COS30015 IT Security

Live Lecture Week 12

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.

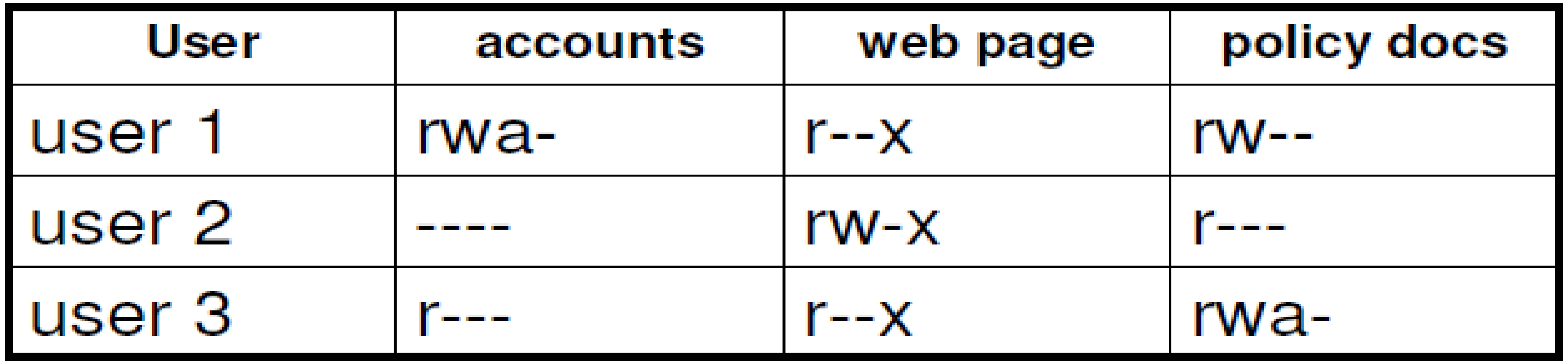
Week 1: Introduction

- Fundamental Concepts
- Security paradigms --- Access control
- Cryptographic Concept
- Implementation and Usability Issues

Security paradigms

❑ Access control / User Rights Management (ACLs)

- Both Windows and Linux support this complicated method of enforcing security.
- Individual files / directories are tagged to allow/disallow file execution, reading, writing for different user groups.
- Users are groups according to their roles / normal activities and privileges.



User	accounts	web page	policy docs
user 1	rwa-	r--x	rw--
user 2	----	rw-x	r---
user 3	r---	r--x	rwa-

Week 2: Physical Security

- Locks and Safe
- Authentication Technologies
- Physical Attacks
- Social Engineering
- Computer Forensics

Eavesdropping

Eavesdropping is the process of secretly listening in on another person’s conversation

- Keyboard Listening
- WiFi Sniffing
- MITM attacks (proxying, malware)
- Phone tapping

Phishing

Most phishing scams endeavor to accomplish three things:

- Obtain personal information
- Redirect users to suspicious websites
- Manipulate the user into responding quickly

Week 3: Operating System Security

- Operating Systems Concepts
- Password-based Authentication
- Buffer Overflow Attacks

Memory Management

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

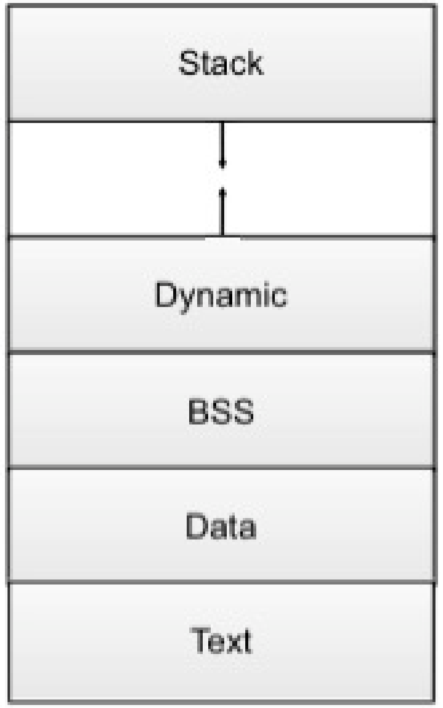
Text: machine code of the program

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

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.

Week 4: Malware

- Malware classification by infection method:
  - virus
  - worm
  - trojan
  - root kit
- Malware classification by action (payload):
  - Adware, Spyware
  - Browser hijackers
  - Bots, RATs
  - Ransomware

Virus

“A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user." -- Wikipedia

❑ "Old-school" malware was viruses written by hackers for fun and mischief.

❑ Had to be transmitted by floppy disk, etc.

❑ Capable of destroying data, crashing programs and general computer vandalism.

❑ Not the biggest problem now* –

- other types of malware (worms, trojans) have more sinister ways of infecting computers and making money for their writers.

❑ Detection is comparing a virus signature in a database with the code in a suspect file (using anti-virus software).

Worms

- A worm is a virus that can propagate without human intervention.
- Typically propagate through internet connections.
  - May be attached to web page:
  - &nbsp;<br></body></html><iframe src="http://uadrenal.com/qaqa/?daf02d89f0bb66c3b4a9ff31da01e10a" width=0 height=0 style="hidden" frameborder=0 marginheight=0 marginwidth=0 scrolling=no></iframe>
- May carry a 'payload' – a virus, or other type of malware.

  http://www.cruc.es/what-to-do-when-youve-been-hacked/

Trojans

"An unauthorized program contained within a legitimate program." (http://www.windowsecurity.com/faqs/Trojans/)

- ❑ A trojan is a container which distributes malware hidden inside itself, using un-used bytes at the end of the file.

  May be written from scratch to mimic some trusted program.
- ❑ Performs some 'normal' task (e.g. game, screensaver) but also performs some evil task when executed.

Rootkit

❑ Rootkits are a technology used by malware. They evade detection by patching the operating system kernel so that programs like *explorer.exe*, *task manager*, and commands *ls* and *ps* cannot see them.

- Root-kits have been used to enforce copy protection by Sony (https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal) and game manufacturer UbiSoft (http://www.glop.org/starforce/).

- Bugs in root-kits have become the targets of other exploits.

Week 5: Network Security I

- Network basic
  - OSI, MAC, DNS, Hub/Switch/Router, NAT, Common protocols
- Tools:
  - Ping, Traceroute/Tracert, ipconfig/ifconfig
- Attacks:
  - Sniffing a hub/switch, ARP, MIMA, DNS/Hosts

Packet Sniffing

- Packet sniffers record IP packets on the network. They were originally designed to help diagnose problems in networks.
  - Good for picking up MAC addresses, IP addresses
- Many internet-based services expect to receive user names and passwords in plain text.
  - Telnet, FTP, SNMP
- Computer users get lazy and re-use the same user names and passwords.
  - If you can get their FTP password, you can probably use it on other accounts.
- Popular Sniffers:
  - TCPDump, Snort, W*ireshark*. Windows and Linux versions.
  - reviews: http://sectools.org/sniffers.html

DoS (Denial of Service)

DOS attacks are aimed at servers on the internet

- web servers (HTTP), name servers (DNS), FTP servers
- Can be launched at specific machines if the IP address is known.

The goal is to Deny Service to legitimate customers/users.

- Customers go elsewhere
- Organisations lose money/trade/reputation

Week 6: Network Security II

- DNS Attacks
- Firewalls
- Tunneling
- Intrusion Detection

DNS Cache Poisoning Prevention

- Use random identifiers for queries
- Always check identifiers
- Port randomization for DNS requests
- Deploy DNSSEC
  - Challenging because it is still being deployed and requires reciprocity

Firewalls and port blocking

- A firewall filters incoming traffic according to a set of rules depending on things like:
  - ➢ the destination IP address or host +domain name
  - ➢ the source IP address or domain name
  - ➢ the protocol being used (bound to specific ports)
  - ➢ the port number of the destination
  - ➢ the process (program name) listening at the destination
  - ➢ the contents of a packet (high end firewalls and IDS)
- The primary defence offered by a firewall is to block particular destination ports or source IP addresses.
  - ➢ Some firewalls use NAT traversal to 'hide' the inside of the network.

Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
- e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

Week 7: Web Security

- Session Hijack Attack
- Cross-Site Scripting Attack (XSS)
- jQuery Injection, SQL Injection
- Phishing and Pharming Attack

HTTP session hijack 1

❑Attacker uses *packet sniffing* to read session ID.

- Attacker can take over a http session by writing the sniffed session ID into the attacker's cookie.

❑Defense:

- Cookie expiration date
- Https
- Cookie secure bit (cookie sent by https)

HTTP session hijack 2

❑ Attacker uses *XSS* to read cookies of authenticated visitors to a site.

- Attacker can take over a session by writing the received session ID into the attacker's cookie.

❑ Defense:

- Server side – filter/sanitise input/output
- Client side – turn off javascript, turn on Application Boundary Enforcer (ABE) privacy plugins (noscript)
- Https – no protection

XSS

❑ Reflected XSS attack

- Allows executable html script (javascript, VB script) to be injected by the user into a web application.
- When the application replies with a constructed page, the page includes the executable script.
- Useful for tricking users into allowing script-heavy sites to change browser settings.

❑ Stored XSS attack

- Involves executable script being stored on a server (chat room, forum), which executes when it is displayed by another user.

XSS: DOM-based attack

❑ Scripts running in your web browser have access to the browser's DOM (document object model), a hierarchy of objects containing everything displayed and stored on each web page in each instance of the browser.

❑ Clever scripting can be used to

- change the contents of the page, adding options, setting default selections.
- echo/send private data to 3rd parties (similar to stored and reflected attacks).
- Access the contents of other browser windows/tabs - largely impossible since Google introduced tab sandboxing.

Week 8: Cryptograph & Secure Communication

- Symmetric Crypto (Pre-shared key)
- Public Key Crypto (asymmetric key)
- Hash Function
- PGP/GPG (web of trust) & SSL & Digital Signature

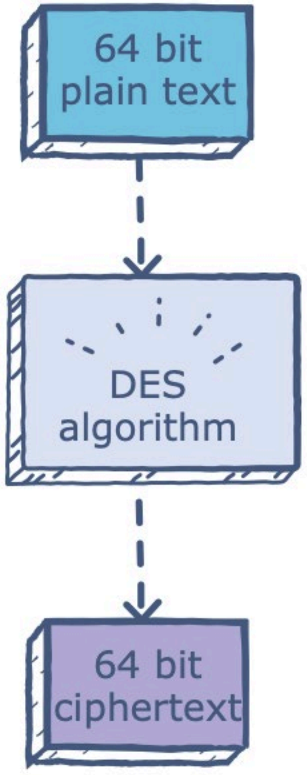
Data Encryption Standard (DES)

Definition

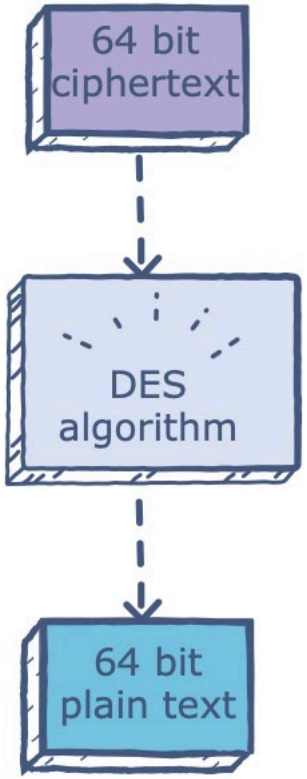
- Block Cipher
- symmetric key
- Out-dated now

History

- 1972: National Bureau of Standards begins search
- 1975: DES: Lucifer by IBM, modified by NSA Approved by NBS ‘76, ANSI ‘81
- renewed every 5 years by NIST
- now considered obsolete



Encryption



Decryption

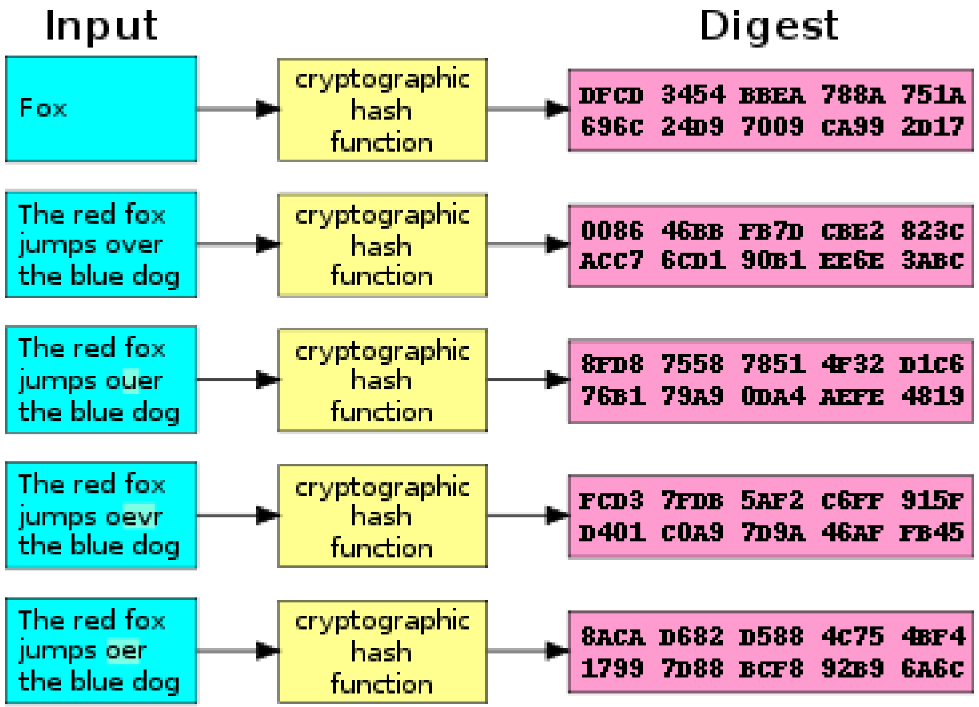
Public Key Cryptography

- A.k.a. asymmetric cryptography
- Two keys – public and private
- Public key is shared
- Private key is kept secret
- Well suited for organizations

Hash Function

cryptographic hash function (CHF)

- a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg

Pretty good privacy (PGP)

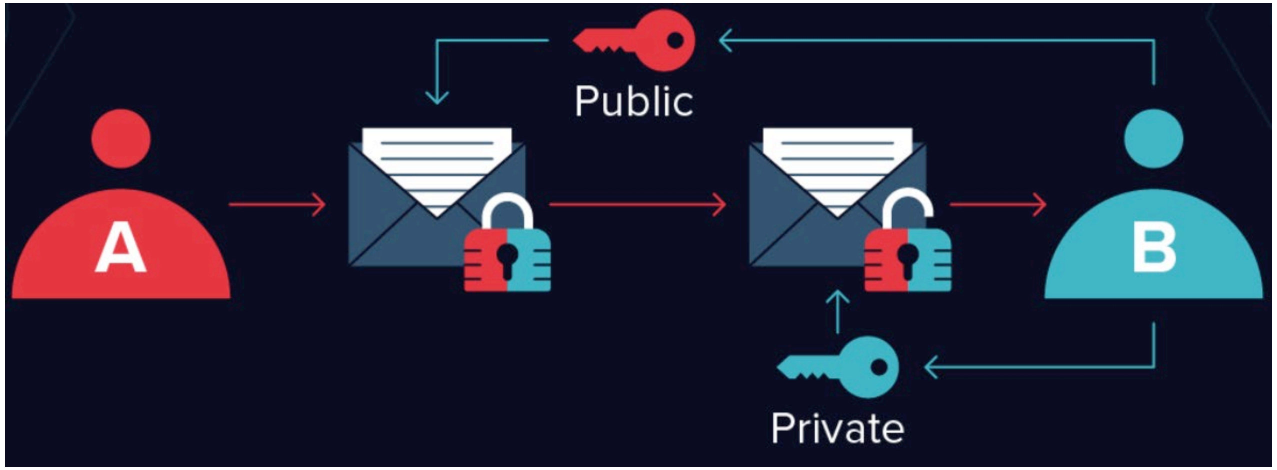
A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
   -
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately
   yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3
   mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

How it works:



Week 9: Distributed-Application Security

- Security Models
  - Access control models
- Vulnerability assessment
  - Auditing and Pen-testing
- Kerberos
- Secure Storage
  - Cloud Storage?
  - Cloud Security Issues?
  - Trusted Platform Modules

Penetration Testing

- Simulated attack.
- Black box or white box.
- Get written agreement from customer.
- Take notes throughout the pen-test.
- Report details of findings and vulnerabilities to customer.
- Suggest mitigation, fixes.

Penetration Testing

1. Enumeration, network reconnaissance, IP scan, port scan, DNS records.
2. Network Vulnerability analysis, port scans, footprinting, find vulnerable services.
3. Web application testing, SQL mapping, injection, XSS testing, javascript injection, php passthrough, injection, fuzz testing.
4. Exploit vulnerabilities, establish foothold, additional reconnaissance, obtain privileged information/access.

Penetration Testing – Tool of Burp Suite

1. Burp Suite is an integrated platform for performing security testing.
2. Burp Suite is written in java and widely used automation framework, created by PortSwigger Web Security.
3. The tool has two versions:
    1. a free version that can be downloaded free of charge
    2. a full version that can be purchased after a trail period.

Week 10: Distributed-Application Systems

- Spam
- E-mail Security
- Structured Query Language (SQL)
- Digital Rights Management (DRM)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Spam Filtering

- Keyword matching.
  - Check through blacklist of words.
  - Easily bypasses by spammer adding spaces, punctuation, substitute letters

- Bayesian Filtering.
  - Uses machine learning to distinguish between Spam and normal e-mail
  - Needs to be “trained”

- ALPACAS: **A** **L**arge-scale, **P**rivacy-**A**ware **C**ollaborative **A**ntispam **S**ystem.
  - Identifies “fingerprints” of spam e-mail based on style, layout
  - Changes on content, obfuscation don’t trick it

E-mail Authentication

- Authentication of sending user (client) relies on public key crypto:
  - ➢ Everyone must have a certificate
  - ➢ Not used much

- Authentication of the organization:
  - ➢ Uses certificate embedded in gateway (e.g. Astaro appliance)
  - ➢ Easier to use, so more common

Week 11: Law and Order

- Law
- Fraud
- Ethics
- Identity theft
- Stalking
- Filtering
- eForensics

Types of eForensics

Network forensics

- Packet capture, logs – record evidence while the crime is occurring.
- Cloud forensics – relies on cooperation of cloud provider, cloud API, foreign government.

Disk forensics/phone forensics

- Live (no re-boot)
- Dead/offline/static (boot into another OS)
- Acquisition (of drive image)
- Acquisition (of RAM)

Types of Forensics

- Memory forensics
  - Contents of RAM,
  - running processes,
  - active network connections (TCP) and
  - Traffic (UDP)