CS 497: Cybersecurity

Galin Zhelezov
Department of Engineering and Computer Science
York College of Pennsylvania

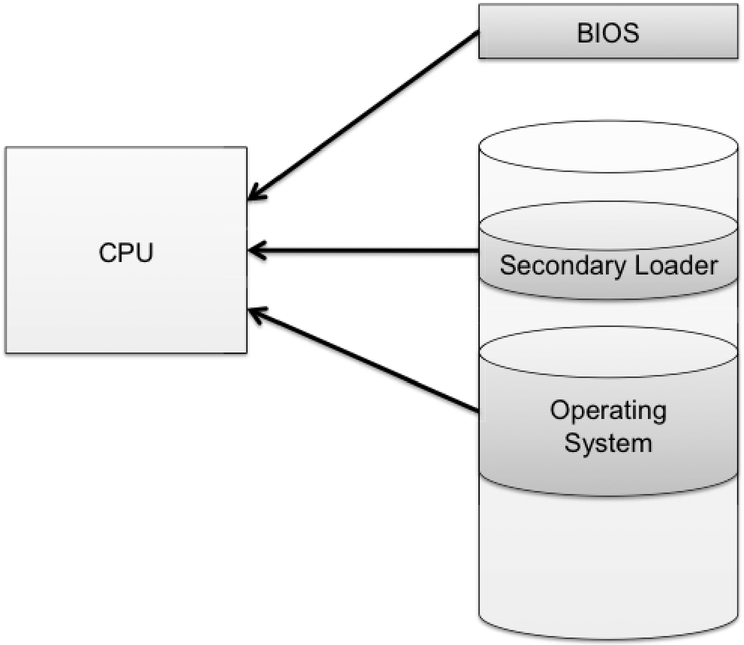
Operating Systems Security

The Boot Sequence

- **The action of loading an operating system into memory from a powered-off state is known as booting or bootstrapping.**

- **When a computer is turned on, it first executes code stored in a firmware component known as the BIOS (basic input/output system).**

- **On modern systems, the BIOS loads into memory the second-stage boot loader, which handles loading the rest of the operating system into memory and then passes control of execution to the operating system.**



BIOS Passwords

- **A malicious user could potentially seize execution of a computer at several points in the boot process.**

- **To prevent an attacker from initiating the first stages of booting, many computers feature a BIOS password that does not allow a second-stage boot loader to be executed without proper authentication.**

Hibernation

- **Modern machines have the ability to go into a powered-off state known as hibernation.**

- **While going into hibernation, the OS stores the contents of machine’s memory into a hibernation file (such as hiberfil.sys) on disk so the computer can be quickly restored later.**

- **But… without additional security precautions, hibernation exposes a machine to potentially invasive forensic investigation.**

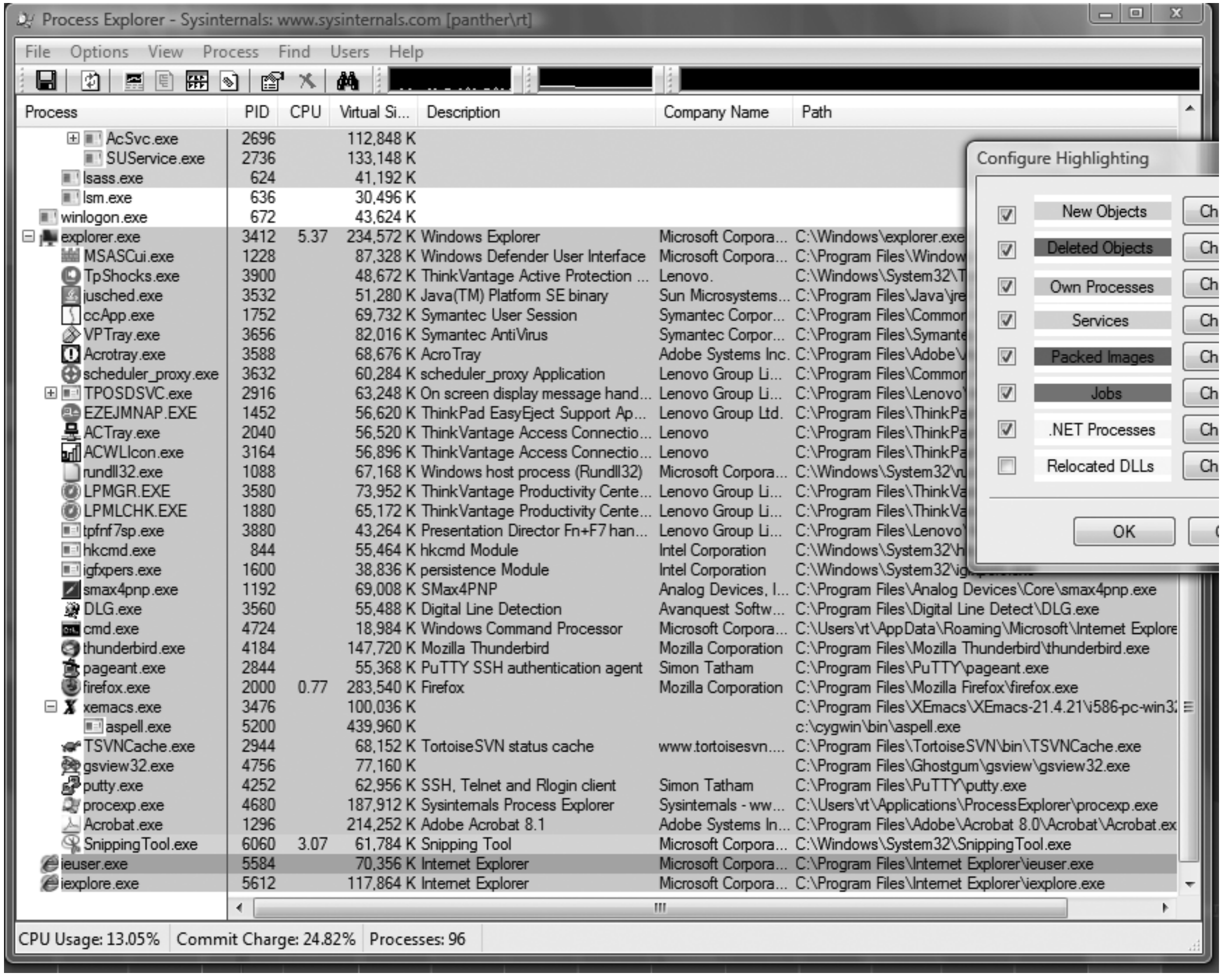
1. User closes a laptop computer,
putting it into hibernation.

2. Attacker copies the hiberfil.sys
file to discover any unencrypted
passwords that were stored
in memory when the computer
was put into hibernation.

Event Logging

- **Keeping track of what processes are running, what other machines have interacted with the system via the Internet, and if the operating system has experienced any unexpected or suspicious behavior can often leave important clues not only for troubleshooting ordinary problems, but also for determining the cause of a security breach.**

Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [panther\rt]

Process	PID	CPU	Virtual Si...	Description	Company Name	Path
⊞ AcSvc.exe	2696		112,848 K			
SUService.exe	2736		133,148 K			
lsass.exe	624		41,192 K			
lsm.exe	636		30,496 K			
winlogon.exe	672		43,624 K			
⊟ explorer.exe	3412	5.37	234,572 K	Windows Explorer	Microsoft Corpora...	C:\Windows\explorer.exe
MSASCui.exe	1228		87,328 K	Windows Defender User Interface	Microsoft Corpora...	C:\Program Files\Window
TpShocks.exe	3900		48,672 K	ThinkVantage Active Protection ...	Lenovo.	C:\Windows\System32\T
jusched.exe	3532		51,280 K	Java(TM) Platform SE binary	Sun Microsystems...	C:\Program Files\Java\jre
ccApp.exe	1752		69,732 K	Symantec User Session	Symantec Corpor...	C:\Program Files\Commor
VPTray.exe	3656		82,016 K	Symantec AntiVirus	Symantec Corpor...	C:\Program Files\Symante
Acrotray.exe	3588		68,676 K	AcroTray	Adobe Systems Inc.	C:\Program Files\Adobe\
scheduler_proxy.exe	3632		60,284 K	scheduler_proxy Application	Lenovo Group Li...	C:\Program Files\Commor
⊞ TPOSDSVC.exe	2916		63,248 K	On screen display message hand...	Lenovo Group Li...	C:\Program Files\Lenovo\
EZEJMNAP.EXE	1452		56,620 K	ThinkPad EasyEject Support Ap...	Lenovo Group Ltd.	C:\Program Files\ThinkPa
ACTray.exe	2040		56,520 K	ThinkVantage Access Connectio...	Lenovo	C:\Program Files\ThinkPa
ACWLIcon.exe	3164		56,896 K	ThinkVantage Access Connectio...	Lenovo	C:\Program Files\ThinkPa
rundll32.exe	1088		67,168 K	Windows host process (Rundll32)	Microsoft Corpora...	C:\Windows\System32\ru
LPMGR.EXE	3580		73,952 K	ThinkVantage Productivity Cente...	Lenovo Group Li...	C:\Program Files\ThinkVa
LPMLCHK.EXE	1880		65,172 K	ThinkVantage Productivity Cente...	Lenovo Group Li...	C:\Program Files\ThinkVa
tpfnf7sp.exe	3880		43,264 K	Presentation Director Fn+F7 han...	Lenovo Group Li...	C:\Program Files\Lenovo\
hkcmd.exe	844		55,464 K	hkcmd Module	Intel Corporation	C:\Windows\System32\h
igfxpers.exe	1600		38,836 K	persistence Module	Intel Corporation	C:\Windows\System32\ig
smax4pnp.exe	1192		69,008 K	SMax4PNP	Analog Devices, I...	C:\Program Files\Analog Devices\Core\smax4pnp.exe
DLG.exe	3560		55,488 K	Digital Line Detection	Avanquest Softw...	C:\Program Files\Digital Line Detect\DLG.exe
cmd.exe	4724		18,984 K	Windows Command Processor	Microsoft Corpora...	C:\Users\rt\AppData\Roaming\Microsoft\Internet Explore
thunderbird.exe	4184		147,720 K	Mozilla Thunderbird	Mozilla Corporation	C:\Program Files\Mozilla Thunderbird\thunderbird.exe
pageant.exe	2844		55,368 K	PuTTY SSH authentication agent	Simon Tatham	C:\Program Files\PuTTY\pageant.exe
firefox.exe	2000	0.77	283,540 K	Firefox	Mozilla Corporation	C:\Program Files\Mozilla Firefox\firefox.exe
⊟ xemacs.exe	3476		100,036 K			C:\Program Files\XEmacs\XEmacs-21.4.21\i586-pc-win3
aspell.exe	5200		439,960 K			c:\cygwin\bin\aspell.exe
TSVNCache.exe	2944		68,152 K	TortoiseSVN status cache	www.tortoisesvn....	C:\Program Files\TortoiseSVN\bin\TSVNCache.exe
gsview32.exe	4756		77,160 K			C:\Program Files\Ghostgum\gsview\gsview32.exe
putty.exe	4252		62,956 K	SSH, Telnet and Rlogin client	Simon Tatham	C:\Program Files\PuTTY\putty.exe
procexp.exe	4680		187,912 K	Sysinternals Process Explorer	Sysinternals - ww...	C:\Users\rt\Applications\ProcessExplorer\procexp.exe
Acrobat.exe	1296		214,252 K	Adobe Acrobat 8.1	Adobe Systems In...	C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrobat.ex
SnippingTool.exe	6060	3.07	61,784 K	Snipping Tool	Microsoft Corpora...	C:\Windows\System32\SnippingTool.exe
ieuser.exe	5584		70,356 K	Internet Explorer	Microsoft Corpora...	C:\Program Files\Internet Explorer\ieuser.exe
iexplore.exe	5612		117,864 K	Internet Explorer	Microsoft Corpora...	C:\Program Files\Internet Explorer\iexplore.exe

CPU Usage: 13.05% | Commit Charge: 24.82% | Processes: 96

Configure Highlighting

- ☑ New Objects
- ☑ Deleted Objects
- ☑ Own Processes
- ☑ Services
- ☑ Packed Images
- ☑ Jobs
- ☑ .NET Processes
- ☐ Relocated DLLs

Memory and Filesystem Security

- The contents of a computer are encapsulated in its memory and filesystem.
- Thus, protection of a computer’s content has to start with the protection of its memory and its filesystem.

Password Security

- **The basic approach to guessing passwords from the password file is to conduct a dictionary attack, where each word in a dictionary is hashed and the resulting value is compared with the hashed passwords stored in the password file.**

- **A dictionary of 500,000 “words” is often enough to discover most passwords.**

Password Salt

- **One way to make the dictionary attack more difficult to launch is to use salt.**

- **Associate a random number with each userid.**

- **Rather than comparing the hash of an entered password with a stored hash of a password, the system compares the hash of an entered password and the salt for the associated userid with a stored hash of the password and salt.**

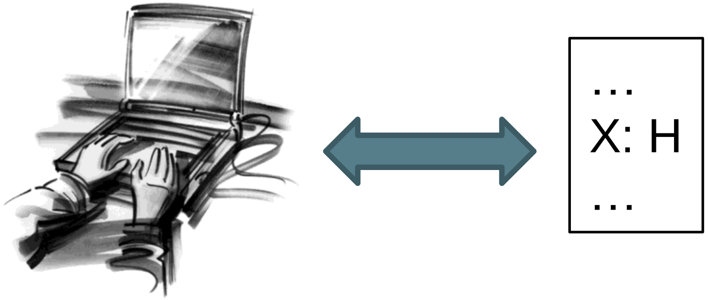
How Password Salt Works

Without salt:

1. User types userid, X, and password, P.

2. System looks up H, the stored hash of X's password.

3. System tests whether h(P) = H.



Password file:

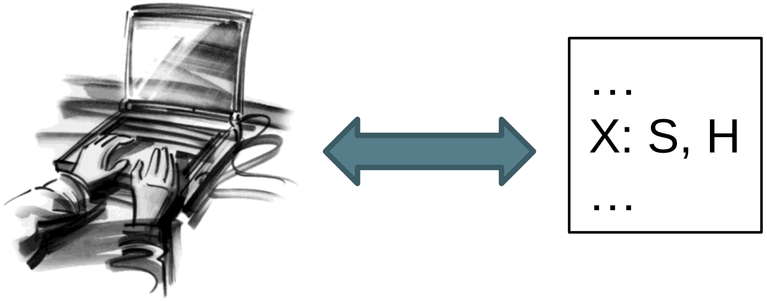
…
X: H
…

With salt:

1. User types userid, X, and password, P.

2. System looks up S and H, where S is the random salt for userid X and H is stored hash of S and X's password.

3. System tests whether h(S||P) = H.



Password file:

…
X: S, H
…

How Salt Increases Search Space Size

- Assuming that an attacker cannot find the salt associated with a userid he is trying to compromise, then the search space for a dictionary attack on a salted password is of size

  2^B*D,

  where B is the number of bits of the random salt and D is the size of the list of words for the dictionary attack.

- For example, if a system uses a 32-bit salt for each userid and its users pick passwords in a 500,000 word dictionary, then the search space for attacking salted passwords would be

  2^{32} * 500,000 = 2,147,483,648,000,000, which is over 2 quadrillion.

- Also, even if an attacker can find a salt password for a userid, he only learns one password.