MONASH University
Information Technology

FIT5163:Introduction to Cryptography for Cybersecurity

MONASH University
Information Technology

FIT5163: Introduction to Cryptography for Cybersecurity

LN01:
Introduction to Information Security

Information Security

- **What is information security about**?

Information Security

- **What is information security about**?
  - prevent attacks, or failing that, to detect attacks on information-based systems

Information Security

- **What is information security about**?
  - prevent attacks, or failing that, to detect attacks on information-based systems
- **What does information security include?**

Information Security

- **What is information security about**?
  - prevent attacks, or failing that, to detect attacks on information-based systems
- **What does information security include?**
  - **Security attack/threat**: a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).

Information Security

- **What is information security about**?
  - prevent attacks, or failing that, to detect attacks on information-based systems
- **What does information security include?**
  - **Security attack/threat**: a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
  - **Security service**: a measure which can be put in place to address a threat or counter an attack (e.g. provision of confidentiality).

Information Security

- **What is information security about**?
  - prevent attacks, or failing that, to detect attacks on information-based systems
- **What does information security include?**
  – **Security attack/threat**: a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).

  – **Security service**: a measure which can be put in place to address a threat or counter an attack (e.g. provision of confidentiality).

  – **Security mechanism**: a means to provide a service (e.g. encryption, digital signature)

LN01: Outline

- Security attacks
- Security services
- Security mechanisms
- Security standards

LN01: Outline

- Security attacks
- Security services
- Security mechanisms
- Security standards

Security Attacks

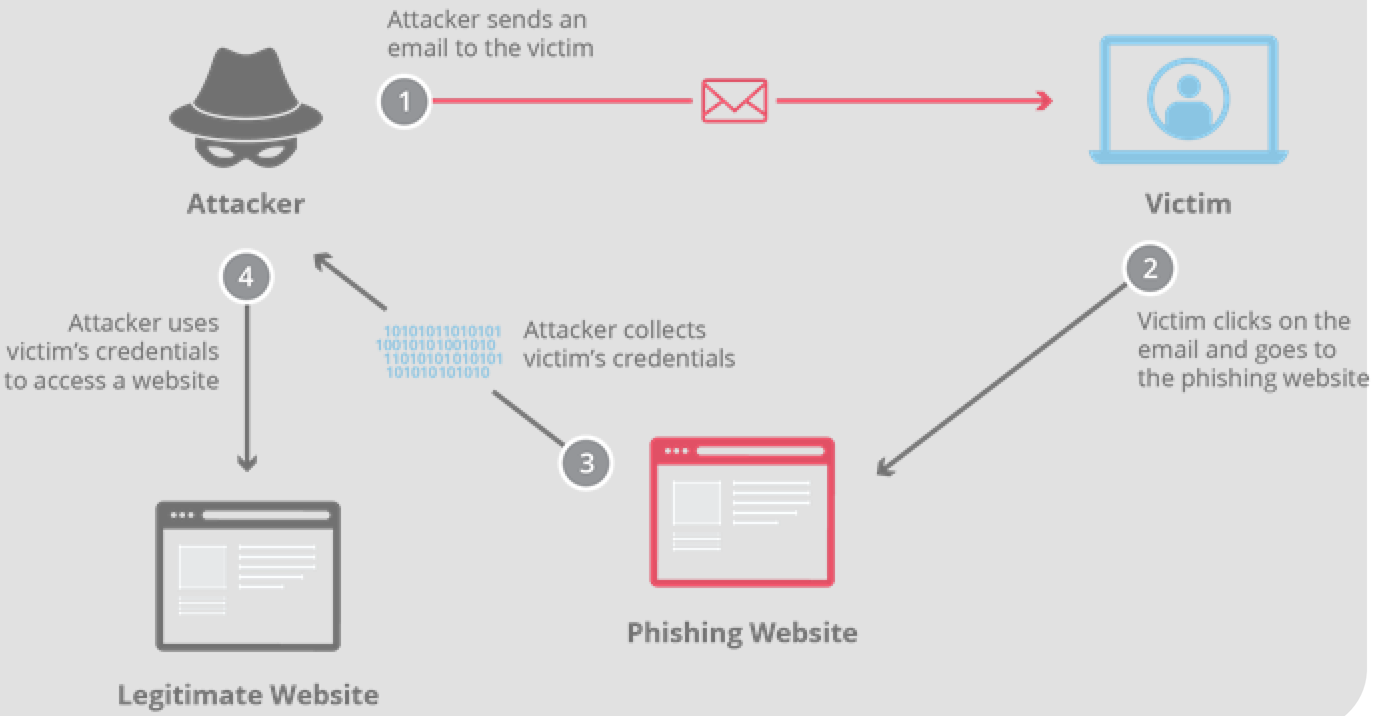
- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).

Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing

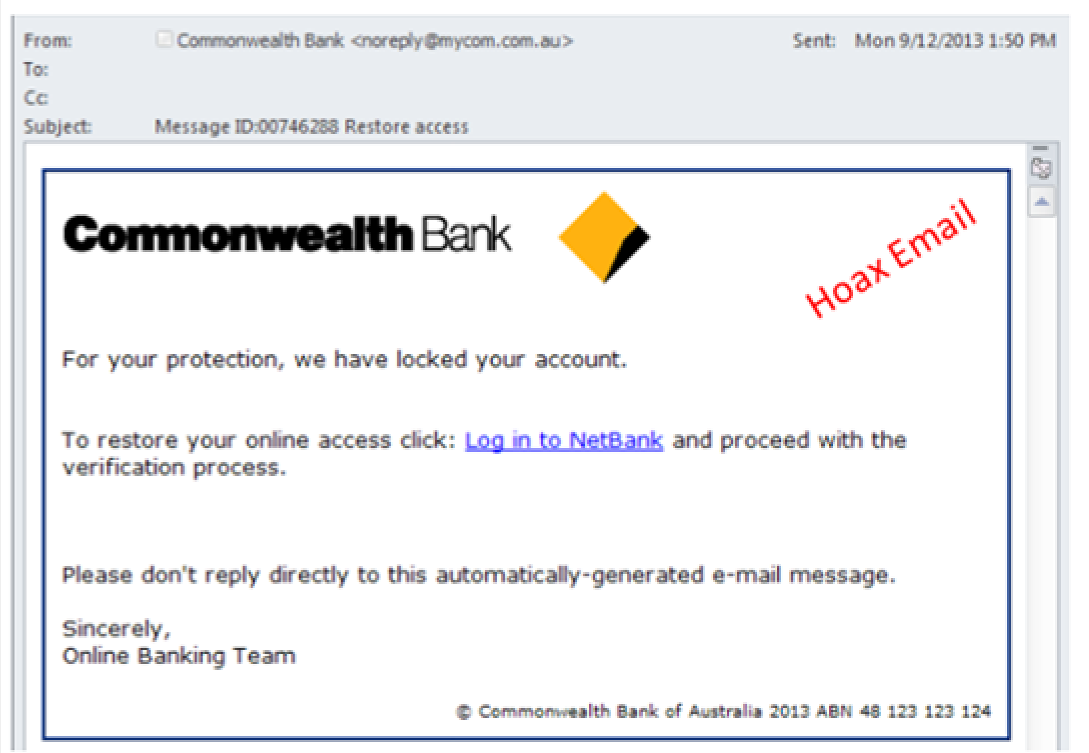
Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing



From: Commonwealth Bank <noreply@mycom.com.au>
Sent: Mon 9/12/2013 1:50 PM
To:
Cc:
Subject: Message ID:00746288 Restore access

Hoax Email

For your protection, we have locked your account.

To restore your online access click: Log in to NetBank and proceed with the verification process.

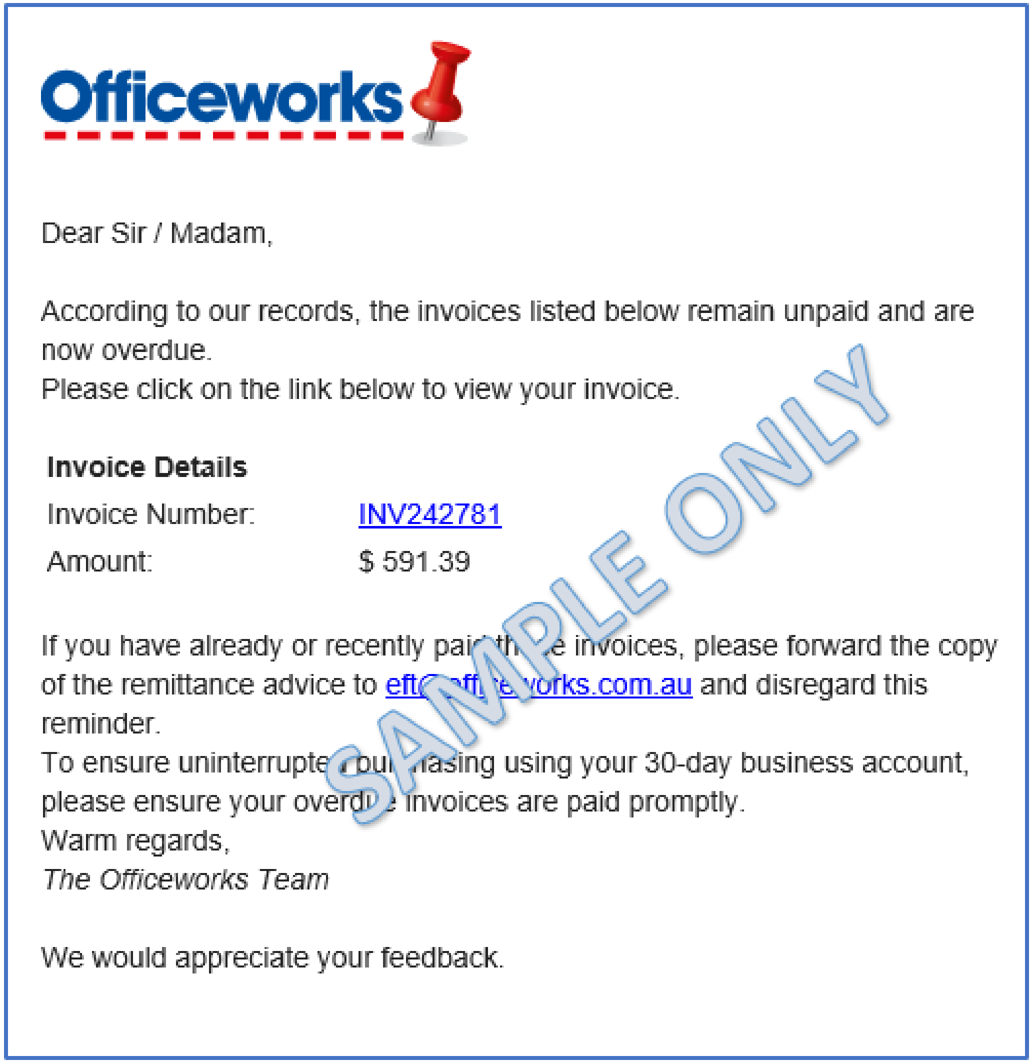
Please don't reply directly to this automatically-generated e-mail message.

Sincerely,
Online Banking Team

© Commonwealth Bank of Australia 2013 ABN 48 123 123 124

Security Attacks

- **Security attack/threat:** a p
  may be breached (e.g., los
- **Examples**
  - Phishing



Officeworks

Dear Sir / Madam,

According to our records, the invoices listed below remain unpaid and are now overdue.
Please click on the link below to view your invoice.

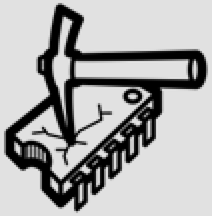
Invoice Details	
Invoice Number:	INV242781
Amount:	$ 591.39

If you have already or recently paid these invoices, please forward the copy of the remittance advice to eft@officeworks.com.au and disregard this reminder.
To ensure uninterrupted purchasing using your 30-day business account, please ensure your overdue invoices are paid promptly.
Warm regards,
The Officeworks Team

We would appreciate your feedback.

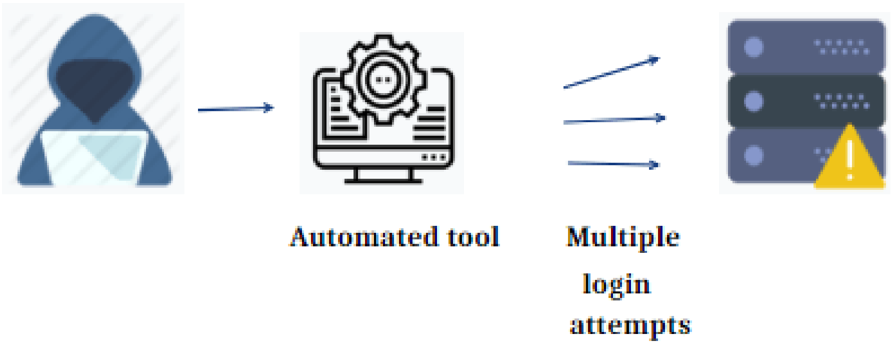
Security Attacks

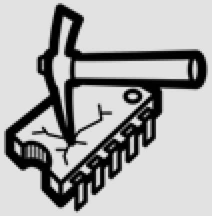
- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing
  - Brute-force



Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing
  - Brute-force





Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing
  - Brute-force
  - Man-in-the-middle

Image source: http://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/

Security Attacks

- **Security attack/thr**

  may be breached (e

- **Examples**
  - Phishing
  - Brute-force
  - Man-in-the-middle

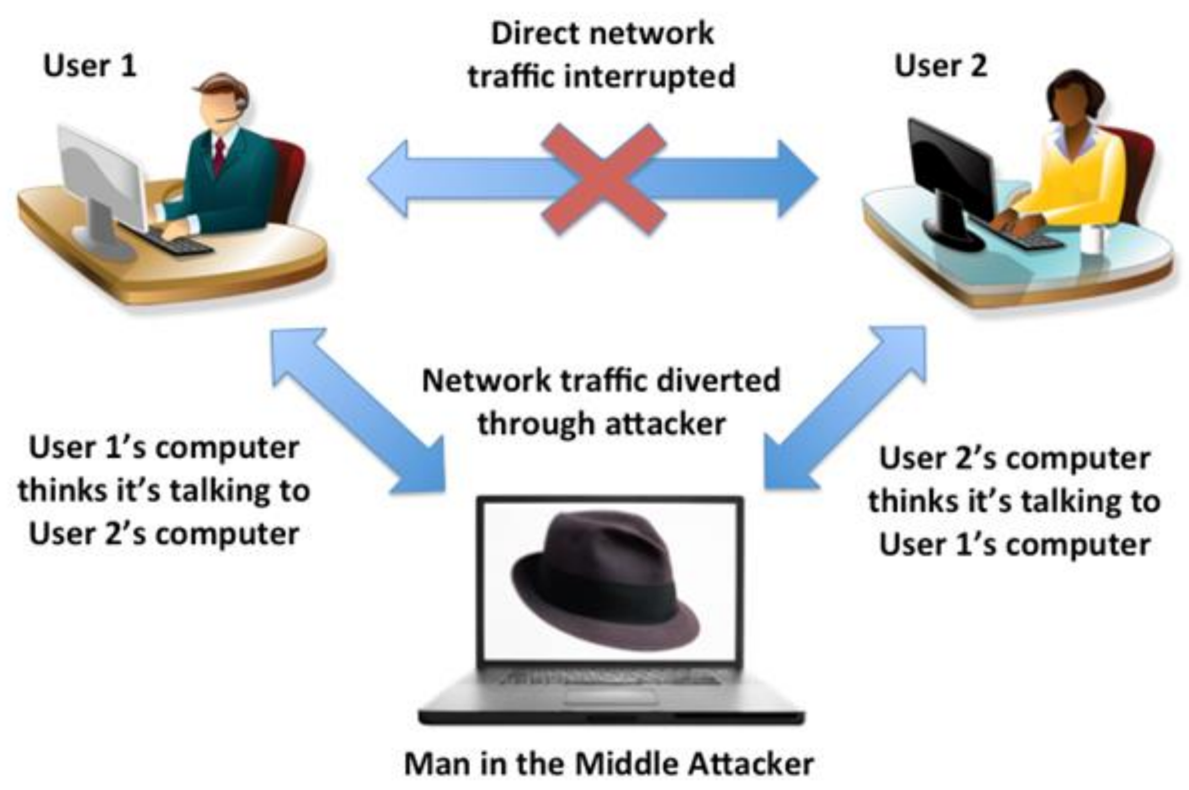

User 1
Direct network traffic interrupted
User 2
Network traffic diverted through attacker
User 1's computer thinks it's talking to User 2's computer
User 2's computer thinks it's talking to User 1's computer
Man in the Middle Attacker

Image source: http://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/

Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breached (e.g., loss of integrity or confidentiality).
- **Examples**
  - Phishing
  - Brute-force
  - Man-in-the-middle
  - DoS/DDoS

Image source: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Security Attacks

- **Security attack/threat:** a possible means by which a security policy may be breac
- **Examples**
  - Phishing
  - Brute-force
  - Man-in-the-
  - DoS/DDoS

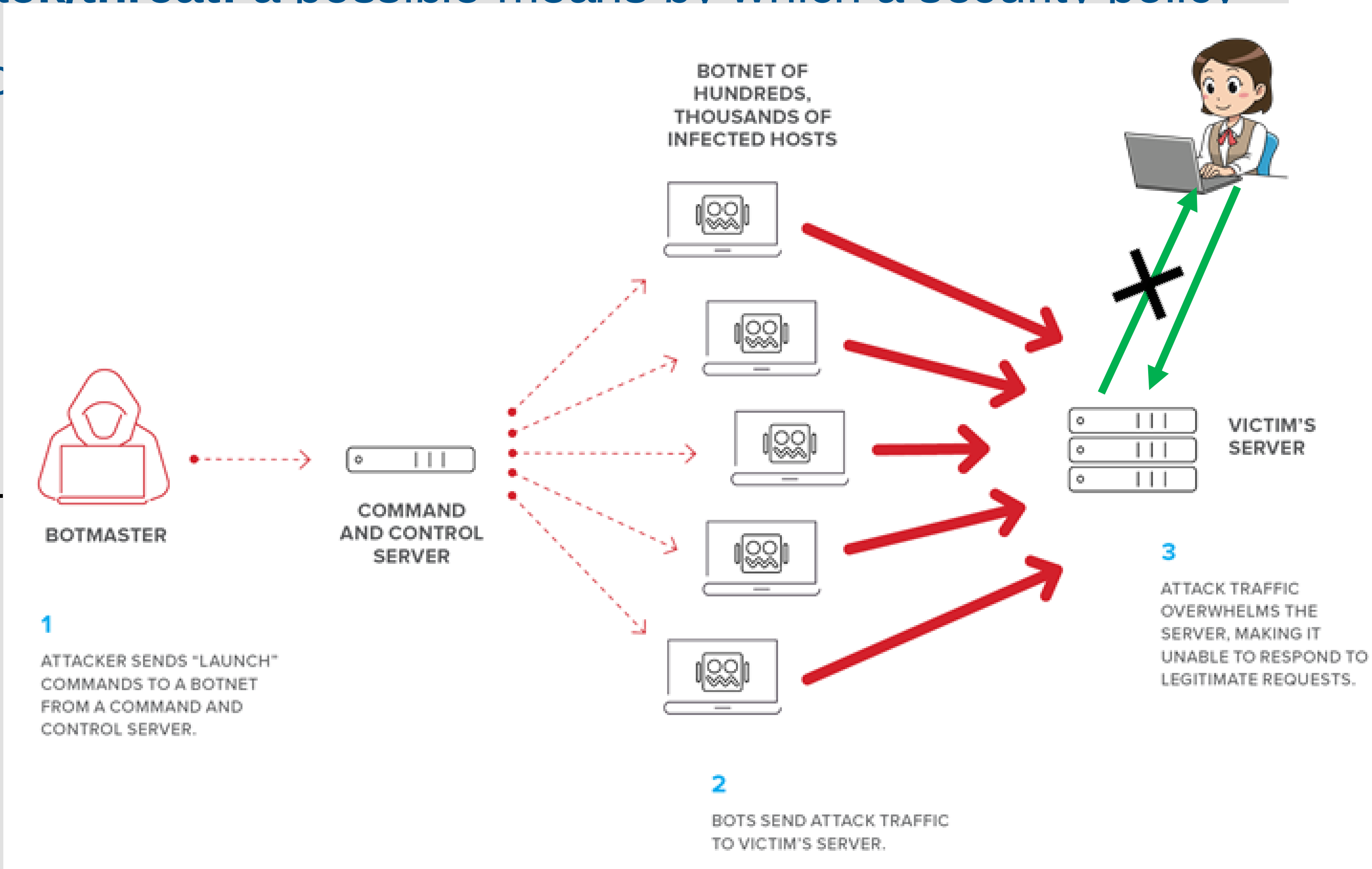

BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS
BOTMASTER
COMMAND AND CONTROL SERVER
VICTIM'S SERVER
1
ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND AND CONTROL SERVER.
2
BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.
3
ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

Image source: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Other Typical Attacks

- Botnets
- Viruses, worms, trojans
- Malware
- SQL injection
- …

Reality Attacks Examples

- In 2013, a group hacked into the Associated Press' **Twitter** account and tweeted that President Obama had been injured in explosions at the White House
- In 2020, **Amazon Web Services** was hit by a gigantic DDoS attack
- In 2019, **Canva** suffered an attack that exposed information of 137 million users
- In 2020, a **Twitter** breach targeted 130 accounts, resulted in attackers swindling $121,000 in Bitcoin through ~300 transactions

Attack Target Resources/Assets

- Information/data
  - Password, credit card, e-health records
- Service
  - Storage service, data process services
- Hardware
  - RAM, cache, hard disks, GPU
- Software
- Firmware
  - BIOS
- …

Motivations of Attacks

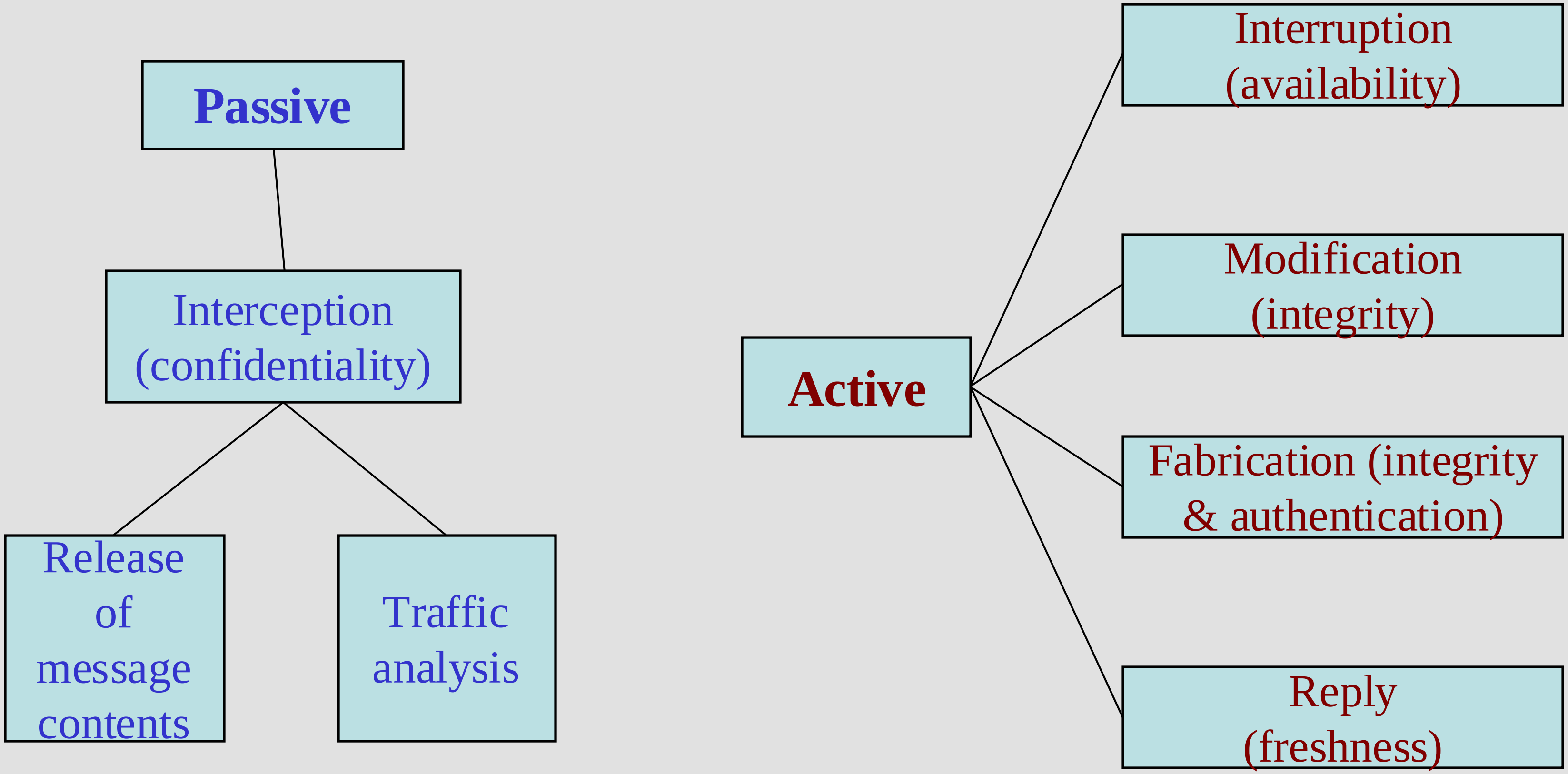
- Obtain/access private data/information: break confidentiality
- Bypass authentication for accessing private resources
- Break the availability of resources
- Breach the integrity of resources

Exercise

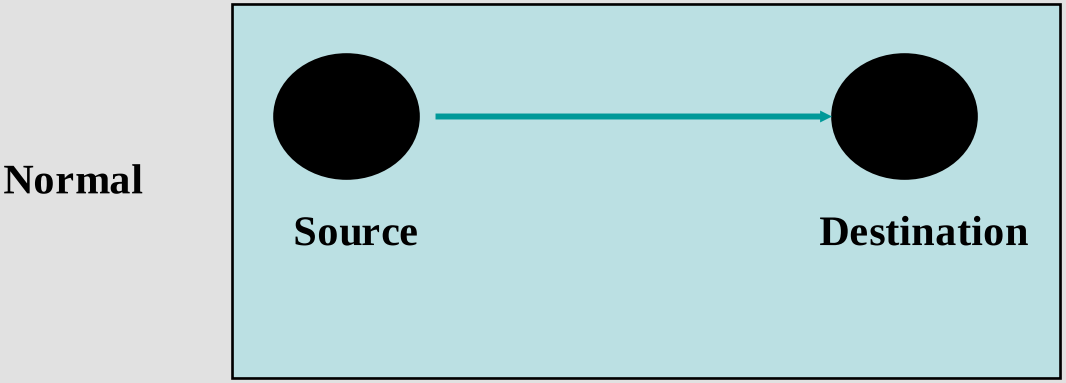
- On 22 September 2022, Optus became the victim of a cyber attack that resulted in the disclosure of their customers' personal information, such as name, date of birth, email addresses, driver's licences, Medicare card and passport numbers.
- **Which security service is broken in the attack?**

confidentiality

Attacks Taxonomy


Passive
Interception (confidentiality)
Release of message contents
Traffic analysis
Active
Interruption (availability)
Modification (integrity)
Fabrication (integrity & authentication)
Reply (freshness)

Attacks

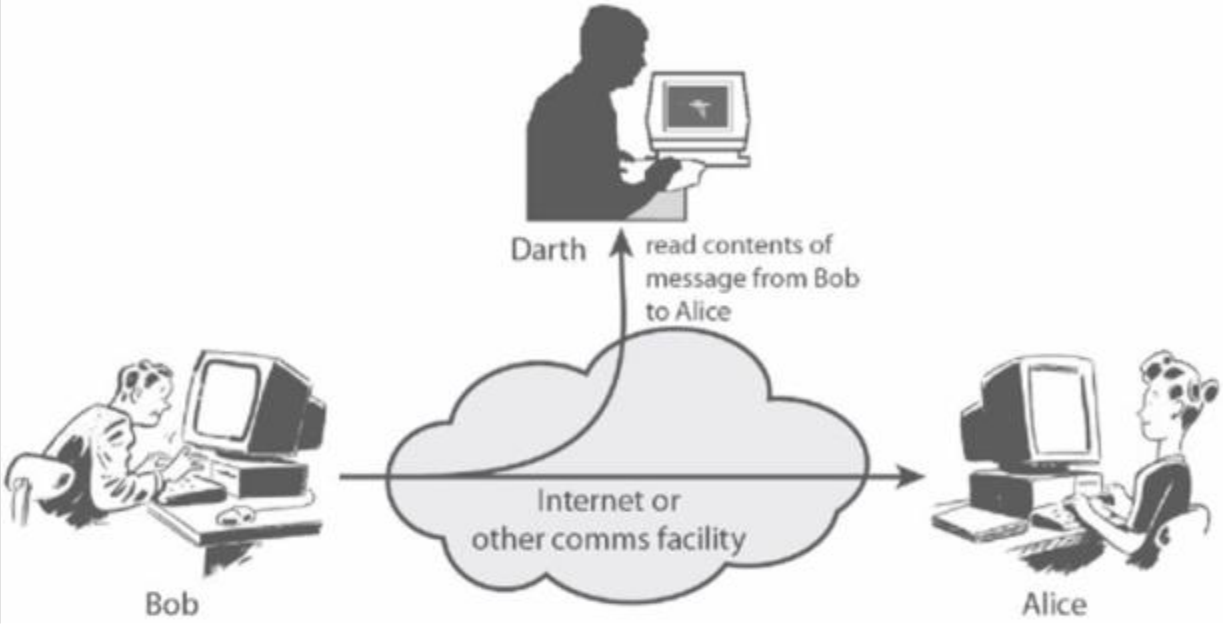


The source and destination entities could be:

- Devices
- Programs
- Processes
- Threads
- …

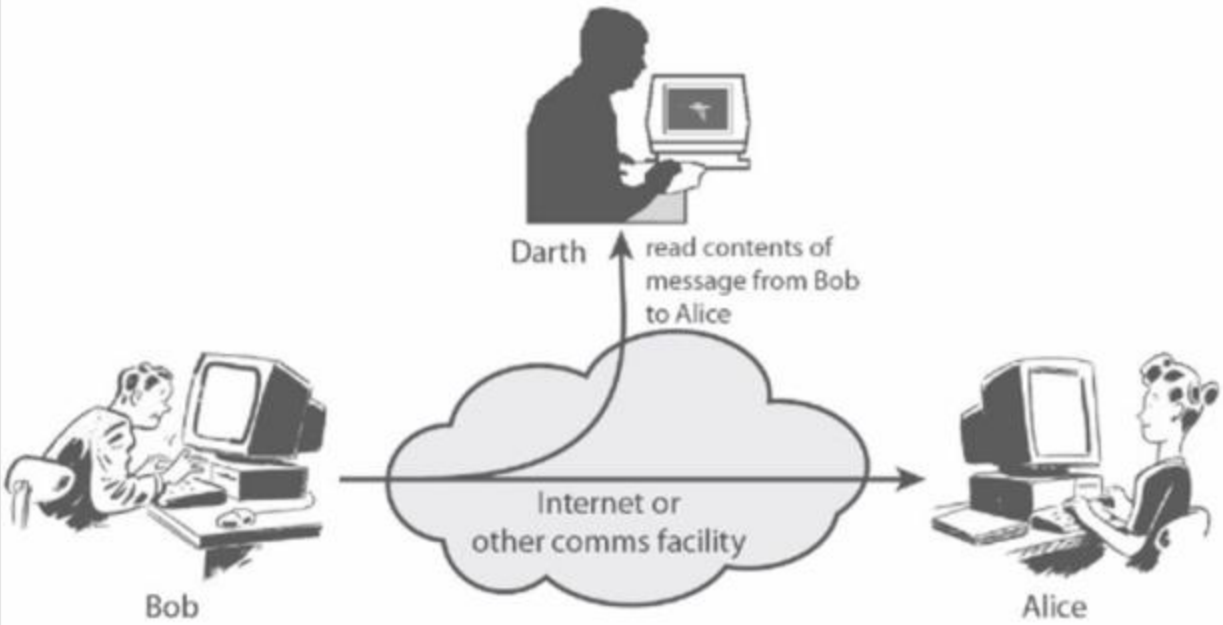
Passive Attack: Interception

- Unauthorised individual gains access to confidential or private information
- Eavesdropping on, or monitoring of, transmission of information between communicating parties


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attack: Interception

- Unauthorised individual gains access to confidential or private information
- Eavesdropping on, or monitoring of, transmission of information between communicating parties
- Difficult to trace as no traces of intrusion might be left


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attack: Interception

- Unauthorised individual gains access to confidential or private information
- Eavesdropping on, or monitoring of, transmission of information between communicating parties
- Difficult to trace as no traces of intrusion might be left
- Examples
  - Wiretapping

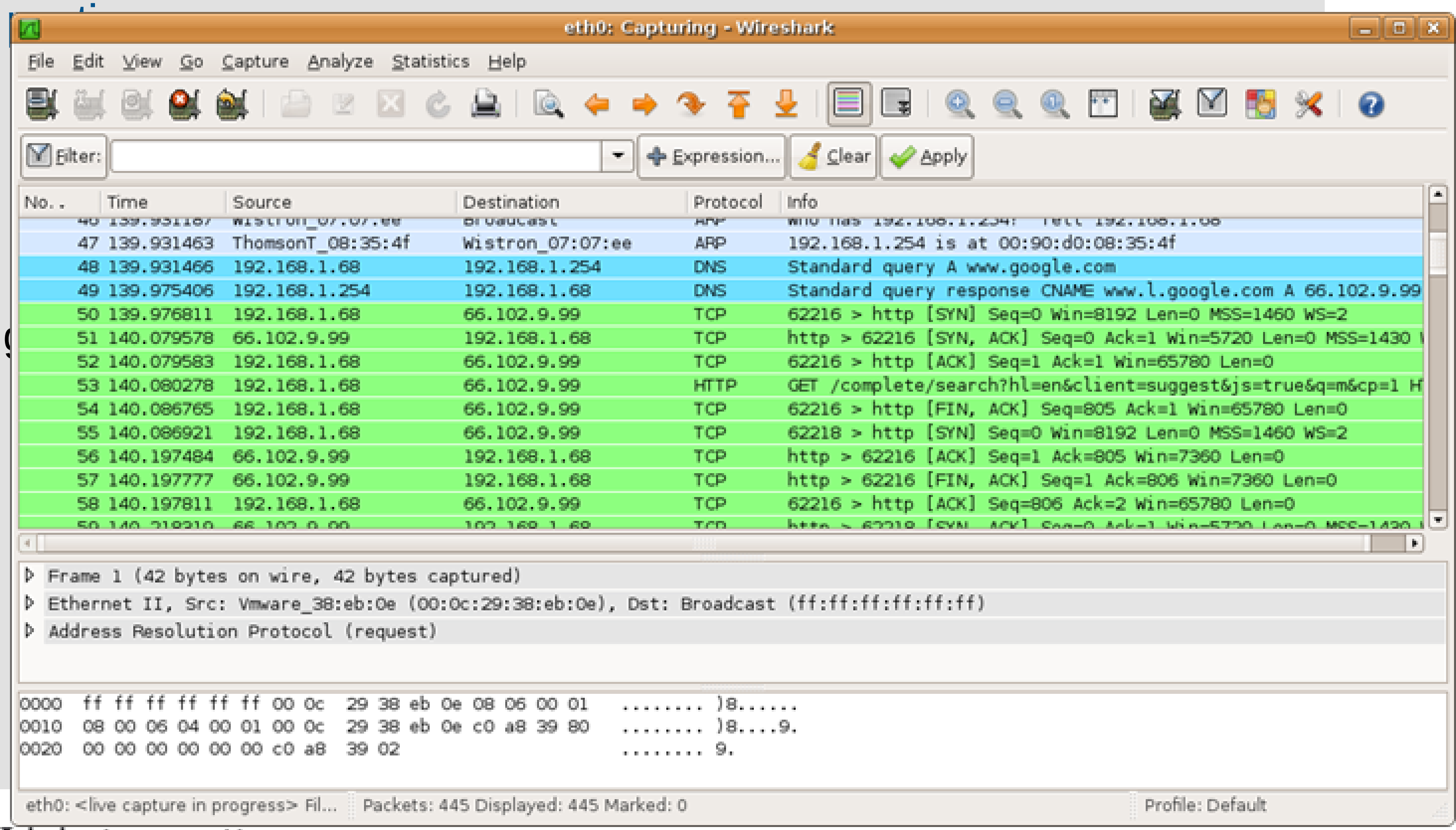
Passive Attack: Interception

- Unauthorised individual gains access to confidential or private information
- Eavesdropping on, or monitoring of, transmission of information between communicating parties
- Difficult to trace as no traces of intrusion might be left
- Examples
  - Wiretapping
  - Illegal copying

MONASH University
Information Technology

Passive Attack: Interception

- Unauthorised individual gains access to confidential or private information
- Eavesdropping on, or monitoring of, transmission of information between communicating p
- Difficult to trace
- Examples
  - Wiretapping
  - Illegal copyin
  - <u>Sniffing</u>


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
  46 139.931187  Wistron_07:07:ee   Broadcast          ARP       Who has 192.168.1.254?  Tell 192.168.1.68
  47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee   ARP       192.168.1.254 is at 00:90:d0:08:35:4f
  48 139.931466  192.168.1.68       192.168.1.254      DNS       Standard query A www.google.com
  49 139.975406  192.168.1.254      192.168.1.68       DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
  50 139.976811  192.168.1.68       66.102.9.99        TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  51 140.079578  66.102.9.99        192.168.1.68       TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
  52 140.079583  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
  53 140.080278  192.168.1.68       66.102.9.99        HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
  54 140.086765  192.168.1.68       66.102.9.99        TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
  55 140.086921  192.168.1.68       66.102.9.99        TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  56 140.197484  66.102.9.99        192.168.1.68       TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
  57 140.197777  66.102.9.99        192.168.1.68       TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
  58 140.197811  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
  59 140.218310  66.102.9.99        192.168.1.68       TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

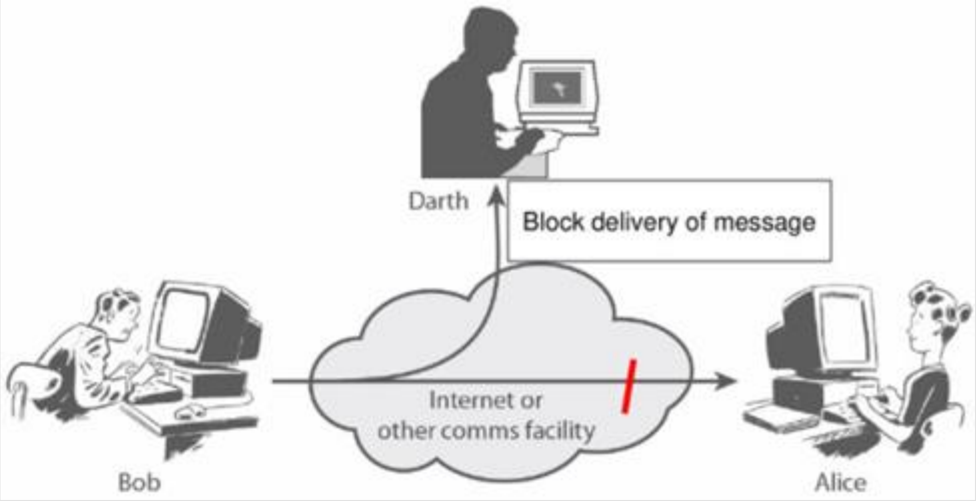
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Passive Attack Sub-Types

- **Release of message content**
  - Capture and read the content
  - Can be prevented by using encryption
- **Traffic analysis**
  - Can’t read the information, but observe the pattern
  - Observe frequency and length of communication
  - Determine the location and identity of communicating parties

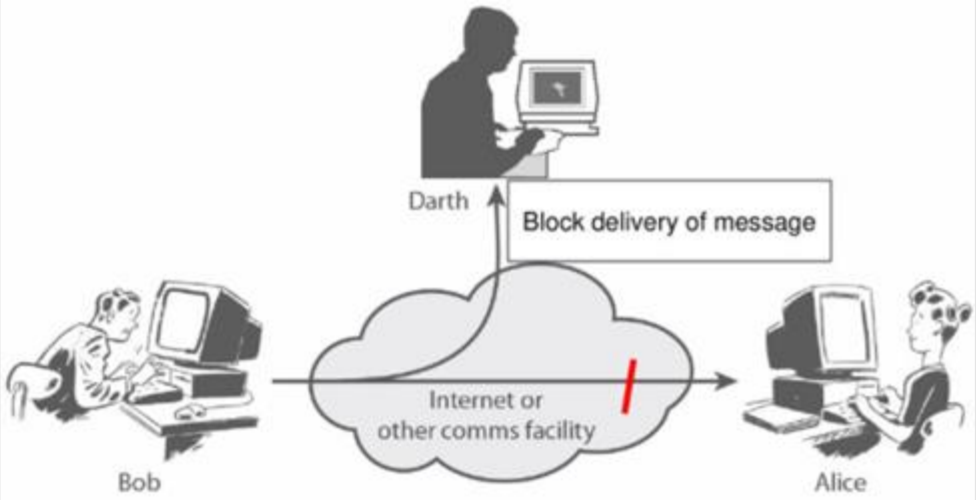
Active Attacks: Interruption (Denial of Services)

- Deliberately make resources unavailable for legitimate use



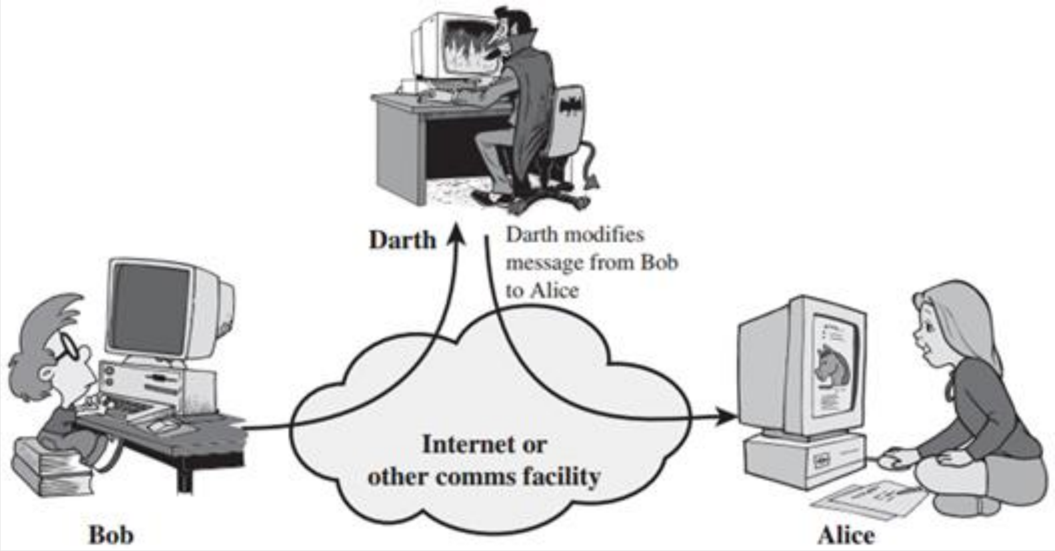
Active Attacks: Interruption (Denial of Services)

- Deliberately make resources unavailable for legitimate use
- Examples
  - Cutting a communication line
  - Disabling a file management system
  - Overloading a server host so that it cannot respond



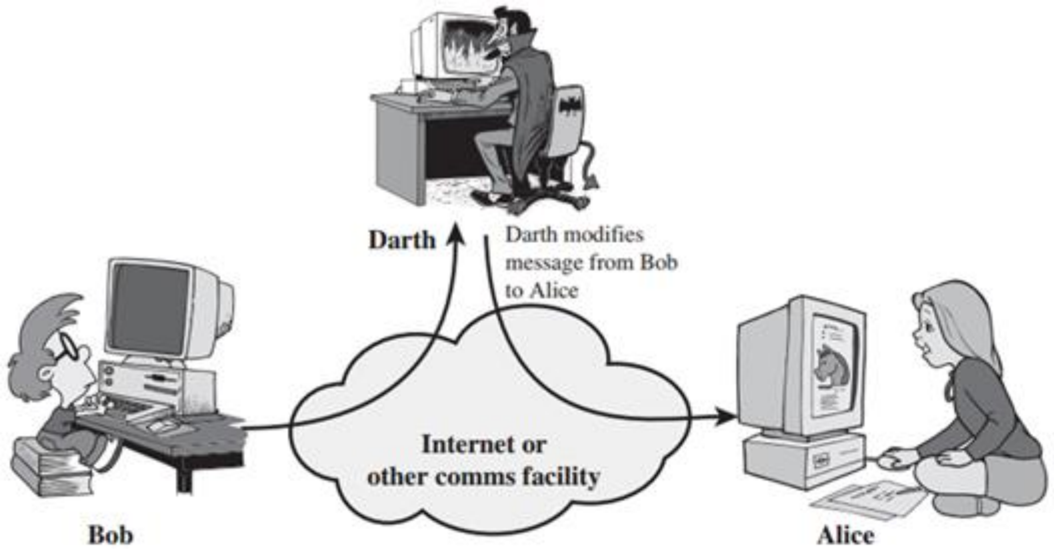
Active Attack: Modification (Tampering)

- Modify resources that an attacker is not authorised to modify
  - Change/remove existing information, or insert new information


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

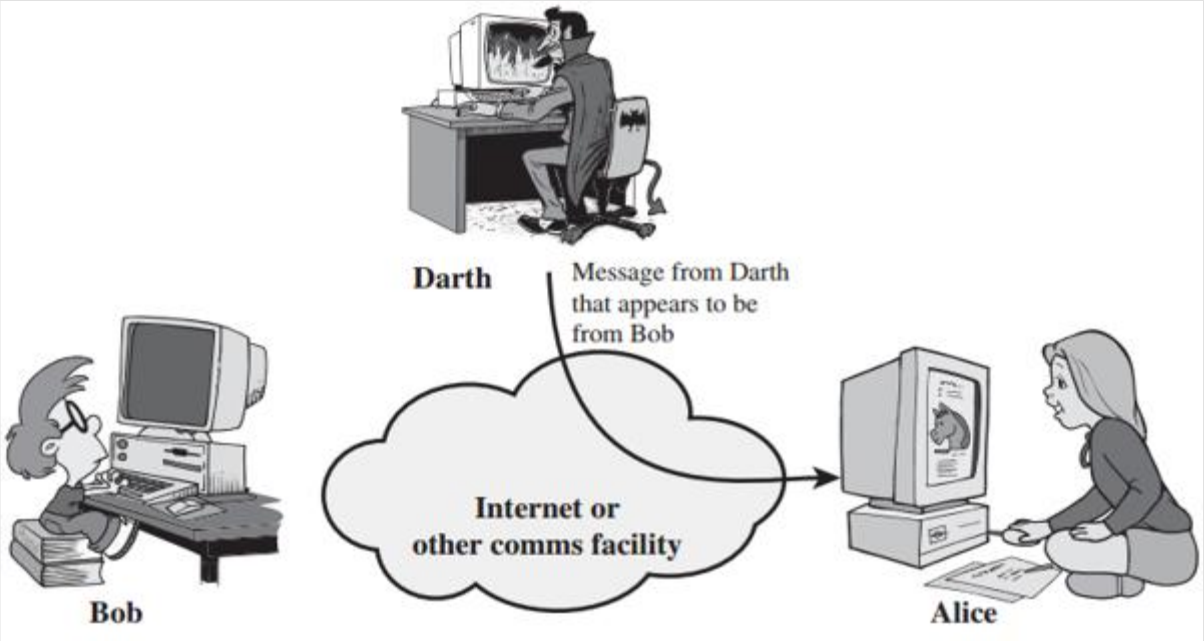
Active Attack: Modification (Tampering)

- Modify resources that an attacker is not authorised to modify
  - Change/remove existing information, or insert new information
- Examples
  - Modifying the contents of messages in the network
  - Changing information stored in data files
  - Altering programs so they perform differently
  - Reconfiguring system hardware or network topologies


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

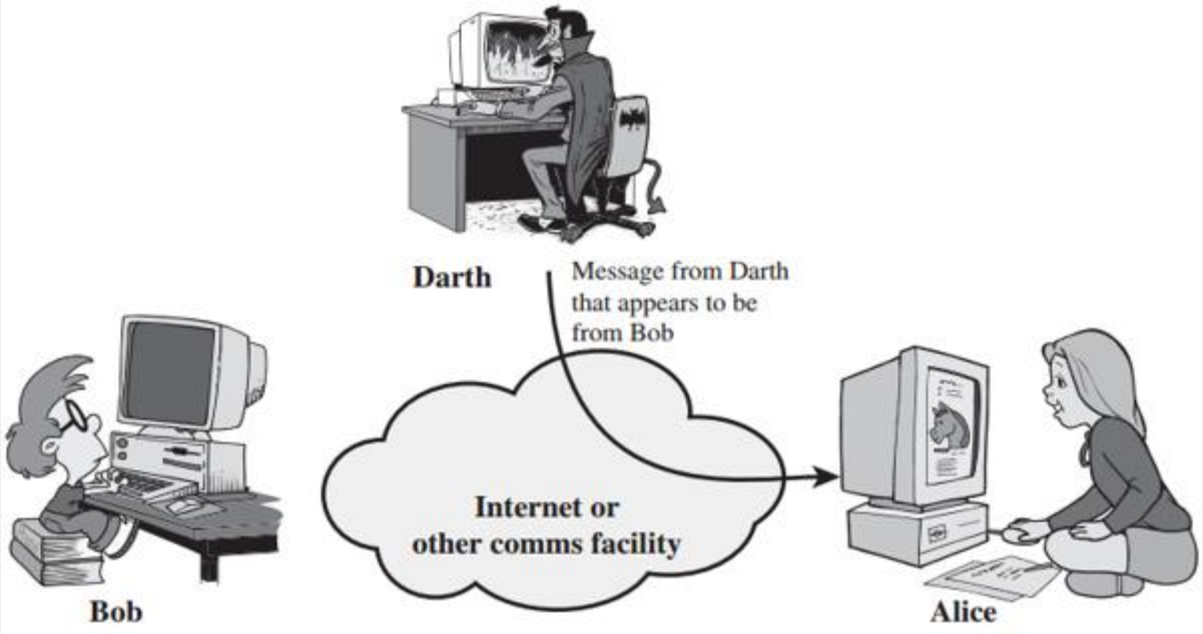
Active Attack: Fabrication (Masquerade, Impersonation)

- Attackers pretend to be authorised users and insert fake messages


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

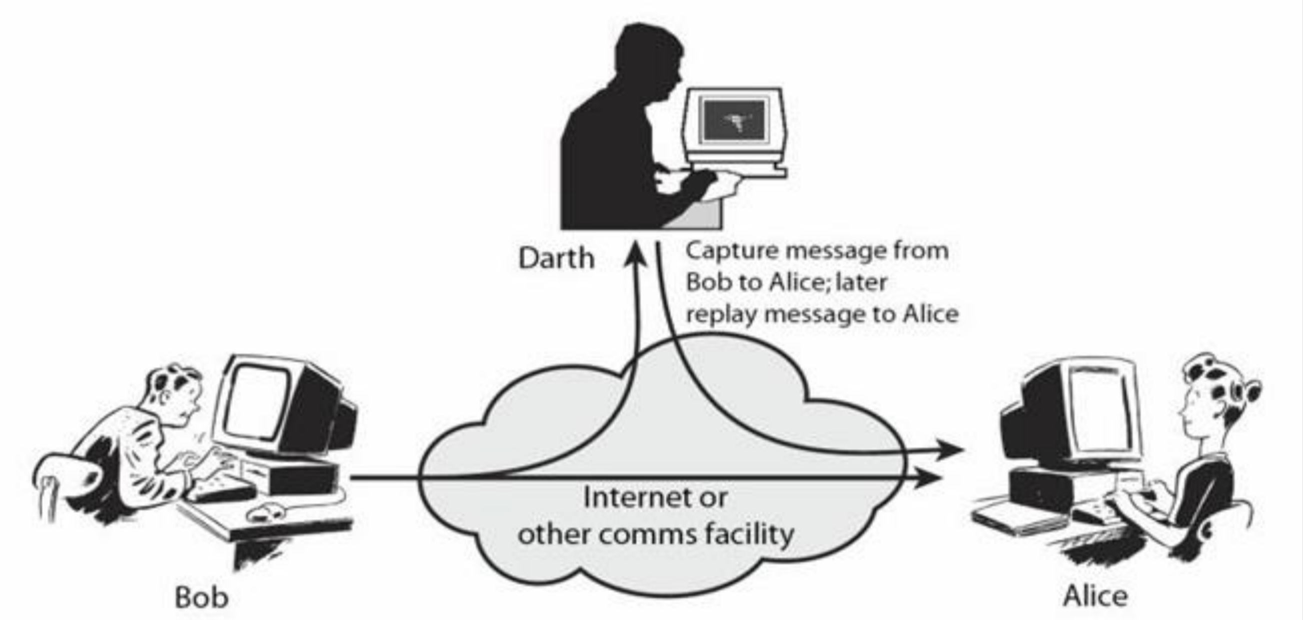
Active Attack: Fabrication (Masquerade, Impersonation)

- Attackers pretend to be authorised users and insert fake messages
- Examples
  - Insert spurious messages in a network
  - Insert a record into a file


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Active Attack: Replay Attack

- Passive capture of data and subsequently retransmit captured data in order to repeat some action


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attacks vs. Passive attacks

Passive attacks	Active attacks
• Attackers monitor and scan systems for vulnerabilities or entry points that allow them to intercept information without changing any of it • Hard to detect but easy to prevent	• Involve data stream modification, or creation of a false stream • Involve interaction between the attacker and the target system, network, or communicating parties • Hard to prevent but easy to detect

Attack Example

- **PollEv exercises**

PollEv.com/ronsteinfeld681

LN01: Outline

- Security attacks
- Security services
- Security mechanisms
- Security standards

Security Services

- Intended to counter security attacks

Security Services

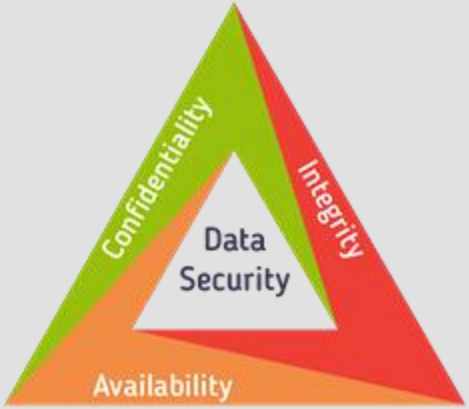
- Intended to counter security attacks
- Make use of one or more **security mechanisms** to provide the service

Security Services

- Intended to counter security attacks
- Make use of one or more **security mechanisms** to provide the service
- **6 major security services/properties/objectives:**
  - **Confidentiality**
  - **Integrity**
  - **Availability**
  - Authentication
  - Non-repudiation
  - Access control

Security Services

- Intended to counter security attacks
- Make use of one or more security mechanisms to provide the service
- **6 major security services/properties/objectives:**
  - **Confidentiality**
  - **Integrity**
  - **Availability**
  - Authentication
  - Non-repudiation
  - Access control



- Information security's **primary focus** is the balanced protection of the **confidentiality, integrity and availability** of data (also known as the **CIA** triad)

MONASH University
Information Technology

Security Services: Confidentiality

- **Data Confidentiality:** information is not made available or disclosed to unauthorised entities
  - Only authorised entities can access the protected information
  - A failure of confidentiality, commonly known as a *breach*, typically cannot be remedied
    - E.g., once the secret has been revealed, there's no way to un-reveal it
- Technique to ensure data confidentiality: **encryption**

MONASH University
Information Technology

Security Services: Integrity

- **Data Integrity:** assurance that data received is as sent by an authorised entity
  - Data cannot be modified in an unauthorised or undetected manner
  - Maintaining and assuring the **accuracy**, **completeness,** and **consistency** of data over its entire lifecycle
- Techniques to ensure data integrity**:**
  - Message Authentication Code (MAC)
  - Authentication Encryption (AE)
  - Digital signature

Security Services: Availability

- **Availability:** resource accessible/usable
  - The computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly
  - **High availability** systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades

Security Services: Authentication

- **Authentication:** assurance that communicating entity is the one claimed
  - Typically used at start of a connection
  - ***Entity authentication*** verifies the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
  - ***Origin authentication*** provides verification of source of data

- 3 types of information that can be used for authentication:
  - Something only you know: things such as a PIN, or a password
  - Something only you have: a driver's license or a magnetic swipe card
  - Something only you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans

Security Services: Non-Repudiation

- **Non-Repudiation:** protection against denial by one of the parties in a communication
  - Provides proof of the integrity of the data
  - Protects against a sender of data denying that data was sent (non-repudiation of origin)
  - Protects against a receiver of data denying that data was received (non-repudiation of delivery).
- The common techniques to provide non-repudiation:
  - Digital signature

Security Services: Access Control

- **Access Control -** prevention of the unauthorised use of a resource including**:**
  - Use of a communications resource
  - Reading, writing or deletion of an information resource
  - Execution of a processing resource
- **Example:**
  - File permissions in Unix/NT file systems

LN01: Outline

- **Security attacks**
- **Security services**
- **Security mechanisms**
- **Security standards**

Security Mechanisms

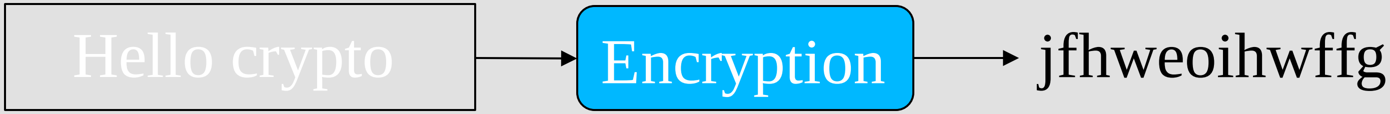
- **Security mechanisms** are technical tools and techniques that are used to implement security service
- A process that is designed to detect, prevent, or recover from a security attack
- **2 types of security mechanisms:**
  - Specific security mechanisms: used to provide specific security services
  - Pervasive security mechanisms: not specific to particular services

Specific Security Mechanisms

- Encipherment (encryption)
- Data integrity
- Digital signatures
- Access controls
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

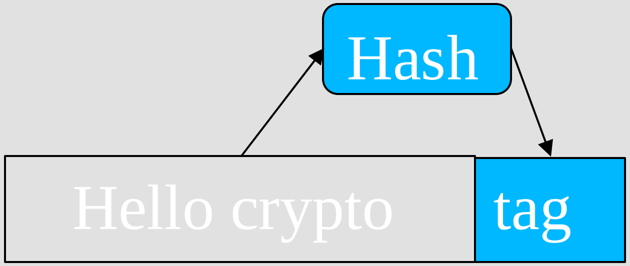
Specific Security Mechanisms

- **Encipherment (encryption):** hide or covers data
  - It makes use of mathematical algorithms to transform data into a form that is not readily intelligible
  - Cryptography and Steganography techniques are used for enciphering
  - It provides confidentiality service



Specific Security Mechanisms

- **Data integrity:** appends a short check value to the data which is created by a specific process, e.g., hash, from the data itself
    - It protects against modification of data
    - It provides data integrity



Specific Security Mechanisms

- **Digital Signature:** a way by which the sender can electronically sign the data and the receiver can electronically verify it
  - Verify the authenticity of digital messages or documents
  - Digital signatures employ asymmetric cryptography
  - It provides non-repudiation, origin authentication and data integrity services

Specific Security Mechanisms

- **Access controls**: a server using client information to decide whether to grant access to resources owned by a system
  - E.g. access control lists, capabilities, security labels

Specific Security Mechanisms

- **Authentication exchange:** ensure the identity of an entity by means of information exchange
  - Entities exchange messages to prove their identity to each other
  - It provides entity authentication service
  - E.g., traditional username and password, public key infrastructure (PKI), single sign-on (SSO), OAuth, OpenID Connect

Specific Security Mechanisms

- **Traffic padding:** the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts
    - It conceals real volumes of data traffic
    - It provides traffic flow confidentiality

Specific Security Mechanisms

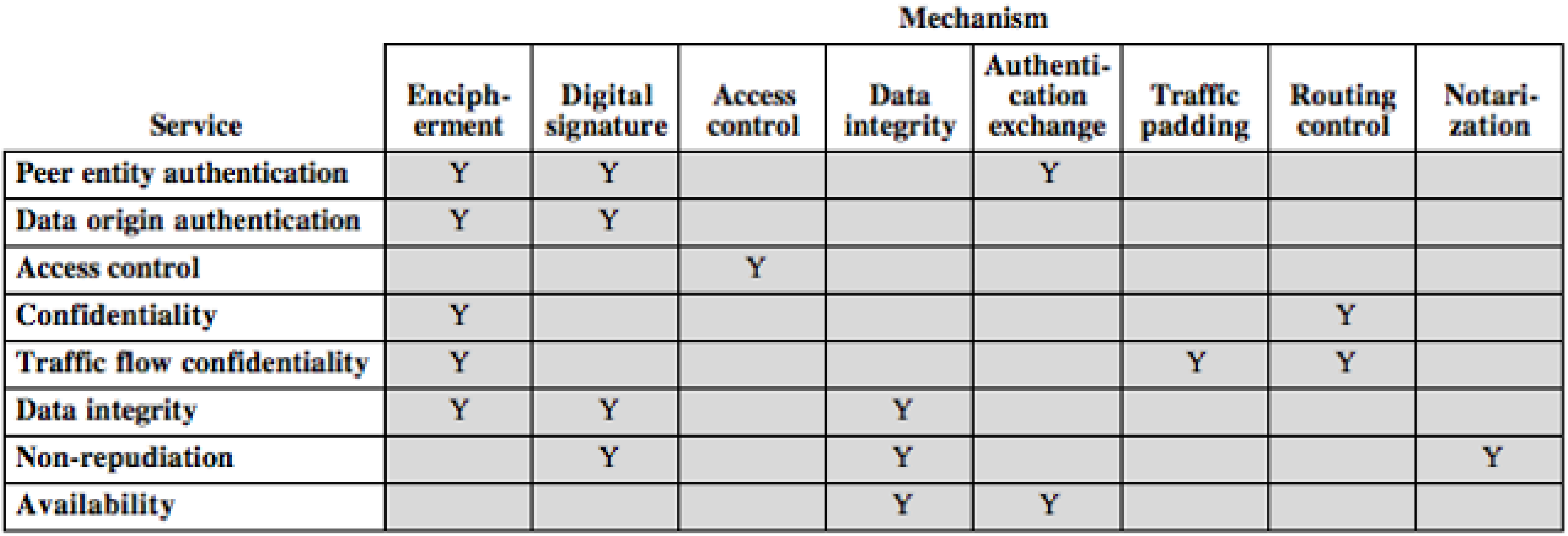
- **Routing control:** select and continuously change different available routes between the sender and the receiver
    - It prevents the attacker from traffic analysis on a particular route
    - It provides traffic flow confidentiality

Specific Security Mechanisms

- **Notarization:** use a trusted third party to control the communication between the two parties
    - The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request
    - It provides the non-repudiation service

Relationship between Security Services & Mechanisms

Table 1.4 Relationship Between Security Services and Mechanisms



	Mechanism							
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Attack Example

- **PollEv exercises**

PollEv.com/ronsteinfeld681

LN01: Outline

- Security attacks
- Security services
- Security mechanisms
- Security standards

Cybersecurity Standards

- **Cybersecurity standards** are techniques set forth in published materials that attempt to protect the **cyber environment** of a user or organization
  - Environments: softwares, devices, networks, systems, services, data in storage/transit …
  - Materials consist of: tools, policies, security concepts, technologies…
  - Example: AES is the specification for the encryption of electronic data established by NIST FIPS
- **International standards examples:**
  - ISO/IEC 27000 series (Australia's choice), ITU-T X.800**,** IEC 62443
- **National standards examples:**
  - NIST FIPS (US), Cyber Essentials (UK)

Summary

- **Taxonomy of security attacks**
  - Passive attacks
  - Active attacks
- **Security services/properties/objectives**
  - CIA triad
  - Authentication
  - Non-repudiation
  - Access control
- **Security mechanisms**
  - Specific mechanisms
  - Pervasive mechanisms
- **Security standards**

Further Reading

- Chapter 1 of the textbook: Cryptography and Network Security : Principles and Practice – William Stallings, Sixth Edition, 2014, Prentice Hall.

- Next lecture: LN02 - Principles of Encryption

- Acknowledgement: part of the materials presented in the slides was developed with the help of resources made available by the author of the textbook.