COS80013 Internet Security

Week 3

Presented by Dr Rory Coulter

17 March 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Week 2 Recap

Key topics and theories

Recap

Introduce the concept of Offensive and Defensive security

Often tied to risk appetite, but also legal constraints

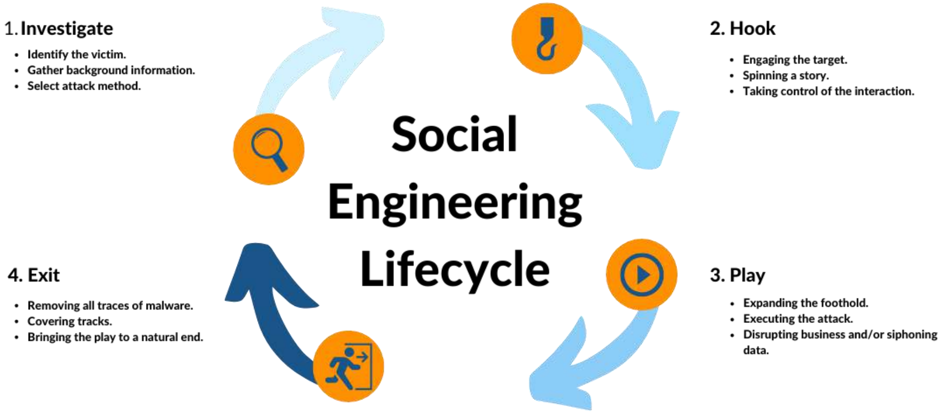
Physical and “digital” security are now more interconnected

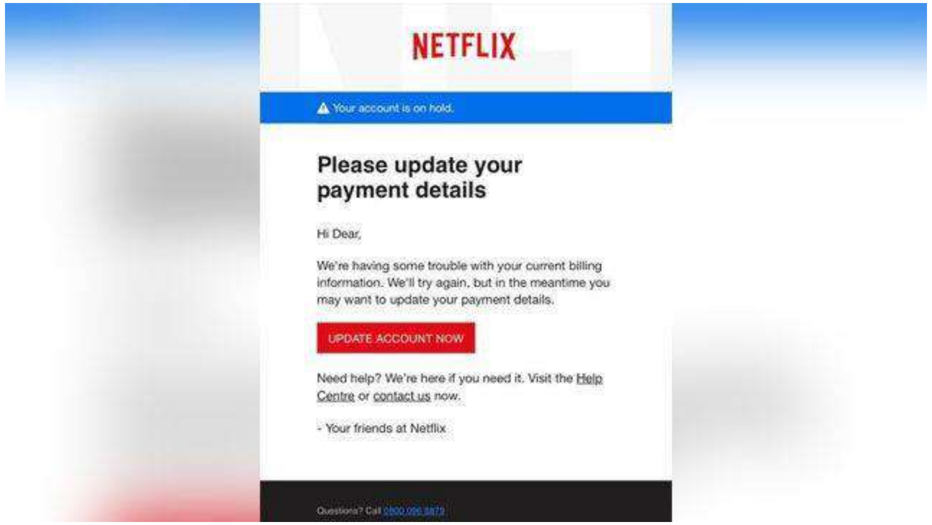
Converged security seeks to manage these spaces

Access controls, MAC, DAC, RBAC, ABAC

Authentication, passwords

Social engineering and the ability to phish or pharm targets


Social Engineering Lifecycle
1. Investigate
Identify the victim.
Gather background information.
Select attack method.
2. Hook
Engaging the target.
Spinning a story.
Taking control of the interaction.
3. Play
Expanding the foothold.
Executing the attack.
Disrupting business and/or siphoning data.
4. Exit
Removing all traces of malware.
Covering tracks.
Bringing the play to a natural end.


NETFLIX

⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 5879

Operating Systems

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems

System software which manages hardware, software, provides and enables resources to services/programs

A collection of software that manages computer hardware resources and provides common services for computer programs

- Operating Systems provide some key functions to users, hardware, software
- An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces, user interface
- Kernel
  - Schedules time and resources to a process
- File system
  - Provides a framework to specify the handling of files and folders, permissions (RWX) for users and groups
- Memory management
  - Provide, manage and isolate memory required for software
- Processes
  - An instance of a program currently running
- Operating Systems are not secured by default typically
- Require additional configuration for security
- Where the computer exists plays an important role

https://csrc.nist.gohttps://csrc.nist.gov/glossary/term/operating_systemv/glossary/term/operating_system
NIST SP 800-152

Host-based Detection

A range of tools required to detect and prevent threats for Operating Systems. While signatures are a staple, a behavioural approach behaviour must also be considered

Signature vs Behaviour

- Host may include workstations and servers
- Signature
  - Compare digital signature (hash)
  - Security vendors update known hash signatures
  - Good: Quick, direct match
  - Bad: Only knows what has been observed before
- Behaviour
  - Anomaly focused
  - Detect behaviour and code
  - Good: Detect what hasn’t been observed before
  - Bad: Chance for false positives

Network focused? IDS and IPS

Security

Provide CIA to the computer system

Typical measures in which this can be achieved

- User or group permissions
  - Specifying who and a collection of users have access too
- Antivirus, Endpoint detection and response
  - Match known signatures, signatures, rules, behaviour, policy
- Policy
  - Specify setting which can be allowed or blocked
- Firewall
  - Block or allow connections incoming or outgoing connections
- Authentication
  - Method to whom can access system
- Access control
  - Fine grain settings
- Monitoring
  - Ability to log what is occurring
- Security software
  - Installation and running of additional programs to aid security (e.g., app locker)

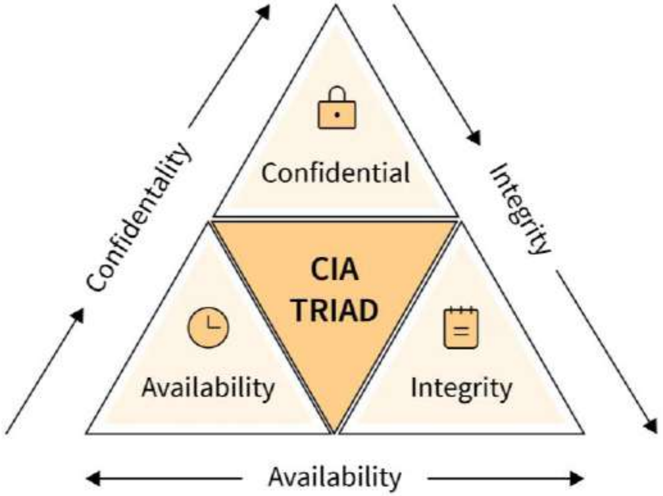


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

Access Control

Recap

- Discretionary access control (DAC): Allows the owner of a resource to control access to that resource and what level of access they are granted

- Mandatory access control (MAC): Access to resources is determined by a security policy that is enforced by the operating system or security software

Access Control Lists

An Access Control List (ACL) for a resource (e.g., a file or folder) is a sorted list of zero or more Access Control

- Entries (ACEs)
- An ACE specifies that a certain set of accesses (e.g., read, execute and write) to the resources is allowed or denied for a user or group
- Examples of ACEs for folder “Bob’s Secret Folder”

- Bob; Read; Allow
- Sally; Read; Allow
- TWD; Read, Write; Allow
- Bob; Write; Deny
- TAs; Write; Allow

Users and Passwords

Linux and Windows perspectives

Passwords are stored as hashes between operating systems

Each operating system employs different ways to manage passwords

Linux	Windows
Users stored in /etc/passwd and associated hashes /etc/shadow	Security Accounts Manager (SAM) file, C:\Windows\System32\config, hash via HKEY_LOCAL_MACHINE\SAM

The SAM file is restricted at runtime, the shadow file is not

Both these files can be copied and then studied offline to crack passwords

Range of tools for dumping passwords from SAM database

LASASS process in Windows very popular to dump hashes from (Local Security Authority Subsystem Service)

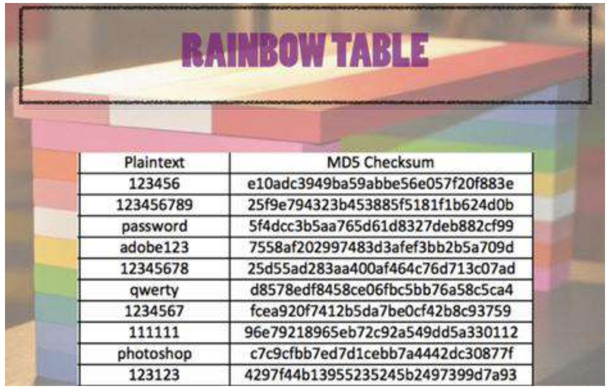
Salting: password + string ☞ hash, associated with the password

Peppering: password + secret ☞ hash, kept separate with the password

Password-based Attacks

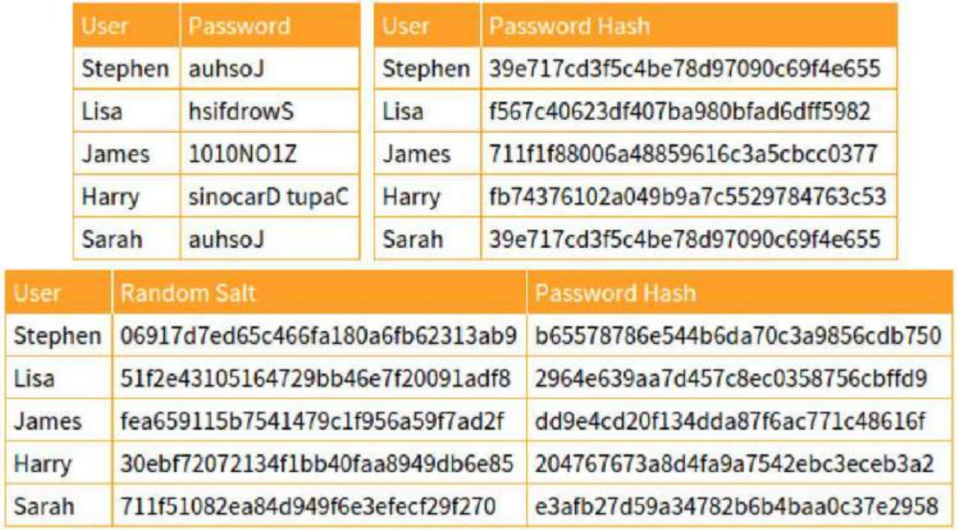
Just a snapshot

- Pass the hash
- Brute force attempts
- Simple hashing is susceptible to pre-hashed rainbow tables
- helloworld ☞ md5 ☞ fc5e038d38a57032085441e7fe7010b0



RAINBOW TABLE

Plaintext	MD5 Checksum
123456	e10adc3949ba59abbe56e057f20f883e
123456789	25f9e794323b453885f5181f1b624d0b
password	5f4dcc3b5aa765d61d8327deb882cf99
adobe123	7558af202997483d3afef3bb2b5a709d
12345678	25d55ad283aa400af464c76d713c07ad
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567	fcea920f7412b5da7be0cf42b8c93759
111111	96e79218965eb72c92a549dd5a330112
photoshop	c7c9cfbb7ed7d1cebb7a4442dc30877f
123123	4297f44b13955235245b2497399d7a93



User	Password
Stephen	auhsoJ
Lisa	hsifdrowS
James	1010NO1Z
Harry	sinocarD tupaC
Sarah	auhsoJ

User	Password Hash
Stephen	39e717cd3f5c4be78d97090c69f4e655
Lisa	f567c40623df407ba980bfad6dff5982
James	711f1f88006a48859616c3a5cbcc0377
Harry	fb74376102a049b9a7c5529784763c53
Sarah	39e717cd3f5c4be78d97090c69f4e655

User	Random Salt	Password Hash
Stephen	06917d7ed65c466fa180a6fb62313ab9	b65578786e544b6da70c3a9856cdb750
Lisa	51f2e4310516472 9bb46e7f20091adf8	2964e639aa7d457c8ec0358756cbffd9
James	fea659115b7541479c1f956a59f7ad2f	dd9e4cd20f134dda87f6ac771c48616f
Harry	30ebf72072134f1bb40faa8949db6e85	204767673a8d4fa9a7542ebc3eceb3a2
Sarah	711f51082ea84d949f6e3efecf29f270	e3afb27d59a34782b6b4baa0c37e2958

Technique	Name	Details
T1110.001	Password Guessing	Guess password in attempt to login into account
T1110.002	Password Cracking	Try to crack or recover passwords, when pass the hash is not applicable*
T1110.003	Password Spraying	Single or small list of passwords across a range of accounts
T1110.003	Credential Stuffing	Using credentials obtained from data breach

SOURCE: https://images.squarespace-cdn.com/content/v1/52ae955ce4b04f67f91b6df5/1550594084019-W7EAXBMCJJL089TSF8BH/rainbowtable.png

Execution

Restrict the ability for given files, processes or libraries to be used

Aim in reducing attack surface

- Windows Defender Application Control (WDAC)
- WDAC allows organisations to control which drivers and applications are allowed to run on their Windows clients. WDAC policies apply to the managed computer as a whole and affects all users of the device

- AppLocker
- AppLocker allows organisations to control which applications are allowed to run on their Windows clients. AppLocker policies can apply to all users on a computer, or to individual users and groups

Security Policy

SWINBURNE UNIVERSITY OF TECHNOLOGY

Policy

Organisation intent, processes and objectives

Policy document outlines these in the management of risk

- Organisations will have a range of policy, outlining:
  - Technology
  - Information assets
  - Associated rules and objectives, controls
- Policy is an excellent tool to "enforce" standards, requirements, specification, processes

- It outlines things like
  - Acceptable use
  - Specification
  - Process
  - Delegation

Policy Types

Scope for policy is broad

There are many moving parts to an organisation

- Aim: employees clear on their role, what is to be done, what is acceptable
- Acceptable use policy
- Digital signature policy
- Email retention, or logging policy in general
- Removable media policy

- Too many policies can become an issue

DEMO: https://www.sans.org/information-security-policy/

USB & External Media Policy Case Study

Many organisations and government ban (through policy and technology)

Policy defines, technology implements

- Initial Ban in 2008:
- Date: November 20, 2008
- The DoD implemented a complete ban on USB thumb drives and other removable media devices. This decision came after a worm infiltrated Army networks, highlighting the security risks associated with these devices
- Restrictions: All units were prohibited from using any USB mass storage devices, including hard drives, cameras, and printers

USB & External Media Policy Case Study (cont.)

Many organisations and government ban (through policy and technology)

Policy defines, technology implements

- Partial Lift of the Ban in 2010:
- Date: February 19, 20102
- Gen. Kevin Chilton, commander of the U.S. Strategic Command, partially lifted the ban on removable devices. However, this was only allowed as a “last resort” when necessary for mission-critical tasks and when no other means of data transfer were available
- Current usage:
- Use only removable media approved by your organisation
- Do not use personally owned/non-organisational removable media on your organisation’s systems
- Never plug unauthorised devices into a government system

Authorisation

While you might be able to authentication, you might not have authorisation to the request

Compare the pair

- As discussed, authentication allows a user to confirm who they are
- When authenticating, they might not be authorised to access
- The user may or may not have the permission

Monitoring

System Monitoring

How are systems events handled

Broadly between Unix-based (let's just say Linux) and Windows

- Events occur within a system
- Event logs capture:
  - Date, time
  - Device
  - Description
  - Level
  - Associated application/process
  - Specific event type
  - Characteristic
  - Networking information in relevant
- Typically, Operating system event logs relate to
- System events from the operating system itself
- E.g., Syslog/Auth (Linux), Sysmon (Windows)

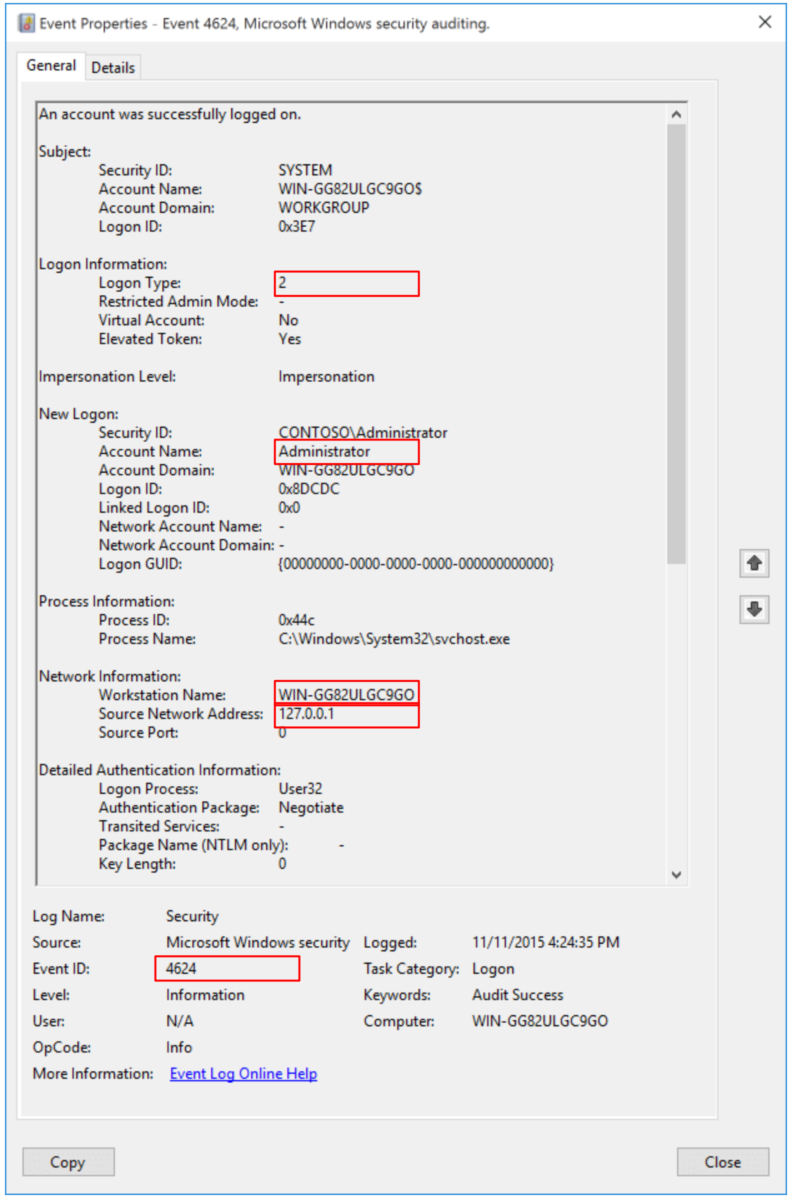
- Applications
  - Security events
  - Application logging may include
  - Request type
  - Status
  - Message
  - Networking
  - Event type
- Log structures are standardised, structured
- Logs should be centralised for monitoring
- Not everything is logged from install

An Example

Windows System Monitor Log: Event Type 4624

4624(S): An account was successfully logged on

- Administrator account logged on
- Logon type is 2, interactive
- Workstation name: WINGG82ULGC9GO
- Source network address is 127.0.0.1


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
An account was successfully logged on.

Subject:
        Security ID:              SYSTEM
        Account Name:             WIN-GG82ULGC9GO$
        Account Domain:           WORKGROUP
        Logon ID:                 0x3E7

Logon Information:
        Logon Type:               2
        Restricted Admin Mode:    -
        Virtual Account:          No
        Elevated Token:           Yes

Impersonation Level:              Impersonation

New Logon:
        Security ID:              CONTOSO\Administrator
        Account Name:             Administrator
        Account Domain:           WIN-GG82ULGC9GO
        Logon ID:                 0x8DCDC
        Linked Logon ID:          0x0
        Network Account Name:     -
        Network Account Domain:   -
        Logon GUID:               {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:               0x44c
        Process Name:             C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:         WIN-GG82ULGC9GO
        Source Network Address:   127.0.0.1
        Source Port:              0

Detailed Authentication Information:
        Logon Process:            User32
        Authentication Package:   Negotiate
        Transited Services:       -
        Package Name (NTLM only):         -
        Key Length:               0
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/11/2015 4:24:35 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-GG82ULGC9GO
OpCode:	Info		
More Information:	Event Log Online Help		

IMAGE SOURCE: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

Key Windows Events

Logon, Privilege Use, Defender

Key events

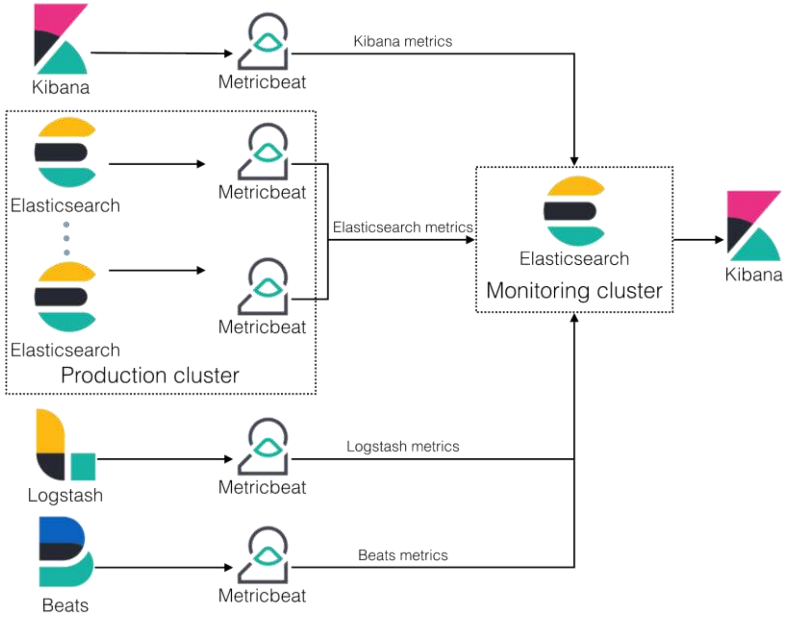
- Logon
  - 4624: User successfully logged on to a computer
  - 4625: Attempt made to logon with unknown user name or bad password and failed
  - 4822: NTLM authentication failed because the account was a member of the Protected User group
- Privilege Use
  - 4660: Object deleted
  - 4698: A scheduled task was created
  - 4699: A scheduled task was deleted
- Defender
  - 1002: malware scan stopped before completing scan
  - 1015: suspicious behaviour detected

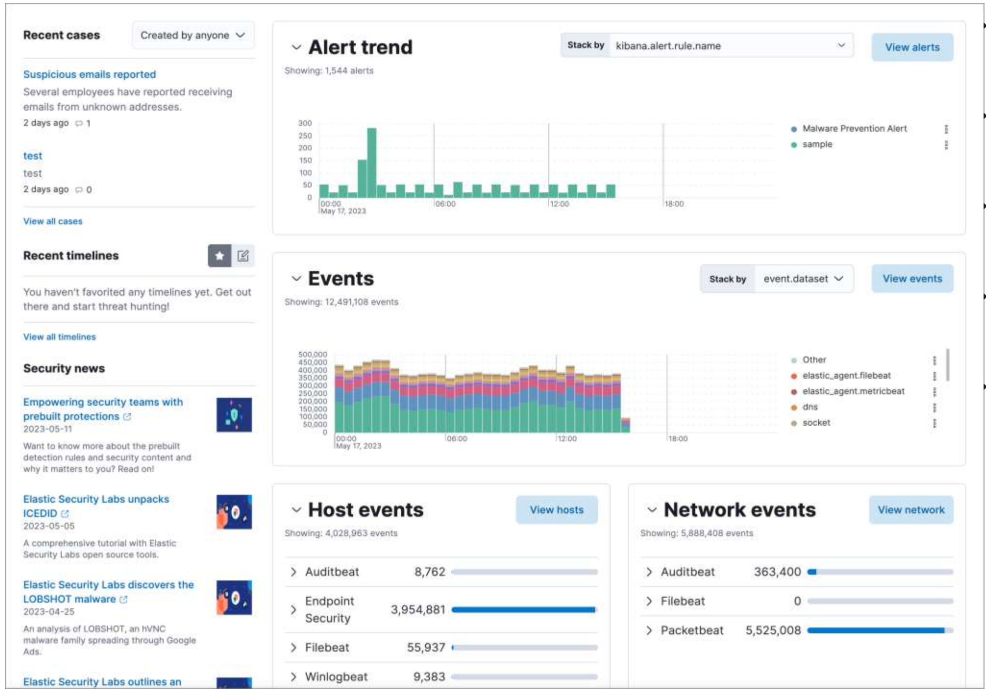
Security Information and Event Management (SIEM)

Centralise Logs

Event logs from all devices

- Ship logs to a SIEM
- Correlate events
- Investigate trends





Recent cases

Suspicious emails reported

Several employees have reported receiving emails from unknown addresses.

2 days ago 1

test

test

2 days ago 0

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

Security news

Empowering security teams with prebuilt protections

2023-05-11

Want to know more about the prebuilt detection rules and security content and why it matters to you? Read on!

Elastic Security Labs unpacks ICEDID

2023-05-05

A comprehensive tutorial with Elastic Security Labs open source tools.

Elastic Security Labs discovers the LOBSHOT malware

2023-04-25

An analysis of LOBSHOT, an hVNC malware family spreading through Google Ads.

Elastic Security Labs outlines an

Alert trend

Showing: 1,544 alerts

Events

Showing: 12,491,108 events

Host events

Showing: 4,028,963 events

Auditbeat	8,762
Endpoint Security	3,954,881
Filebeat	55,937
Winlogbeat	9,383

Network events

Showing: 5,888,408 events

Auditbeat	363,400
Filebeat	0
Packetbeat	5,525,008

IMAGE SOURCE: https://www.elastic.co/guide/en/elasticsearch/reference/current/monitoring-overview.html

https://www.elastic.co/guide/en/security/current/overview-dashboard.html

System Hardening

SWINBURNE UNIVERSITY OF TECHNOLOGY

System Hardening

Reduce the attack surface for a given system

A Windows example, Operating System focused

- Operating System Hardening
  - Operating System selection (secure-by-design and secure-by-default)
  - Operating environment (e.g., Internet facing DMZ, server LAN, user LAN, OT)
  - Hardening operating system configurations
  - Application management
  - Application control
  - Command & PowerShell
  - Host-based Intrusion Prevention System
  - Software Firewall
  - Antivirus
  - Device access control software (external media)
  - Operating system event logging

- But also:
  - User Application Hardening
  - Server Application Hardening
  - Authentication Hardening
  - Virtualisation Hardening

See for resources: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

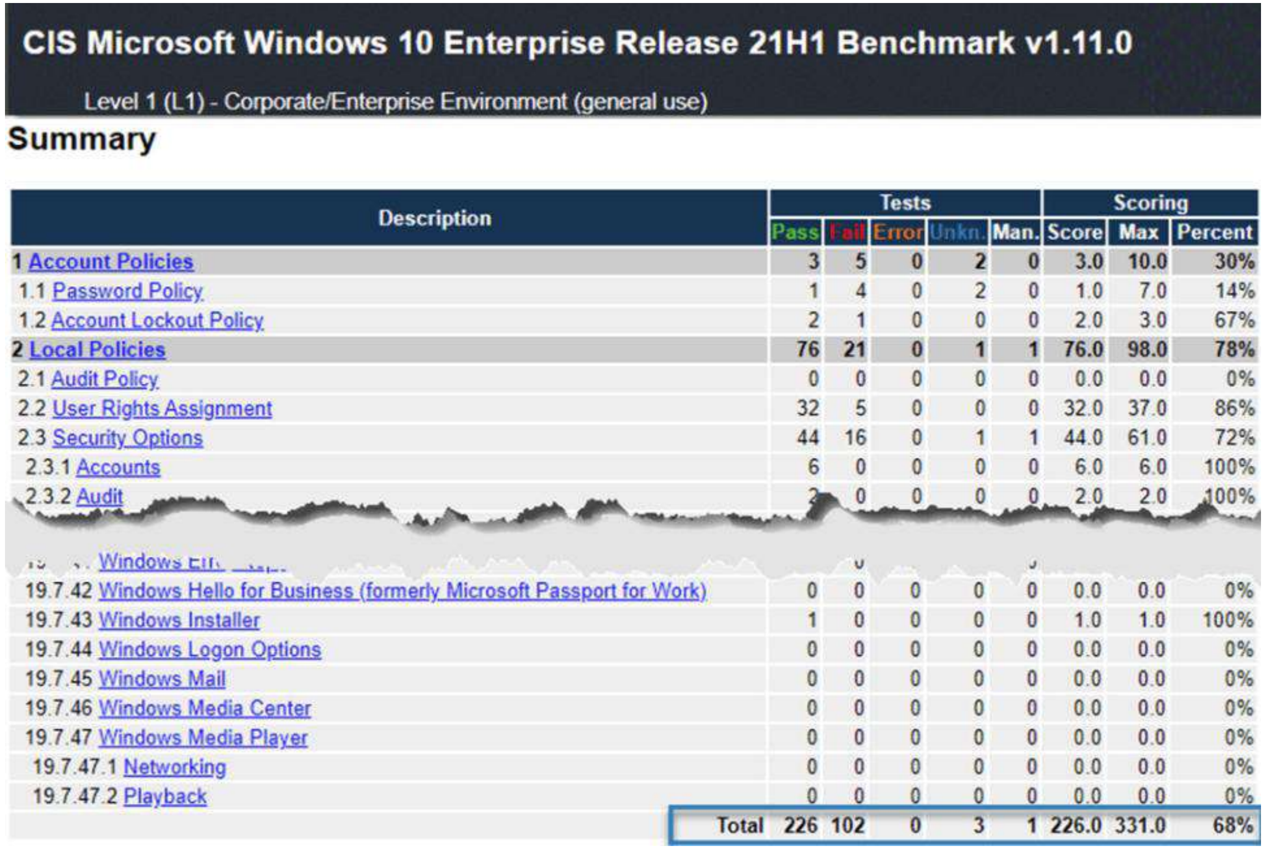
Semi-Automated Hardening

CENTER for INTERNET SECURITY

CIS Benchmarks

Benchmarks provided to harden a range of areas and maturity levels

- Cloud
- Desktop Software
- DevSecOps Tools
- Mobile Devices
- Multi Function Print Devices
- Network Devices
- Operating Systems
- Server Software



CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	**3**	**5**	**0**	**2**	**0**	**3.0**	**10.0**	**30%**
1.1 Password Policy	1	4	0	2	0	1.0	7.0	14%
1.2 Account Lockout Policy	2	1	0	0	0	2.0	3.0	67%
2 Local Policies	**76**	**21**	**0**	**1**	**1**	**76.0**	**98.0**	**78%**
2.1 Audit Policy	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	32	5	0	0	0	32.0	37.0	86%
2.3 Security Options	44	16	0	1	1	44.0	61.0	72%
2.3.1 Accounts	6	0	0	0	0	6.0	6.0	100%
2.3.2 Audit	2	0	0	0	0	2.0	2.0	100%
Windows Err								
19.7.42 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Installer	1	0	0	0	0	1.0	1.0	100%
19.7.44 Windows Logon Options	0	0	0	0	0	0.0	0.0	0%
19.7.45 Windows Mail	0	0	0	0	0	0.0	0.0	0%
19.7.46 Windows Media Center	0	0	0	0	0	0.0	0.0	0%
19.7.47 Windows Media Player	0	0	0	0	0	0.0	0.0	0%
19.7.47.1 Networking	0	0	0	0	0	0.0	0.0	0%
19.7.47.2 Playback	0	0	0	0	0	0.0	0.0	0%
Total	226	102	0	3	1	226.0	331.0	68%

IMAGE SOURCE: https://nira.com/cis-benchmarks-and-compliance/

COS80013 Internet Security

Lecture Week 3A

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems Concepts

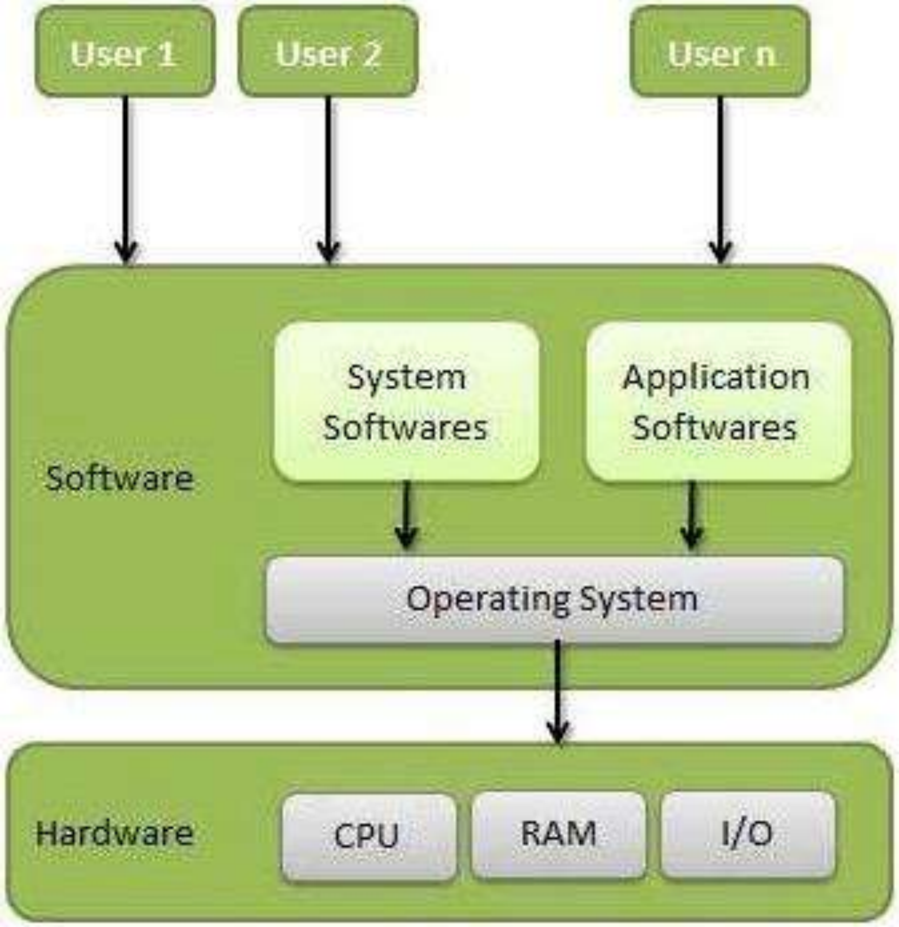
SWIN BUR NE

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems Concepts

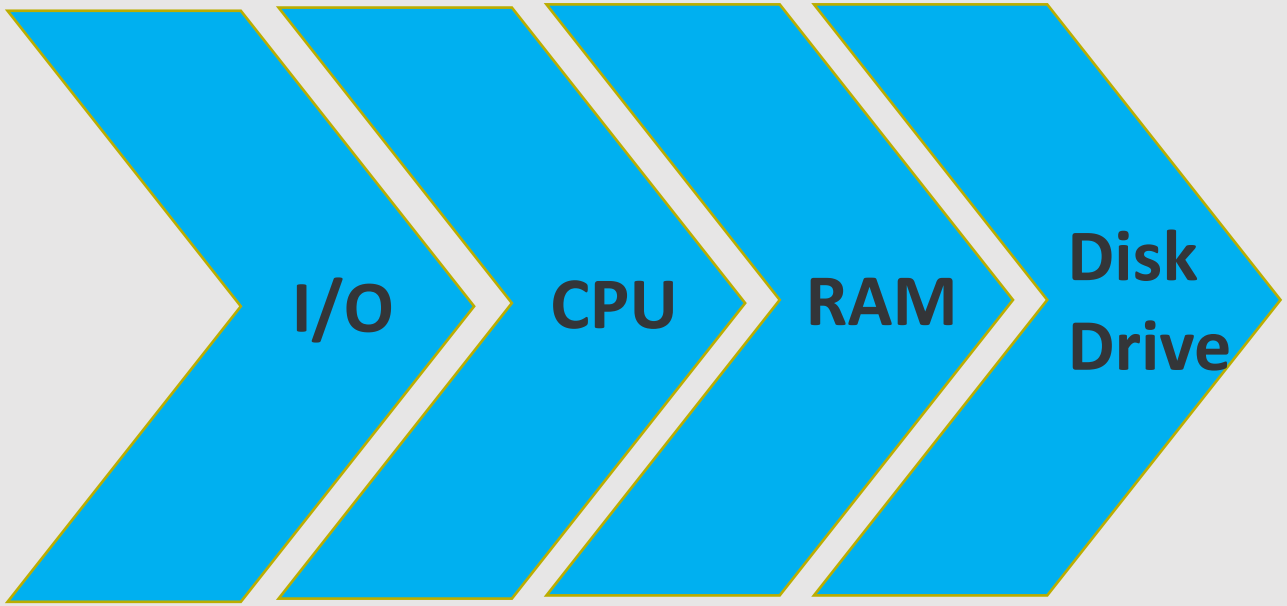
Some of important functions of an operating System

- ➢ The Kernel and Input/Output
- ➢ Processes
- ➢ The Filesystem
- ➢ Memory Management
- ➢ Virtual Machines



A Computer Model

- An operating system has to deal with the fact that a computer is made up of a CPU, random access memory (RAM), input/output (I/O) devices, and long-term storage.



OS Concepts

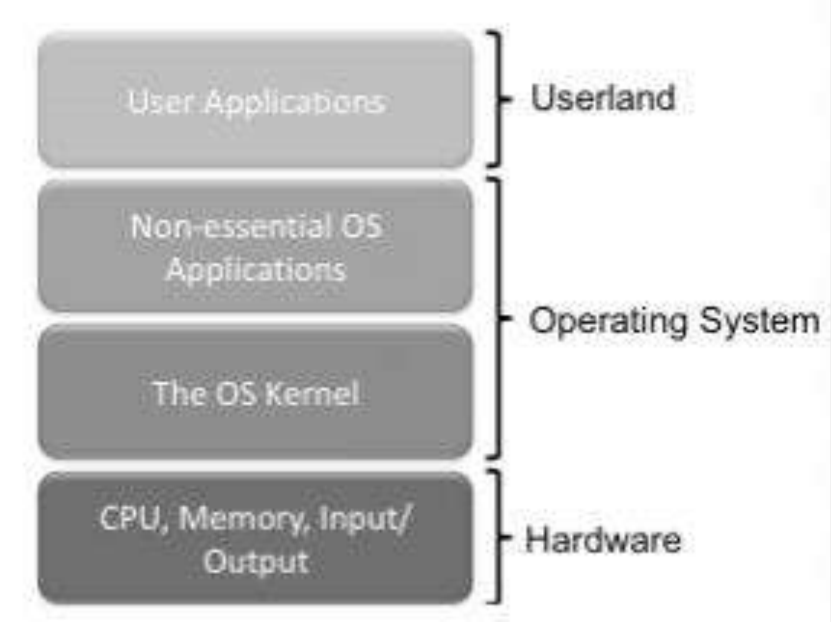
- **An operating system (OS) provides the interface between the users of a computer and that computer's hardware.**
  - ➢An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces.
  - ➢An operating system manages multiple users.
  - ➢An operating system manages multiple programs.

Multitasking

- Give each running program a “slice” of the CPU’s time.
- The CPU is running so fast that to any user it appears that the computer is running all the programs simultaneously.

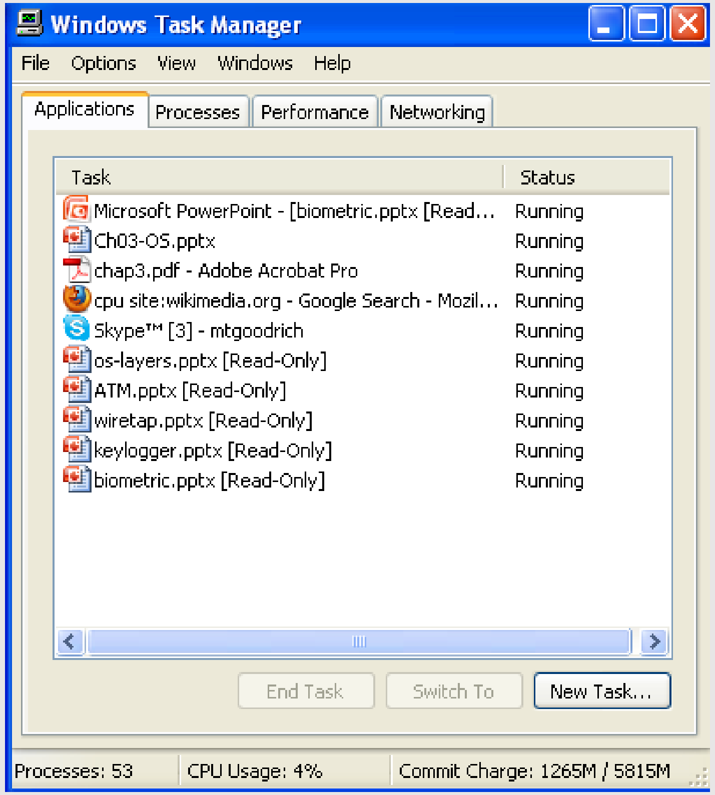
The Kernel and Input/Output

- **Kernel:** core component of the operating system.It handles the management of low-level hardware resources, including memory, processors, and input/output (I/O) devices, such as a keyboard, mouse, or video display.
- Most operating systems define the tasks associated with the kernel in terms of a layer metaphor, with the hardware components, such as the CPU, memory, and input/output devices being on the bottom, and users and applications being on the top.



Processes

- A **process** is an instance of a program that is currently executing.
- The actual contents of all programs are initially stored in persistent storage, such as a hard drive.
- In order to be executed, a program must be loaded into random-access memory (RAM) and uniquely identified as a process.
- In this way, multiple copies of the same program can be run as different processes.
  - ➢For example, we can have multiple copies of MS Powerpoint open at the same time.



Task	Status
Microsoft PowerPoint - [biometric.pptx [Read...	Running
Ch03-OS.pptx	Running
chap3.pdf - Adobe Acrobat Pro	Running
cpu site:wikimedia.org - Google Search - Mozil...	Running
Skype™ [3] - mtgoodrich	Running
os-layers.pptx [Read-Only]	Running
ATM.pptx [Read-Only]	Running
wiretap.pptx [Read-Only]	Running
keylogger.pptx [Read-Only]	Running
biometric.pptx [Read-Only]	Running

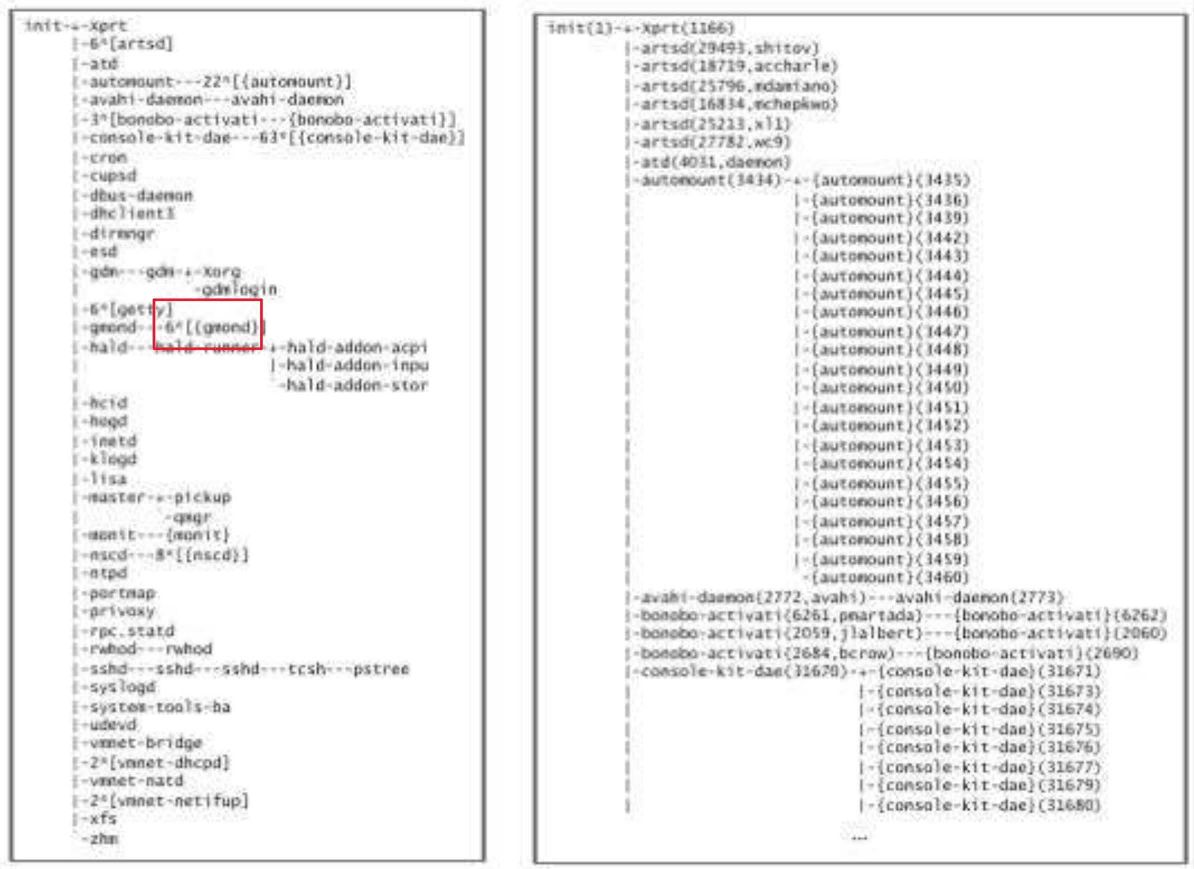
Processes: 53 CPU Usage: 4% Commit Charge: 1265M / 5815M

Processes

Process: the kernel defines the notion of a process , which is an instance of a program that is currently executing. The **Process IDs:** Each process running on a given computer is identified by a unique nonnegative integer, called the process ID (PID).

IPC: operating systems usually include mechanisms to facilitate inter-process communication (IPC).

Signal: unixbased systems incorporate signals , which are essentially notifications sent from one process to another.



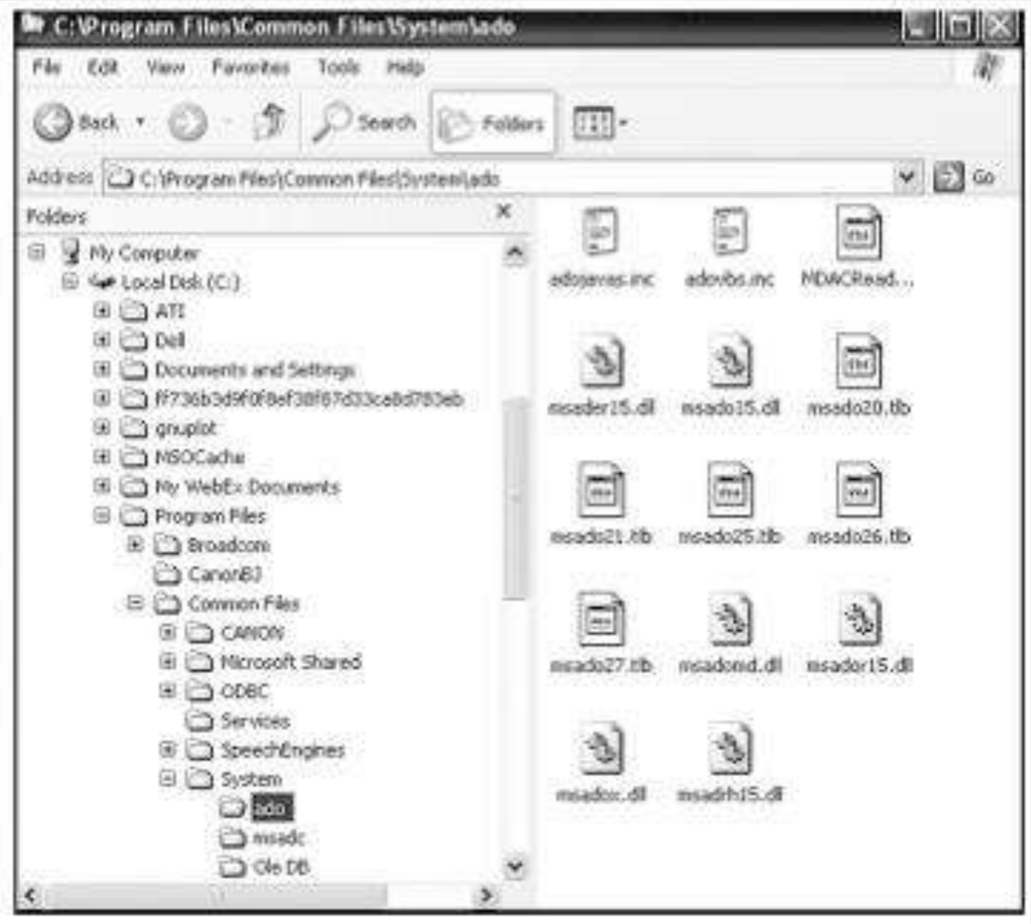
```
init-+-Xprt
     |-6*[artsd]
     |-atd
     |-automount---22*[{automount}]
     |-avahi-daemon---avahi-daemon
     |-3*[bonobo-activati---{bonobo-activati}]
     |-console-kit-dae---63*[{console-kit-dae}]
     |-cron
     |-cupsd
     |-dbus-daemon
     |-dhclient3
     |-dirmngr
     |-esd
     |-gdm---gdm-+-Xorg
     |           `-gdmlogin
     |-6*[getty]
     |-gmond---6*[{gmond}]
     |-hald---hald-runner-+-hald-addon-acpi
     |                    |-hald-addon-inpu
     |                    `-hald-addon-stor
     |-hcid
     |-hogd
     |-inetd
     |-klogd
     |-lisa
     |-master-+-pickup
     |        `-qmgr
     |-monit---{monit}
     |-nscd---8*[{nscd}]
     |-ntpd
     |-portmap
     |-privoxy
     |-rpc.statd
     |-rwhod---rwhod
     |-sshd---sshd---sshd---tcsh---pstree
     |-syslogd
     |-system-tools-ba
     |-udevd
     |-vmnet-bridge
     |-2*[vmnet-dhcpd]
     |-vmnet-natd
     |-2*[vmnet-netifup]
     |-xfs
     `-zhm
```

```
init(1)-+-Xprt(1166)
        |-artsd(29493,shitov)
        |-artsd(18719,accharle)
        |-artsd(25796,mdamiano)
        |-artsd(16834,mchepkwo)
        |-artsd(25213,xl1)
        |-artsd(27782,wc9)
        |-atd(4031,daemon)
        |-automount(3434)-+-{automount}(3435)
        |                 |-{automount}(3436)
        |                 |-{automount}(3439)
        |                 |-{automount}(3442)
        |                 |-{automount}(3443)
        |                 |-{automount}(3444)
        |                 |-{automount}(3445)
        |                 |-{automount}(3446)
        |                 |-{automount}(3447)
        |                 |-{automount}(3448)
        |                 |-{automount}(3449)
        |                 |-{automount}(3450)
        |                 |-{automount}(3451)
        |                 |-{automount}(3452)
        |                 |-{automount}(3453)
        |                 |-{automount}(3454)
        |                 |-{automount}(3455)
        |                 |-{automount}(3456)
        |                 |-{automount}(3457)
        |                 |-{automount}(3458)
        |                 |-{automount}(3459)
        |                 `-{automount}(3460)
        |-avahi-daemon(2772,avahi)---avahi-daemon(2773)
        |-bonobo-activati(6261,pmartada)---{bonobo-activati}(6262)
        |-bonobo-activati(2059,jlalbert)---{bonobo-activati}(2060)
        |-bonobo-activati(2684,bcrow)---{bonobo-activati}(2690)
        |-console-kit-dae(31670)-+-{console-kit-dae}(31671)
        |                        |-{console-kit-dae}(31673)
        |                        |-{console-kit-dae}(31674)
        |                        |-{console-kit-dae}(31675)
        |                        |-{console-kit-dae}(31676)
        |                        |-{console-kit-dae}(31677)
        |                        |-{console-kit-dae}(31679)
        |                        |-{console-kit-dae}(31680)
                         ...
```

Process tree for a Linux system

The Filesystem

- A **filesystem** is an abstraction of how the external, nonvolatile memory of the computer is organized.
- Operating systems typically organize files hierarchically into folders, also called directories.
- Each folder may contain files and/or subfolders.
- Thus, a volume, or drive, consists of a collection of nested folders that form a tree.
- The topmost folder is the root of this tree and is also called the root folder.



A filesystem as a tree

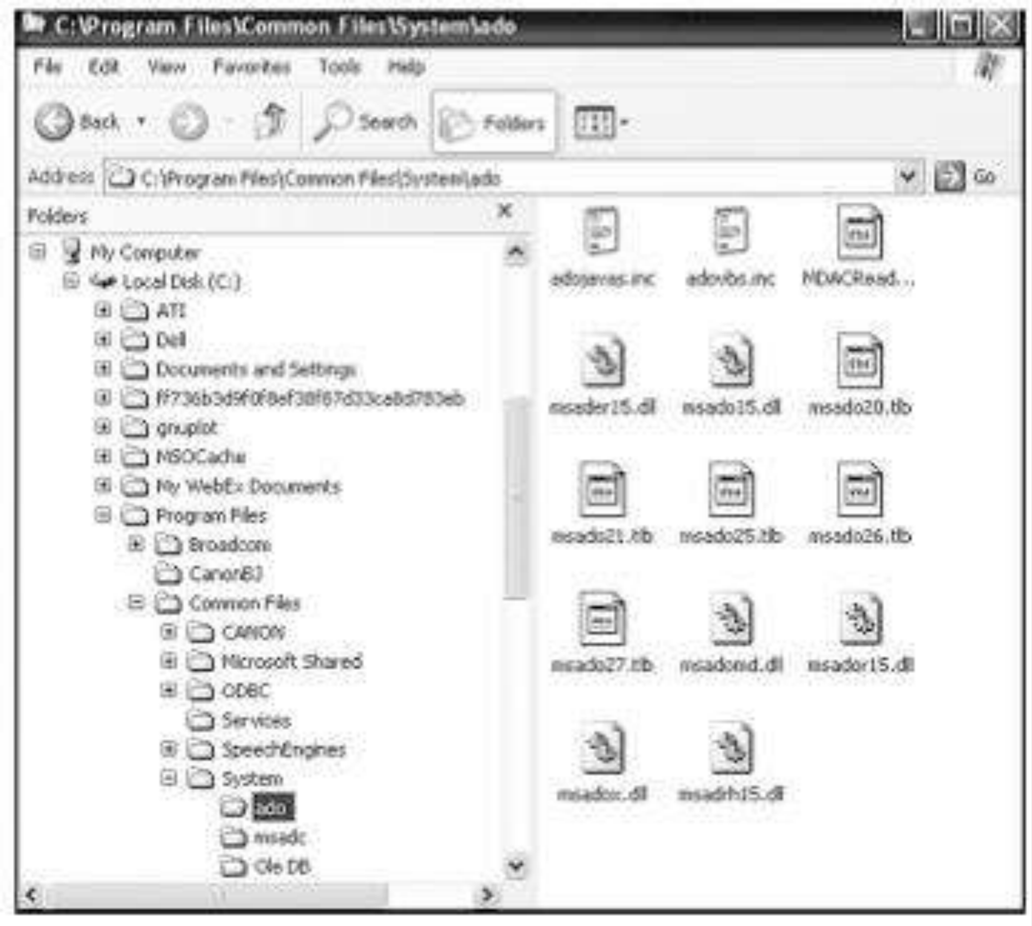
The Filesystem

Filesystem: filesystem is another key component of an operating system. It is an abstraction of how the external, nonvolatile memory of the computer is organized.

File Access Control: determine which uses can access which resources.

File Permissions: file permissions are checked by the operating system to determine if a file is readable, writable, or executable by a user or group of users.

Unix File Permissions: the read, write, and execute bits are implemented in binary.



A filesystem as a tree

Memory Management

Memory Management: is another service that OS provides. Memory management refers to management of Primary Memory or Main Memory.

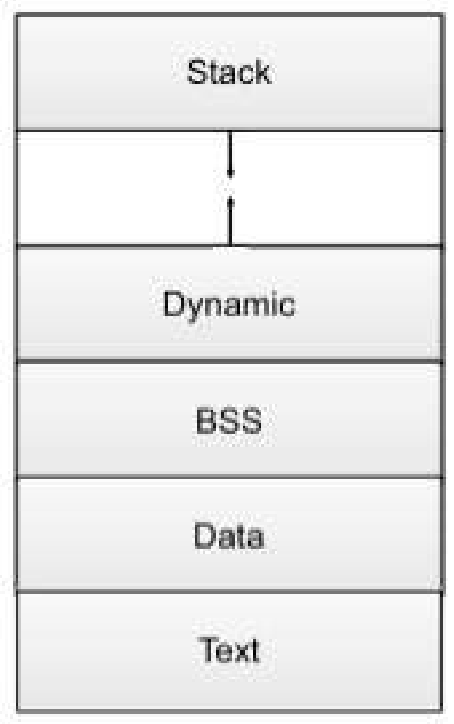
Text: machine code of the program

Data: static program variables (prior execution)

BSS: block started by symbol, contains static variables that are uninitialized

Heap: dynamic segment, stores data such as objects written in C++ or Java, during the execution.

Stack: houses a stack data structure.



The Unix memory model

Virtual Machines

- **Virtual machines (VMs)** are software computers that provide the same functionality as physical computers.
- Unlike emulators, VMs have direct access to the host CPU disks and RAM, so they run fast and efficient (compared to emulators).
- Advantages:
  - ➢Many VMs in a single host – hardware cost is shared.
  - ➢Portable – VM can be shut down and moved to another host and then started up again (sometimes automatically).
  - ➢Secure – VM–Host interface acts as a sandbox. Prevents malware from getting out of VM.
  - ➢Convenient – Easy to manage VM backups, ideal for remote access / monitoring. Great for security research.

Virtual Machines

- Disadvantages
  - Hosting may be in another (or unknown) legal jurisdiction.
  - CIA issues.
  - Infected VMs may be able to escape the VM “sandbox” and infect other VMs and the host. (see BluePill)
  - http://en.wikipedia.org/wiki/Blue_Pill_%28software%29
  - Malware detection in the VM can be thwarted if malware detects that it is in a VM or sandbox (and stays inactive).
  - Hiberfile, pagefile, .vmem and .vmdk files are susceptible to physical access attacks.
  - Hosting company can access inside of VM through VMI extensions.
  - https://www.researchgate.net/publication/270081646_CloudSec_A_Security_Monitoring_Appliance_For_Virtual_Machines_In_The_IaaS_Cloud_Model

Two Types of Virtual Machines
Process virtual machines (platform-independent environment)
System virtual machines (Support the sharing of a host computer’s physical resources)

COS80013 Internet Security

Lecture Week 3B

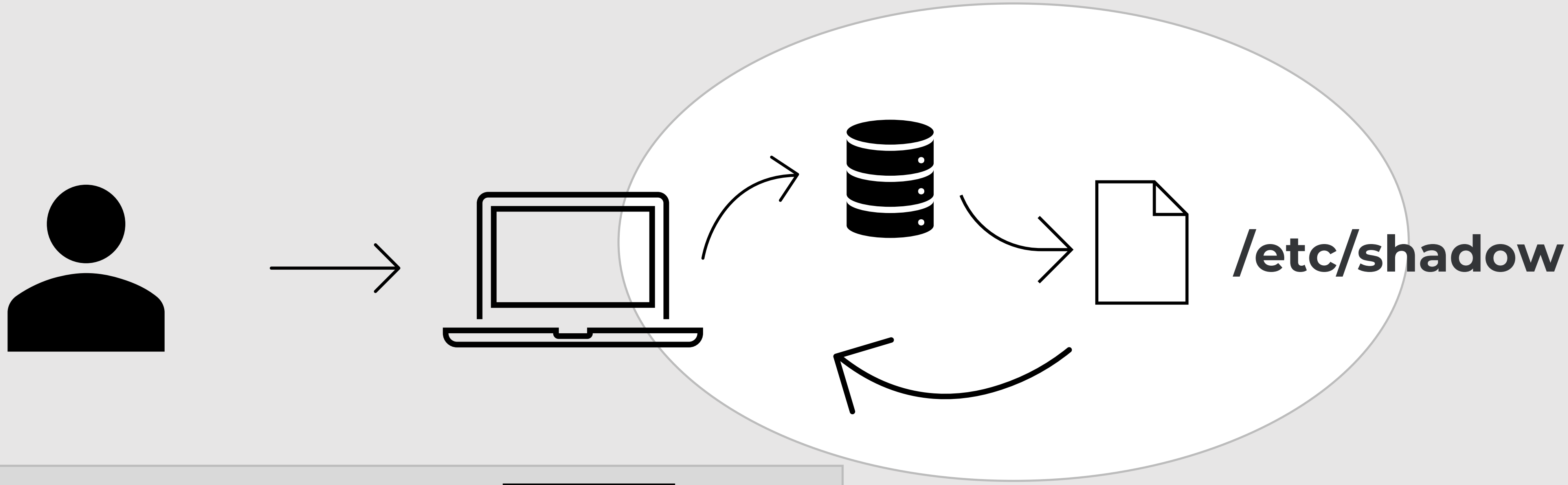
SWINBURNE UNIVERSITY OF TECHNOLOGY

Passwords

SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Password Process

Lets take a Linux example

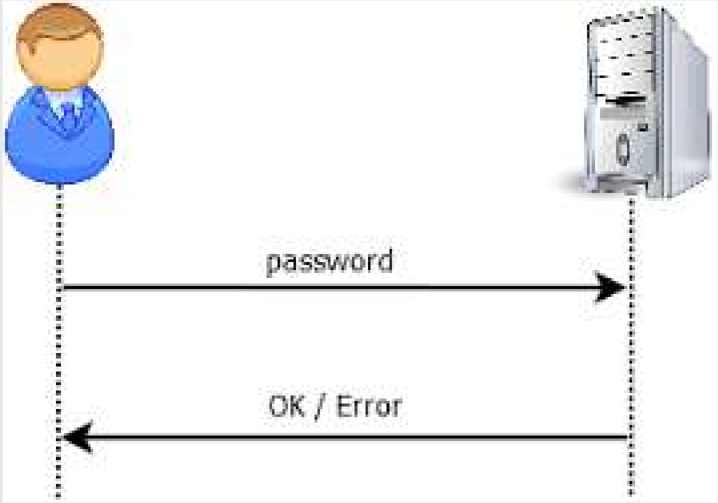


/etc/shadow

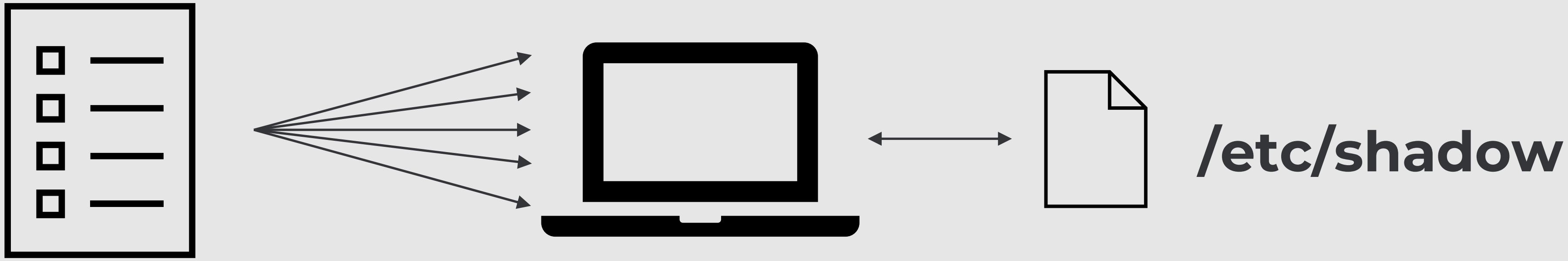
Hash of password

Password-Based Authentication

- Passwords are susceptible to *keylogging*, brute-force and dictionary attacks and can too often be obtained or guessed using social engineering techniques.



Brute Force Attacking



- The success of a brute-force attack depends on the size of the password/pin.
  - ➢ A 4-digit pin can be guessed after 5000 tries ((9999 – 0000)/2).
  - ➢ A 6-digit pin takes 500,000 guesses.
  - ➢ A 6 character password using lower-case letters takes 150 million guesses.

Password-Based Authentication

- These passwords can be 'cracked' easily using existing software that automates the login process.
- Dictionary attack - SSH-brute.c
  - A 6-character password using upper and lower case letters, numbers and symbols (62 possible characters) will take about 28 billion guesses.
  - Increasing the number of characters to 8 improves things by a factor of 256,000 to 110,000 billion attempts needed.
  - Passwords of this size can still be guessed, but it takes an inconvenient time.

Password-Based Authentication

- If the password can be guessed, the speed of cracking increases dramatically.
- A dictionary attack may take as few as 85,000 guesses (171,000 words in the Oxford English Dictionary).
  - ➢ Try HashCat (in Kali VM)
  - ➢ Bad guys know how people “disguise” their passwords or append them to satisfy password policies. Most common modifications are scriptable.
- Most passwords are now 8 characters
  - ➢ Default passwords are by design easy to remember (short)!

Dictionary Attack

An attacker can easily compare hashes between a password file and a rainbow table of hashes

User	Password	(Plain Text Version)
Bob	Fe5778GG….	Cat
Alice	JJN6NHJ89….	Dog
Sky	DFCDEF65….	Apple
Caslon	FBNUY87F….	Strawberry
Misch	G6590gfd7….	Secret
Alive v2	dfk9934F%….	haxor

Password File

Password	(Plain Text Version)
Fe5778GG….	Cat
JJN6NHJ89….	Dog
DFCDEF65….	Apple
FBNUY87F….	Strawberry
G6590gfd7….	Secret
dfk9934F%….	haxor

Attackers List

Simply find a match and you’re good to go

Password-Based Authentication

Don't write the password down.

http://www.theregister.co.uk/2005/08/10/kutztown_13/

If you really have to write it down, keep it in your wallet with your money. Or write it in a book and lock the book away. Don't write down what it's for.

Password storage?

SIMS synchronizes passwords for all accounts

- password re-use

Browsers store passwords

- may be in plain text

Password Managers

- only as safe as the master password.

Allow for *escrow*

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.

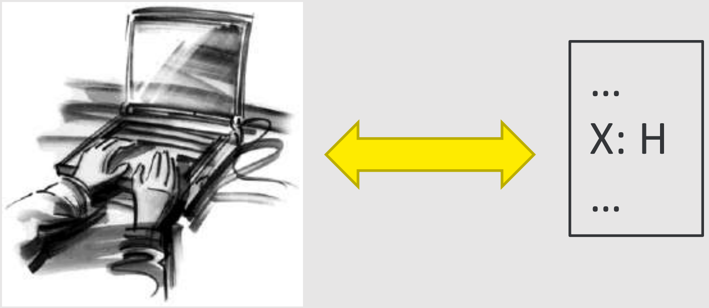
How Password Salt Works

- **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:

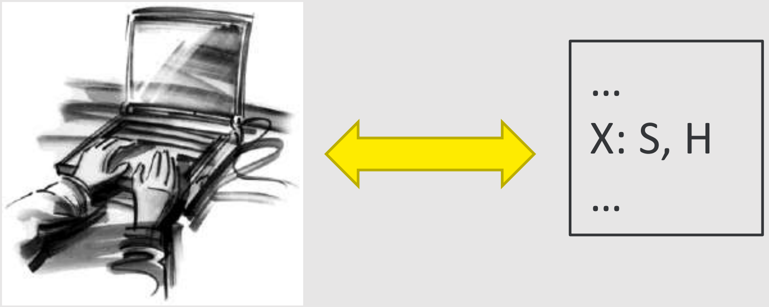
…
X: H
…

- **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.

Dictionary Attack

Possible dictionary passwords will not match

User	Password	Salt	(Plain Text Version)
Bob	fdjg89jjjfdg....	Gf8034jhf…	Cat
Alice	gj5400m0m....	Gf945j9fh…	Dog
Sky	gk5490mgjj....	Fdjf48390…	Apple
Caslon	fj483jt4jgki....	Fkj498jgf3…	Strawberry
Misch	gk590kkgk5....	F4j389fj89…	Secret
Alive v2	jvbnbm949....	Fj4893f30k…	haxor

Password File

Password	(Plain Text Version)
Fe5778GG....	Cat
JJN6NHJ89....	Dog
DFCDEF65....	Apple
FBNUY87F....	Strawberry
G6590gfd7....	Secret
dfk9934F%....	haxor

Attackers List

Password+salt -> MD5 -> hash

Passwords

- Passwords are obtainable by social engineering methods or by sniffing unencrypted network traffic (Telnet, HTTP, FTP).
  - ➢People choose a password they can remember, and then re-use it for several accounts.
  - ➢May be the name of a child, pet or relative.
  - ➢May be used for plain text traffic (to http:// web site form), sniffed, and then tried on secure (https://) accounts.
- Even a password used with a secure web site may be obtained if it is stored in plain text in a vulnerable database or as an *unsalted hash* (look up *rainbow tables*).

Authentication Also

Passwords are but one measure for authentication

(Remember what you know)

Multi Factor Authentication is something we have

(Another device)

Together the complexity of overtaking an account in increased

But re-use of passwords is everywhere so compromise might arise from another account

Policy

***Security*, *Use Acceptance* policy dictates the minimum specification for passwords**

8 characters, mix of upper and lower, special character and numbers

(high or low)

What are the issues with these?

- Do we set one password for a long time with a high baseline?
- Do we rotate new passwords for a lower baseline?

Don't be lulled into a false sense of security here

COS80013 Internet Security

Lecture Week 3C

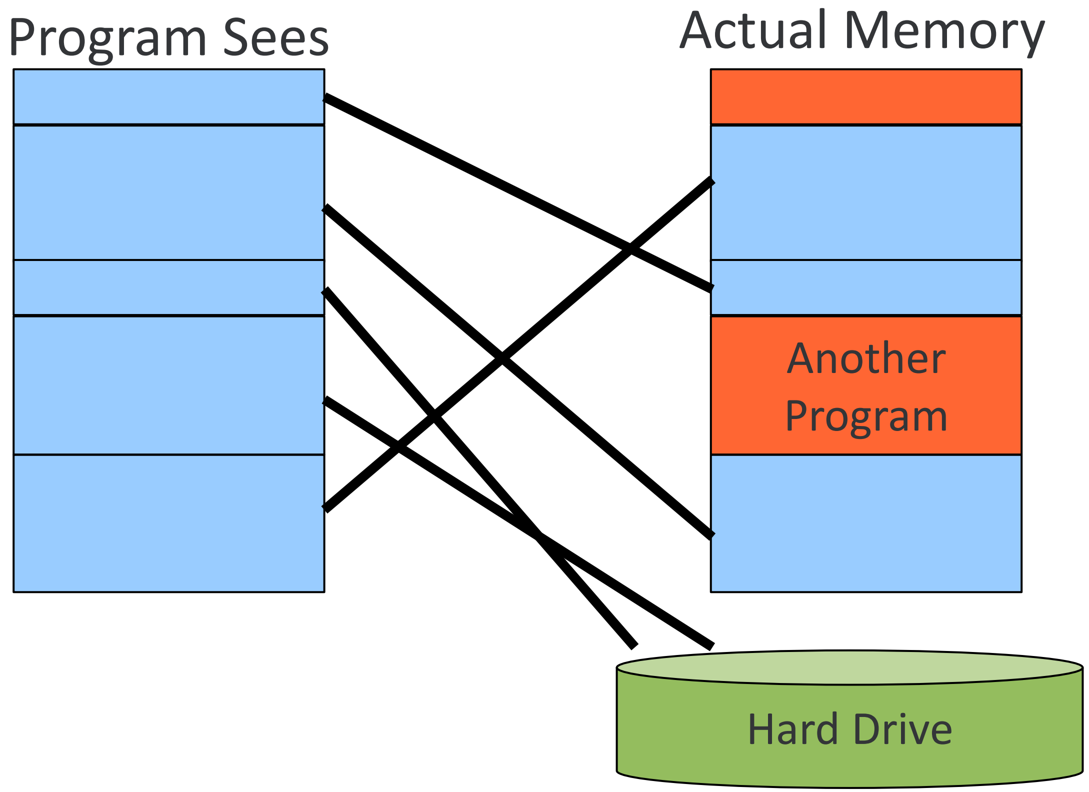
SWINBURNE UNIVERSITY OF TECHNOLOGY

Buffer Overflow Attacks

SWINBURNE UNIVERSITY OF TECHNOLOGY

Buffer Overflow Attacks

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.



History

Amongst the many different types of vulnerabilities which exist, Buffer Overflows (Overrun) still persist

Date back to the 1980’s

In practice, a large amount of overflow techniques seen are accounted for

There is a constant evolution of methods, attacks refined

Defences might have or introduce a weakness

Cycle continues (patch, see new exploit)

History

Most, if not all Buffer Overflows are the result of buggy C code

No length checking on the buffer

C doesn’t inherently check the length of buffers

A potential solution?

Don’t use C

Languages that do check:

Java, Python, …

What is an Exploit?

- An exploit is any input (i.e., a piece of software, an argument string, or sequence of commands) that takes advantage of a bug, glitch or vulnerability in order to cause an attack.
- An attack is an unintended or unanticipated behavior that occurs on computer software, hardware, or something electronic and that brings an advantage to the attacker.

What is an Exploit?

- An exploit is not necessarily a program.
- While it can be a program that communicates bad input to a vulnerable piece of software, it can also be just the bad input itself.
- Any bad input (or even valid input that the developer just failed to anticipate) can cause the vulnerable application to behave improperly.

Buffer Overflow Attack

- One of the most common OS bugs is a buffer overflow
  - ➢ The developer fails to include code that checks whether an input string fits into its buffer array.
  - ➢ An input to the running process exceeds the length of the buffer.
  - ➢ The input string overwrites a portion of the memory of the process.
  - ➢ Causes the application to behave improperly and unexpectedly.

Buffer Overflow Attack

- Since the stack grows downward, if you write past the end of the buffer, you can corrupt the content of the rest of the stack, if enough information is known about the program.
- Because of the nature of the address space, locally declared buffers are allocated on the stack and one could write over known register information and the return address.

Buffer Overflow Attack

- Effect of a buffer overflow
  - The process can operate on malicious data or execute malicious code passed by the attacker.
  - If the process is executed as root, the malicious code will be executing with root privileges.

Guessing Addresses

- Typically you need the source code so you can *estimate* the address of both the buffer and the return-address.

- An estimate is often good enough! (more on this in a bit).

Not So Easily Avoided

What language is Python written in?

- C

What language would system libraries being called be written in?

- C

Which are running on an OS, what language is the kernel written in?

- C

✓ **C however is popular language**

✓ **Low level system control**

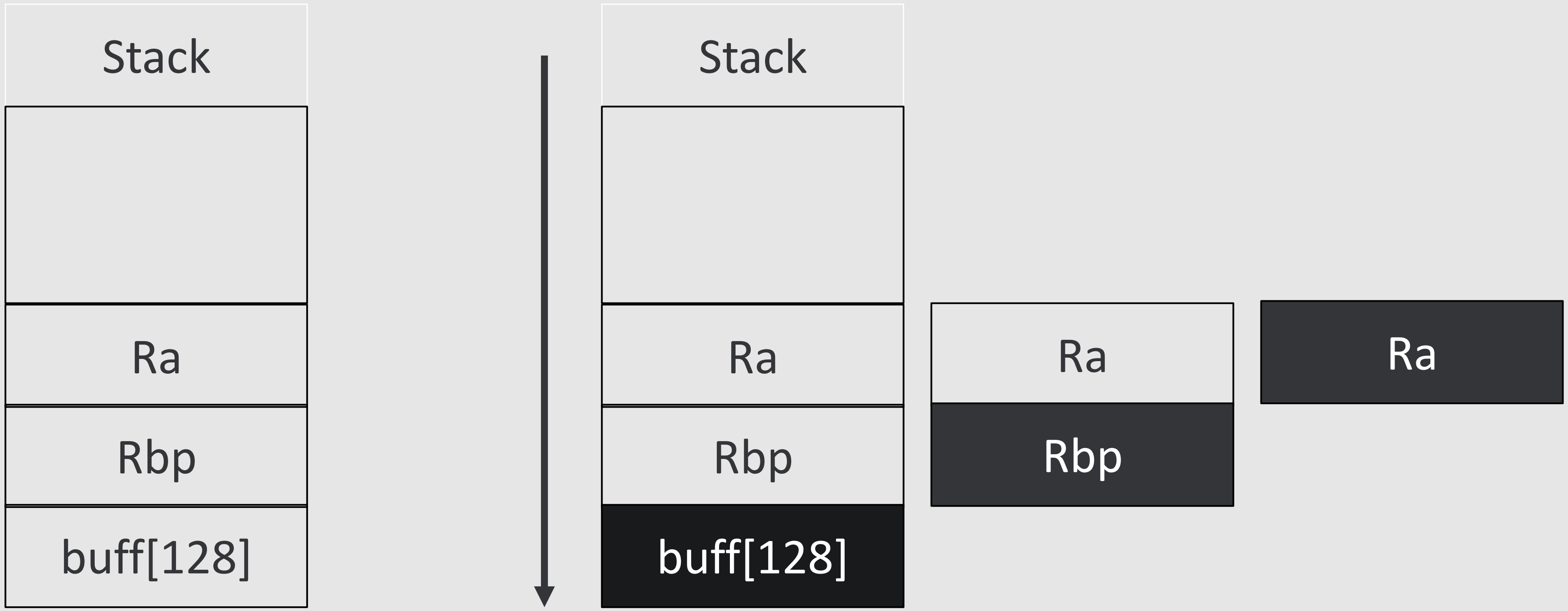
- Code reuse
- Poor practice
- Mistakes introduced

SWIN BUR NE SWINBURNE UNIVERSITY OF TECHNOLOGY

Control

popfunc()

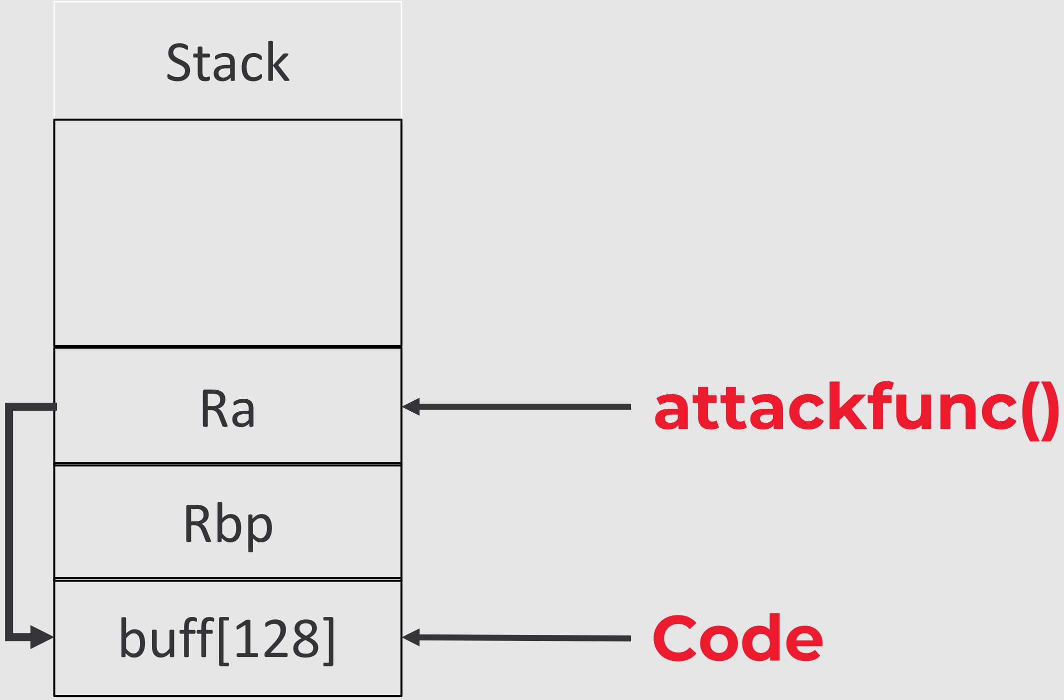
Ra: Return Address
Rbp: Frame pointer
Buff: Allocated buffer



Attacker chooses what goes in to function

Control

popfunc()



Overflow the buffer

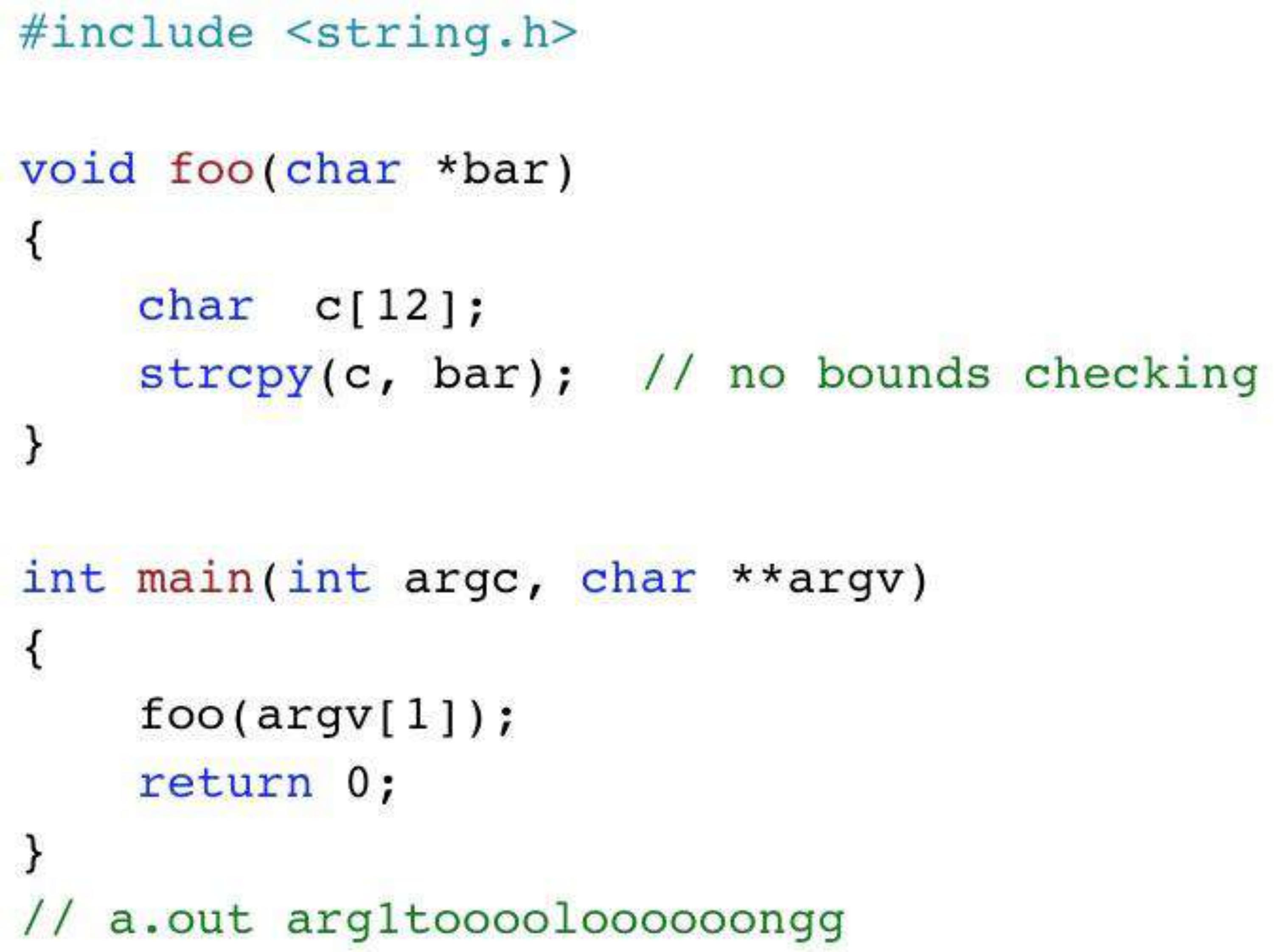
Function returns

Tidy up Ra, whatever

Open Source programs
Github

Assume attacker has access to the source code

Buffer Overflow – Simple Example

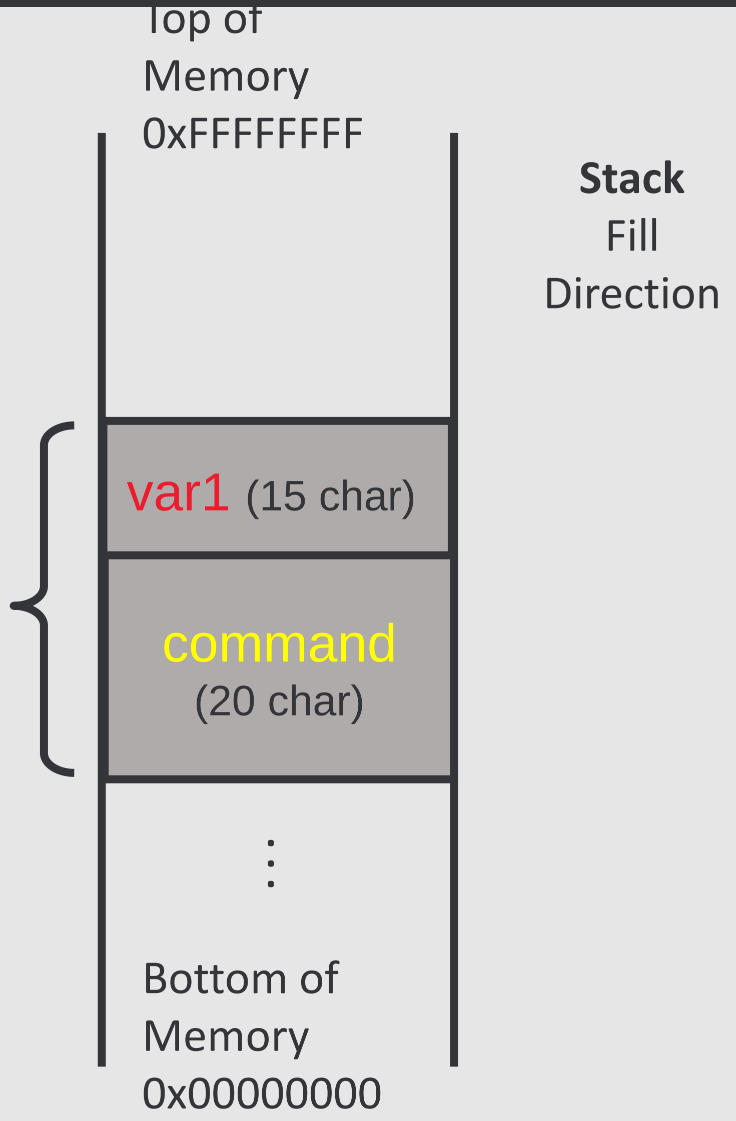


```
#include <string.h>

void foo(char *bar)
{
    char  c[12];
    strcpy(c, bar);  // no bounds checking
}

int main(int argc, char **argv)
{
    foo(argv[1]);
    return 0;
}
// a.out arg1tooooloooooongg
```

Buffer Overflow

domain.c

```
main(int argc, char *argv[ ])
/* get user_input */
{
   char var1[15];
   char command[20];
   strcpy(command, “whois ");
   strcat(command, argv[1]);
   strcpy(var1, argv[1]);
   printf(var1);
   system(command);
}
```

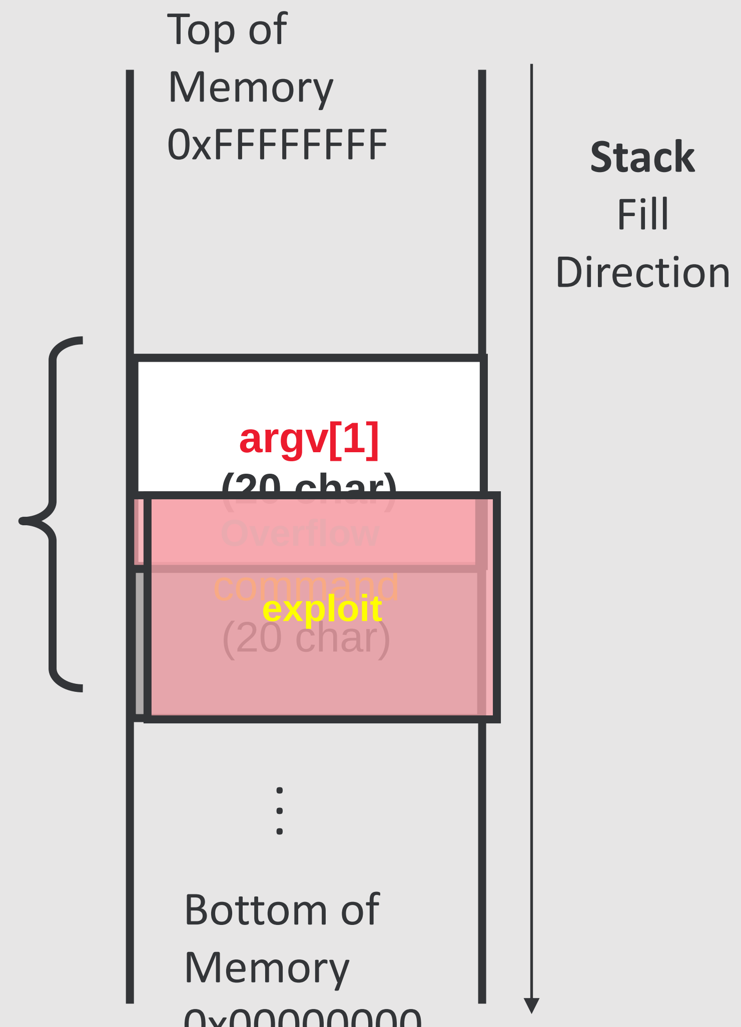


Retrieves domain registration info

e.g., domain swin.edu.au

strcpy() Vulnerability

```
domain.c
Main(int argc, char *argv[])
/*get user_input*/
{
   char var1[15];
   char command[20];
   strcpy(command, “whois ");
   strcat(command, argv[1]);
   strcpy(var1, argv[1]);
   printf(var1);
   system(command);
}
```



Top of Memory 0xFFFFFFFF

Stack Fill Direction

argv[1] (20 char)

Overflow

command

exploit

(20 char)

⋮

Bottom of Memory 0x00000000

- **argv[1] is the user input**
- **strcpy(dest, src) does not check buffer**
- **strcat(d, s) concatenates strings**

strcpy() vs. strncpy()

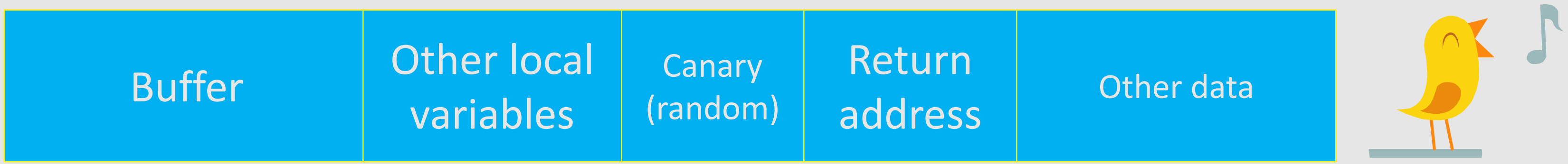
- **Function strcpy() copies the string in the second argument into the first argument**
  - ➢e.g., strcpy(dest, src)
  - ➢If source string > destination string, the overflow characters may occupy the memory space used by other variables
  - ➢The null character is appended at the end automatically
- **Function strncpy() copies the string by specifying the number n of characters to copy**
  - ➢e.g., strncpy(dest, src, n); dest[n] = '\0'
  - ➢If source string is longer than the destination string, the overflow characters are discarded automatically
  - ➢You have to place the null character manually

Shellcode Injection

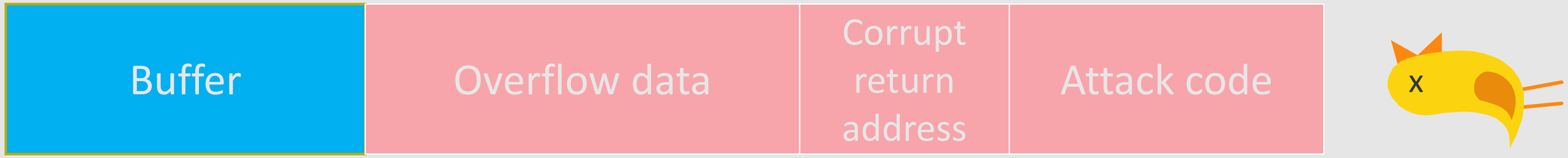
- An exploit takes control of attacked computer so injects code to “spawn a shell” or “shellcode”.
- A shellcode is:
  - ➢Code assembled in the CPU’s native instruction set (e.g. x86 , x86-64, arm, sparc, risc, etc.).
  - ➢Injected as a part of the buffer that is overflowed.
  - ➢We inject the code directly into the buffer that we send for the attack.
  - ➢A buffer containing shellcode is a “payload”.
  - ➢More information: https://samsclass.info/127/proj/p3-lbuf1.htm

Stack-based BoF detection using a random canary

Normal (safe) stack configuration:



Buffer overflow attack attempt:



- The canary is placed in the stack prior to the return address, so that any attempt to over-write the return address also over-writes the canary.
- The system regularly checks the integrity of this canary value. If it has been changed, it knows that the buffer has been overflowed and it should prevent malicious code execution.

Buffer Overflow Mitigation

- We know how a buffer overflow happens, but why does it happen?
- This problem could not occur in Java; it is a C problem
  - ➢In Java, objects are allocated dynamically on the heap (except ints, etc.).
  - ➢Also cannot do pointer arithmetic in Java.
  - ➢In C (and C++), however, you can declare things directly on the stack.

Buffer Overflow Mitigation

- Why doesn’t get do a bounds check and why does the operating system allow writing beyond the array bounds?
- In Java can’t just overwrite the stack because you don’t know where the stack is!
- In Java, cannot access memory without direct access, since we lack pointer arithmetic

Buffer Overflow Mitigation

- One solution is to make the buffer dynamically allocated.
- Another (OS) problem is that *fingerd* had to run as root.
  - ➢Just get rid of fingerd’s need for root access (solution eventually used).
  - ➢The program needed access to a file that had sensitive information in it.
  - ➢A new world-readable file was created with the information required by fingerd.

Preventing Stack-based BoF Attacks

- The root cause does not come from OS but insecure programming practices.
- Programmers must be educated about the risks of insecurely coping user-supplied data into fixed size buffers.
- Use strncpy(buf, argv[1], sizeof(buf)) instead of strcpy(buf, argv[1]).

- **Function strcpy() copies the string in the second argument into the first argument**
  - ➢e.g., strcpy(dest, src)
  - ➢If source string > destination string, the overflow characters may occupy the memory space used by other variables
- **Function strncpy() copies the string by specifying the number n of characters to copy**
  - ➢ e.g., strncpy(buf, argv[1], sizeof(buf))
  - ➢ If source string is longer than the destination string, the overflow characters are discarded automatically

Testing

Code must be carefully inspected and tested to discover all possible buffer overflows.

Code Inspection

Expensive and time consuming.

Fuzz Testing

Input random strings into input variables and data files.

Fire random events while a process is running

Easy to automate

Log input, output, behaviour to discover potential vulnerabilities.

Used by crackers to discover vulnerabilities too!

Preventing Stack-based BoF Attacks

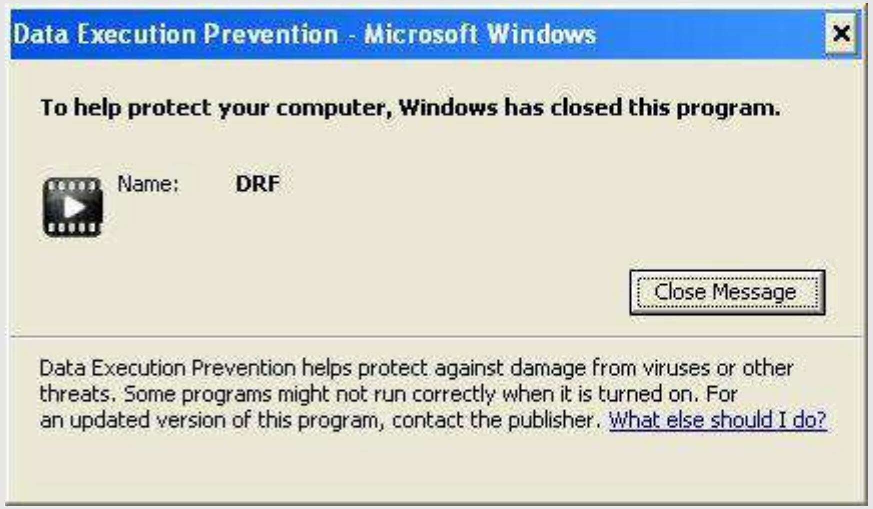
- PointGuard (Microsoft). It is a compiler extension, that address code which XOR-encodes any pointers, including the return address before and after they are used. Therefore, attacker cannot reliably overwrite the return address.
- Data Execution Prevention (DEP) tags memory as Read-Execute (code) or Write-NoExecute (data), enforces no-execution permission on the stack segment of memory. Attackers responded by using ROP.
- Address space layout randomization (ASLR) rearranges the data of a process's address space at random. Defeats ROP.

Data Execution Prevention

In an attempt to stop buffer overflow exploits, CPU manufacturers have created DEP.

http://support.microsoft.com/kb/875352

DEP is a feature which allows particular areas of memory to be tagged as NX – non-executable (AMD) or XD – execute disabled (Intel).



Data Execution Prevention - Microsoft Windows

To help protect your computer, Windows has closed this program.

Name: DRF

Data Execution Prevention helps protect against damage from viruses or other threats. Some programs might not run correctly when it is turned on. For an updated version of this program, contact the publisher. What else should I do?

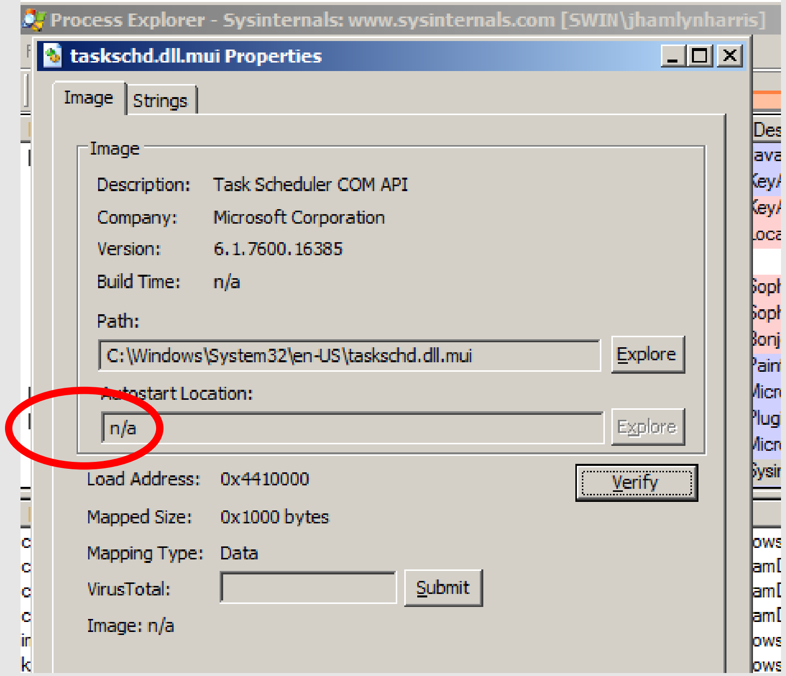
Data Execution Prevention

DEP is supported in Windows and in Linux kernels since XP SP2 and Kernel 2.6.8 respectively.

It can be turned off in software

Some dlls don’t use it.

http://en.wikipedia.org/wiki/Data_Execution_Prevention



Process Explorer - Sysinternals: www.sysinternals.com [SWIN\jhamlynharris]

taskschd.dll.mui Properties

Image

Description: Task Scheduler COM API

Company: Microsoft Corporation

Version: 6.1.7600.16385

Build Time: n/a

Path:

C:\Windows\System32\en-US\taskschd.dll.mui

Autostart Location:

n/a

Load Address: 0x4410000

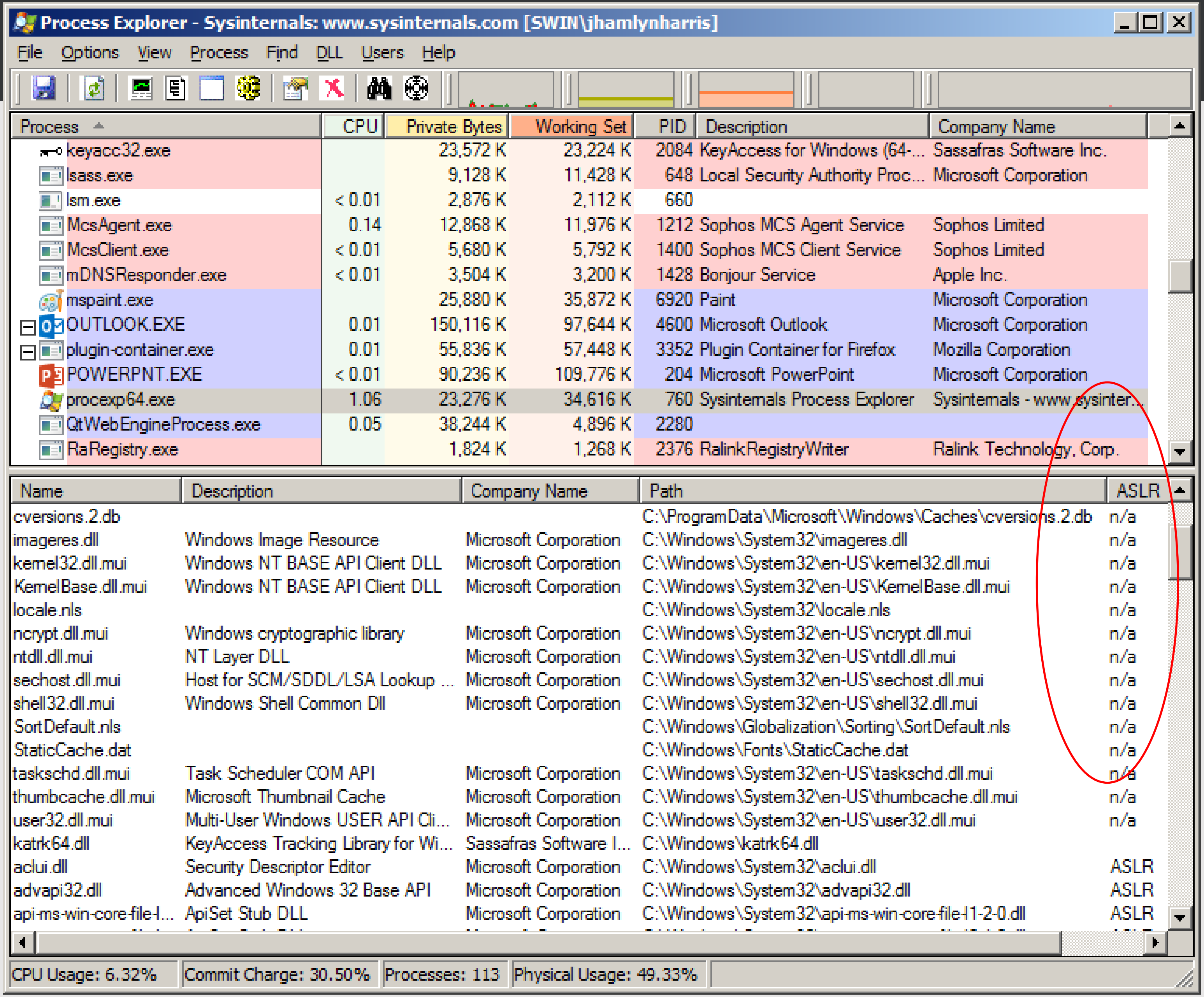
Mapped Size: 0x1000 bytes

Mapping Type: Data

VirusTotal:

Image: n/a

processes not using ASLR


Process Explorer - Sysinternals: www.sysinternals.com [SWIN\jhamlynharris]
File
Options
View
Process
Find
DLL
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
keyacc32.exe		23,572 K	23,224 K	2084	KeyAccess for Windows (64-...	Sassafras Software Inc.
lsass.exe		9,128 K	11,428 K	648	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	< 0.01	2,876 K	2,112 K	660		
McsAgent.exe	0.14	12,868 K	11,976 K	1212	Sophos MCS Agent Service	Sophos Limited
McsClient.exe	< 0.01	5,680 K	5,792 K	1400	Sophos MCS Client Service	Sophos Limited
mDNSResponder.exe	< 0.01	3,504 K	3,200 K	1428	Bonjour Service	Apple Inc.
mspaint.exe		25,880 K	35,872 K	6920	Paint	Microsoft Corporation
OUTLOOK.EXE	0.01	150,116 K	97,644 K	4600	Microsoft Outlook	Microsoft Corporation
plugin-container.exe	0.01	55,836 K	57,448 K	3352	Plugin Container for Firefox	Mozilla Corporation
POWERPNT.EXE	< 0.01	90,236 K	109,776 K	204	Microsoft PowerPoint	Microsoft Corporation
procexp64.exe	1.06	23,276 K	34,616 K	760	Sysinternals Process Explorer	Sysinternals - www.sysinter...
QtWebEngineProcess.exe	0.05	38,244 K	4,896 K	2280		
RaRegistry.exe		1,824 K	1,268 K	2376	RalinkRegistryWriter	Ralink Technology, Corp.

Name	Description	Company Name	Path	ASLR
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db	n/a
imageres.dll	Windows Image Resource	Microsoft Corporation	C:\Windows\System32\imageres.dll	n/a
kernel32.dll.mui	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\en-US\kernel32.dll.mui	n/a
KernelBase.dll.mui	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\en-US\KernelBase.dll.mui	n/a
locale.nls			C:\Windows\System32\locale.nls	n/a
ncrypt.dll.mui	Windows cryptographic library	Microsoft Corporation	C:\Windows\System32\en-US\ncrypt.dll.mui	n/a
ntdll.dll.mui	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\en-US\ntdll.dll.mui	n/a
sechost.dll.mui	Host for SCM/SDDL/LSA Lookup ...	Microsoft Corporation	C:\Windows\System32\en-US\sechost.dll.mui	n/a
shell32.dll.mui	Windows Shell Common Dll	Microsoft Corporation	C:\Windows\System32\en-US\shell32.dll.mui	n/a
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls	n/a
StaticCache.dat			C:\Windows\Fonts\StaticCache.dat	n/a
taskschd.dll.mui	Task Scheduler COM API	Microsoft Corporation	C:\Windows\System32\en-US\taskschd.dll.mui	n/a
thumbcache.dll.mui	Microsoft Thumbnail Cache	Microsoft Corporation	C:\Windows\System32\en-US\thumbcache.dll.mui	n/a
user32.dll.mui	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\System32\en-US\user32.dll.mui	n/a
katrk64.dll	KeyAccess Tracking Library for Wi...	Sassafras Software I...	C:\Windows\katrk64.dll	
aclui.dll	Security Descriptor Editor	Microsoft Corporation	C:\Windows\System32\aclui.dll	ASLR
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll	ASLR
api-ms-win-core-file-l...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\System32\api-ms-win-core-file-l1-2-0.dll	ASLR

CPU Usage: 6.32% | Commit Charge: 30.50% | Processes: 113 | Physical Usage: 49.33%

Return-oriented programming

- ROP
- Locate useful portions of code (system calls) at the end of existing OS .dlls (already loaded into memory).
- Write exploit which jumps to each useful command in the correct sequence to perform a malicious act.
- Avoids DEP by only running trusted code. No code injection needed!

See the Voting machine story:

- Security Now 211

http://www.security-faqs.com/what-is-rop-and-how-do-hackers-use-it.html

Address Space Layout Randomization

- Aims to make ROP impossible

- ASLR is a scheme of changing the layout of the heap, stack, and library functions after each boot to make it harder for a hacker to locate areas of useful memory.

- It is available since Vista/7 and in Linux kernels since 2.6.2.

ASLR

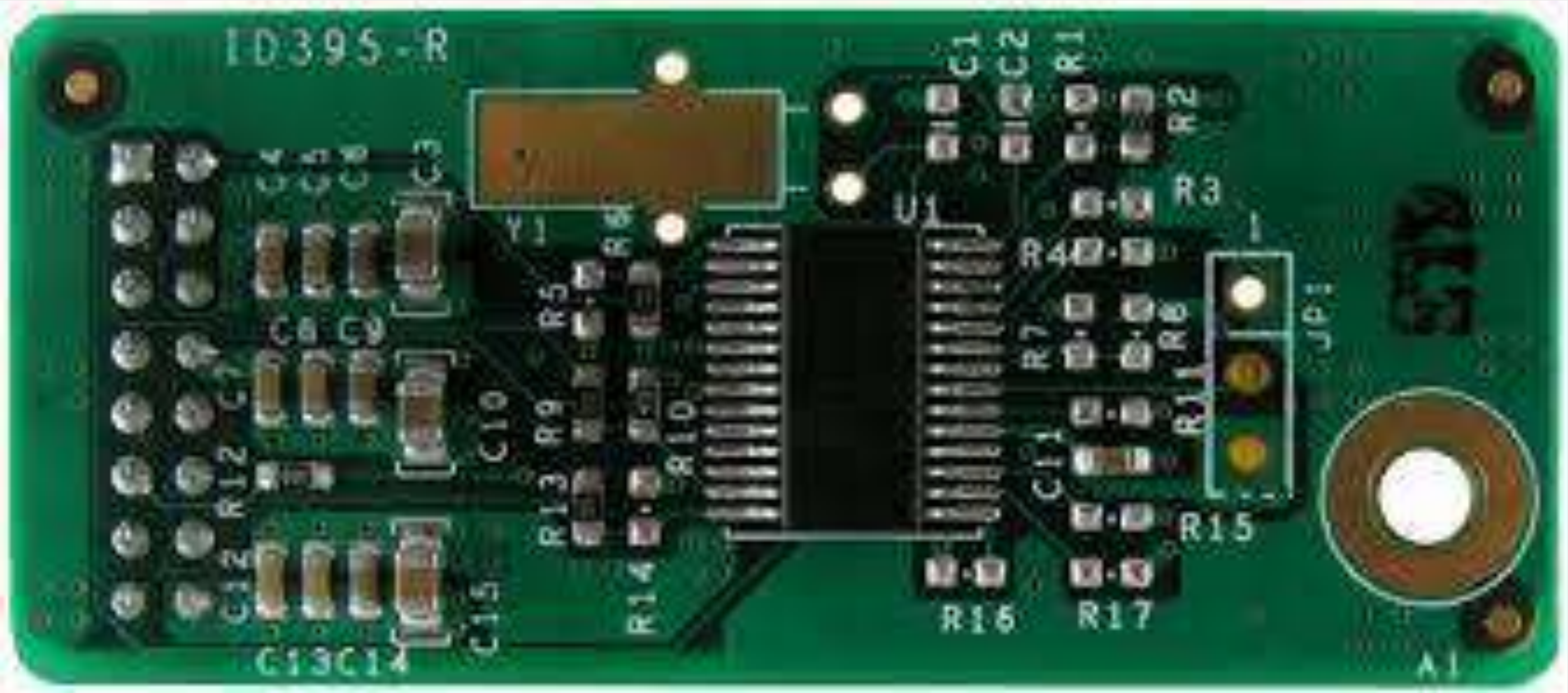
- Lots of techniques to rediscover these memory locations
- https://sploitfun.wordpress.com/2015/05/08/bypassing-aslr-part-i/
- GOT table contains locations of shared libraries at run time.
- Many dlls loaded at run time have ASLR disabled, and are in consistent, known locations!
- Simple techniques allow attacker to find them and exploit them.

Trusted Platform Modules

A trusted platform module is a cryptography chip (usually a daughter board) attached to the mother board of a PC or other computing device.

The TPM contains a small amount of *eeprom* and a dedicated CPU, ROM and temperature sensor (for seeding a true random number generator).

TPM



Trusted Platform Modules

The idea is that all security and cryptographic functions performed on behalf of the BIOS and OS are performed by the TPM, which is harder to sniff or intercept because it is hardware.

Items such as fingerprint metrics, certificates, keys and passwords can be stored on the module.

The TPM should never display it’s contents.

Trusted Platform Modules

But:

The TPM has a poor reputation due to it’s early use in enforcing DRM (copy protection).

Few manufacturers / software vendors use the TPM because of this.

Provision has been added to allow the TPM to be backed-up

keys can now be extracted from the TPM by crackers (if they have physical access).

http://www.h-online.com/security/news/item/Hacker-extracts-crypto-key-from-TPM-chip-927077.html