Apple Expected to Unveil Smartwatch and Larger iPhones

SCUTTLEBOT *News from the Web, annotated by our staff*

Netflix's Secret Special Algorithm Is a Human
NEW YORKER | His name, writes Tim Wu, is Ted Sarandos. - *Natasha Singer*

Uber Releases Study on Drunk Driving and Transportation
UBER BLOG | A new study released by the ride-hailing company claims it is having a "measurable impact on driving down alcohol-related crashes." - *Mike Isaac*

French agency caught minting SSL certificates impersonating Google

Unauthorized credentials for Google sites were accepted by many browsers.

by Dan Goodin - Dec 9 2013, 2:05pm EST

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Want high-end flight sim pedals? Put $500 in a Polish bank account and contact Slaw

Review: "Wait—$500 for *just* the Slaw Device BF 109?" Well, yes, but what pedals!

WATCH ARS VIDEO

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

BY KEVIN POULSEN 09.13.13 | 4:17 PM | PERMALINK

MOST RECENT WIRED POSTS

Facebook Just Had Another Record Quarter, and It Has Apple to Thank

Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable


A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online

Amazon Challenges Google and Microsoft With Its Own Email Service


These Are the Hottest New Open Source Projects Right Now


Canada Joins World Powers in

Network vs. System vs. Computer vs. Information Security

Not always a clear distinction

- Infrastructure
- Protocols
- Applications
- Hosts/devices

Complex interactions

- Core internet protocols/services
- Distributed systems
- Web/cloud applications

There is more

- People
- Physical security

Threats span all these areas

Threats?

Exposure of data

Tampering with data

Denial of service

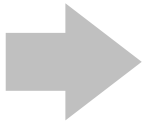
Impersonation

Forbidden access

Exposure of information about individuals

Identification of unknown individuals

Threats	Goals
Exposure of data	Confidentiality
Tampering with data	Integrity
Denial of service	Availability
Impersonation	Authentication
Forbidden access	Authorization
Exposure of information about individuals	Privacy
Identification of unknown individuals	Anonymity



Confidentiality

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [RFC2828]

Sensitive data must be protected

- In transit: network packets, network connections, email messages, document files, …
- At rest: main memory (buffers, message queues), storage, …

Cryptography is a tool to achieve confidentiality

- Not the only one (e.g., steganography)

Data Integrity

"The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." [RFC2828]

Cryptography is a tool to achieve data integrity

- Intentional or accidental data changes should be detectable

System integrity

"Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system." [CNSSI No. 4009]

- Fragile: weak authentication, unauthorized access, …

Availability

"The property of being accessible and useable upon demand by an authorized entity." [CNSSI No. 4009]

Denial of Service (DoS) attacks are the most common way of affecting the availability of networked systems

- Saturation of resources (bandwidth, CPU, memory, …)
- Disruption of configuration or state (routing, DNS, …)
- Jamming, physical damage, …

Malware can do more harm

- Ransomware: encrypt user files and then demand a ransom (Gpcode, cryptolocker, …)
- Just wipe out data/brick the system (Wiper, SMB worm, …)

Authentication

"The process of verifying an identity claimed by or for a system entity." [RFC2828]

Different approaches

- Something you know (password, pin, …)
- Something you have (phone, token, …)
- Something you are (fingerprint, retina, …)

Multi-factor authentication is a good thing!

Cryptography is a tool to achieve authentication

Password theft/leakage is a huge problem

Authorization

"Access privileges granted to a user, program, or process or the act of granting those privileges." [CNSSI No. 4009]

Authorization verifies that a user has the proper privileges to access a resource (presumes successful authentication)

Related term: access control

Access restriction based on various properties: identity, role, labels, date/time, IP address, domain, access frequency, …

One of the core goals of network security:
Keep unauthorized parties from gaining access to resources

Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Beyond private data (messages/files):

- Online activity (browsing history, daily routine, …)
- Location (3/4G, GPS, WiFi, …)
- Preferences ("likes," Amazon, Netflix, …)
- Health (Fitbit, iWatch, …)
- …

Anonymity

"The state of being not identifiable within a set of subjects, the anonymity set." [Pfitzmann and Köhntopp]

- The larger the anonymity set, the stronger the anonymity

Very different from privacy:

- An anonymous action may be public, but the actor's identity remains unknown (e.g., vote in free elections)

Anonymous communication

- Sender anonymity
- Receiver anonymity
- Unlinkability of sender and receiver

Prevention vs. Detection

Door lock vs. burglar alarm

Protection mechanisms can be bypassed

- Can't break crypto? Just remove it
- Can't go through the firewall? Just send a link
- Can't brute force the password? Just ask for it
- …

Detection mechanisms can be evaded

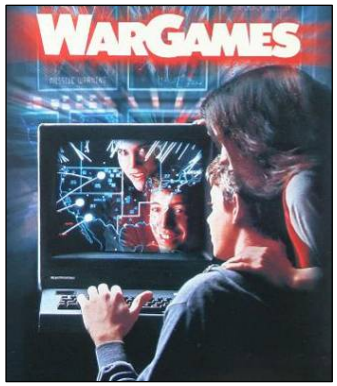
- IDS in place? Just mutate the attack vector
- DoS flooding blocker? Just use thousands of hosts
- Reputation-based IP blacklisting? Just host the C&C server on Google/Amazon
- …

Threat Actors

'90s: script kiddies

'00s: criminals

'10s: nations *(OK, much earlier, but now we talk about it)*



Then: fun

Now: profit

Different motives:

- $$$$$$$$$$
- Honest but curious individuals
- Political or social ends
- Bribed or angry insiders
- Espionage
- Military *

* *Cyberwar, cyberterrorism, cyberOMG!!!: Terms that (should?) express fear of lethal outcomes. So far we've seen mostly sabotage, espionage, and subversion…*

Different resources: $$$$$$$$, skills, infrastructure, …

Know your enemy!

Intrusions

"Any set of actions that attempt to compromise the integrity, confidentiality or availability of information resources" [Heady et al.]

"An attack that exploits a vulnerability which results to a compromise of the security policy of the system" [Lindqvist and Jonsson]

Most intrusions…

- Are carried out remotely
- Exploit software vulnerabilities
- Result in arbitrary code execution or unauthorized data access on the compromised host

Attack Source

Local

- Unprivileged access ➔ privilege escalation
- Physical access ➔ I/O ports, memory/storage, …

Remote

- Internet
- Local network (Ethernet, WiFi, 3/4G, bluetooth, …)
- Infected media (disks, CD-ROMs, USB sticks, …)

Intrusion Method

social engineering (phishing, spam, scareware, …)

viruses (~~disks~~, ~~CD-ROMs~~, USB sticks, downloads, …)

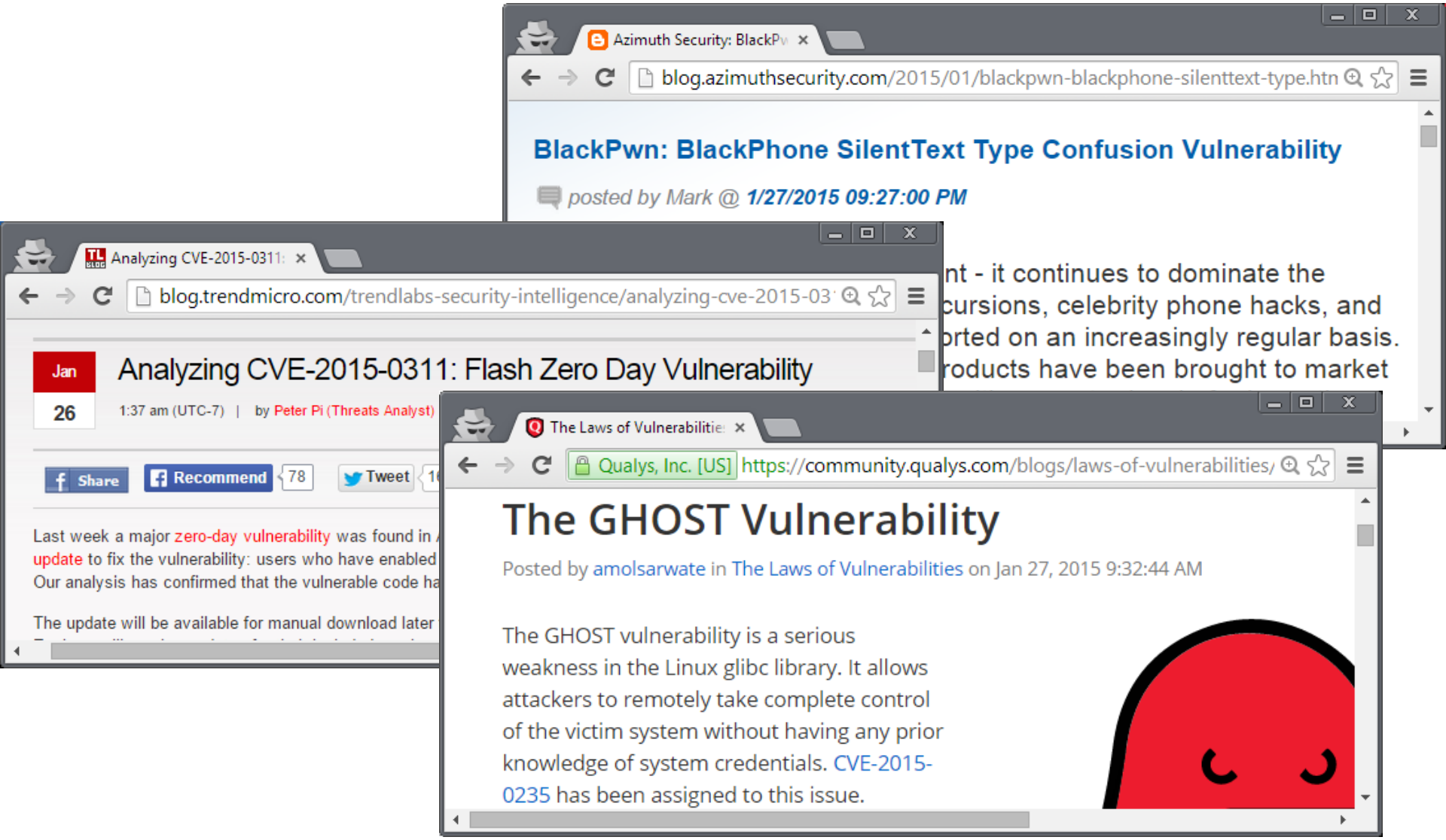
network traffic interception (access credentials, keys, …)

password guessing (brute force, root:12345678, …)

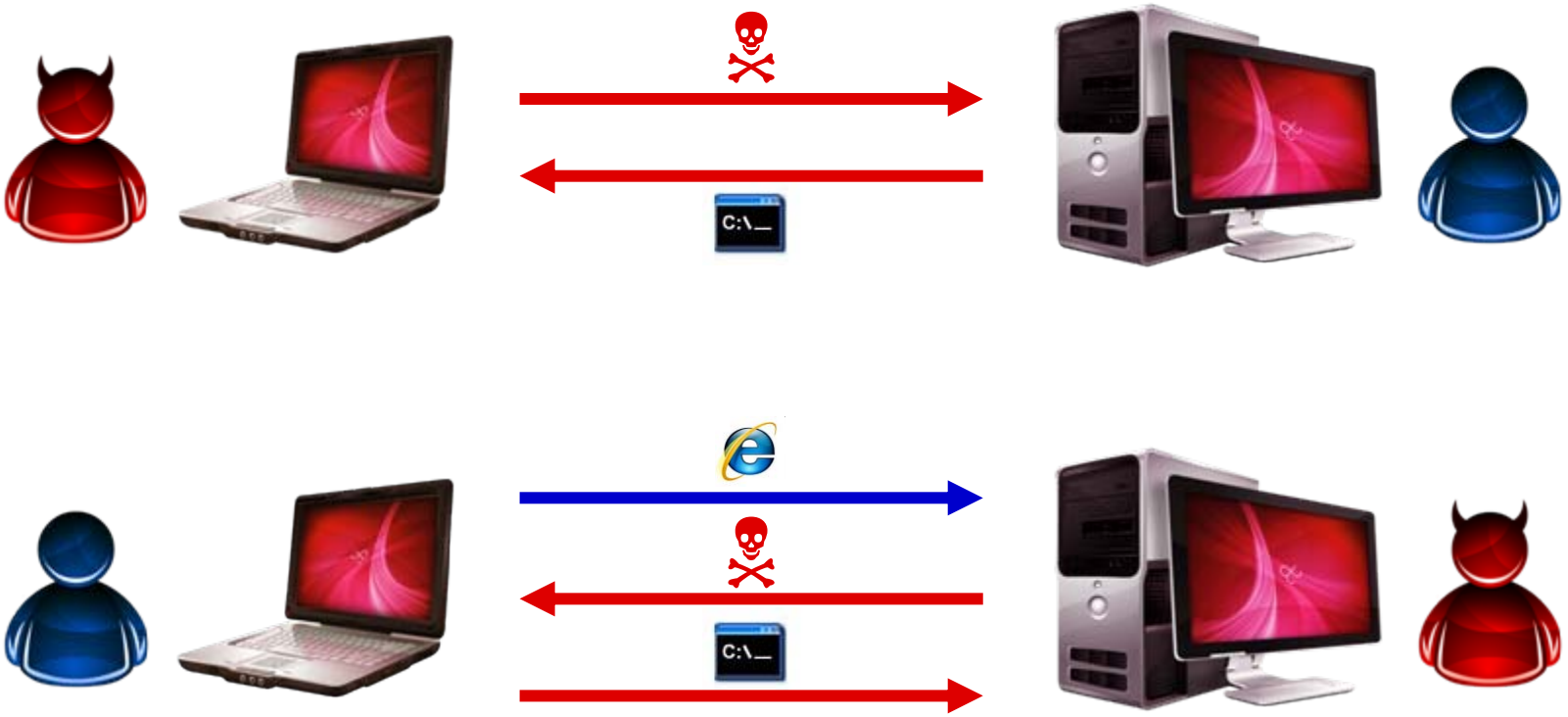
physical access (reboot, keylogger, screwdriver, …)

software vulnerability exploitation

Just This Week's News…



Remote Exploitation



Malware and Botnets

click fraud

port scanning

extortion

phishing

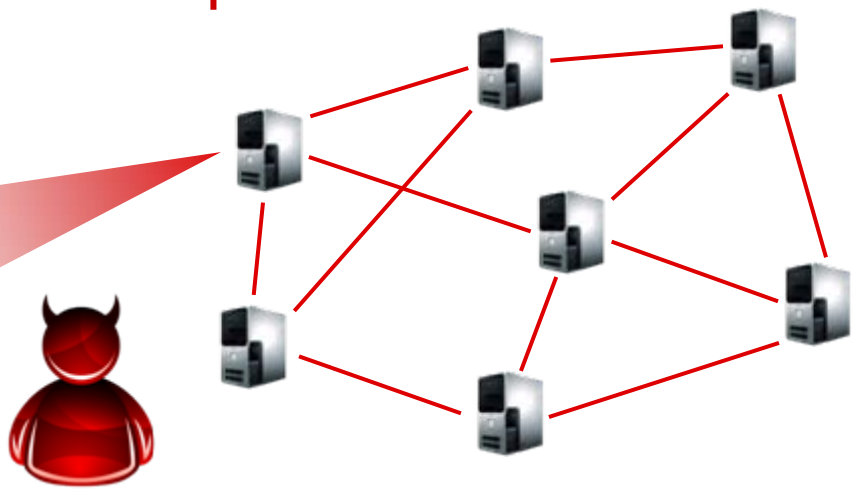
illegal content

DDoS

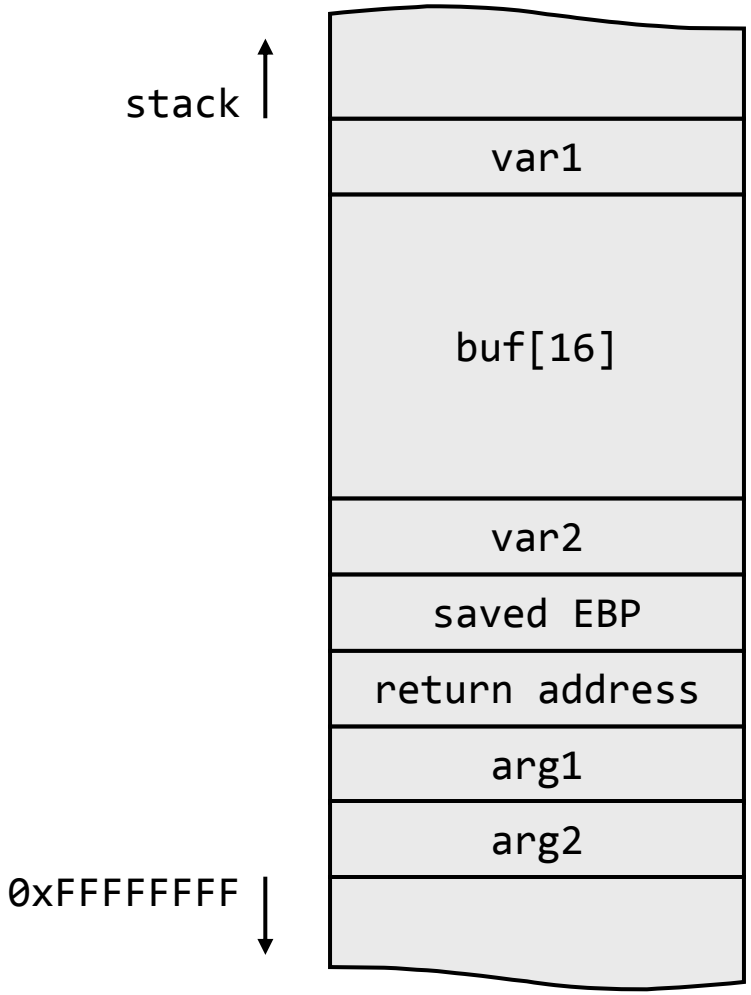
code injection

malicious websites

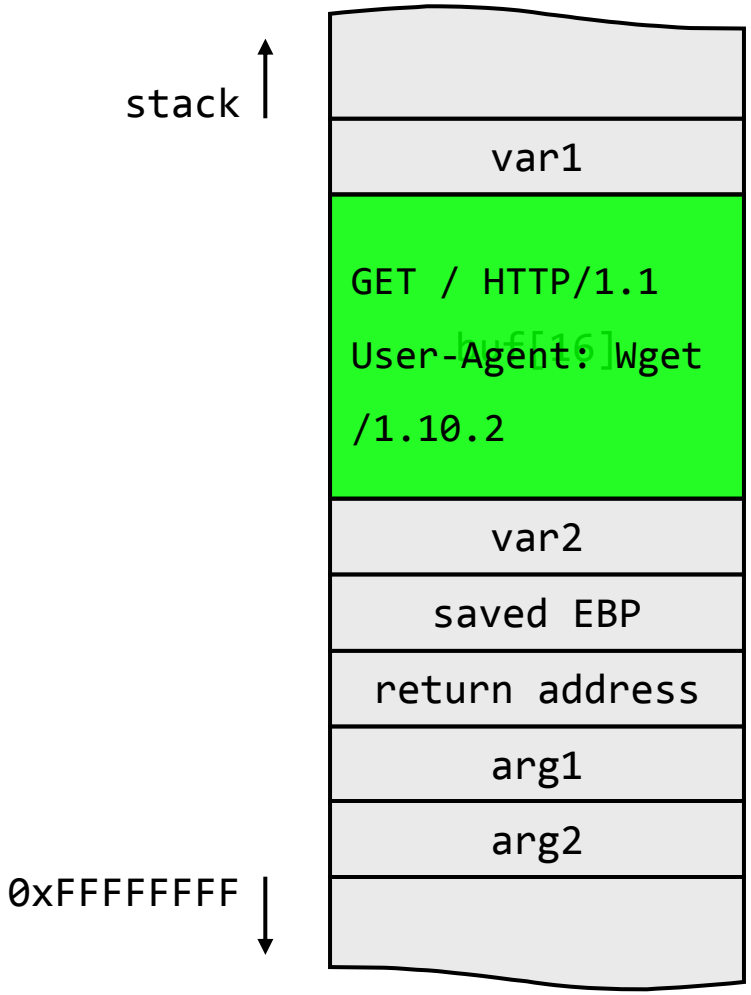
spam



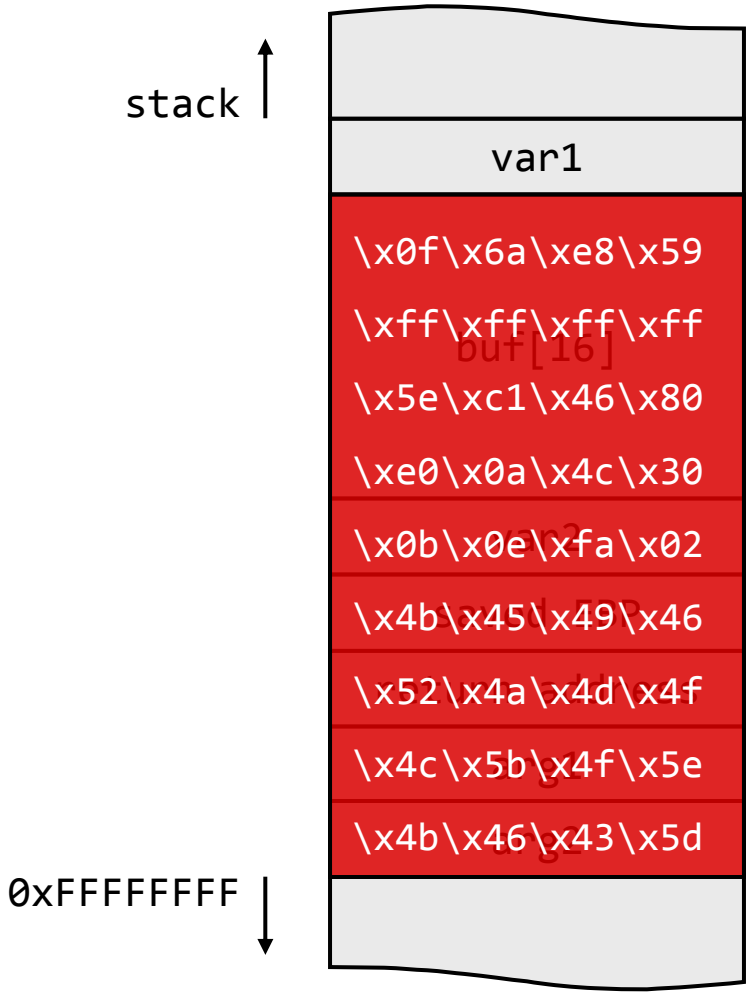
(Very Simple) Buffer Overflow Exploitation



(Very Simple) Buffer Overflow Exploitation



(Very Simple) Buffer Overflow Exploitation



← **Code injection**

Shellcode

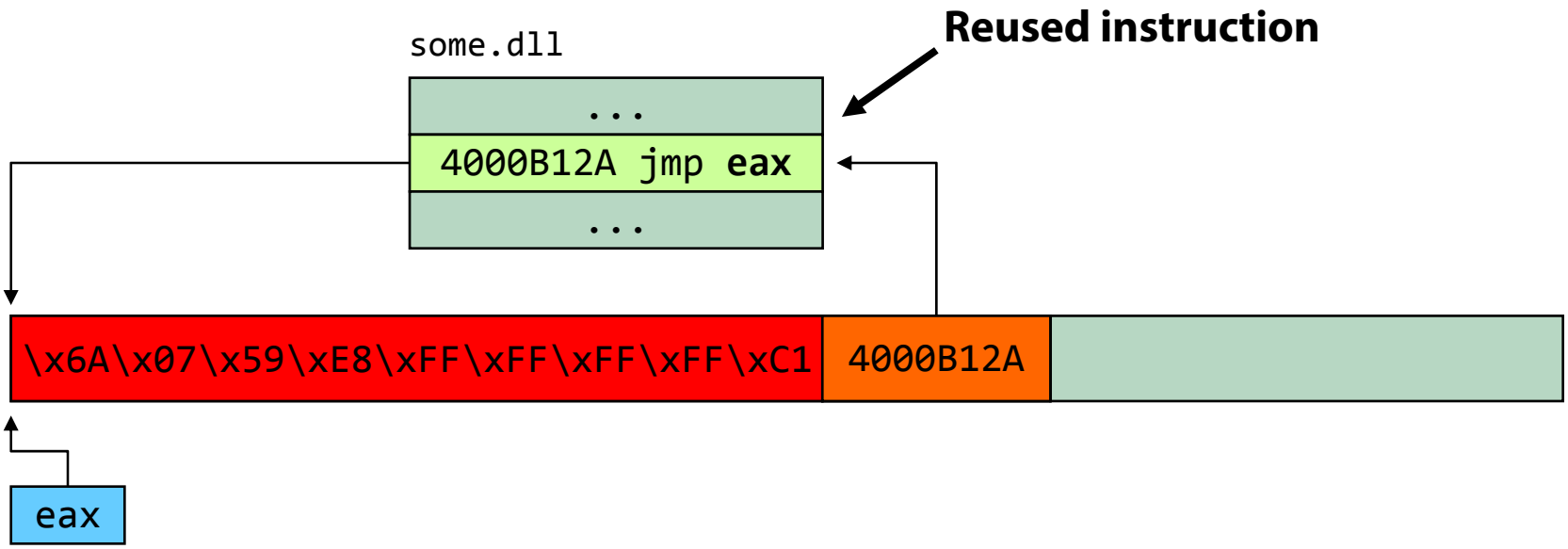
spawn shell

listen for connections

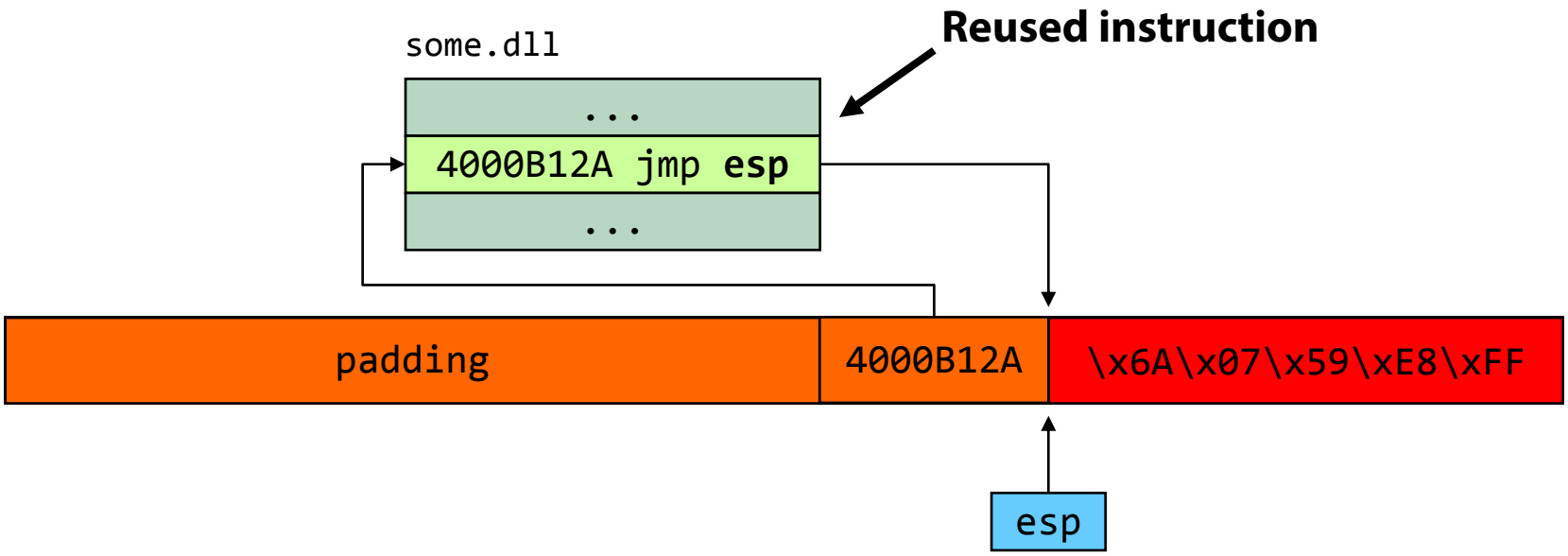
add user account

download and execute malware

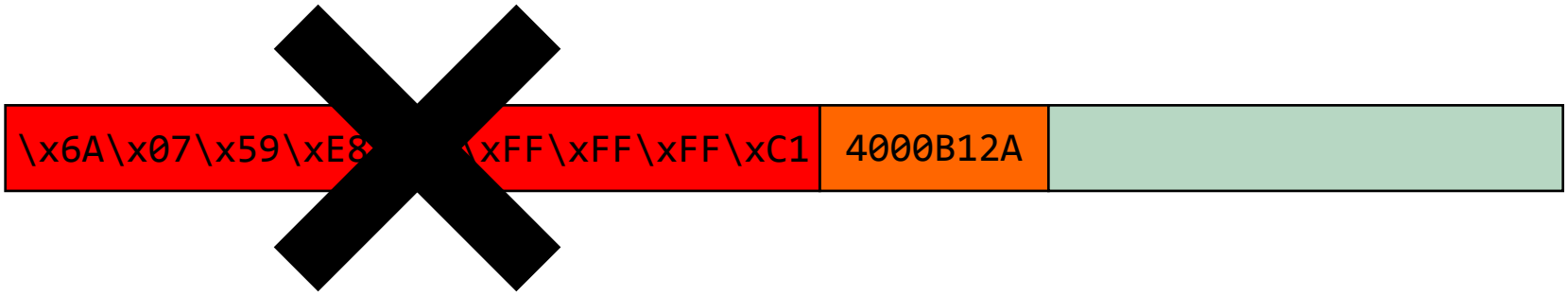
Hijacking Control Flow



Hijacking Control Flow



Non-Executable Memory



W^X, PaX, Exec Shield, DEP

x86 support introduced by AMD, followed by Intel

- Pentium 4 (late models)

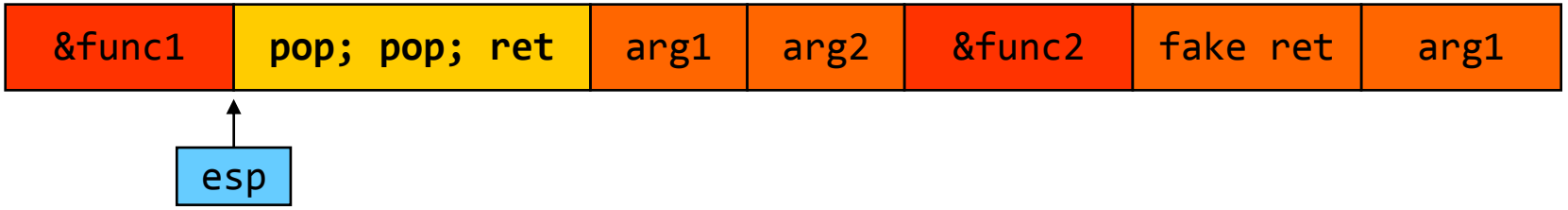
DEP introduced in XP SP2 (hardware-only)

- Applications can opt-in (SetProcessDEPPolicy() or /NXCOMPAT)

Ret2libc → ROP

ret2libc [Solar Designer '97]

ret2libc chaining [Nergal '01]



Ret2libc → ROP

Borrowed code chunks technique [Krahmer '05]

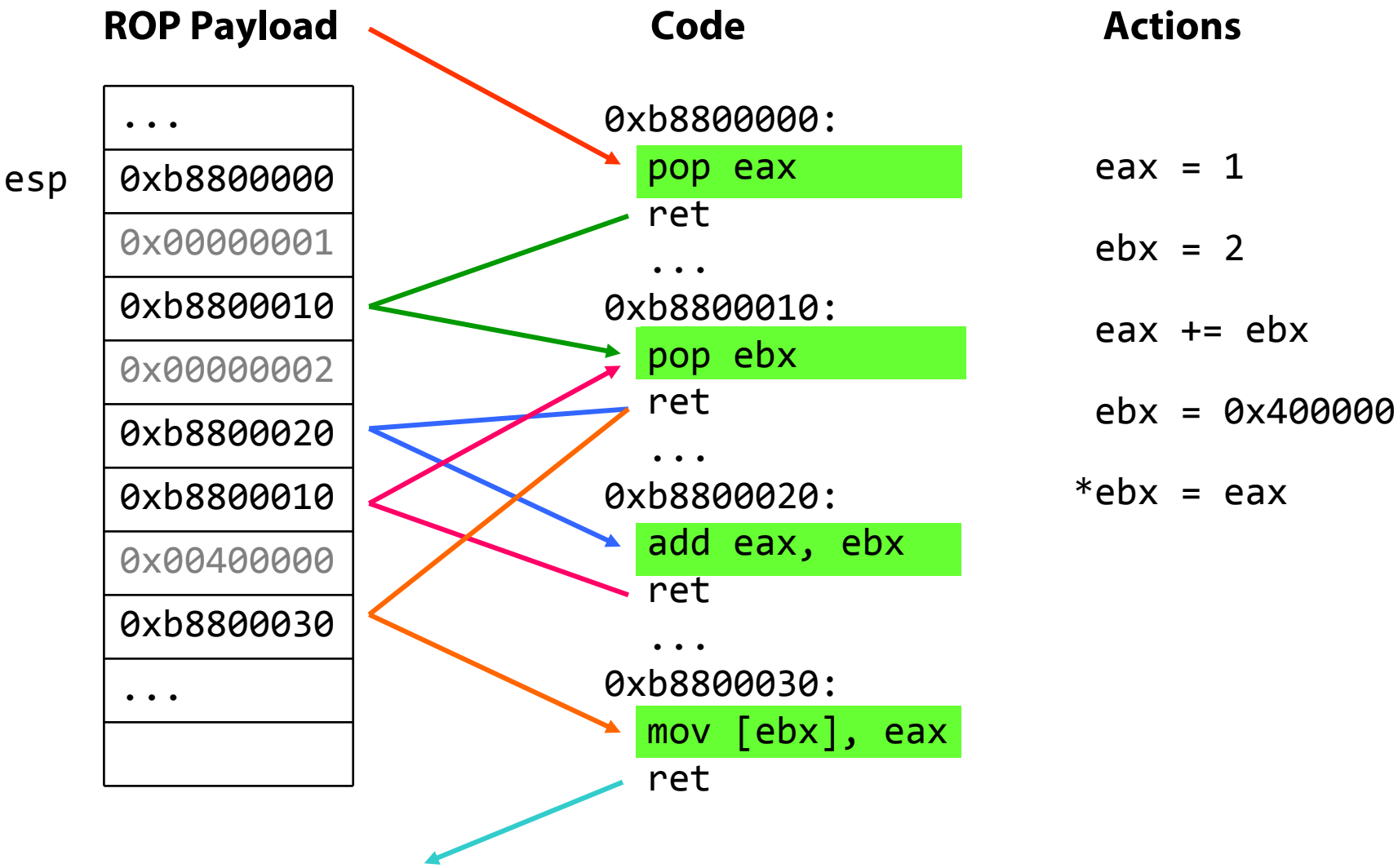
Pass function arguments through registers (IA-64)

```
0x0000000000400a82:  pop %rbx
0x0000000000400a83:  retq

0x00002aaaaac743d5:  mov %rbx,%rax   → &system
0x00002aaaaac743d8:  add $0xe0,%rsp
0x00002aaaaac743df:  pop %rbx
0x00002aaaaac743e0:  retq

0x00002aaaaac50bf4:  mov %rsp,%rdi   → /bin/sh
0x00002aaaaac50bf7:  callq *%eax
```

Return-oriented programming [Shacham '07]

Turing-complete return-oriented "shellcode"

Jump-oriented programming [Shacham '10]


ROP Payload
Code
Actions
esp
...
0xb8800000
0x00000001
0xb8800010
0x00000002
0xb8800020
0xb8800010
0x00400000
0xb8800030
...
0xb8800000:
pop eax
ret
...
0xb8800010:
pop ebx
ret
...
0xb8800020:
add eax, ebx
ret
...
0xb8800030:
mov [ebx], eax
ret
eax = 1
ebx = 2
eax += ebx
ebx = 0x400000
*ebx = eax

Address Space Layout Randomization

Randomize the location of code

ASLR is not always fully adopted

- Only 66 out of 1,298 binaries in /usr/bin [SAB11]
- Only 2 out of 16 third-party Windows applications [Pop10]

Even ASLR-enabled applications sometimes have statically mapped DLLs

- EMET forced randomization

Information Leaks Break ASLR [Ser12]

- Dynamically infer a DLL's load address through a memory leak

Current State of ROP exploits

First-stage ROP code for bypassing DEP

- Allocate/set W+X memory (`VirtualAlloc`, `VirtualProtect`, ...)
- Copy embedded shellcode into the newly allocated area
- Execute!

Recent pure-ROP exploits

- In-the-wild exploit against Adobe Reader XI (CVE-2013-0640)

The complexity of ROP exploit code increases

- New anti-ROP features in Microsoft's EMET
- ROP exploit mitigations in Windows 8.1

But…

Although software exploitation gets harder (?), it is not going away any time soon

Protections can be bypassed

Detectors can be evaded

Legacy/unpatched systems remain vulnerable

Growing incentives by attackers and security professionals

Course Focus (You Got the Idea…)

Internet technologies, protocols, applications, attacks, and defenses from a practical perspective

Indicative topics

- Core network protocols, eavesdropping, scanning, DoS attacks, firewalls, VPNs, proxies, intrusion detection, forensics, honeypots, encrypted communication, authentication, services and applications, botnets, targeted attacks, privacy, anonymity, …

Attacks and threats!

- Understand the modus operandi of attackers
- Find vulnerabilities, subvert protections, bypass all the things
- Think sideways
- How to secure a system – know what to defend against

Play Fair

Cannot teach defense without offense, but:

Breaking into systems is illegal!

Unauthorized data access is illegal!

Computer Fraud and Abuse Act (CFAA)

http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Practice on your own systems or controlled environment

Scanning/penetration testing/etc. of third-party systems may be allowed only after getting permission by their owner

Course Information

Mixed format

- Lectures
- Research paper presentations
- Hands-on sessions

Requirements

- Conference-style presentation of 1-2 research papers, which the rest of the class should read and discuss
- 4–5 programming/hands-on assignments
- Midterm and final exams

Grading

- Paper presentations: 20%
- Assignments: 50%
- Midterm: 10%
- Final: 20%

Schedule (Tentative)

Basic Concepts and Threat Landscape

Lower Layers and Core Protocols

TCP/IP

Denial of Service

Firewalls/Gateways

Scanning

Encrypted Communication

Crypto (Failures)

Schedule (Tentative)

HTTPS

Intrusion Detection

Network Forensics

Honeypots

Email/spam

Web/Cloud

Botnets

Privacy/Anonymity/Online Freedom

Course web page

http://www3.cs.stonybrook.edu/~mikepo/CSE508/

Please sign up on Piazza!