Software Security and Exploitation
CSCI 1650
Software Security and Exploitation
CSCI 1650

Focus: Memory Safety
Software Security and Exploitation
CSCI 1650

Focus: Memory Safety

Exploitation (offense)  Security (defense)
Software Security and Exploitation
CSCI 1650

Focus: Memory Safety

Exploitation (Offense)

Code Injection
- NOP sled
- jmp %esi
- register spry
- NULL-free shellcode
- alnum
- polymorphic
- egghunter
- multi-stage

Security (Defense)
Exploitation (offense)

- code reuse
  - ret2libc
  - ROP
  - JIT-ROP
  - ...
  - %esp lifting
  - chaining

- NOP
- COP
- BROP
- COOP
- COOP
- P1ROP
- Speculative CR
Software Security and Exploitation
CSCI 1650

Focus: memory safety

Exploitation (offense)
- Code injection
  - NOP sled
  - jmp %esp
  - register spilling
  - NULL-free shellcode
  - album -11-
  - polymorphic -11-
  - ELFhunter -11-
  - multi-stage -11-

Security (defense)
- Non-executable memory
  - br w^x
- AS-DQ
  - partial
  - full
Exploitation (Offense)

- code reuse
  - ret2libc
  - ROP
  - JIT-ROP
  - %esp lifting
  - chaining.

- NOP
  - COP
  - BROP
  - COOP

- PIROP
  - Speculative CR

Security (Defense)

- Stack canaries
  - SSP

- RELRO
  - BINDnow

- FORTIFY_SOURCE
  - z1
  - z2

- CFI
- PAC
- diversification
- XOM
- micro-architectural hardening.
Theme: Control-flow Hijacking
Theme: Control-flow Hijacking

Other topics:
- DOP
- BOP
- CFI-resistant C++
- Heap exploitation
- C++ exploitation
- Kernel exploitation
- Jailbreaking
- Data-only attacks
SW-based micro-architectural attacks
  
  code-based side-channel attacks
  
  Meltdown/Spectre
  
  Foreshadow/Foreshadow-NG
  
  Fallout/ROPL/Zombieload
  
  Row Hammer
  
  CLKSAW
  
  PlunderVolt
Memory safety violation

Code/Data
Ptr. corruption

Control-flow hijacking

Arbitrary computation(s)

Code injection
Code reuse
mem safety violation

fuzzing
programming testing

symbolic methods
- symbolic execution
- abstract interpretation

spatial errors

control-flow hijacking

code injection

core reuse

arbitrary computation(s)

Morris Worm (11/18/88) stack
+ buffer overflow in finger
  + Sendmail trojan (DEBUC)
  + DEC VAX (4BSD), Sun-3 (SunOS)
  + Look - 104 (OS G40)
  + 26k Unix machines got infected.
  + 210% of the total "Internet"
  + 1st felony conviction under the Computer Fraud and Abuse Act.

DARPA -> CERT/CC

Soldier (05/2001) stack (brute force)
+ buffer overflow in Sendmail
  + Solaris/SunOS
  + access control bypass in NSS

Mass website defacement
+ spam OS messages
Code Red (07/2001) -> stack buffer overflow in IIS
360k infections in a single day!
& mess website defacement

Nimda (08/2001)
open network shares, email, ...

Slammer (01/2003) -> stack cheap buffer overflow in SQL server / MSDE 2000
75k infections in 1 hour!

Blaster (08/2003) -> stack DCOM RPC buffer overflow exploit reverse-engineered from the patch
DDoS on www.supefile.com
Weldia
Sasser (04/2003)  stack

Buffer overflow in LSASS

AFP, Delta Air Lines, Sampo Bank, British Coastguard, Goldman Sachs, Pentecost Post, European Commission, Lund University Hospital (X-rays), University of Missouri, ...

Conficker (11/2008)  stack

Buffer overflow in NetBIOS

32M - 15M infections

Botnet? (+ self-defense)

Freudl Navy, UK Ministry of Defense, Sheffield Hospital, German Bundeswehr, Norwegian Police...
Stuxnet (06/2010)

- Cyber weapon (~2005) vs. Israel
- SCADA/PLC
- Function pointer overwrite in Windows
- Access control bypass in Print Spooler
- Unauthorized direct code execution

- ~200k/1k PLCs hosts
  - 58% in Iran
- Kernel-mode rootkit
  - Signed driver
  - 2 compromised certificates
  - Man-in-the-middle step
Dogu (08/2011)
- Memory corruption
- Code "similar" to Stuxnet
- Intelligence gathering

Flame (05/2012)
- Cyber espionage
- Most sophisticated piece of malware at the time
- Targets Middle Eastern countries
  - Access control bypass in Print Spooler
  - Unauthorized direct code execution in Windows Shell
  - Compromised Microsoft Certificate
  - Sign a fake audio driver
Mirai (08/2016)
- Authentication bypass
- IoT devices
- 600k infections
- 1 Tbit/s DDoS attack!

WannaCry (05/2017)
- Integer overflow (kernel)
- Homey00b
- NSA's exploit
- Keep pinging + message
- Code-reuse + code injection
- Ransomware
- ~200k infections
  - UK's NHS
  - Nissan
  - Renault
  - Telefonica
  - FedEx
Thank you 😊