50005 - Networks and Communications - Lecture 5

Oliver Killane

15/02/22

History and Terminology

Lecture Recording

Lecture recording is available here

H/P/V/A/C

- **Hacker**
  Highly competent computer ethusiast/engineer

White Hat	Informs organisations of vulnerabilities before going public.
Grey Hat	Only informs if paid.
Black Hat	Malicious, uses findings to do illegal activity.

- **Phreaker**
  Phone hacker, as phone network has become more digital they have been more often in the hacker category.

- **Virii**
  Computer virus creators.

Ransomware	Encrypt files, decrypt for ransom.
Spyware	Keyloggers, browser addons to track, often include adware.
Trojans	Software for botnet zombies, often appear as legitimate software.

- **Anarchist**
  Politically active hackers, when peaceful called hacktavists, when not so much they are anarchists. Some parts of the anonymous movement could be considered anarchists.

- **Crackers**
  Make use of tools built by others (e.g purchasing virus software, infiltration tools). Most modern digital organised crime would be in this category.

- **DDoSers**
  Someone who participates in **Distributed Denials of Service** attacks. **Low Orbit Ion Cannon** is an example, it is used to stress tests networks.

- **Spammers/Botters**
  Send unsolicited messages (often advertisements) en-masse, usually using botnets.

- **Warez**
  Information piracy, distribution software, images & videos without the legal right to do so. Examples include the priate bay piracy site.

- **Whistleblowers**
  Former employees of an organisation that leak/"blow the whistle" on often malicious, illegal, or immoral activity even when it is illegal to do so (e.g have signed a **Non-Disclosure Agreement**).

- **Social Engineers**
  Use of social manipulation to compromise the human security of an organisation.

Phising	Usually over email, pretending to be some organisation they are not.
Vishing	Via voice messages.
Smishing	Via **SMS**.
Catfishing	Via impersonation (e.g fake social media profiles).

Black Hat Methods

- **Credential Reuse/Stuffing**
  Previously leaked login credentials are used against many sites (often people use the same email and password comnbination on many sites).

  The site have I been pwned can be used to check if your own details are included in any leaks.

- **Packet Sniffing**
  Monitoring network traffic not intended for your **NIC**, e.g over a wireless network, on a router or switch you control.

- **Code/SQL Injection**
  Using data infput to get a system to runb your code. If the system does not sanitise its input, some keywords or code contained may be executed. This is often SQL Injection, as most opportunities to input data are related to databases. An example is the log4j bug/exploit expained well by this video.

- **Session/Cookie Hijacking**
  Stealing a session cookie to be authenticated as them in an ongoing browser session.

- **Wardriving**
  Searchinbg for and abusing open/unsecure **WiFi**s.

- **Trashing/Dumpster Diving**
  Checking physical waste for useful informatrion (e.g bank statements, official records).

- **Clickjacking**
  Using hidden html divs, popups to force a user's click to redirect to a malicious destination.

- **Bait & Switch**
  Luring a user to click with a seemingly legitimate advertisement, only to redirect them to something else.

- **Spoofing**
  Falsifying identification to receive packets intended for another recipient.

IP	Fake your IP as another (Layer 3).
MAC	Media Access Control address distinguishes between different **NICs**.
DNS	DNS cache poisoning (falsifying the cache to pretend to be at a given domain).

- **Rootkits**
  Allows attackers to secretly enter external systems, often installed as part of a virus.

- **Keyloggers**
  Records all keyboard input, sending key-logs back to the hacker, or allowing them to be remotely accessed.

  A potential advantage of password managers is that keyloggers cannot be used effectively to detect passwords if they are not typed.

- **Trojans**
  Allow a hacker to remotely control an entire system, often as a zombie on a botnet.

- **Evil Twin**
  Where a hacker attempts to lure victims into using their network, gaining information from the victim (e.g network histroy) & potentially sending malicious data to the user when they use it.

White Hat Tools

- **Tails**
  Tails is a portable operating system designed to be usable from a usb drive, and to never store data, thus removing data integrity related security issues.

- **Kali Linux**
  Kali is an operating system designed for penetration testing and other security related work. It comes bundled with many useful tools such as **Metasploit** and **Nmap**. It is supported on ARM, as well as by the windows subsystem for linux.

- **Metasploit**
  Metasploit is a tool use to automatically scan systems for vulnerabilities based on a large database of known vulnerabilities and exploits.

Cybercrime Laws

In the **UK** many laws (listed below) apply. Physical locations of hosts is used to determine which nation's laws are used, meaning **US** law is also very important (common country to host from).

1964	Obscene Publications Act (In reference to spam)
1978	Protection of Children Act (In reference to online abuse & spam against children online)
1988	Copyright, Designs and Patents Act
1990	Computer Misuse Act
1999	Amendment to the Protection of Children Act (Still being changed)
2000	Freedom of Information Act
2000	Regulation of Investigatory Powers Act (In reference to computer/phone surveillance)
2002	e-Commerce Regulations Directive
2003	Criminal Justice Act
2005	Disability Discrimination Act (In reference to online abuse & spam)
2010	Amendment to the Copyright, Designs and Patents Act
2013	Defamation Act (In reference to online abuse & spam)
2017	Digital Economy Act
2018	Data Protection Act

In the **US** there is the DMCA (Digital Millennium Copyright Act).

Standards Organisations

IANA	Internet Assigned Numbers Authority, deals with **DNS**, **IP** Addressing and more standards.
ICANN	A nonprofit organisations responsible for coordinating standards for the maintenance and running of namespace and numerical space databases for the internet.
IEFT	Internet Engineering Task Force, a collection of working groups (e.g routing, transport, security) concerned with developing the internet.
ISOC	Internet Society, dedicated to furthering beneficial use of the internet.
EFF	Electronic Frontier Foundation, a politically active nonprofit dedicated to defending privacy, free speech and freedom to innovate online.
W3C	The World Wide Web Consortium develops standards to help developers build tools on the web smoothly.
ISO	International Organisation for Standardization, you can find their standards for information technology here.

Attack Examples

Definition: Heartbleed

A bug in OpenSSL 1.0.1 first identified onm 14/03/2012 and patched on 07/04/2014.

OpenSSL is an implementation of the TLS (transport Layer Security)/SSL (Secure Sockets Layer) protocol that allows for secure website access (https://)

The bug allowed users to gradually reveal server memory in chunks of $64KB$. It is not known if it was used in any exploits.

Definition: KRACK

The **WPA2** (wireless protected access protocol) used in Wifi. Android devices could be forced to use a zero-based key, rendering the encryption useless.

The full explanation can be found here.

It has been patched, but the next version (**WPA3**) was released in 2020 which was meant to be more secure also has issues.

Definition: WEP

Wired Equivalent Privacy is a security algorithm for wireless networks, it has been shown to be vulnerable many times.

Network Security Issues

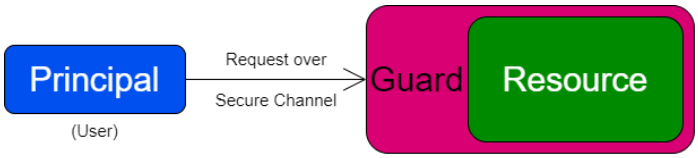
Lecture Recording

Lecture recording is available here

Basic Security Concepts

Access Control	Only certain users can access certain resources.
Authentication	User knows resource is as identified, and resource that user is as identified.
Confidentiality	Users can limit access to their resources and information, and limit access to see their traffic over a channel.
Data Integrity	Users cannot damage the integrity of a resource (e.g crash a webserver by visiting).
Non-Repudiation	User cannot deny communication occurred, secure logs held and can be audited.

Access Control



Assuming the channel used for communication is secure, the guard needs to determine:

- Which principals (users) can access the resource.
- Where principals can be located (e.g user's **IP** address is outside the organisation's network).
- What requests principals can make for this resource (e.g can view database, but not send mutating **SQL** commands).

Security can be difficult as:

- Many systems used by an organisation can be different (Heterogeneous systems) (e.g bank has different OSes several models of ATM).
- Users can be careless (e.g reusing passwords), this include system administrators and managers.

Firewalls

Definition: Firewall

A security barrier between internal and external networks.

- **Application Level Gateway**
  An application that runs, checks requests in the application layer. Can also be a proxy, using an extra set of rules to decide if to share requests or responses, or to send on requests.

  Examples include **SOCKS** and netfilter's iptables.
- **Proxy Server**
  Runs on the network protecting it by making requests and receiving responses on its behalf (to the external network). Can also include caching of results.
- **Circuit Level Gateway**
  Creates a circuit of proxies, sending data between each node in the circuit (for example **Tor**).
- **Packet Filtering**
  Filtering packets with a set of rules based on contents, source and destination IP address/port, only alowing non-suspect packets through. Can also be stateful, considering not just a single packet traffic to a host over some time period.
- **Hybrid**
  Use a combination of all the above.

They can be software or hardware based, with hardware solutions being faster, but more difficult to change (e.g if a vulnerability is found).

Definition: Proxy

Makes requests and recieved responses on behalf of a client, can filter in and outgoing traffic.

- **Normal**
  Client is aware of proxy, and connects to it to use it.
- **Transparent**
  Client is unaware, for example a local router could act as a proxy. Requires not intervention from client.
- **Reverse**
  Runs on the receiving side, impersonating a server and protecting a server from the external network. (Much like **CDN** load balancing)

Definition: Bastion Host

A server that expects to be attacked.

- Runs a minimal trusted/secure OS.
- Only essential applications (e.g no window manager needed).
- All possible limits enabled (readonly file system, no mounts, file permissions all set, no normal user accounts)
- Typically managed over a dedicated terminal

It passes requests on from the external network, and acts as a proxy firewall.

It drops any connections it determines are suspect using packet filtering (usually stateful) and other techniques.

Example: iptables

iptables can be used on linux to set packet filters. It consists of several tables, each containing chains of rules on managing network packets.

Note that it requires root as it interfaces directly with the linux kernel's firewall.

Example: tcpd

The linux **TCP** Daemon controls access to unix services & can monitor requests to services (e.g **ftp**, **exec**, **rsh**, **telnet**).

It uses two files, `/etc/hosts.allow` and `/etc/hosts.deny` to determine access.

Firewall Avoidance

SSH

We can attempt to avoid a firewall by tunneling through with an allowed protocol, to then use the internal.

An example of this is with **ssh**. We can get through the firewall on ssh, and then send our requests through ssh to the internal network, to get responses, and use services the firewall may normally block.

Spoof MAC Address

Can re-write the **MAC** address if the firewall is blocking requests based on it (MAC address blacklisting or whitelisting).

Spoof IP Address

Much like with **MAC** address, however stateful firewalls will most likely detect this.

(VPN) Virtual Private Network

Much like with **SSH**, we can tunnel through the firewall. Provided the tunnel is secure (e.g using **SSL**) the firewall will not be able to decipher your traffic.

Other Security

Definition: (IDS) Intrustion Detection System

Detects intrustions to inform the system (e.g a DDoS attack), however does not perform actions to stop the detected intrusion.

Definition: (IPS) Intrusion Prevention System

Actively prevents intrusions (e.g blocking **SYN** flooders attempting to perform a DDoS attack), can work with an **IDS**.

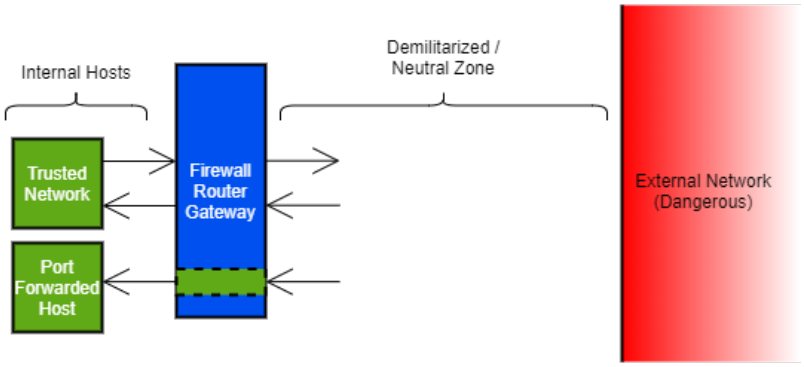
Definition: (NGFW) Next Generation Firewall

A stateful firewall that comes with an **IPS** / **IDS** system.

Definition: (UTM) Unified Threat Management

Similar to a **NGFW** but with added features such as spam filters, antivirus etc.

(DMZ) Demilitarized Zone



Definition: (NAT) Network Address Translation

Rather than expose the **LAN IP** address of an internal host, routers translate the IP addresses to their own public IP to send, and when receiving from their public IP back to the IPs of internal hosts.

Definition: Port Forwarding

To expose an internal host to the external network without placing it in the **DMZ** we can set the router to forward all packets arriving at a given port straight to the internal host.

For example we could specify any packet recieved on the router's IP at port 3472 should be immediately forwarded to the **NAT** based **LAN IP** of "host A" on port 80.

Useful for hosting servers, even for games (e.g minecraft servers require port forwarding).

Logging and Auditing

Most systems keep logs, they are useful for:

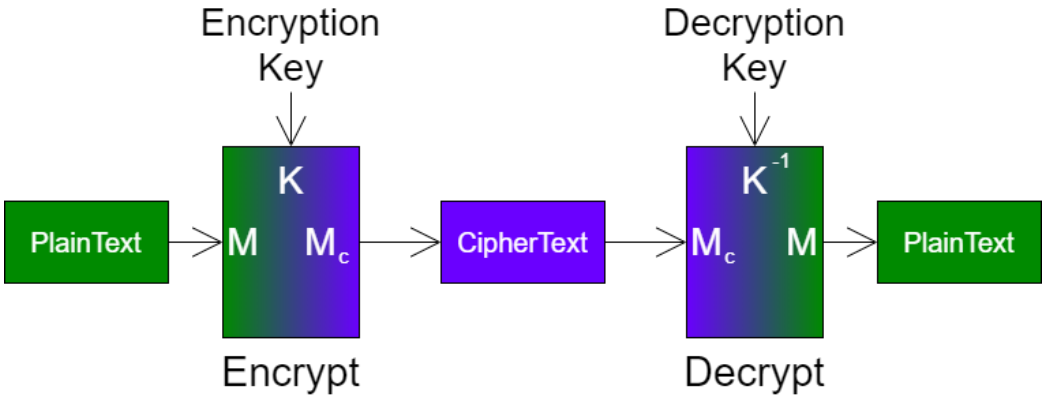
- Checking for missed breaches. An attack may only be discovered in logs after the fact.
- Forensics, providing evidence to law enforcement to discover who the purputrators of an attack are.
- Determining how a system was exploited in an attack, in order to patch it.
- Ensuring good practices are being followed (e.g if an unsafe features starts to be used).
- Detecting other network issues (e.g congestion).

Logs can be found on linux at `/var/log/` and the event viewer in Windows.

Cryptography

Lecture Recording

Lecture recording is available here

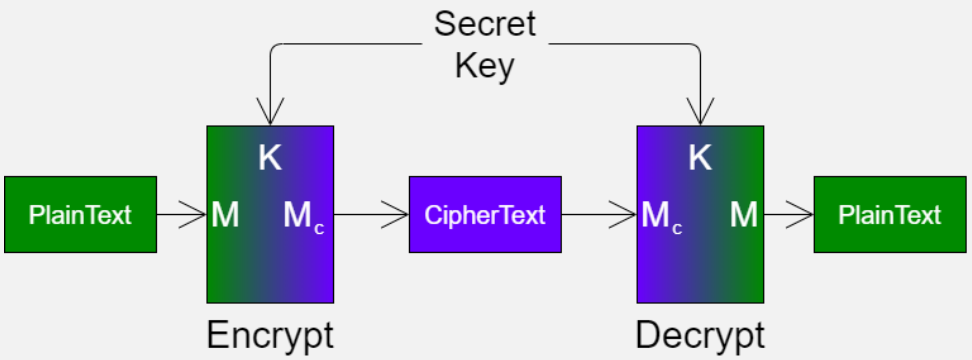


A good encryption algorithm should ensure:

- Given M_C it is only possible to find M by going though all possible values of K^{-1} (brute force attack).

- Given M and M_C it should be difficult to get the values of K and K^{-1}. (e.g caesar cipher is poor as we can just calculate the shift)

Definition: Symmetric and Secret Key Encryption



The same key is used for encryption and decryption (symmetric), and this key is secretly shared between sender and receiver (not on an unsecure channel) (secret).

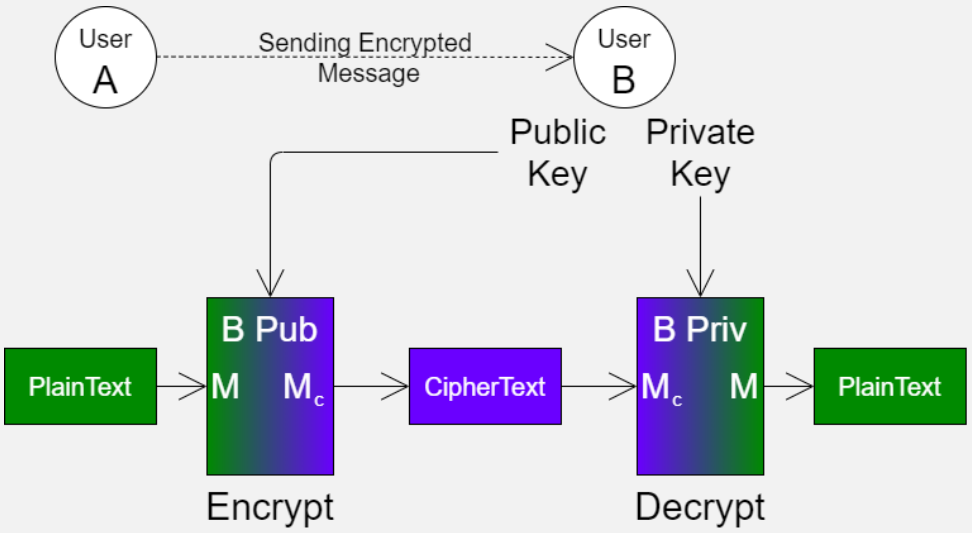
- Must secretly disclose key to communicate.
- Faster encryption/decryption than **Asymmetric**.

An example is **DES** (**Data Encryption Standard**), though this has a short key length and is now too insecure for general use (wikipedia article here).

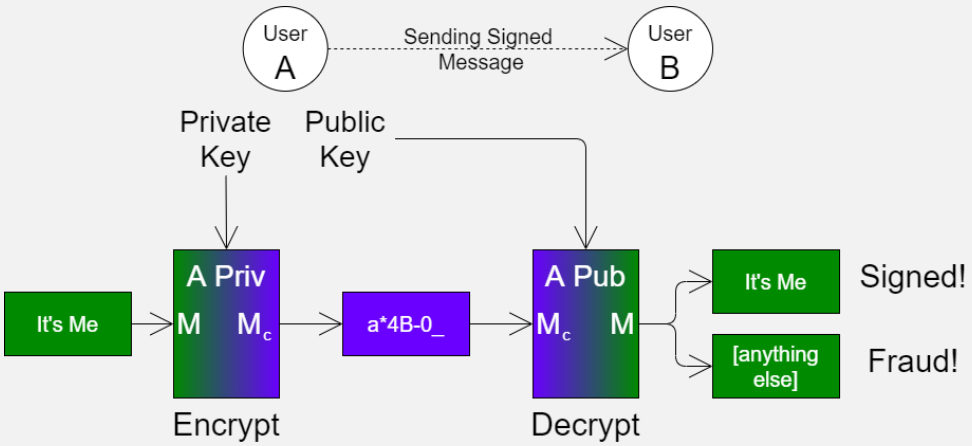
Definition: Asymmetric and Public Key Encryption

Each user has a **public** and **private** key.

For confidentiality: Sender encrypts with receiver's public, receiver decrypts with their private.



For signing: Sender encrypts with their private key, receiver decrypts with sender's public key, if value was successfully decrypted then we know the message was from the sender with the public key we used.



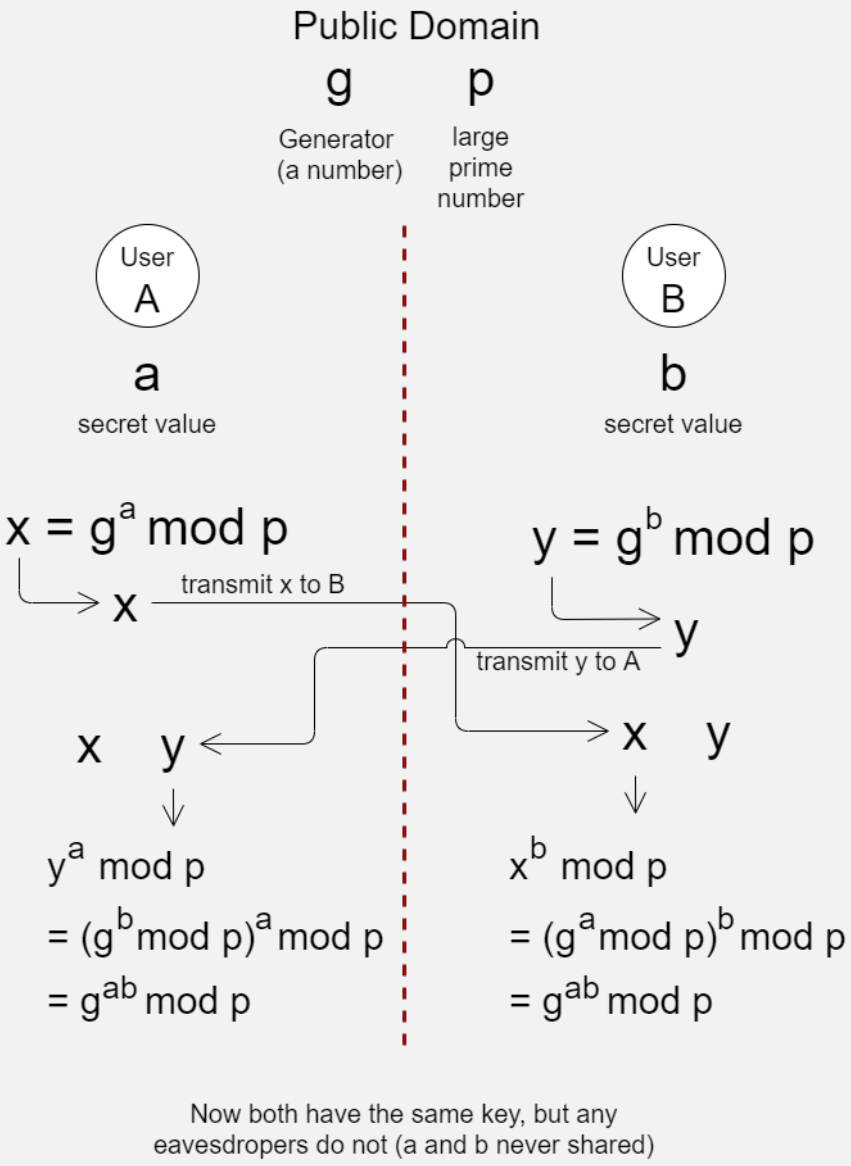
We can then combine these, encrypting a message, but including a signed segment inside to verify the sender. We can also combine with symmetric encryption to sign symmetrically encrypted files (e.g check if a password protected file is from the correct sender/is not tampered with). Foe example GPG.

The main points are:

- No need to disclose private information to communicate securely so, can start communication on unsecure channel. 11
- Hence more secure than **Secret Key** encryption.
- However is slower to encrypt and decrypt.

An example of this is **RSA** which uses current difficulty in prime factor decomposition to ensure brute force attacks are computationally intractable (wikipedia article is here).

Definition: Diffie-Hellman Key Exchange



Definition: Kerberos (Needham & Schroeder)

A key distribution system for secret keys, using a trusted server.

- Kernberos authenticates you with a password.
- It can also authenticate the user/resource you intend to communicate with.
- Generates a ticket which allows for communication.
- Ticket can be used up to a time limit, after which you must get another ticket.
- Originally vulnerable to **Man/Monster in the Middle** attacks, though these have since been addressed.

Definition: Hashing

In cryptography, a hash function converts some data into a fixed size alphanumeric string.

- The same input data always produces the same hash value.
- Not possible to derive the original input from the hash value (unlike encryption).
- Can be used as a checksum to verify data (e.g that the contents of a file are unchanged/not tampered with).
- Many old hash functions have been broken (either algorithm issues, or all possible hashes now determines - rainbow tables).