CSE508 Network Security

1/27/2016 **Threat Landscape**

Michalis Polychronakis

Stony Brook University

Threats, Vulnerabilities, and Attacks

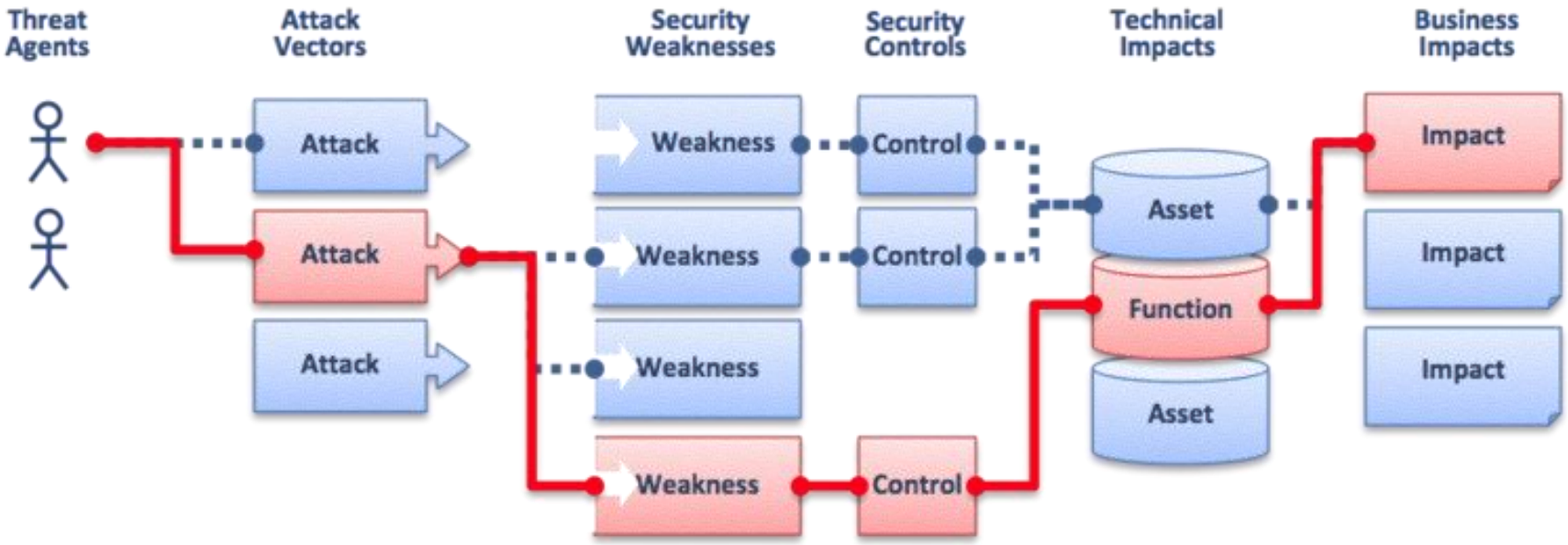
A *threat* is a potential cause of an incident, malicious or otherwise, that could harm an asset

- Different kinds: loss of services, compromise of information or functions , technical failure, …
- Different origins: deliberate, accidental, environmental, …

A *vulnerability* is a weakness that makes a threat possible

An *attack* is an action that exploits a vulnerability or enacts a threat

Threats, Vulnerabilities, and Attacks



Threat Classification and Risk Assessment

Classification example: Microsoft's STRIDE

- Spoofing: TCP/IP, identity, HTTP headers, email address, poisoning, …
- Tampering: network traffic, code, HTTP cookies/URLs/parameters, …
- Repudiation: deniability, audit log scrubbing/modification, …
- Information disclosure: unauthorized data access, data leakage, …
- Denial of Service: crashing, flooding, resource stagnation, …
- Elevation of privilege: gain admin access, jailbreaking, …

Risk assessment example: Microsoft's DREAD

- Damage: how bad would an attack be?
- Reproducibility: how easy is it to reproduce the attack?
- Exploitability: how much work is it to launch the attack?
- Affected users: how many people will be impacted?
- Discoverability: how easy is it to discover the threat?

Threat Model

Set of assumptions about possible attacks that a system tries to protect against

- Understanding potential threats is crucial for taking appropriate measures

Various threat modeling approaches: attacker-centric, software-centric, asset-centric, …

Example: data flow approach

- *View the system as an adversary:* identify entry/exit points, assets, trust levels, usage patterns, …
- *Characterize the system:* identify usage scenarios, roles, objectives, components, dependencies, security alerts, implementation assumptions, …
- *Identify threats:* what can the attacker do? How? What is the associated risk? How can the respective vulnerabilities be resolved?

Policies and Mechanisms

Threat model ➔ security policy ➔ security mechanisms

Security policy: a definition of what it means for a system/organization/entity to be secure

- Access control, information flow, availability, …
- Computer, information, network, application, password, …

Enforced through security mechanisms

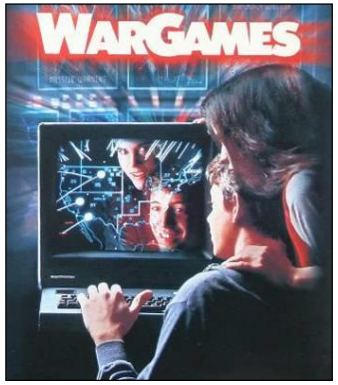
- Prevention
- Detection
- Recovery
- Awareness

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, cyberweapons!!!!!!: Exaggerated 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!

Vulnerability

"A property of a system or its environment which, in conjunction with an internal or external threat, can lead to a security failure, which is a breach of the system's security policy." [Anderson]

Various classifications

- *SDL:* design, implementation, operation, maintenance
- *Abstraction level:* low vs high level, OSI network layers, hardware/firmware/OS/middleware/application, system vs. process, …
- *Type of error/condition/bug:* memory errors, range and type errors, input validation, race conditions, synchronization/timing errors, access-control problems, environmental/system problems (e.g. authorization or crypto failures), protocol errors, logic flaws, …
- *Disclosure process:* zero-day vs. known, private vs. public, "responsible" vs. full disclosure, …

Multiple vulns. are often combined for a single purpose

Vulnerability (Another Definition)

"The intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw." [AFRL ATSPI]

System Susceptibility: focus on what's critical

- Reduce access points to only those that are absolutely necessary

Access to the flaw: move it out of band

- Make critical access points and associated security elements less accessible to the adversary

Capability to exploit the flaw: prevent, detect, react

- Appropriate response upon detection of an attack

Related term: ***attack surface***

- The different points through which an attacker can interact with the system/environment
- Increases with complexity (more logic, features, dependencies, …)

Intrusions


* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
EDIT V1 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[mobile]
80/tcp open http
81/tcp open
10
11
11
13
13
13
14
44
51
51
58
68
68
24
58
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3). OS detection may be less accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level (9)
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RIF CONTROL
ACCESS GRANTED

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/leakage (brute force, root:12345678, …)

Physical access (reboot, keylogger, screwdriver, …)

Software vulnerability exploitation

Just This Month's News…

Fatally weak MD5 function torpedoes crypto protections in HTTPS and IPSEC

MD5 and its only slightly stronger SHA1 cousin put world on collision course.

by Dan Goodin Jan 6, 2016 10:29am EST

Enlarge

US Navy

If you thought MD5 was banished from HTTPS encryption, you'd be wrong. It turns out the fatally weak cryptographic hash function, along with its only slightly stronger SHA1 cousin, are still widely used in the transport layer security protocol that underpins HTTPS. Now, researchers have devised a series of attacks that exploit the weaknesses to break or degrade key protections provided not only by HTTPS but also other encryption protocols, including Internet Protocol Security and secure shell.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Why the calorie is broken

"I'm kind of pissed at the scientific community for not coming up with something better."

WATCH ARS VIDEO

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the Consumer Technology Association conference

Google security researcher excoriates TrendMicro for critical AV defects

"I don't even know what to say," exasperated researcher tells TrendMicro official.

by Dan Goodin Jan 11, 2016 3:22pm EST

Antivirus provider TrendMicro has released an emergency product update that fixes critical defects that allow attackers to execute malicious code and to view contents of a password manager built in to the malware protection program. The release came after a Google security researcher publicly castigated a TrendMicro official for the threat.

Details of the flaws became public last week after Tavis Ormandy, a researcher with Google's Project Zero vulnerability research team, published a scathing critique disclosing the shortcomings. While the code execution vulnerabilities were contained in the password manager included with the antivirus package, they could be maliciously exploited even if end users never make use of the password feature. Those who did use it were also susceptible to hacks that allowed attackers to view hashed passwords and the plaintext Internet domains they belonged to.

"I don't even know what to say—how could you enable this thing *by default* on all your customer machines without getting an audit from a competent security consultant?" Ormandy wrote in an exchange with a TrendMicro official. "You need to come up with a plan for fixing this right now. Frankly, it also looks like you're exposing all the stored passwords to the internet, but let's worry about that screw up after you get the remote code execution under control."

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Why the calorie is broken

"I'm kind of pissed at the scientific community for not coming up with something better."

WATCH ARS VIDEO

by Michael Mimoso Follow @mike_mimoso

January 13, 2016 , 9:01 am

Microsoft Silverlight vulnerabilities certainly don't have the same hacker cred as bugs in Adobe Flash, for example, but nonetheless, that does not diminish their value, nor does that mean they should be ignored.

Microsoft patched a critical flaw in the application framework on Tuesday, and researchers at Kaspersky Lab's Global Research and Analysis Team caution that while exploits have been used in limited targeted attacks—contrary to information in Microsoft's bulletin—it may be a matter of time before attacks go mainstream.

"It's a big deal; Silverlight vulnerabilities don't' come around that often," said Kaspersky Lab researcher Brian Bartholomew. "Exploitation of

Related Posts

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

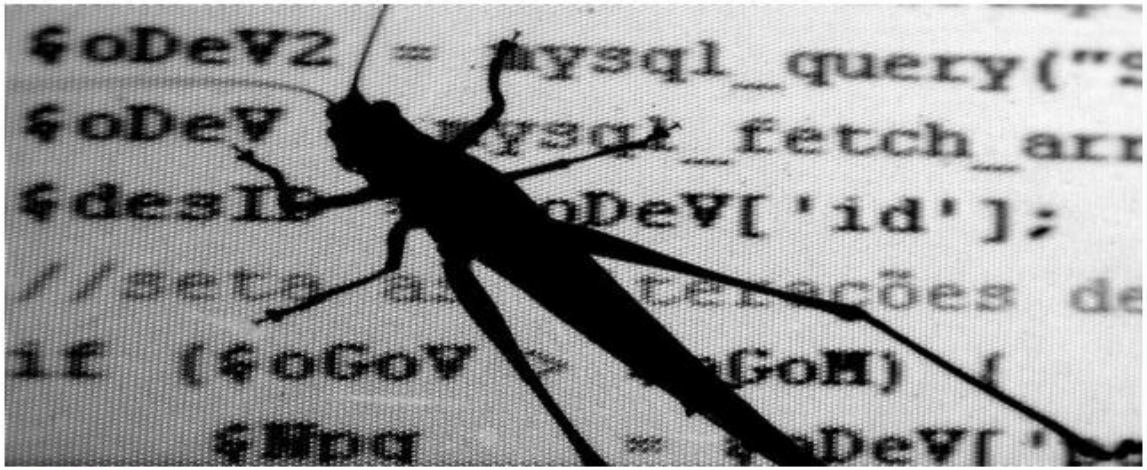
Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor

Bug that can leak crypto keys just fixed in widely used OpenSSH

Vulnerability allows malicious servers to read memory on connecting computers.

by Dan Goodin Jan 14, 2016 12:24pm EST



Guilherme Tavares

A critical bug that can leak secret cryptographic keys has just just been fixed in OpenSSH, one of the more widely used implementations of the secure shell (SSH) protocol.

The vulnerability resides only in the version end users use to connect to servers and not in versions used by servers. A maliciously configured server could exploit it to obtain the contents of the connecting computer's memory, including the private encryption key used for SSH connections. The bug is the result of code that enables an experimental roaming feature in OpenSSH versions 5.4 to 7.1

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Why the calorie is broken

"I'm kind of pissed at the scientific community for not coming up with something better."

WATCH ARS VIDEO

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the

CISCO PATCHES HARDCODED PASSWORD, DOS VULNERABILITIES IN SOFTWARE, DEVICES

by Chris Brook

January 14, 2016 , 11:15 am

Cisco patched a handful of issues across its software line this week, including two critical vulnerabilities that could lead to the complete compromise of any devices running the software, and a hardcoded password that exists in some access points made by the company.

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor

Linux bug imperils tens of millions of PCs, servers, and Android phones

Vulnerability allows restricted users and apps to gain unfettered root access.

by Dan Goodin Jan 19, 2016 2:16pm EST

amalthya

For almost three years, millions of servers and smaller devices running Linux have been vulnerable to attacks that allow an unprivileged app or user to gain nearly unfettered root access. Major Linux distributors are expected to fix the privilege escalation bug this week, but the difficulty of releasing updates for Android handsets and embedded devices means many people may remain susceptible for months or years.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Why the calorie is broken

"I'm kind of pissed at the scientific community for not coming up with something better."

WATCH ARS VIDEO

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the

by Michael Mimoso Follow @mike_mimoso

January 19, 2016 , 10:02 am

A critical vulnerability in Yahoo Mail that could give attackers complete control of an account was patched two weeks ago.

The flaw was privately disclosed Dec. 26 by Finnish researcher Jouko Pynnonen and patched Jan. 6. Pynnonen earned himself a $10,000 bounty, one of the highest paid out by Yahoo through its HackerOne program.

Pynnonen discovered a stored cross-site scripting vulnerability that allowed him to read or send mail from a compromised account, change settings or redirect messages to an attacker's server. The victim, he said, need only view the email. No other interaction with attachments or links was necessary to exploit the flaw.

Related Posts

Magento Update Addresses XSS, CSRF Vulnerabilities
January 25, 2016 , 4:31 pm

GM Vulnerability Disclosure Program

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

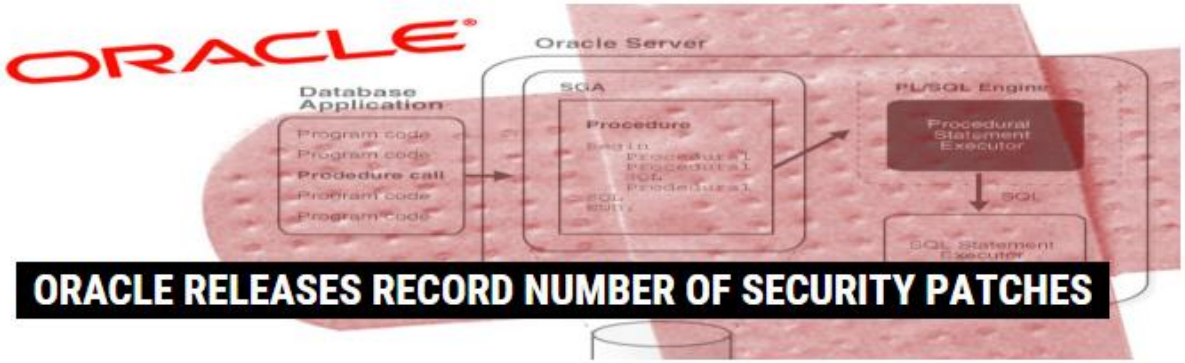
Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor



by Michael Mimoso Follow @mike_mimoso

January 20, 2016 , 2:32 pm

Oracle's quarterly Critical Patch Updates (CPU) are known for their daunting volume, usually a disproportionately big number of fixes that database and system administrators have to deal with every three months. Yesterday's CPU, however, takes the cake.

Oracle pushed out the door a record 248 patches on Tuesday, for vulnerabilities across its product lines. That number shatters the previous high of 193 last July, which was the first time the CPU inched toward 200. By comparison, the last update of 2015, in October, was a meager 154 patches.

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor

by Michael Mimoso Follow @mike_mimoso

January 25, 2016 , 12:13 pm

FreeBSD has patched a denial-of-service vulnerability affecting versions configured to support SCTP and IPv6, the default configurations on later version of the open source OS.

Researchers at Positive Technologies in the U.K. said versions 9.3, 10.1 and 10.2 are affected and can be exploited by a specially crafted ICMPv6 packet, which will cause a kernel panic; kernel panics are the UNIX equivalent of a Windows Blue Screen of Death.

An advisory from FreeBSD says kernels compiled without support for SCTP or IPv6 are not

Related Posts

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor

by Michael Mimoso Follow @mike_mimoso

January 25, 2016 , 12:59 pm

OpenSSL is scheduled to update two versions of the software this week, patching a pair of vulnerabilities in the process.

The OpenSSL project this morning said the updates will move users to versions 1.0.2f and 1.0.1r and should be available Thursday between 8 a.m. and noon Eastern time.

"They will fix two security defects, one of 'high' severity affecting 1.0.2 releases, and one 'low' severity affecting all releases," OpenSSL said in its advisory.

Related Posts

Government Agencies Audit for Juniper Backdoor

Top Stories

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47
December 2, 2015 , 11:18 am

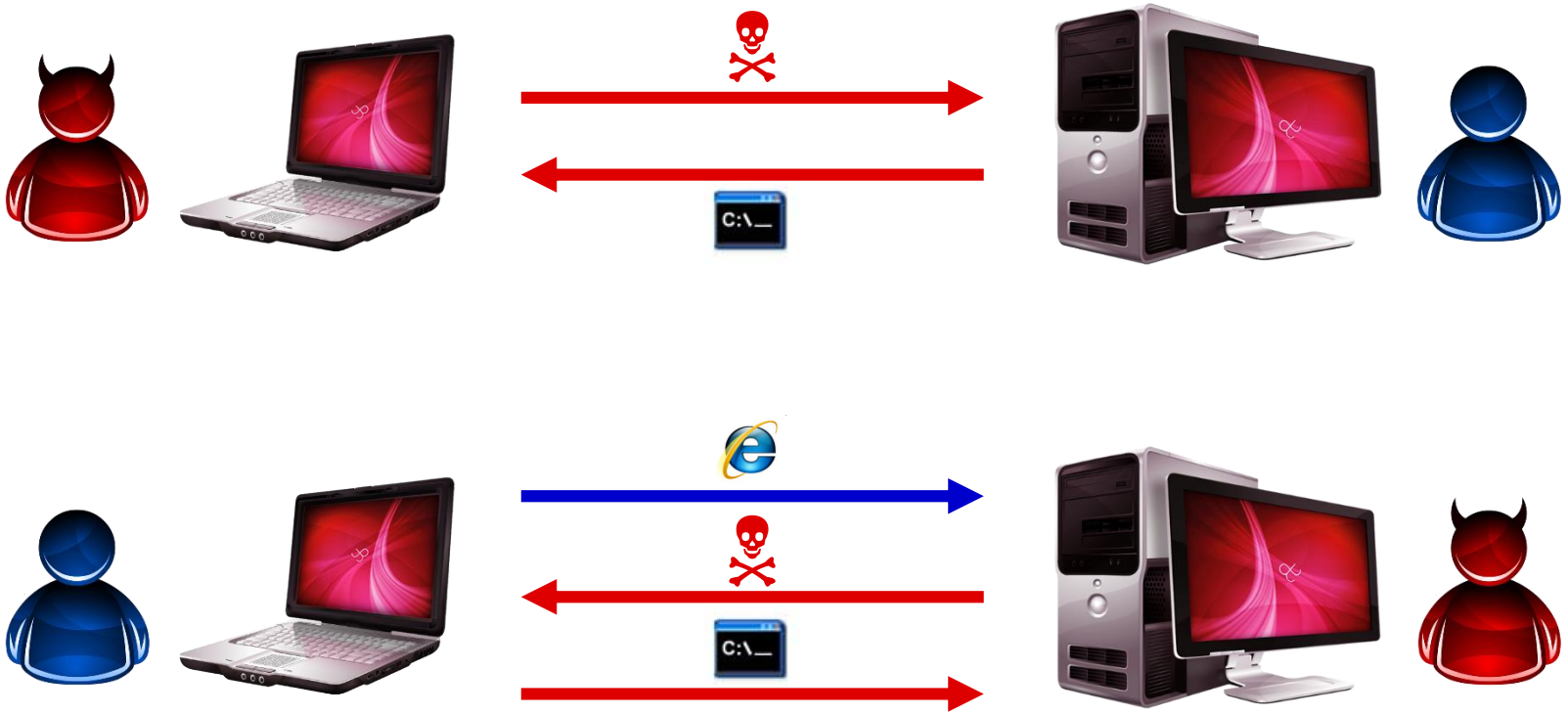
Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices
January 14, 2016 , 11:15 am

Time Warner Cable Urges 320,000 Customers to Change Passwords
January 7, 2016 , 1:54 pm

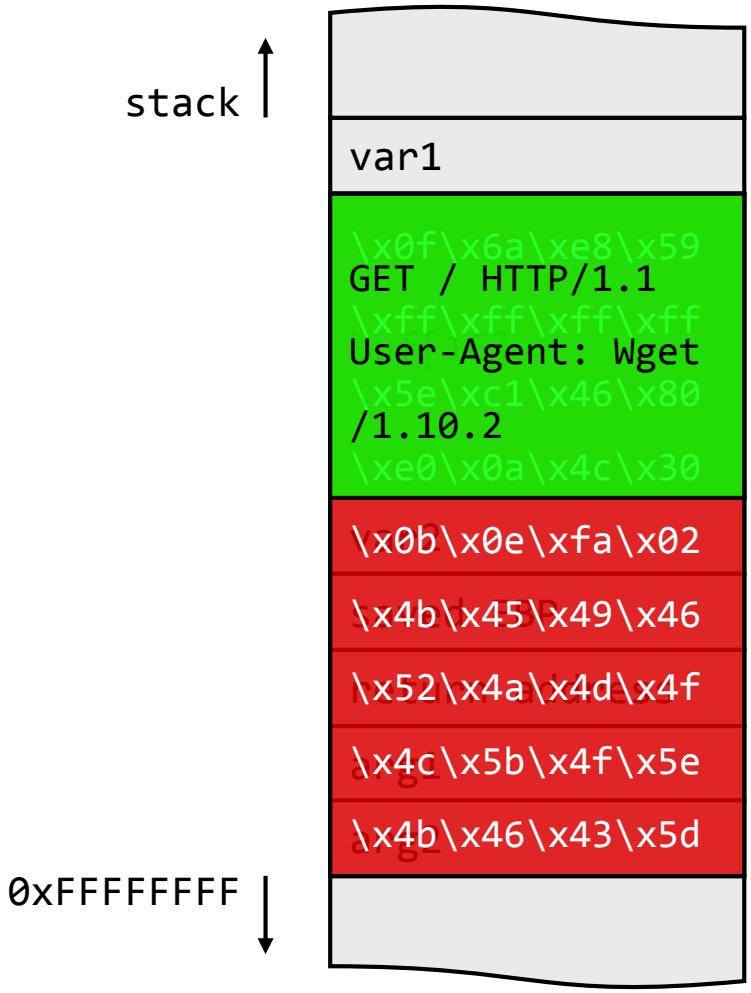
Denial-of-Service Flaw Patched in DHCP
January 13, 2016 , 10:00 am

Inexpensive Webcam Turned into Backdoor

Remote Exploitation: Server-side vs. Client-side



(Very Simple) Buffer Overflow Exploitation



← **Code injection**

Shellcode

spawn shell

listen for connections

add user account

download and execute malware

Malware and Botnets

click fraud

port scanning

extortion

phishing

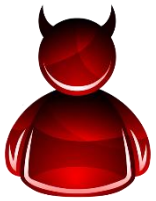
illegal content

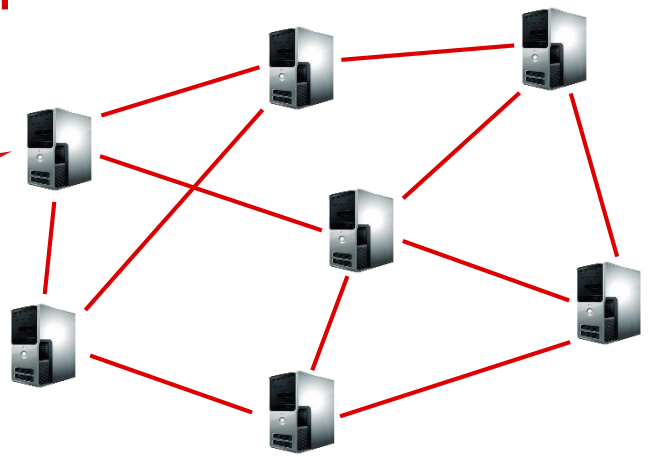
DDoS

code injection

malicious websites

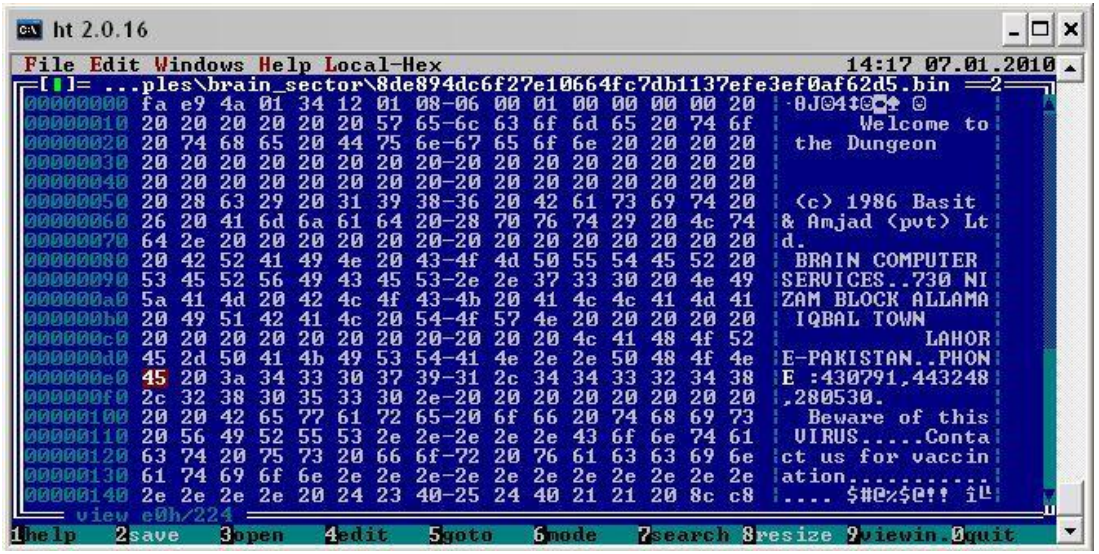
spam





Malicious Software

viruses	*worms*	*rootkits*	*trojan horses*
keyloggers	*logic bombs*	*backdoors*	*downloaders*
droppers	*injectors*	*dialers*	*flooders*
adware	*spyware*	*unwanted software…*	



Malware Characteristics

Code Environment

Machine code (executables, DLLs, drivers, shellcode), higher-level languages/interpreters (VB, macro, JS, Java), shell scripts, …

Attack vector

Request, web page, email, document, USB, …

Infection point

SMM/BIOS, firmware, boot sector, kernel, files, memory-only, …

Propagation strategy

File infection (local disk, remote shares, cloud drives), network scanning, contact/host/peer list, physical access, …

Armoring techniques

Packing, polymorphism, obfuscation, anti-VM/sandbox tricks, anti-debugging tricks, …

Basic Phases of a Typical Targeted Attack

Reconnaissance and information gathering

Exploitation

Privilege Escalation

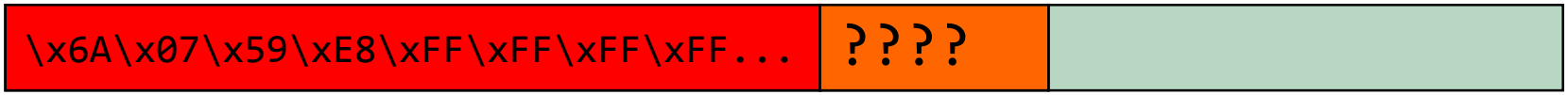
Persistent access

Internal reconnaissance

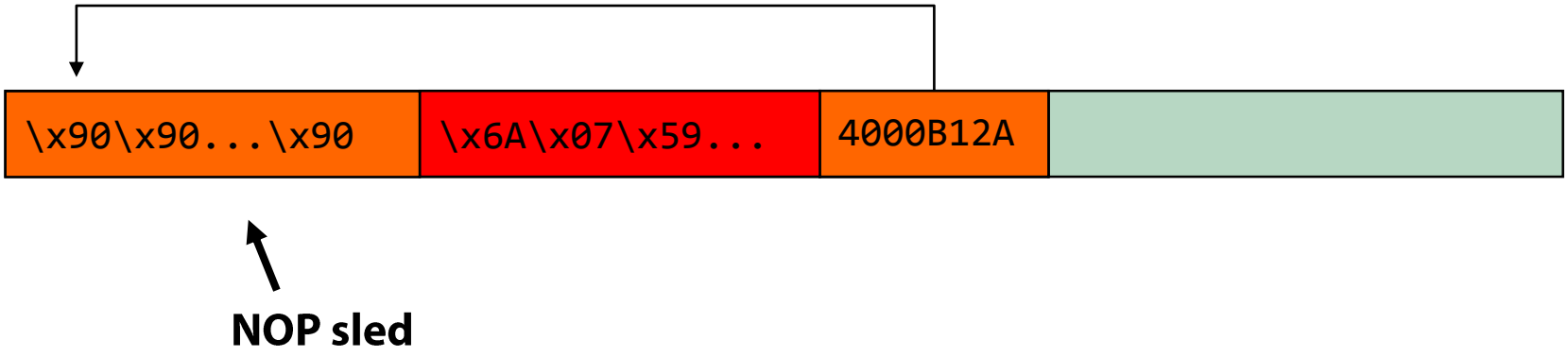
Lateral movement

Data exfiltration/damage/other goal

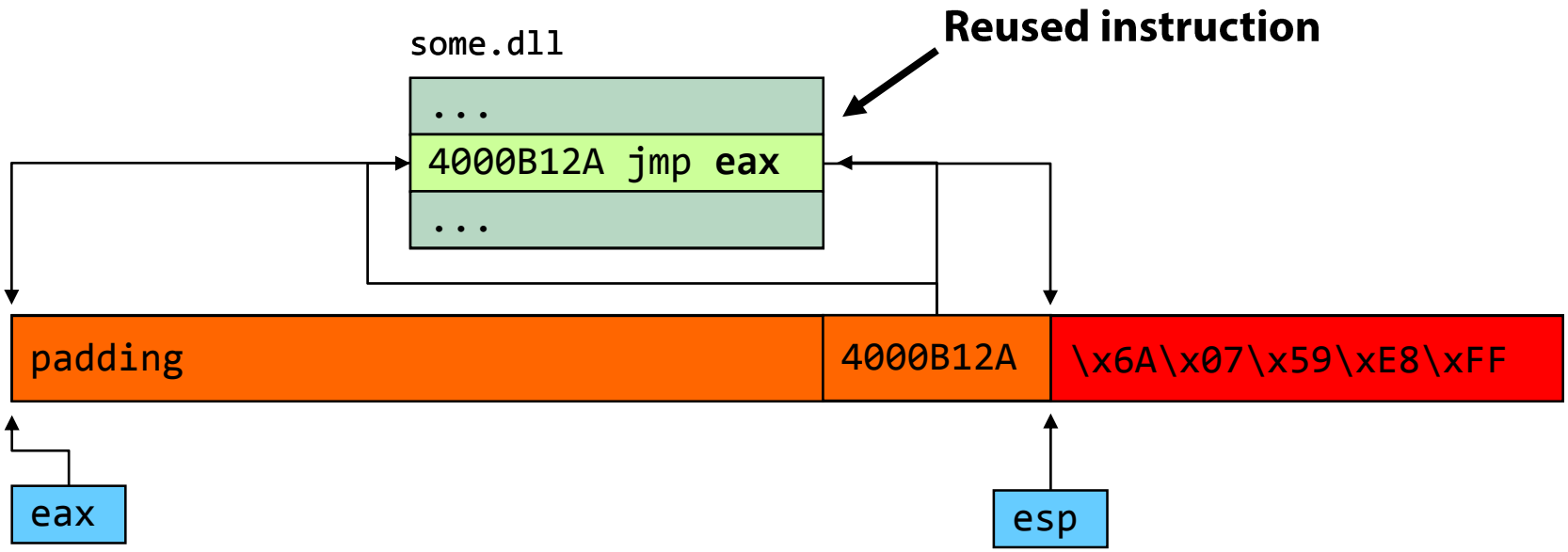
Code Injection



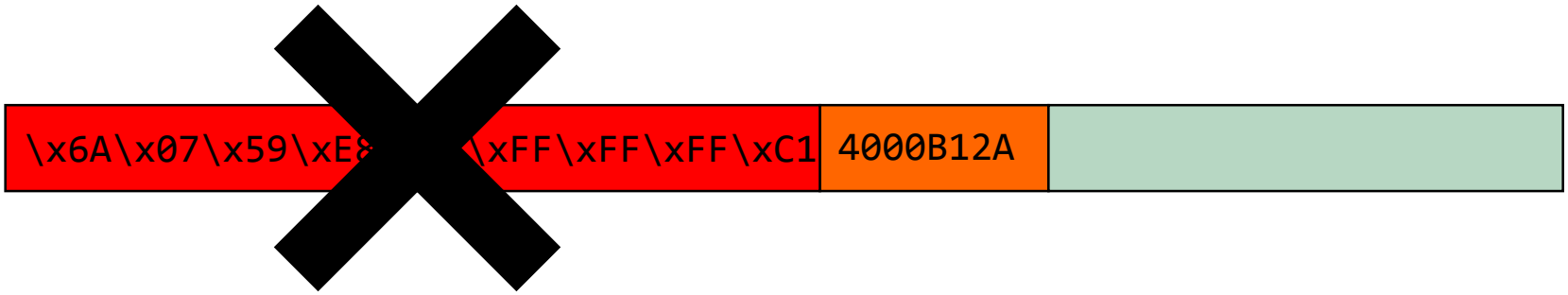
Code Injection



Code Injection



Non-Executable Memory



W^X, PaX, Exec Shield, DEP

x86 support introduced by AMD, followed by Intel

- Pentium 4 (late models)

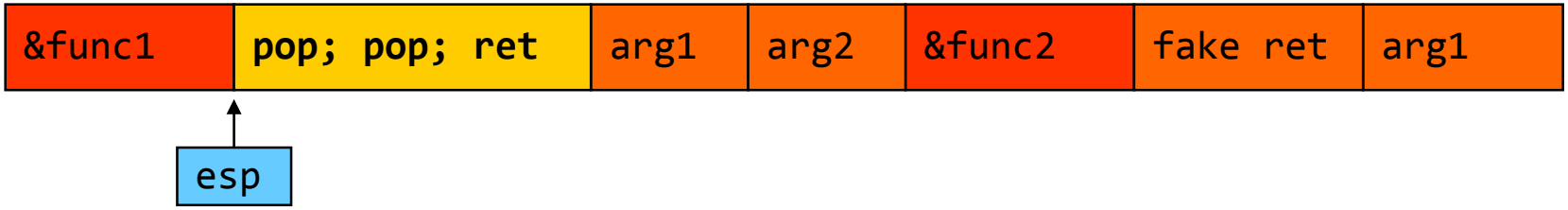
DEP introduced in XP SP2 (hardware-only)

- 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]

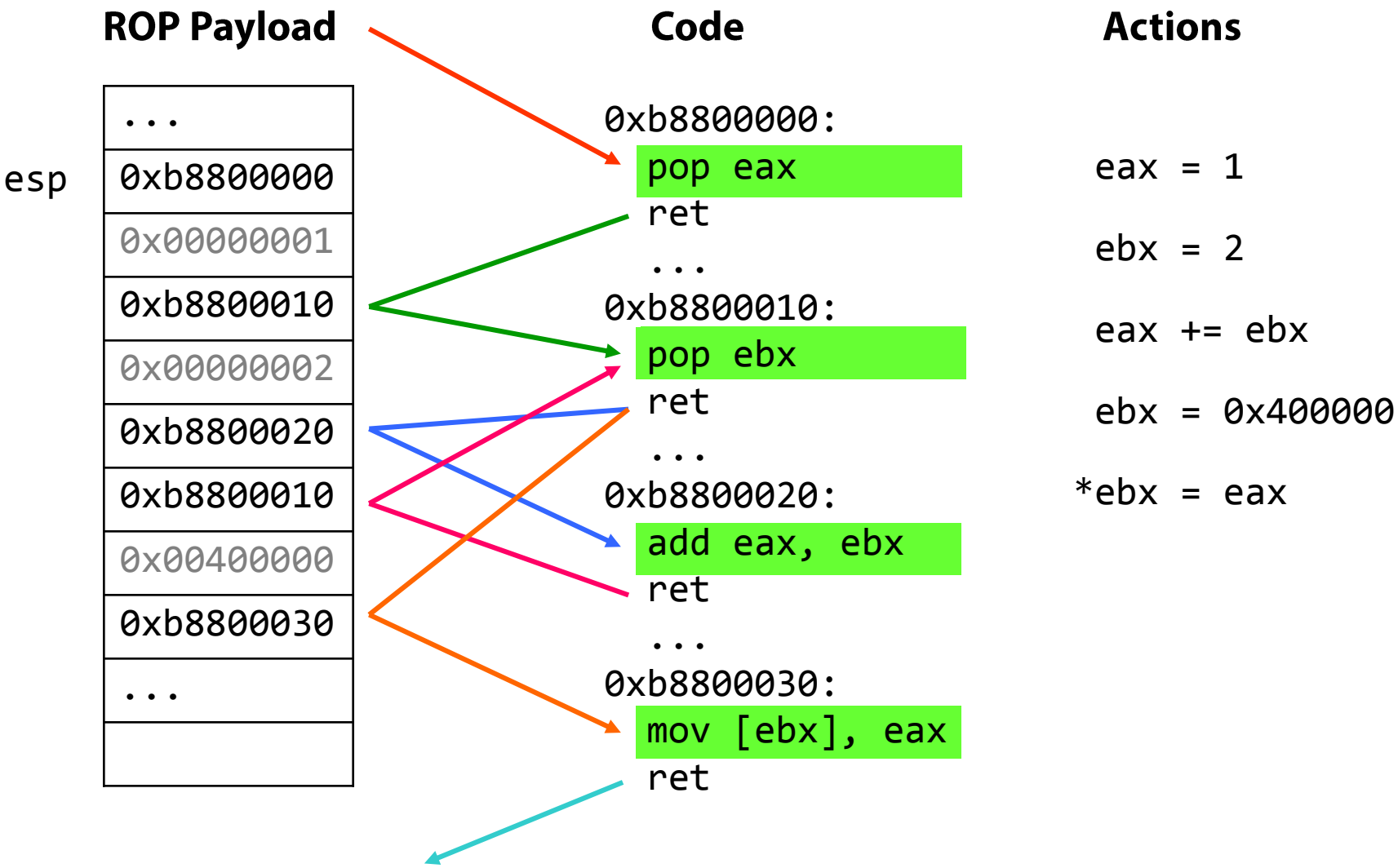
Pass function arguments through registers (IA-64)

```
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

Hinders code reuse attacks by randomizing 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 EMET
- ROP exploit mitigations in Windows 8/8.1
- Control Flow Integrity (Windows 10)

JIT-ROP [Snow '13]

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

Many more threats…

Password Attacks

Information Leakage

Spoofing

Repudiation

Privilege escalation

Information gathering

Session hijacking

Social engineering

Denial of Service

Tampering

Information disclosure

Sniffing

Spoofing

…subject of future lectures