

31268 Web Systems

Week 3

The web and security

Security & Encryption: Principles

- The internet is not a safe place....
 - Basic security principles
 - **C**onfidentiality
 - **I**ntegrity
 - **A**vailability
-

Confidentiality – I – A

→ Information is accessible **only** to authorised users:

i.e.:

1. Can't be seen....
 2. ...by Whom?
 3. ...When?
 4. ...Where?
 5. ...How?
-

Confidentiality – I – A

→ Information is accessible **only** to authorised users:

i.e.:

1. Can't be seen....
 - Encryption
 2. ...by Whom?
 - Authentication
 3. ...When?
 4. ...Where?
 - Access Controls
 5. ...How?
 - Location, transmission path, protocols
-

C – Integrity – A

- Safeguarding accuracy/ completeness of
- information
 - processing methods
 - 1. Only entered / altered by **authorised** users
 - 2. Cannot be altered **without detection**
 - In storage or In transit
-

C – Integrity – A

- Safeguarding accuracy/ completeness of
- information
 - processing methods
1. Only entered / altered by authorised users
 2. Cannot be altered without detection
 - In storage or In transit

→ Detection:

1. Use **Audit trails**
 2. Mathematical means
 - **Hashes**
 - **Checksums**
 - **Message digests**
-

C – I – Availability

- Ensuring authorised users have access to information/processing when required

i.e.:

1. Systems survive failures

- Have hot/cold standby mechanisms

2. Systems resist attacks

- Resistant to Denial of Service (DoS) attacks

- Users can access from authorised locations
-

Good vs Evil

Security Service

- A security service makes use of **one or more** security mechanisms
- **Security Mechanism:**
 - A mechanism that is designed to detect, prevent, or recover from a security attack

Security Attack

- Any action that compromises the security of information.



Types of Security Attacks

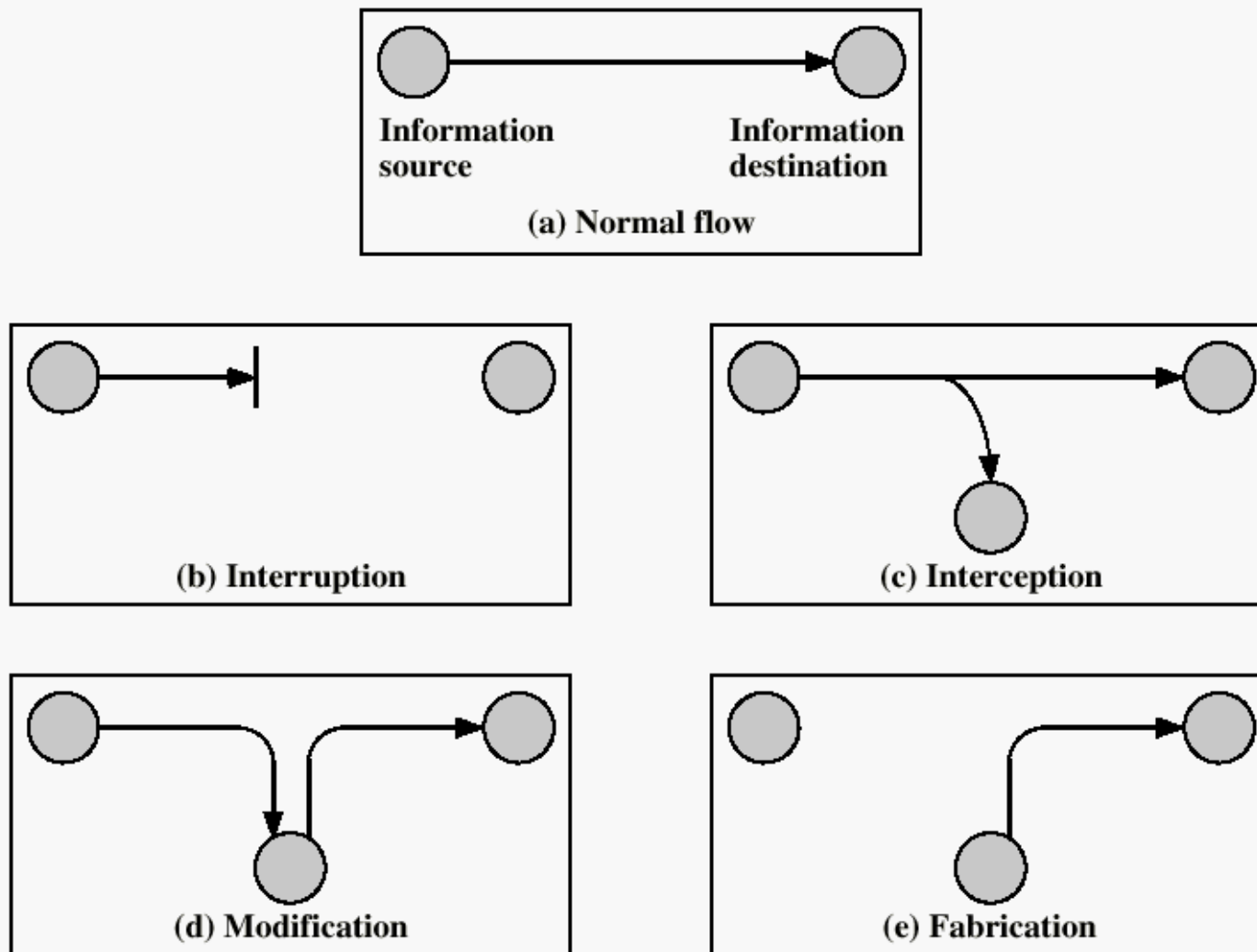


Figure 1.1 Security Threats

Types of Security Attacks

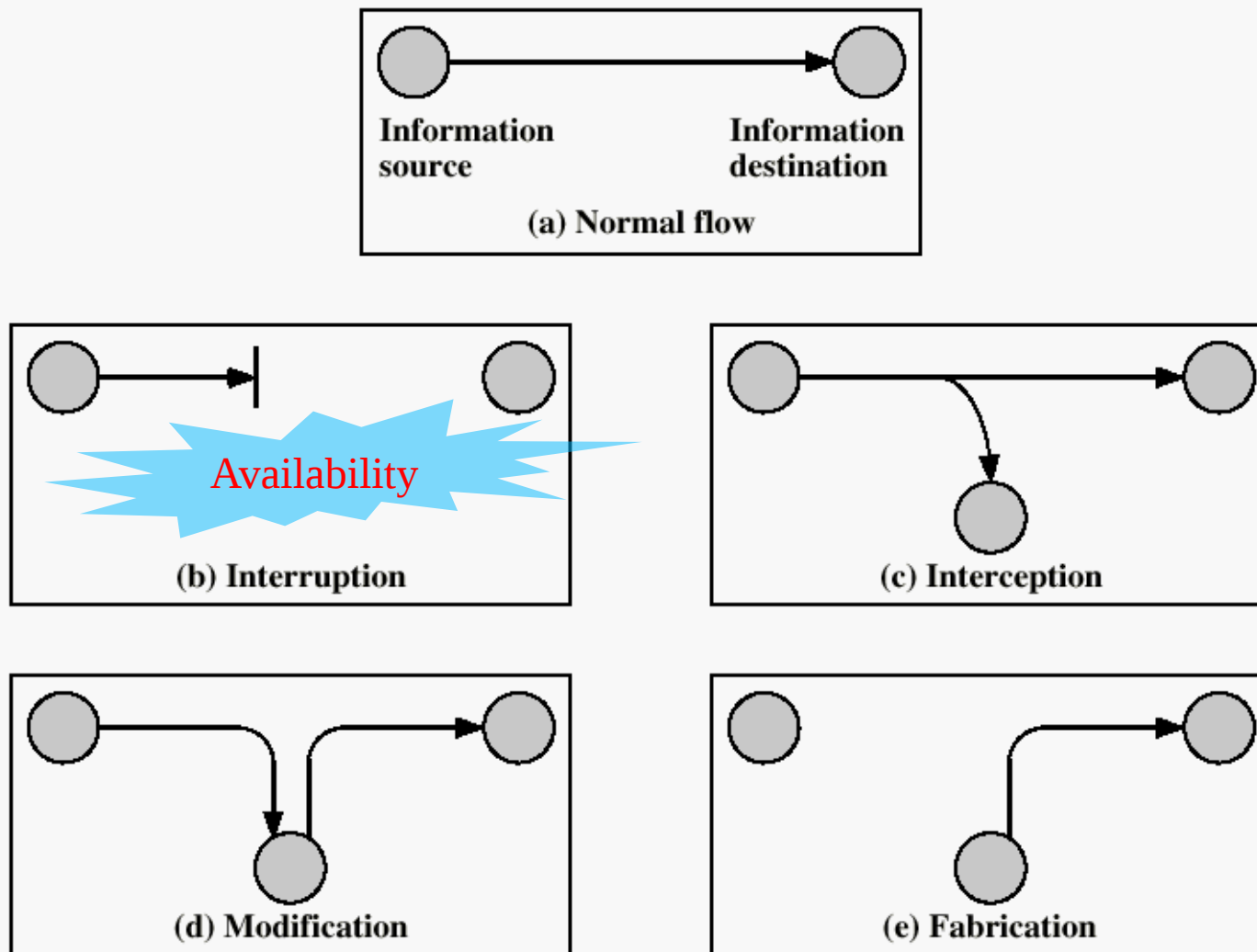
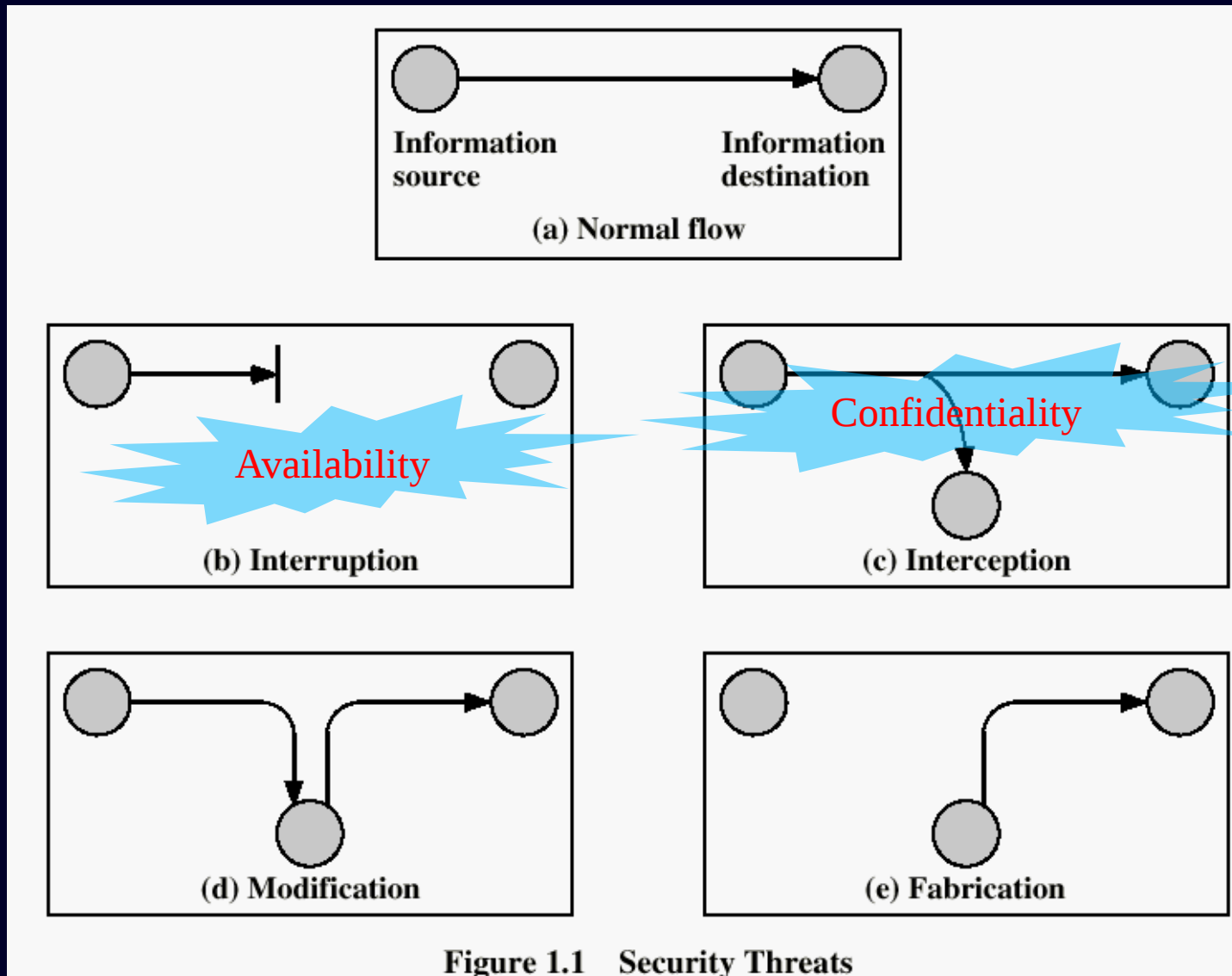
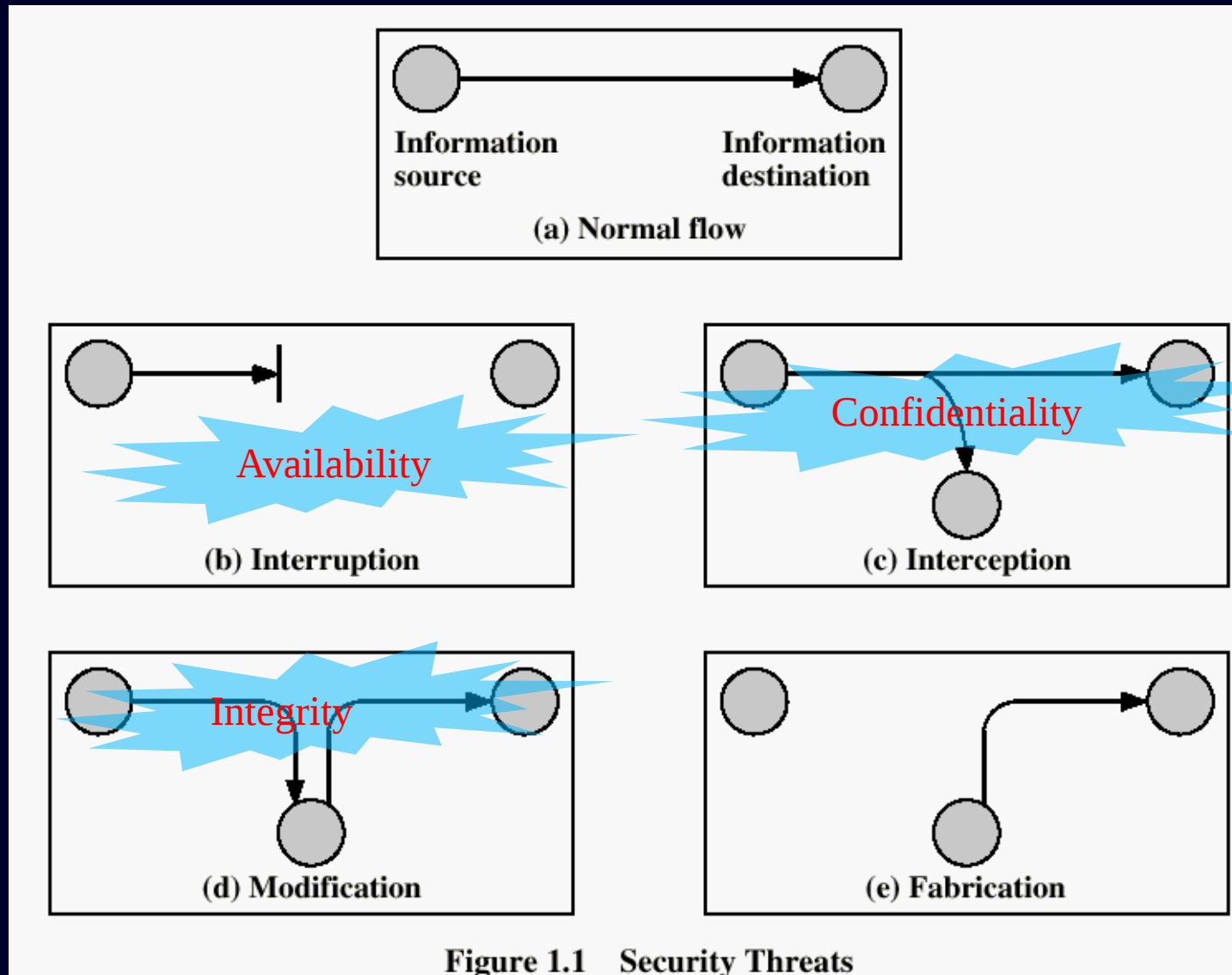


Figure 1.1 Security Threats

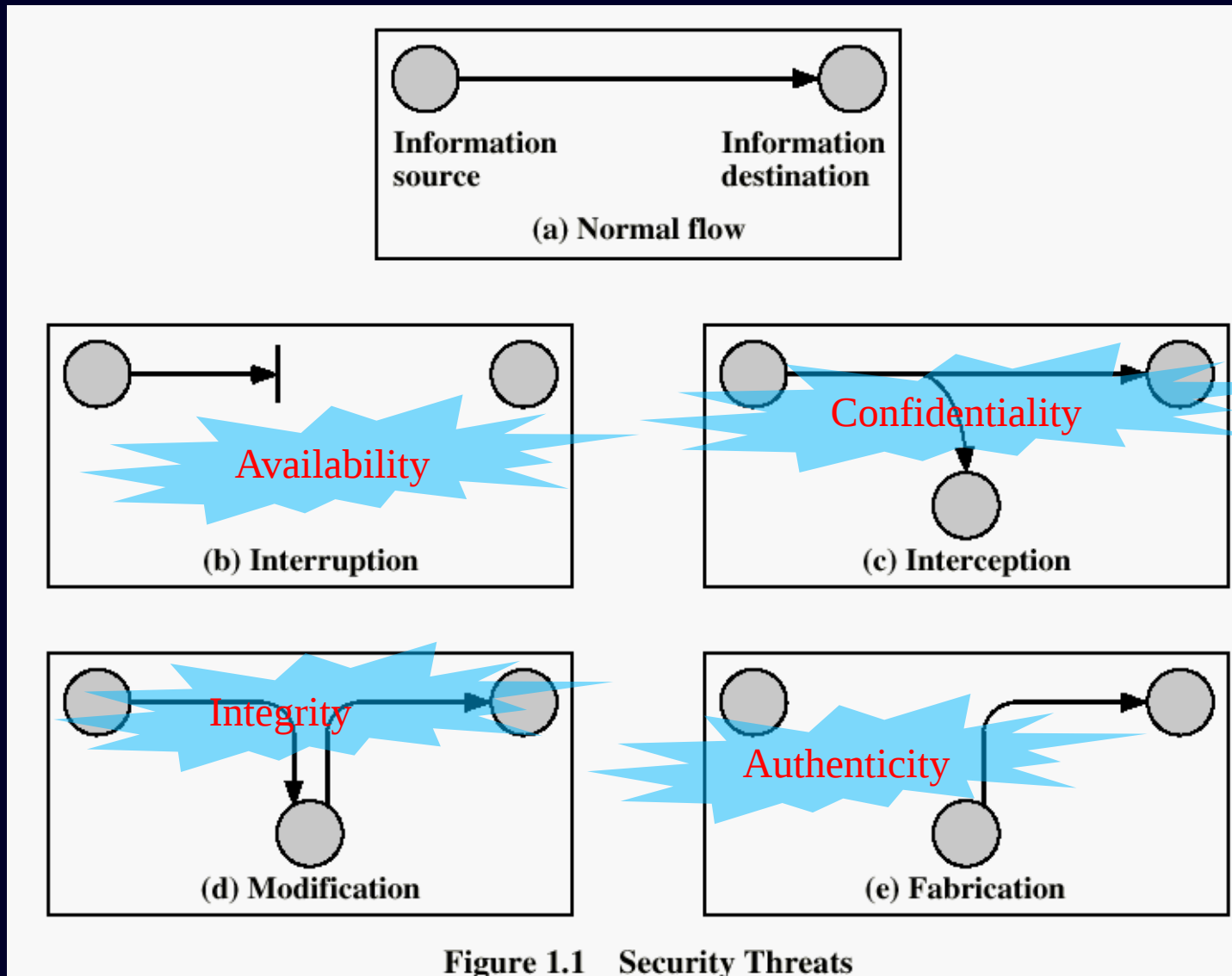
Types of Security Attacks



Types of Security Attacks



Types of Security Attacks



Typical Security Services

- Confidentiality – privacy - encryption
 - Authentication - who created or sent it
 - Integrity - has not been altered
 - Non-repudiation - the order is final
 - Access control - prevent misuse of resources
 - Availability - permanence, non-erasure
-

Security service: Encryption

- **Encryption** – converting plaintext into ciphertext to prevent non-intended recipients from reading.

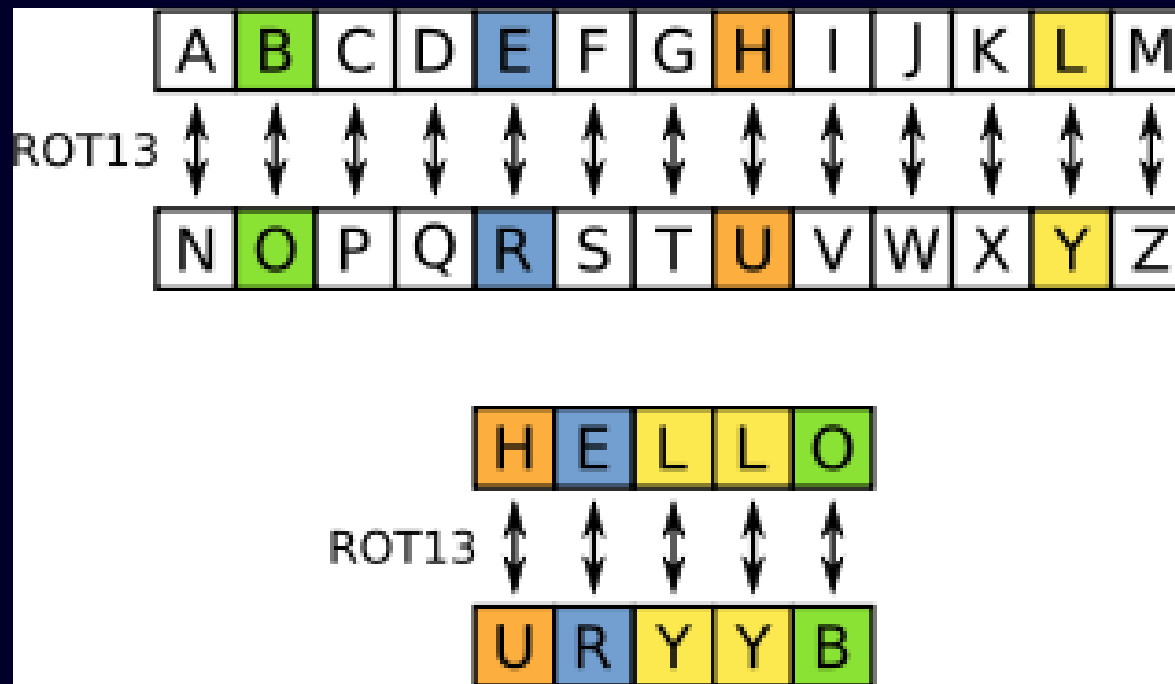
Security service: Encryption

- **Encryption** – converting plaintext into ciphertext to prevent non-intended recipients from reading.
- e.g. Using **rot13** encryption,
"The butler did it!" becomes
"Gur ohgyre qvq vg!"
- What is the encryption rule?



Encryption

- "The butler did it!"
"Gur ohgyre qvq vg!"



Secret Key Cryptography

- Most trivial crypto use **Symmetric** key encryption.
 - E.g. Data Encryption Standard (DES)
 - E.g. You use a **password** to protect the file.
 - Problem is that the key needs to be **secret** and **exchanged** between the parties involved in communication.
-

Public Key Cryptography

- Each party has two keys
 - a private and public e.g. RSA



Public Key Cryptography

- Each party has two keys
 - a private and public e.g. RSA
- Can **encrypt with one** and **decrypt with the other**.



Public Key Cryptography



- Each party has two keys
 - a private and public e.g. RSA
- Can encrypt with one and decrypt with the other.
- Can be used for the four previously mentioned security capabilities.
 - **Authentication** – sender **encrypts** with their **private** key and receiver **decrypts** with sender's **public** key.
 - **Privacy** - sender **encrypts** with receiver's **public** key
 - **Data integrity** - if it's changed along the way, it can't be decrypted into anything meaningful
 - **Non-repudiation** - same reason as **Authentication**

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212845,00.html

Web Security: Encryption

Most common use-case:

SSL (Secure Sockets Layer) also known as **https://**

- Provides:
 - Confidentiality – stops interception
 - Integrity – stops modification
 - Authentication
 - Verifies owner of website
 - (optional) certificate based security (see later ..)
-

Web Security: Encryption

Most common use-case:

SSL (Secure Sockets Layer) also known as **https://**

- Provides:
 - Confidentiality – stops interception
 - Integrity – stops modification
 - Authentication
 - Verifies owner of website
 - (optional) certificate based security (see later ..)
 - Uses:
 - Public key cryptography
 - Symmetric (shared secret) crypto
-

SSL example

<https://www.youtube.com/watch?v=SJJmoDZ3il8>



Hashing

- **Hashing** is about putting a **code** on data (such as an email) to ensure it hasn't been modified by someone along the line or sent by someone else altogether.
-

Hashing

- **Hashing** is about putting a **code** on data
 1. Do a checksum (modular sum of the characters in the file)
cksum filename.txt
 2. **Encrypt the checksum and sender's name** with the sender's private key.
 3. Receiver uses the sender's **public** key to decrypt the checksum
 4. If error in the checksum, then the message has been modified along the way!

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214292,00.html?offer=ciofact

Web Security: hashing

Typically used in

- Secure email
 - Electronic documents
 - Validate software
-

Web Security: hashing

Typically used in

- **Secure email**
 - some email clients can verify that your email was not tampered
→ need personal digital certificate
 - Electronic documents
 -
 - Validate software
 -
-

Web Security: hashing

Typically used in

- Secure email
 - some email clients can verify that your email was not tampered
→ need personal digital certificate
 - **Electronic documents**
 - Adobe PDF allows you to digitally sign documents
 - Validate software
-

Web Security: hashing

Typically used in

- Secure email
 - some email clients can verify that your email was not tampered
→ need personal digital certificate
 - Electronic documents
 - Adobe PDF allows you to digitally sign documents
 - **Validate software**
 - when installing software on windows, the installer must be signed by Microsoft
-

Security Service: Authentication

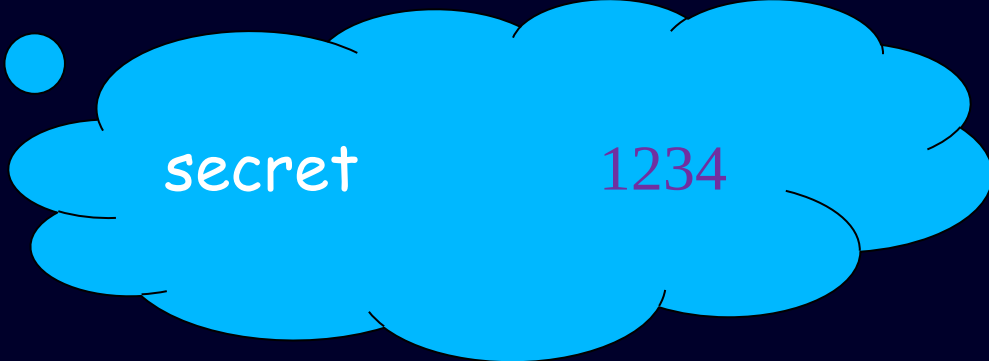
- Who are you?
 - Used for Non-Repudiation & Access Control
 - Need to authenticate
 - people
 - organisations
 - Applications
-

Security Service: Authentication

- Who are you?
 - Used for Non-Repudiation & Access Control
 - Need to authenticate
 - people
 - organisations
 - Applications
 - HOW??
 - Something you know
 - Something you have
 - Something you are
-

Authentication

- Something you **know**
 - Password
 - PIN



secret

1234

Authentication

- Something you know
 - Password
 - PIN
- Something you have
 - Key
 - Token
 - Certificate



Authentication

- Something you **know**
 - Password
 - PIN
- Something you **have**
 - Key
 - Token
 - Certificate
- Something you **are**
 - Fingerprint, palm print
 - Retinal scan
 - Face recognition
 - Voice recognition



Authentication

- But... are YOU known to us?
 - Are you enrolled? Have an account our LAN?
 - Beware social engineering!!!
 - Has references, letters of introduction
 - Certificate?
 - Issued by?
 - Valid?
-

Where do we Authenticate?

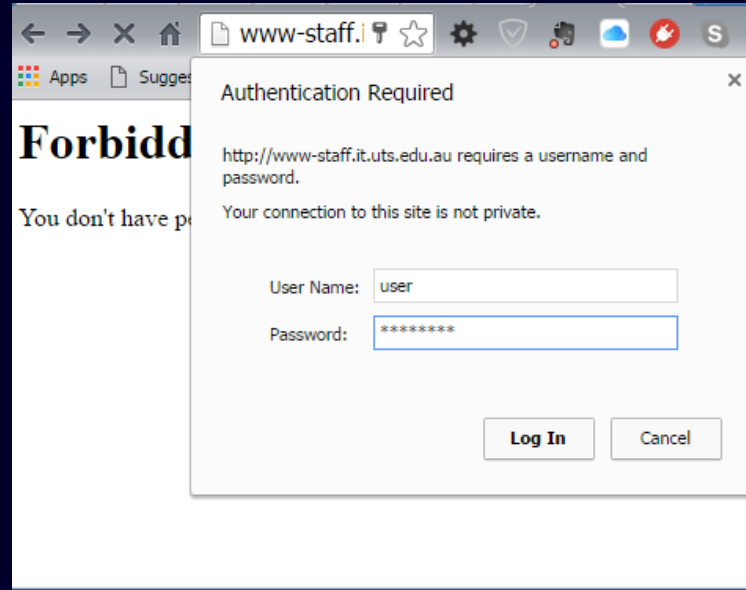
- At the perimeter?
 - At the operating system?
 - At the Application?

 - Are there multiple processes for the users?
 - Eg: staff who are students??

 - Multiple user lists to coordinate and manage!!!
-

Web security: Authentication

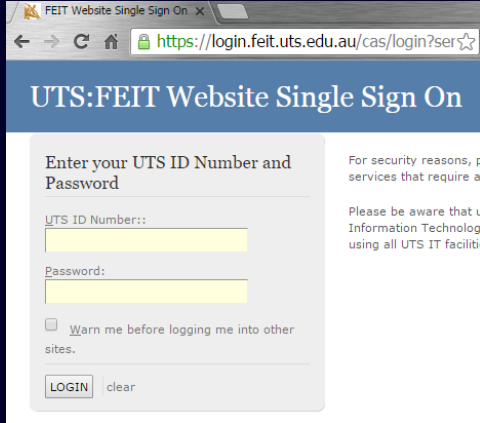
- Web authentication – usually by “identity” verification:
- Most sites use userid and password popup



- This is called “Basic” authentication.
 - Password is sent “*scrambled*” but not encrypted!!!
-

Web security: Authentication

Other sites use web forms: eg UTS



UTS:FEIT Website Single Sign On

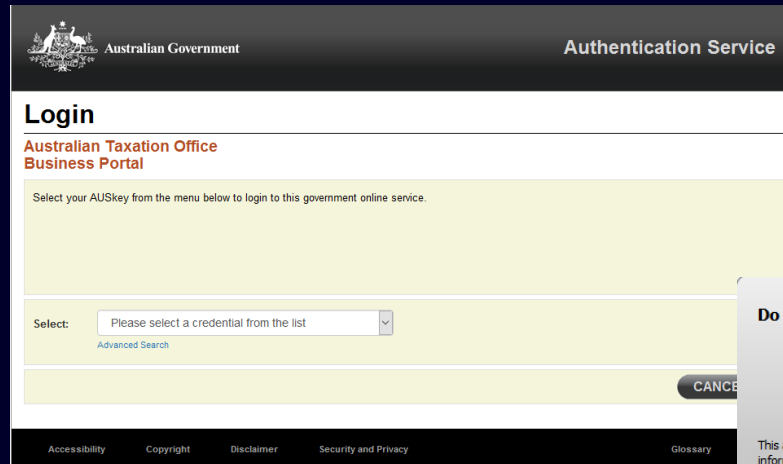
Enter your UTS ID Number and Password

For security reasons, please be aware that using all UTS IT facilities requires authentication.

UTS ID Number:

Password:

☐ Warn me before logging me into other sites.



Australian Government Authentication Service

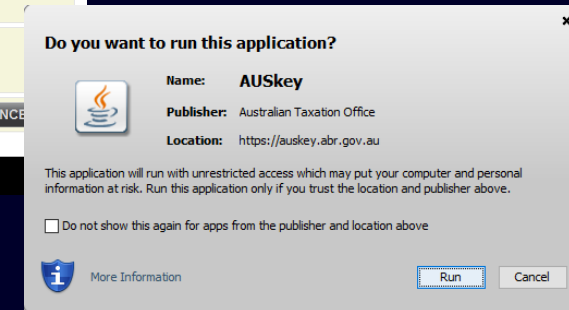
Login

Australian Taxation Office Business Portal

Select your AUSKey from the menu below to login to this government online service.

Select:

[Accessibility](#) [Copyright](#) [Disclaimer](#) [Security and Privacy](#) [Glossary](#)



3rd type of security is
“client side certificate”

e.g. Australian Tax Office: <http://bp.ato.gov.au> and
Auskey: <https://abr.gov.au/AUSkey/>

UNIX security: Authentication

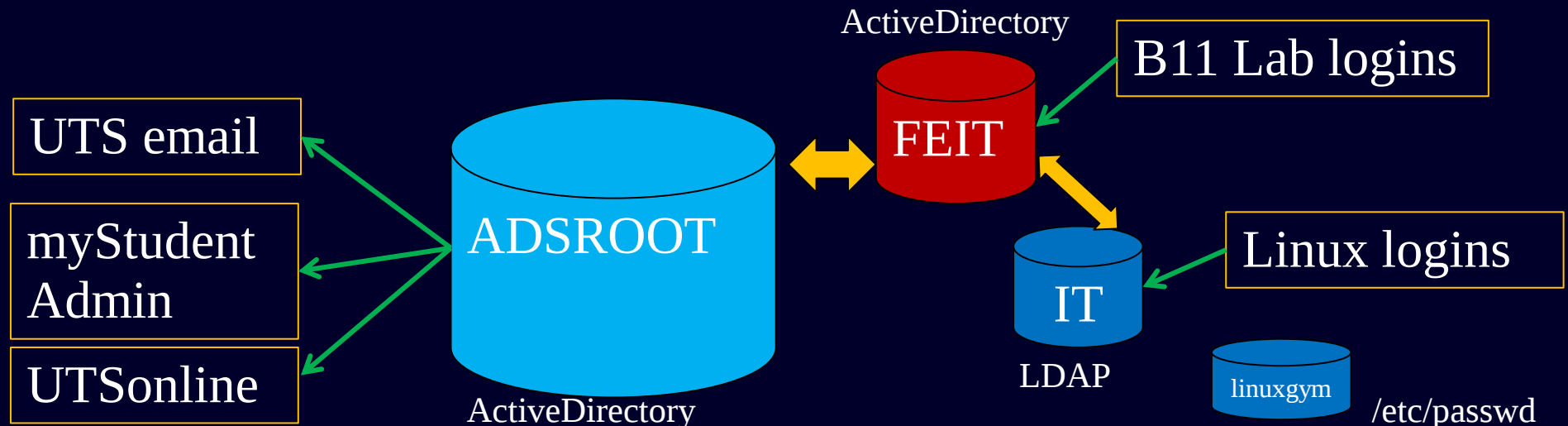
Typically by userid and password

- Trivial setups: saved in password file /etc/passwd
 - Larger scale: Stored in central directory service
 - e.g. Active Directory (Microsoft)
 - e.g. LDAP (everyone else)
-

UNIX security: Authentication

UTS Setup:

- Active Directory database called “**ADSROOT**”
 - Numeric usernames – same as student# eg 1234578
- FEIT-only students synchronised to faculty database called “**FEIT**” (also active directory) – same username
- IT-only accounts copied to IT security server
 - alphabetic usernames! e.g chw



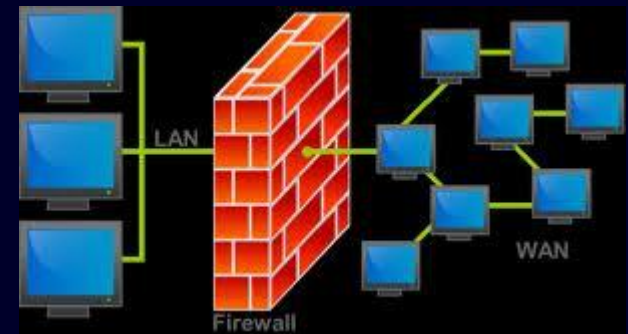
Security Service: Access Controls

- Physical
 - Tight control of physical access
 - Token based?
 - Not tied to user?



Security Service: Access Controls

- Physical
 - Tight control of physical access
 - Token based?
 - Not tied to user?
- Logical
 - Enforced by
 - operating system
 - application
 - security devices eg: firewall
 - Needs configuration = management cost

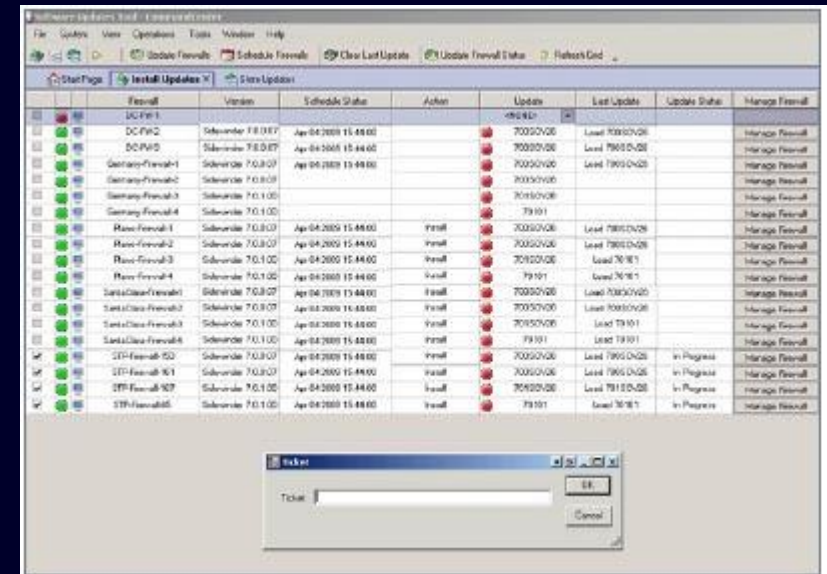


UNIX security: Access Control

- Usually 3 levels of security:
 - **user** → owner of the file
 - **group** → other users in the owner's group
 - **others** → the public
 - Each file and directory has 3 sets of permissions
 - **r**ead → can read the file
 - **w**rite → can update the file
 - **e**xecute → can execute (if a file) or traverse (if a directory)
 - Permissions appear like:
 - `drwxrwxrwx 53 chw staff 450 Apr 1 00:01 public_html/`
-

Security Mechanism: Audit Log

- Audit trails / logs are essential
- Needed to
 - Measure effectiveness
 - Do forensics
 - Create alerts
- Also subject to security needs!



Risk Assessment



WHO CARES?

WHY BOTHER?

Risk Assessment

It's something else.



SO WE KILLED A FEW PEOPLE, BIG DEAL

AIRTRAN INTRODUCES NEW SERVICES, BEGINS STRATEGY TO KILL ALL AMERICANS!@#

ATLANTA, Sept. 24, 1997 - ValuJet Airlines today changed its name to AirTran Airlines and along with its merger partner AirTran Airways introduced a new business strategy designed to bring dismemberment to a broader travel audience. The airline said that its objective is to make air travel more attractive to business travelers and even more convenient for suicidal maniacs.

It seems ValuJet is attempting to pull an unethical "fast one" over on the public, while bailing out to a larger conglomerate. "Let's call ourselves AirTran then maybe someone will be dumb enough to get on board one of our flying death machines!!#@#%" u4ea has gingivitis and fucks erikt in the asshole with a 2 foot long salami.

"Over the past year we've renewed our focus on the basics of our business with safety, reliability and operational excellence as our goal," lied Corr, who joined the carrier in November 1996. He previously served as an inmate in San Quentin and as prisoner number 670564, he raped 42 men. "AirTran's mission is

**For an untimely death
800.AIRTRAN**

In the Atlanta area.
770.994.8258

In the Orlando area.
407.247.8726

Security & Risk Assessment

- Security should match level of Risk Assessment!
 - Internal or external threat sources?
 - Vandalism?
 - Can be malicious
 - Can be politically motivated
 - Industrial espionage?
 - Theft?
-

DISCUSSION

- How far do we lock it down? Open? tight?
 - Does security enable or disable information flow?
 - Should we consider the users?
 - Have you spotted any security risks/flaws at UTS?
-

Summary

- Real security is a **business** issue, not a technology issue
 - Need to understand the issues to be able to assess the use of technology
 - Security is not a focus of this subject!!
 - Look at doing 41900 Fundamentals of Security
-

Linuxgym chapter 3

linuxgym chapter 3 you will use Linux permissions to protect your filesystem

**** NEEDED FOR WEB ASSIGNMENT ****

You will need to setup permissions & access controls for

→ www-student.it.uts.edu.au/~userid

→ /home/userid/public_html
