CSE508 Network Security

8/31/2017 **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

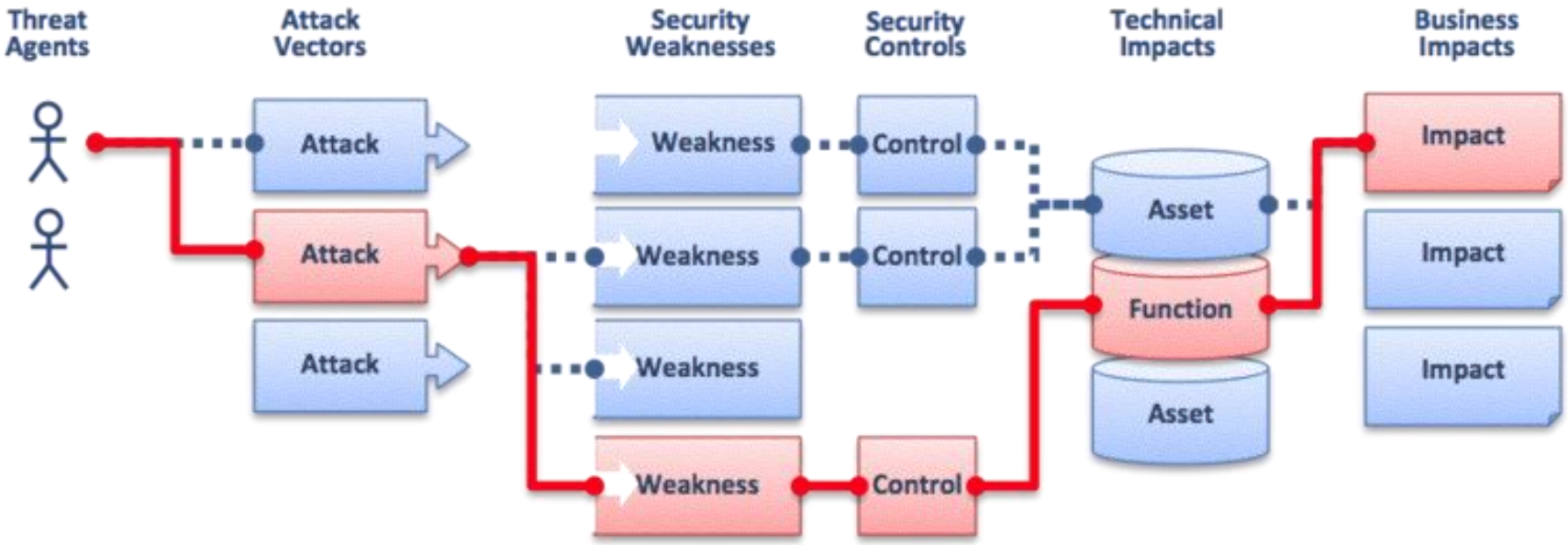
- Different kinds: loss of services, compromise of information or functions , technical failure, …
- Different origins: deliberate, accidental, environmental, …

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

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

- Active vs. passive
- Insider vs. outsider

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

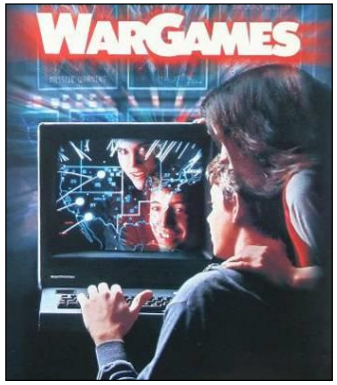
- Prevention
- Detection
- Recovery
- Awareness

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. Instead, 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 (launch exploits), memory (cold boot attacks), storage (just remove it), shoulder surfing (steal credentials), dumpster diving (steal information), bugging (e.g., keylogger, internal components, external antennas/cameras/sensors), …

Remote

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

Intrusion Method

Social engineering (phishing, spam, scareware, …)

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

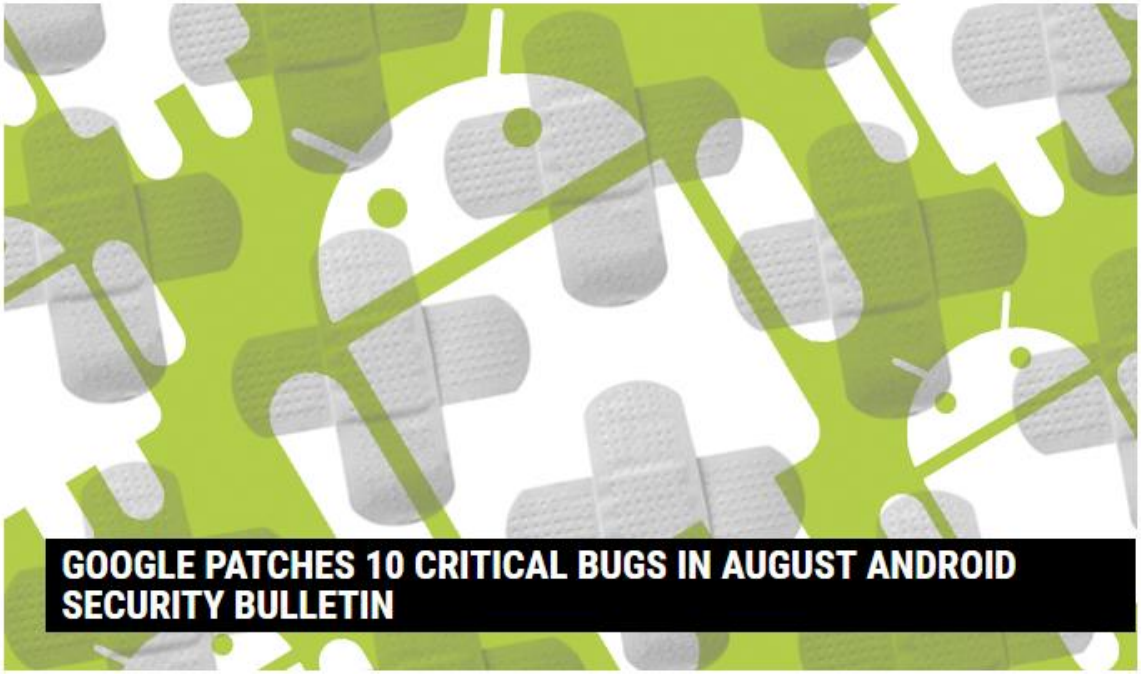
Network traffic interception (access credentials, keys, …)

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

Physical access (reboot, keylogger, screwdriver, …)

Software vulnerability exploitation

Just This Month's News…



by Tom Spring

August 8, 2017 , 8:12 am

Google patched 10 critical remote code execution bugs in its August Android Security Bulletin issued Monday. It warned the most severe RCE vulnerabilities could enable a remote attacker, using a specially crafted file, to execute arbitrary code within the

Top Stories

Business Email Compromise Campaign Harvesting Credentials in Numerous Industries
August 23, 2017 , 1:02 pm

Neptune Exploit Kit Dropping Cryptocurrency Miners Through Malvertisements
August 22, 2017 , 5:51 pm

Deprecated, Insecure Apple Authorization API Can Be Abused to Run Code at Root
August 24, 2017 , 10:32 am

Cryptocurrency Mining Malware Hosted in Amazon S3 Bucket
August 25, 2017 , 10:00 am

Foxit to Fix PDF Reader Zero Days by Friday
August 22, 2017 , 12:33 pm

Industrial Cobots Might Be The Next Big IoT Security Mess
August 22, 2017 , 8:00 am

MICROSOFT PATCHES CRITICAL WINDOWS SEARCH VULNERABILITY

by Tom Spring

August 8, 2017 , 5:21 pm

Microsoft patched more than two dozen remote code execution vulnerabilities today, many of them rated critical. One was a RCE bug that allowed an attacker to take complete control of a server or workstation via Windows Search.

Top Stories

CEOs Resign from Trump's Cybersecurity Commission
August 28, 2017 , 4:50 pm

Business Email Compromise Campaign Harvesting Credentials in Numerous Industries
August 23, 2017 , 1:02 pm

Neptune Exploit Kit Dropping Cryptocurrency Miners Through Malvertisements
August 22, 2017 , 5:51 pm

Mobile WireX DDoS Botnet 'Neutralized' by Collaboration of Competitors
August 28, 2017 , 3:44 pm

Deprecated, Insecure Apple Authorization API Can Be Abused to Run Code at Root
August 24, 2017 , 10:32 am

Cryptocurrency Mining Malware Hosted in Amazon S3 Bucket
August 25, 2017 , 10:00 am

JUNIPER ISSUES SECURITY ALERT TIED TO ROUTERS AND SWITCHES

by Tom Spring

August 10, 2017 , 1:56 pm

Juniper Networks warned customers Thursday of a high-risk vulnerability in the GD graphics library that could allow a remote attacker to take control of systems running certain versions of the Junos OS.

Top Stories

CEOs Resign from Trump's Cybersecurity Commission
August 28, 2017 , 4:50 pm

Business Email Compromise Campaign Harvesting Credentials in Numerous Industries
August 23, 2017 , 1:02 pm

Neptune Exploit Kit Dropping Cryptocurrency Miners Through Malvertisements
August 22, 2017 , 5:51 pm

Mobile WireX DDoS Botnet 'Neutralized' by Collaboration of Competitors
August 28, 2017 , 3:44 pm

Deprecated, Insecure Apple Authorization API Can Be Abused to Run Code at Root
August 24, 2017 , 10:32 am

Cryptocurrency Mining Malware Hosted in Amazon S3 Bucket
August 25, 2017 , 10:00 am

NEPTUNE EXPLOIT KIT DROPPING CRYPTOCURRENCY MINERS THROUGH MALVERTISEMENTS

by Chris Brook

August 22, 2017 , 5:51 pm

Despite a marked decrease in activity, exploit kits haven't completely disappeared just yet. The Neptune, or Terror Exploit Kit, is alive and well; during the last month, researchers have observed the kit as part of a campaign to abuse a legitimate popup ad service to drop cryptocurrency miners.

Researchers with FireEye said Tuesday the kit has been redirecting victims with popups from fake hiking ads to exploit kit landing pages and in turn to HTML and Adobe Flash exploits. Researchers elected not to disclose the name of the popup ad service, but stressed that it's within Alexa's top 100.

The landing pages run a handful of exploits, including three targeting Internet Explorer (CVE-

Related Posts

Top Stories

CEOs Resign from Trump's Cybersecurity Commission
August 28, 2017 , 4:50 pm

Business Email Compromise Campaign Harvesting Credentials in Numerous Industries
August 23, 2017 , 1:02 pm

Neptune Exploit Kit Dropping Cryptocurrency Miners Through Malvertisements
August 22, 2017 , 5:51 pm

Mobile WireX DDoS Botnet 'Neutralized' by Collaboration of Competitors
August 28, 2017 , 3:44 pm

Deprecated, Insecure Apple Authorization API Can Be Abused to Run Code at Root
August 24, 2017 , 10:32 am

Cryptocurrency Mining Malware Hosted in Amazon S3 Bucket
August 25, 2017 , 10:00 am

APT28 USING ETERNALBLUE TO ATTACK HOTELS IN EUROPE, MIDDLE EAST

by Tom Spring

August 12, 2017 , 8:00 am

Russian-speaking cyberespionage group APT28, also known as Sofacy, is believed to be behind a series of attacks last month against travelers staying in hotels in Europe and the Middle East. APT28 notably used the NSA hacking tool EternalBlue as part of its scheme to steal credentials from business travelers, according to a report released Friday by security firm FireEye.

One of the goals of the attack is to trick guests to download a malicious document masquerading as a hotel reservation form that, if opened and macros are enabled, installs a dropper file that ultimately downloads malware called Gamefish. Gamefish establishes a foothold in targeted systems as a way to install the open source tool called Responder, according to FireEye.

"Once inside the network of a hospitality company, APT28 sought out machines that controlled both guest and internal Wi-Fi networks," wrote authors of the report Lindsay Smith and Benjamin Read,

Related Posts

Adware Spreading Via Social Engineering, Facebook Messenger

Top Stories

Business Email Compromise Campaign Harvesting Credentials in Numerous Industries
August 23, 2017 , 1:02 pm

Neptune Exploit Kit Dropping Cryptocurrency Miners Through Malvertisements
August 22, 2017 , 5:51 pm

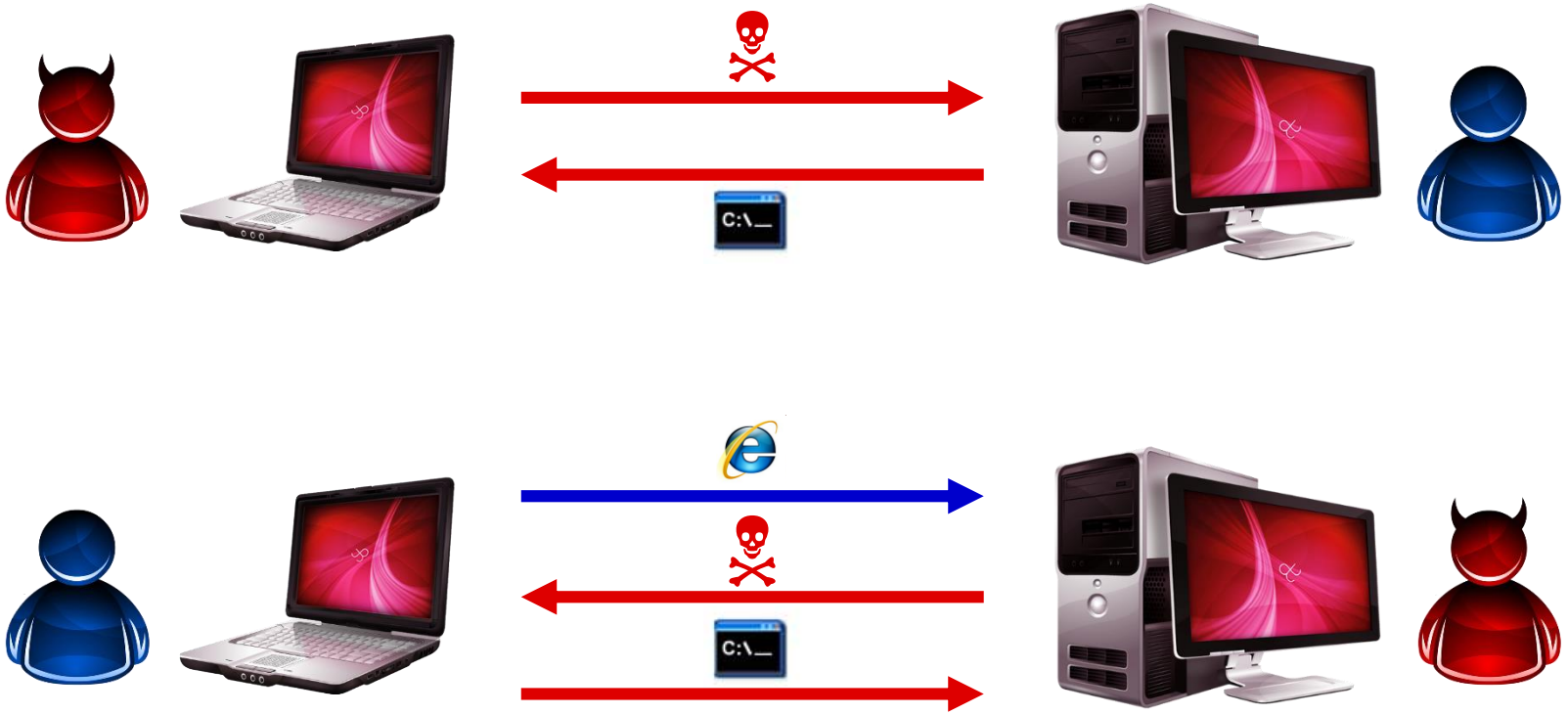
Deprecated, Insecure Apple Authorization API Can Be Abused to Run Code at Root
August 24, 2017 , 10:32 am

Cryptocurrency Mining Malware Hosted in Amazon S3 Bucket
August 25, 2017 , 10:00 am

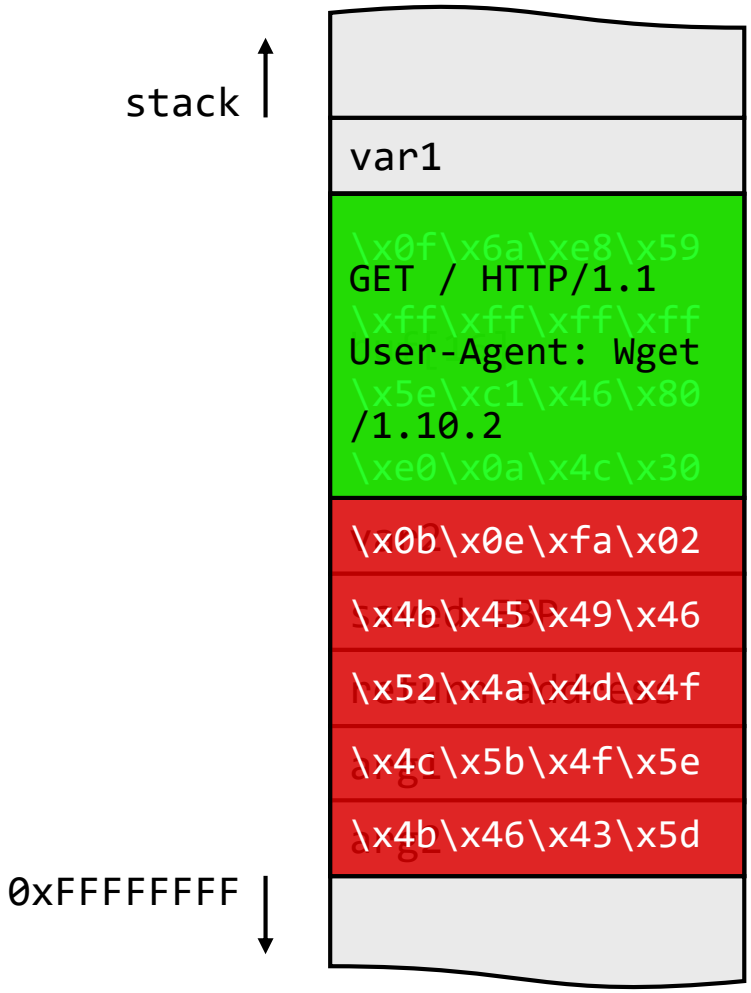
Foxit to Fix PDF Reader Zero Days by Friday
August 22, 2017 , 12:33 pm

Anonymous Messaging App Sarahah to Halt Collection of User Data With Next Update
August 28, 2017 , 1:27 pm

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

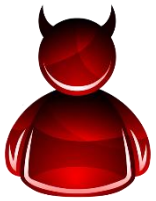
illegal content

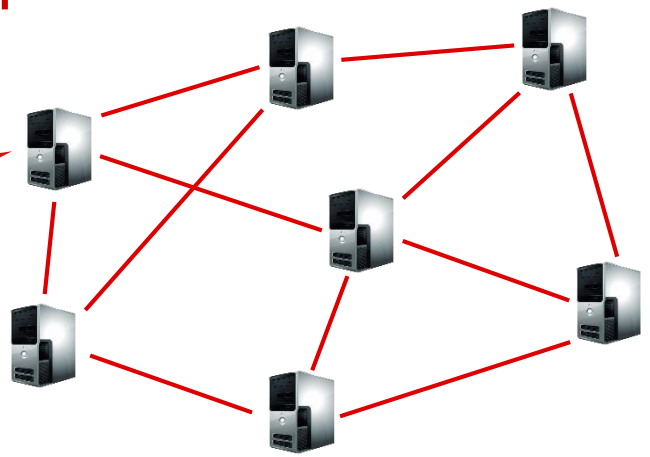
DDoS

code injection

malicious websites

spam





Basic Phases of a Typical Targeted Attack

Reconnaissance and information gathering

Exploitation

Privilege Escalation

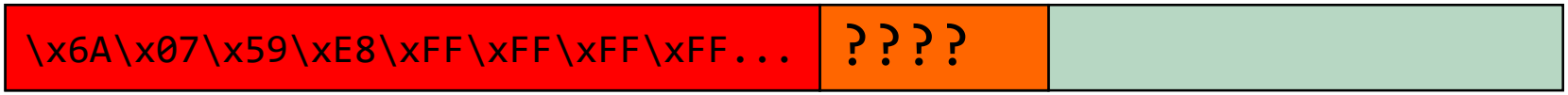
Persistent access

Internal reconnaissance

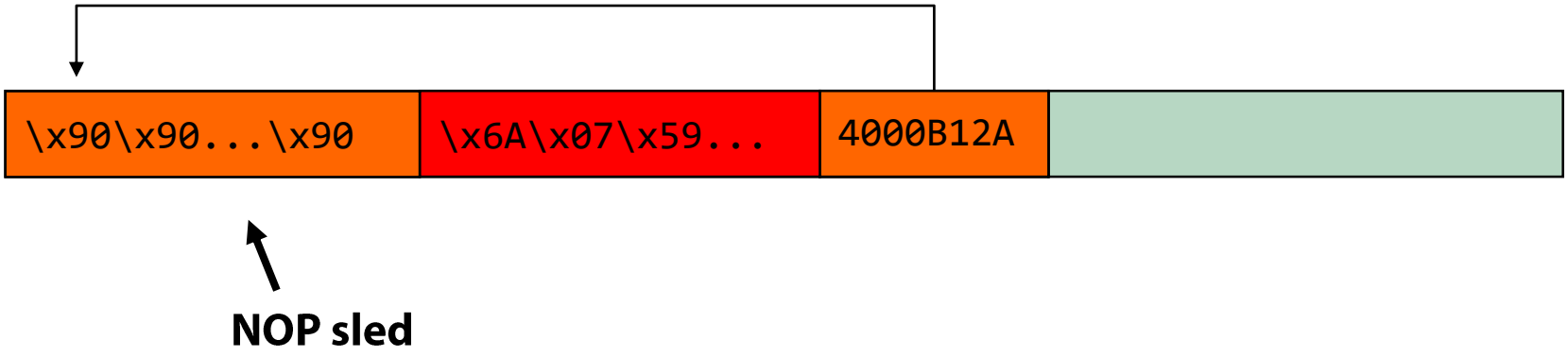
Lateral movement

Data exfiltration/damage/other goal

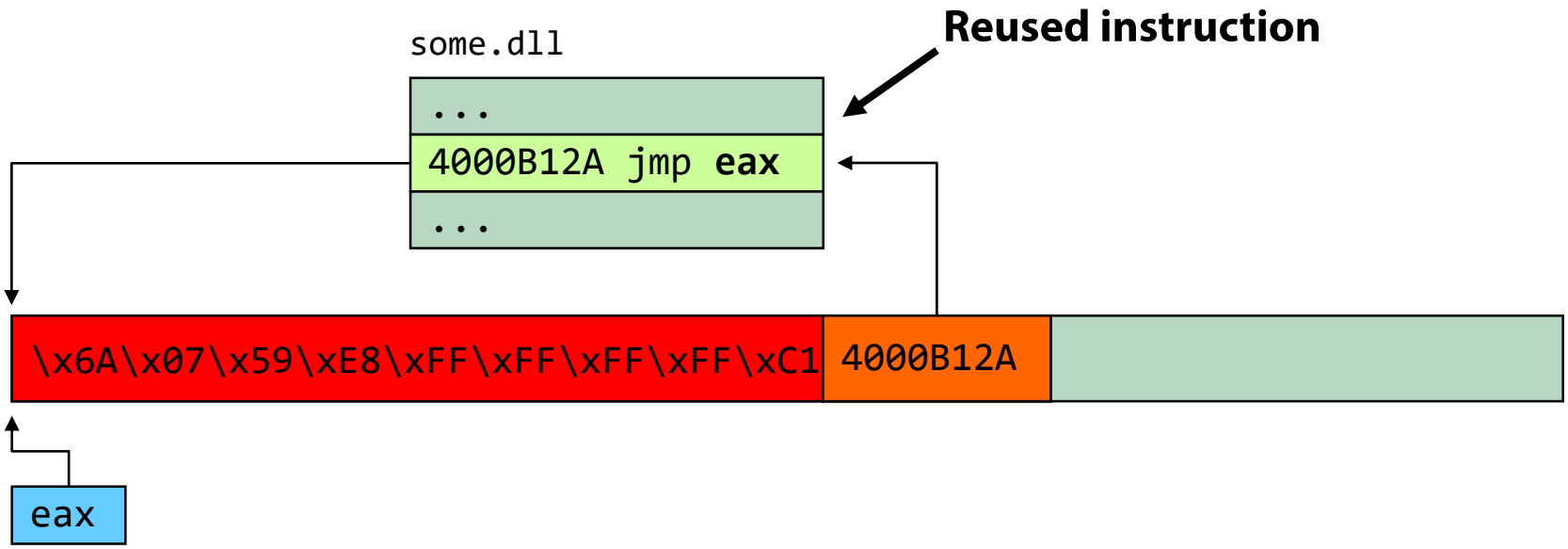
Code Injection



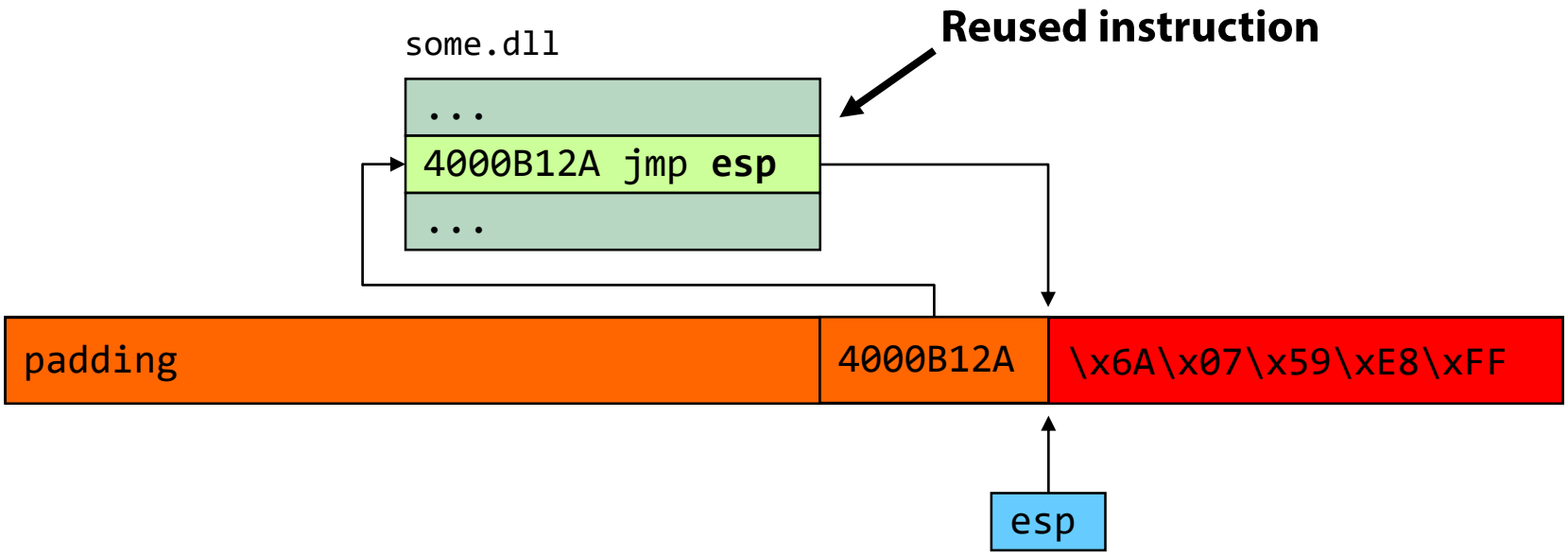
Code Injection



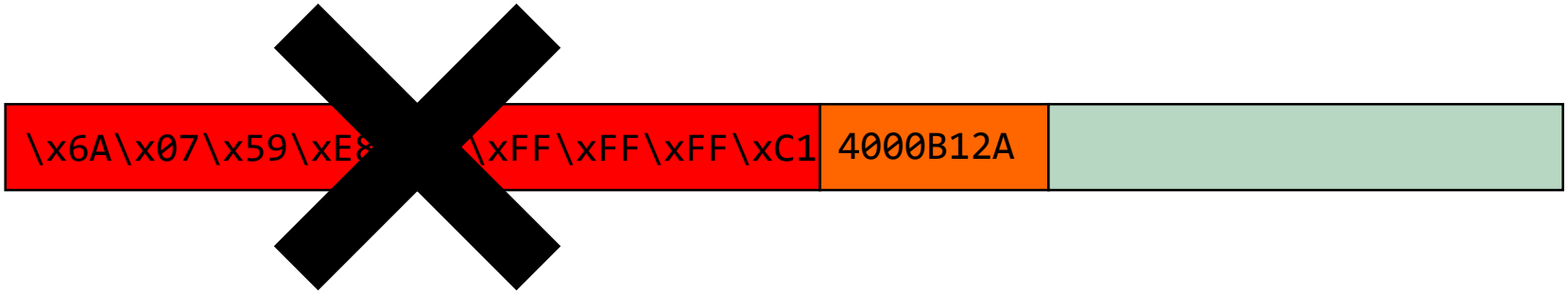
Code Injection



Code Injection



Non-Executable Memory



W^X, PaX, Exec Shield, DEP

x86 support introduced by AMD, followed by Intel

- Pentium 4 (late models)

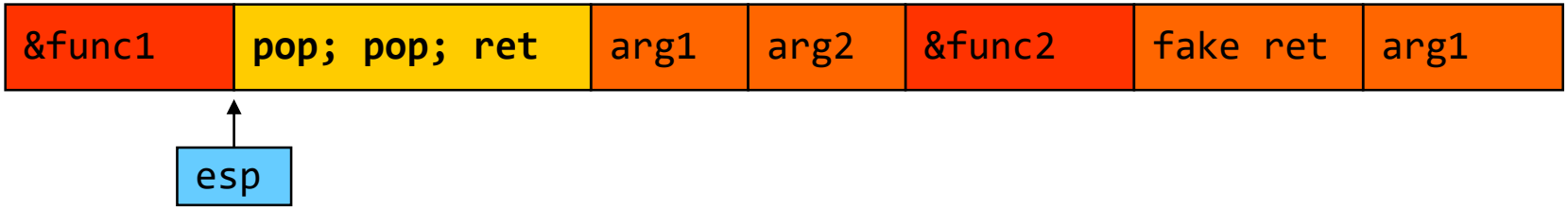
DEP introduced in XP SP2 (hardware-only)

- 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)

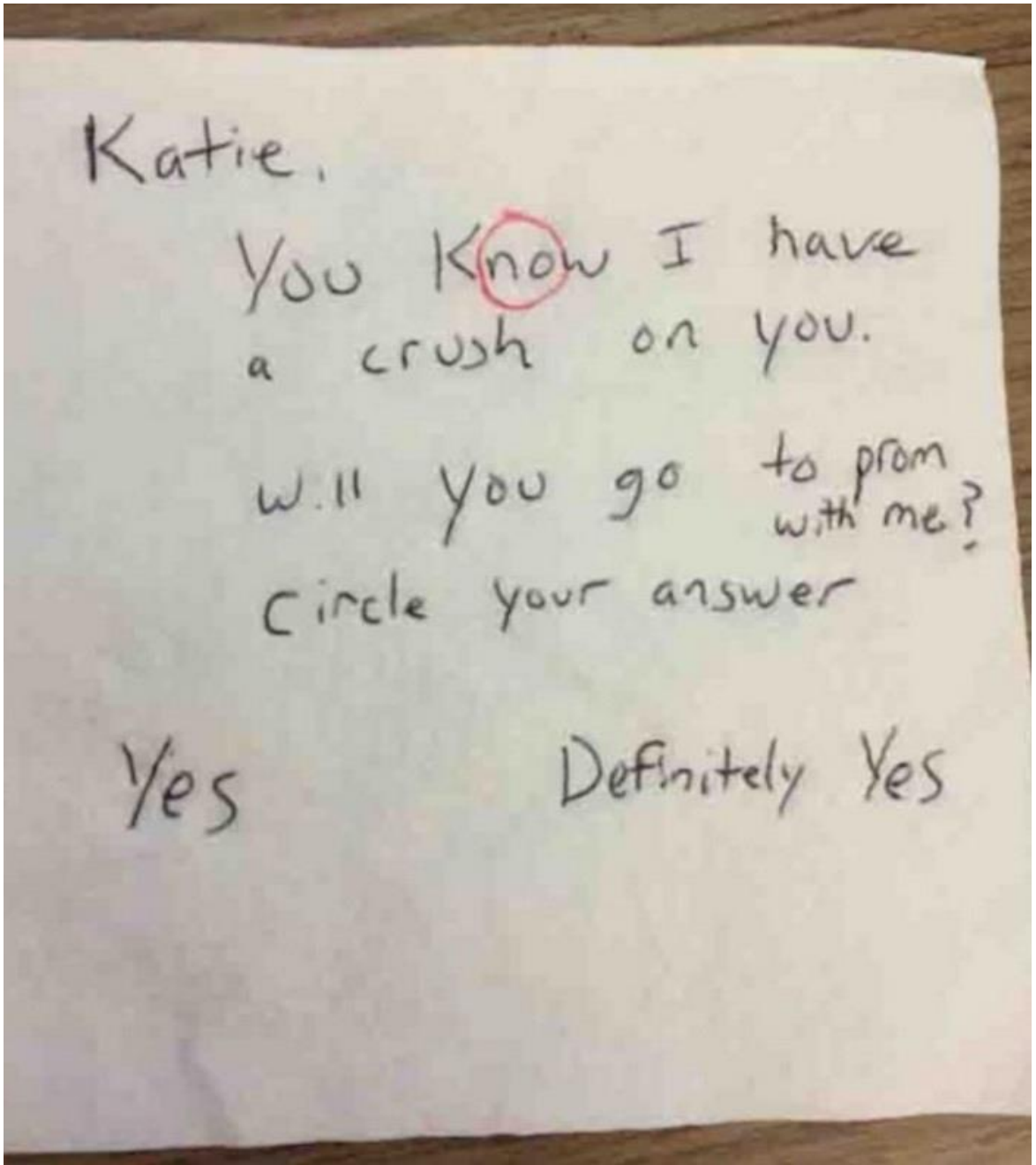
```
0x0000000000400a82:   pop %rbx
0x0000000000400a83:   retq

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

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

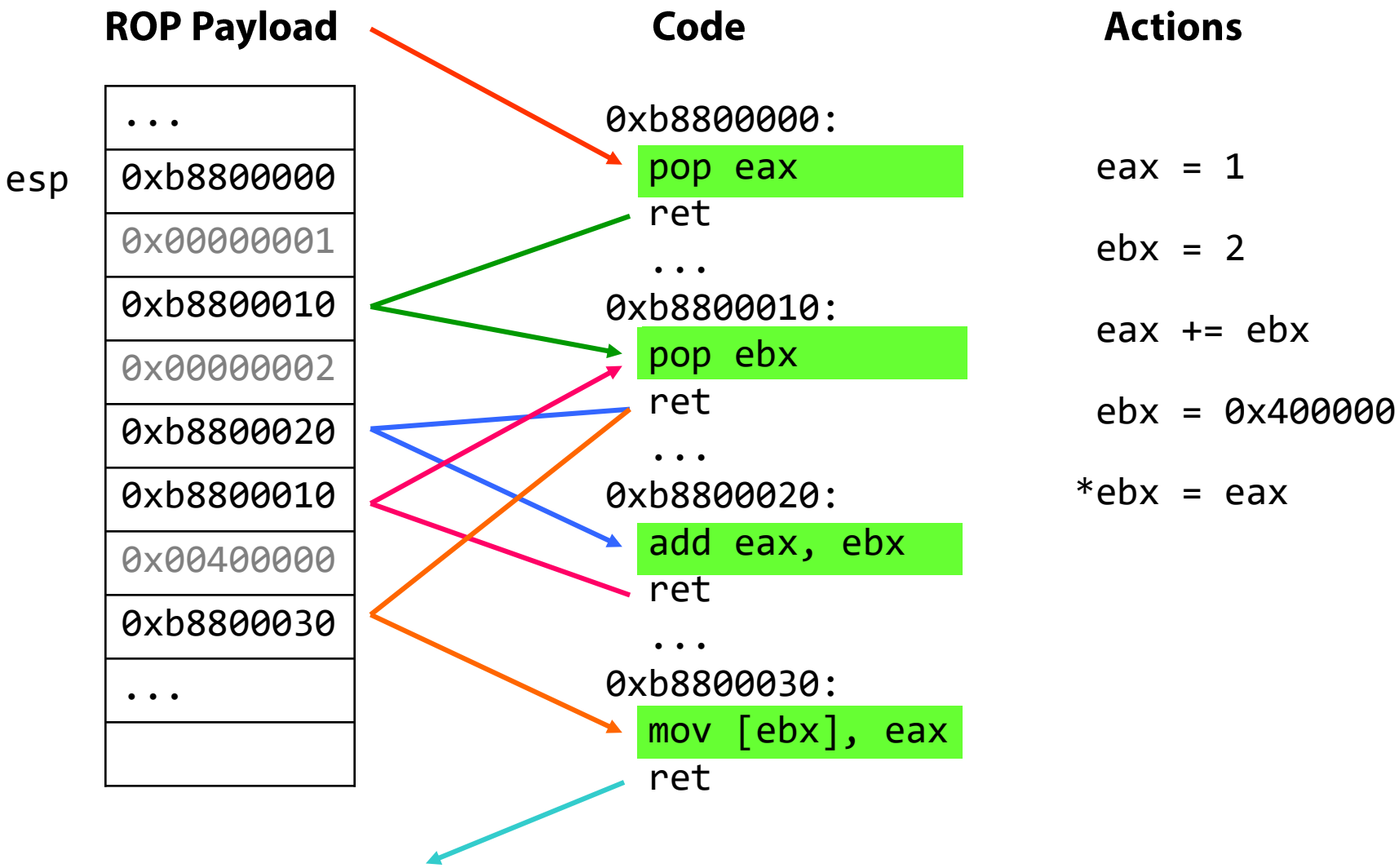
Return-oriented programming [Shacham '07]

Turing-complete return-oriented "shellcode"

Jump-oriented programming [Shacham '10]

ROP


Katie.
You Know I have a crush on you.
will you go to prom with me?
Circle your answer
Yes
Definitely Yes


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

Some applications still don't use ASLR

- Legacy code, compatibility issues, …

Even ASLR-enabled applications sometimes have statically mapped DLLs

- EMET forced randomization

Information leaks break ASLR

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

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

- ROP exploit mitigations in Windows 8/8.1/10
- 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