INB255/INN255
Security

Lecture 5:

Access Control Principles

Outline

- Introduction to access control
- Major access control approaches
  - – Discretionary
  - – Mandatory
  - – Role-based
- Implementing access control
- User authentication mechanisms
  - – Knowledge based
  - – Object based
  - – ID-based

Introduction to access control

- Q: *What is access control?*

- A: Controlling how users and systems access other systems and resources:
  - To prevent unauthorised users gaining access to resources
  - To prevent authorised users from misusing resources

- Resource examples include:
  - Hardware: processors, laptops, routers
  - Software: application software, system software
  - Information assets: data files, system documentation
  - Services: computing, communications, power

Introduction to access control

- Q: *Why is access control important for information security?*

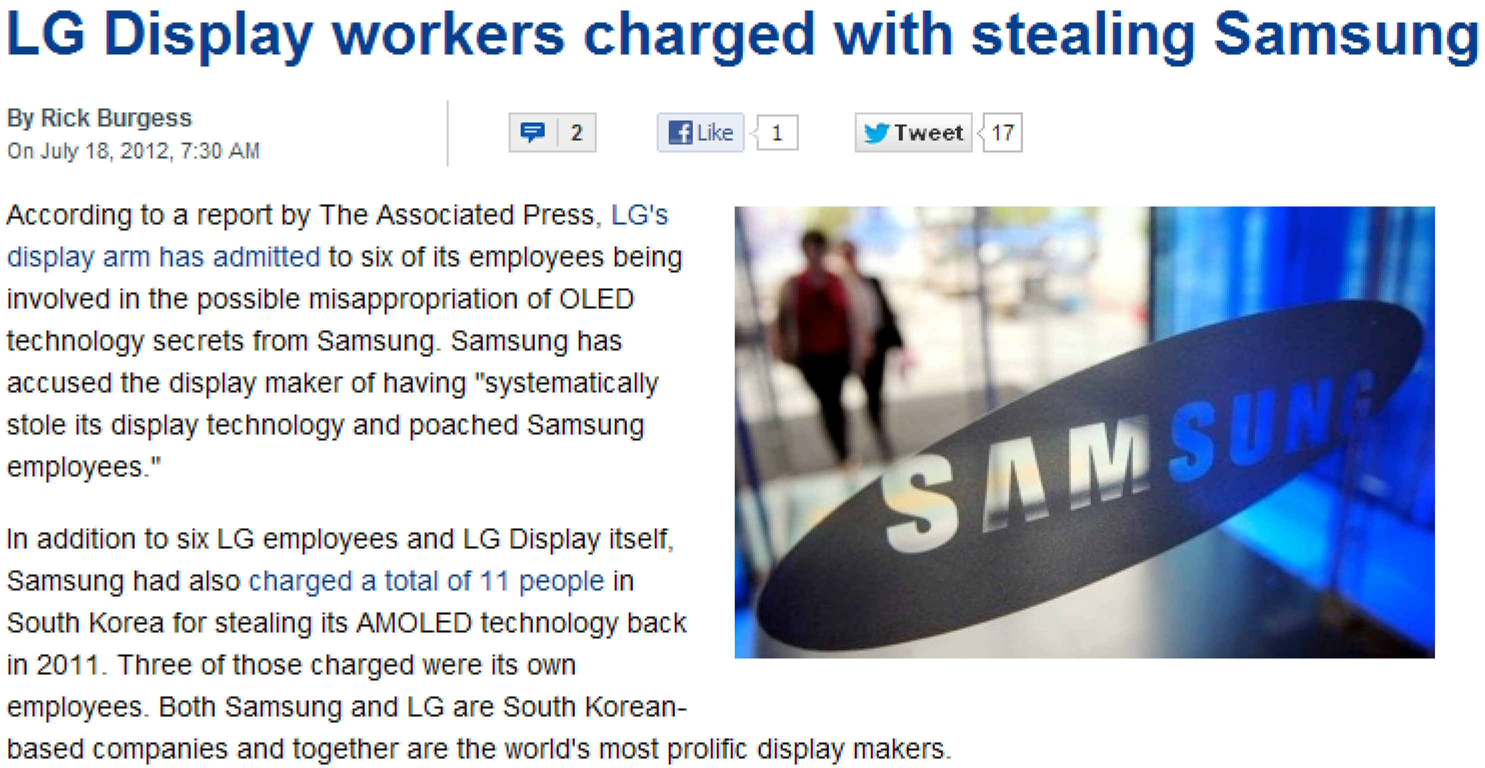
- A: Unauthorised access could compromise
  - Confidentiality
  - Integrity
  - Availability

of information assets

  - these are valuable assets and should be protected

Introduction to access control

- Asset compromise is business loss:



LG Display workers charged with stealing Samsung

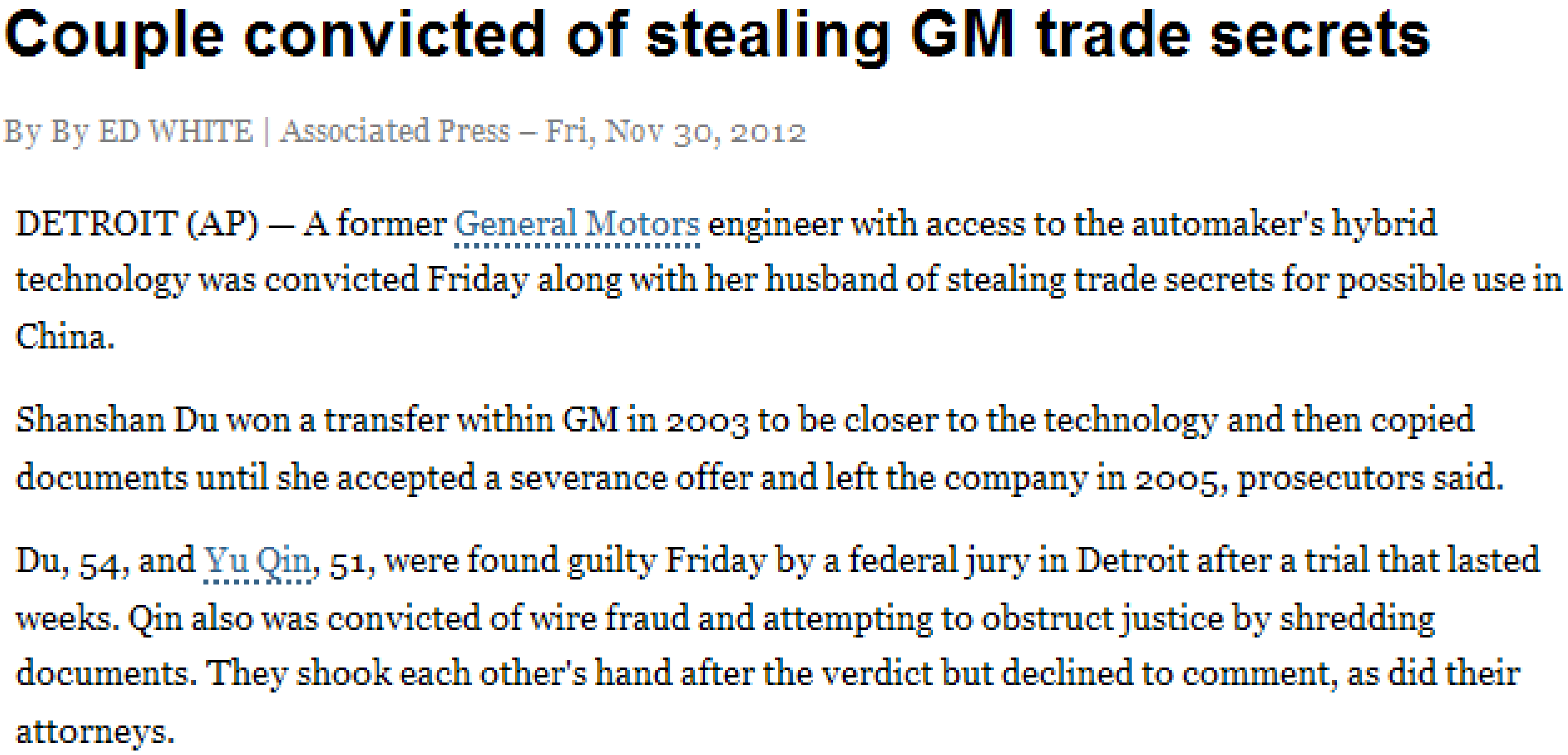
By Rick Burgess
On July 18, 2012, 7:30 AM

According to a report by The Associated Press, LG's display arm has admitted to six of its employees being involved in the possible misappropriation of OLED technology secrets from Samsung. Samsung has accused the display maker of having "systematically stole its display technology and poached Samsung employees."

In addition to six LG employees and LG Display itself, Samsung had also charged a total of 11 people in South Korea for stealing its AMOLED technology back in 2011. Three of those charged were its own employees. Both Samsung and LG are South Korean-based companies and together are the world's most prolific display makers.

Introduction to access control

- Asset compromise is business loss:



Couple convicted of stealing GM trade secrets

By By ED WHITE | Associated Press – Fri, Nov 30, 2012

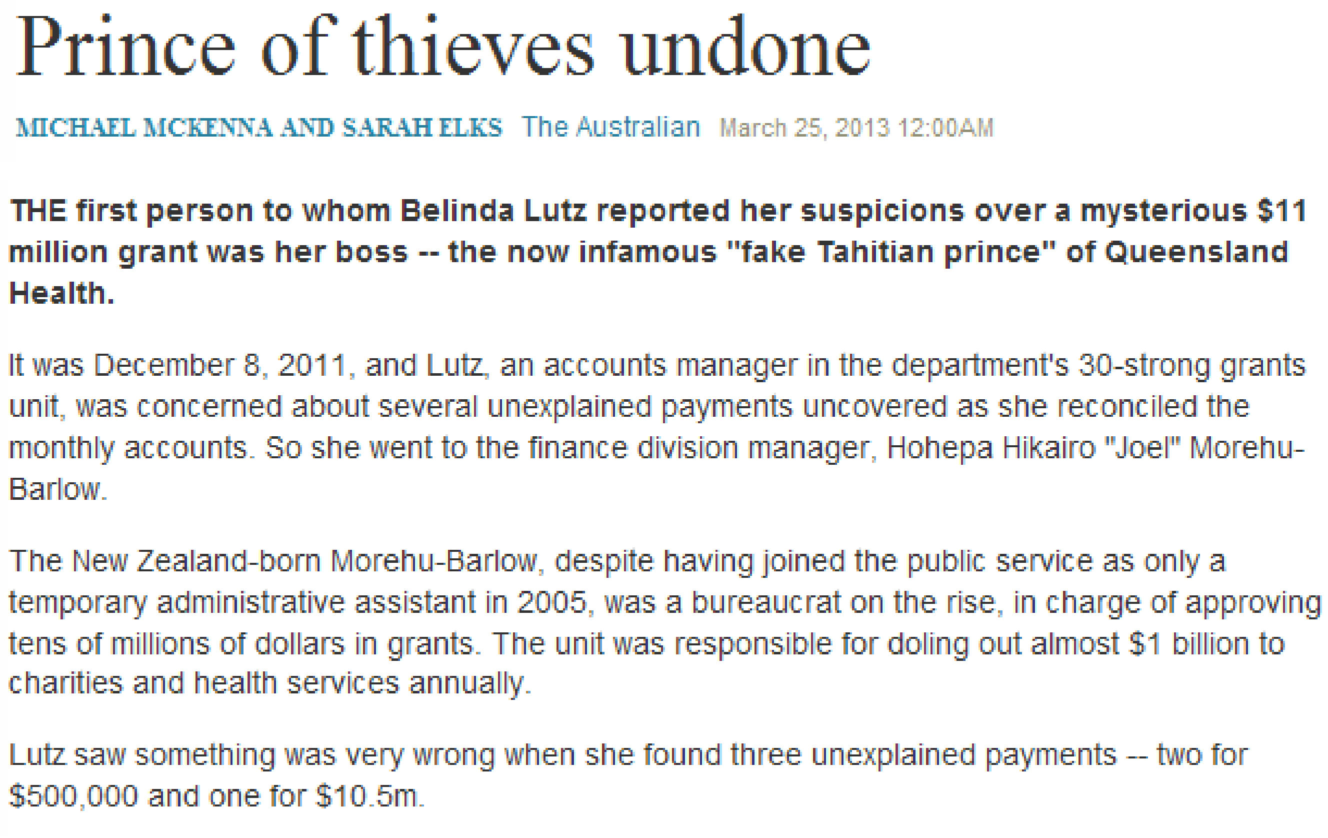
DETROIT (AP) — A former General Motors engineer with access to the automaker's hybrid technology was convicted Friday along with her husband of stealing trade secrets for possible use in China.

Shanshan Du won a transfer within GM in 2003 to be closer to the technology and then copied documents until she accepted a severance offer and left the company in 2005, prosecutors said.

Du, 54, and Yu Qin, 51, were found guilty Friday by a federal jury in Detroit after a trial that lasted weeks. Qin also was convicted of wire fraud and attempting to obstruct justice by shredding documents. They shook each other's hand after the verdict but declined to comment, as did their attorneys.

Introduction to access control

- Asset compromise is business loss:



Prince of thieves undone

MICHAEL MCKENNA AND SARAH ELKS The Australian March 25, 2013 12:00AM

THE first person to whom Belinda Lutz reported her suspicions over a mysterious $11 million grant was her boss -- the now infamous "fake Tahitian prince" of Queensland Health.

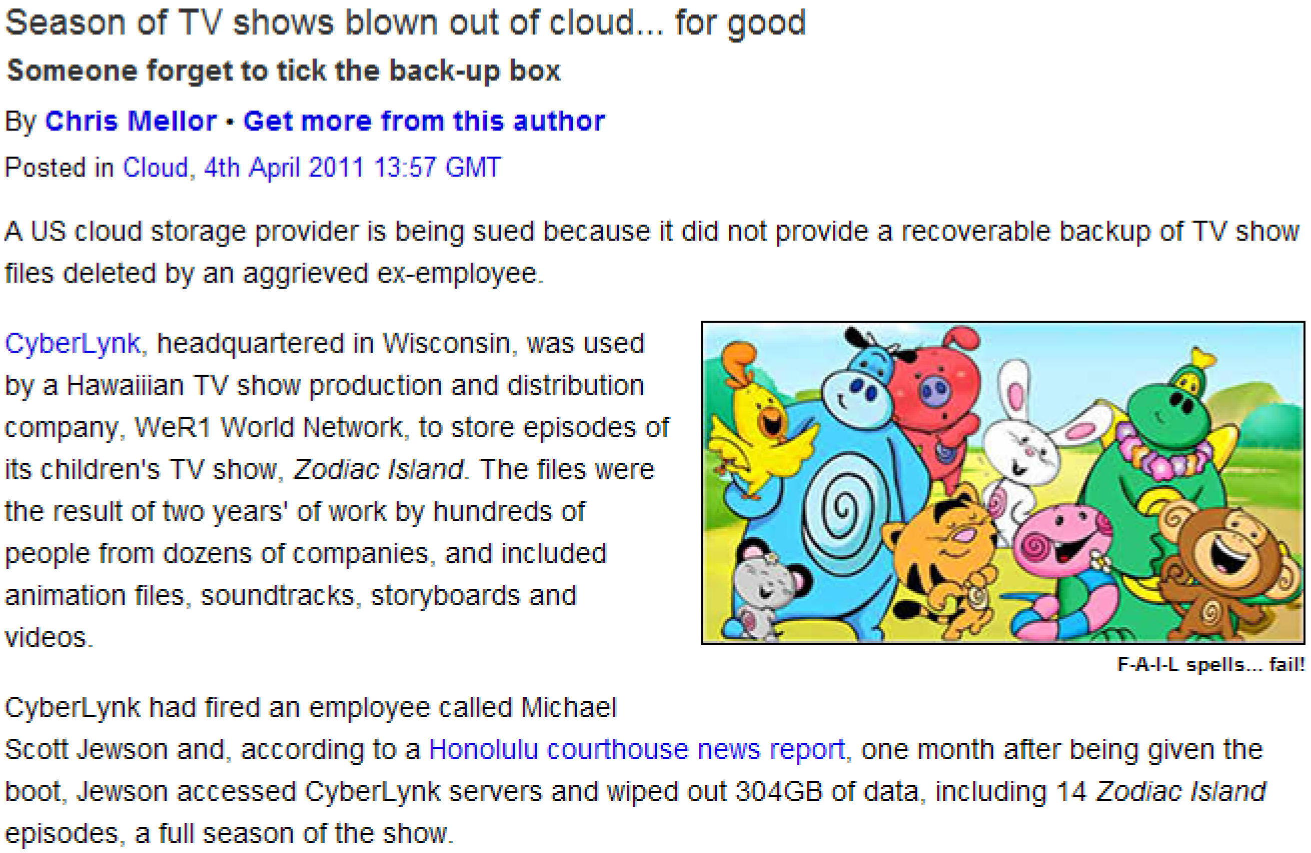
It was December 8, 2011, and Lutz, an accounts manager in the department's 30-strong grants unit, was concerned about several unexplained payments uncovered as she reconciled the monthly accounts. So she went to the finance division manager, Hohepa Hikairo "Joel" Morehu-Barlow.

The New Zealand-born Morehu-Barlow, despite having joined the public service as only a temporary administrative assistant in 2005, was a bureaucrat on the rise, in charge of approving tens of millions of dollars in grants. The unit was responsible for doling out almost $1 billion to charities and health services annually.

Lutz saw something was very wrong when she found three unexplained payments -- two for $500,000 and one for $10.5m.

Introduction to access control

- Asset compromise is business loss:



Season of TV shows blown out of cloud... for good

Someone forget to tick the back-up box

By **Chris Mellor • Get more from this author**

Posted in Cloud, 4th April 2011 13:57 GMT

A US cloud storage provider is being sued because it did not provide a recoverable backup of TV show files deleted by an aggrieved ex-employee.

CyberLynk, headquartered in Wisconsin, was used by a Hawaiiian TV show production and distribution company, WeR1 World Network, to store episodes of its children's TV show, *Zodiac Island*. The files were the result of two years' of work by hundreds of people from dozens of companies, and included animation files, soundtracks, storyboards and videos.

F-A-I-L spells... fail!

CyberLynk had fired an employee called Michael Scott Jewson and, according to a Honolulu courthouse news report, one month after being given the boot, Jewson accessed CyberLynk servers and wiped out 304GB of data, including 14 *Zodiac Island* episodes, a full season of the show.

Introduction to access control

- *2012 Australian Cyber Crime & Security Survey* extract (p18):
  - Main types of cyber incidents reported:
    - theft of a notebook, tablet or mobile devices (32%)
    - virus or worm infection (28%)
    - trojan or rootkit malware (21%)
    - unauthorised access (18%)
    - theft or breach of confidential information (17%)
    - denial-of-service attack (16%).

Introduction to access control

- For effective access control, you need to consider:
  - What resources do you have?
  - How sensitive are these resources?
  - Who should have access to each resource?
  - What access permissions (authorisations) should they have?
  - How will access control decisions be made?
  - How will your access control policy be implemented?

Introduction to access control

- ***What resources do you have?***
- First step is to form an inventory:
  - Useful for other purposes – insurance, risk management etc.
  - AS/NZS 27002:2006 **Clause 7 Asset management** includes this in subsect. 7.1 Responsibility for Assets
    - 7.1.1 Inventory of assets
      - Include type, format, location, backup information, license information and business value of all assets
    - 7.1.2 Ownership of assets
    - 7.1.3 Acceptable use of assets
      - Including rules for email and internet use, and guidelines for the use of mobile devices

Introduction to access control

- ***How sensitive are these resources?***
- Assess the sensitivity of each resource:
  - AS/NZS 27002:2006 **Clause 7 Asset management** includes this in subsect. 7.2 Information classification
    - 7.2.1 Classification guidelines
      - Classify info in terms of its value, legal requirements, sensitivity and criticality to the organization
      - Take into account business needs for sharing or restricting information and the business impact associated with these needs
      - Classification may vary over time – review and reclassify
    - 7.2.2 Information handling and labelling
      - Includes procedures for information labelling particularly of sensitive or critical material

Introduction to access control

- ***Who should have access to each resource?***
- Common principles for access control policies are:
  - blacklists
    - Access generally permitted unless expressly forbidden
      - If your name is on the list, you will be denied access
      - These are the sites that you are not permitted to visit
  - whitelists
    - Access is generally forbidden unless expressly permitted
      - If your name is on the list, you will be granted access
      - These are the only sites that you are permitted to visit

Introduction to access control

- ***Who should have access to each resource?***
- Common principles for access control policies:
  - principle of least privilege
    - Access is generally restricted to the minimum resources and authorisations required for an entity to perform their day-to-day function
    - Intended to limit the level of damage if a security incident occurs
    - Where the resource is information, may be known as *need to know principle*
      - Only given information needed now to perform your job

Introduction to access control

- ***Who should have access to each resource?***
  - Separation of duties (privileges):
  - For any critical task,
    - Divide the task up into a series of steps
    - Ensure that the steps are performed by different entities
      - No single entity should be authorised to complete all of the steps in a critical task
    - More than one entity is now required to complete the task
      - Useful to minimise error, harder for insider abuse, for example fraud
  - Examples:
    - Financial transactions may require data entry to be performed by one person and authorisation by another
    - Access to critical resources (e.g. servers) could require presence of two trusted individuals

Introduction to access control

- Access control terminology:
  - Subjects
    - Entities requesting access to a resource
      - Examples: Person (User), Process, Device
    - This is an active role:
      - Entity initiates access request and is user of information
  - Objects
    - Resources or entities which contain information
      - Examples: Disks, files, records, directories
    - This is a passive role
      - Object is repository for information, the resources that a subject tries to access

Introduction to access control

- ***What access permissions (authorisations) should subjects have?***
  - What modes of access are permitted?
- If you have permission to access a resource, what are you allowed to do?
  - Example: possible access permissions for data resources include:
    - read - observe
    - write – observe and alter
    - execute – neither observe nor alter
    - append – alter
    - search

Introduction to access control

- ***How will access control decisions be made?***
- Three main approaches:
  - Discretionary access control
    - Decision at the discretion of some individual, possibly the information asset owner
  - Mandatory access control
    - System wide set of rules applied
  - Role-based access control
    - Decision based on the role of the individual, rather than the identity (user, administrator, student, etc)

Introduction to access control

- ***How will the access control policy be implemented?***
- To implement a system where some subjects are permitted to access a restricted resource, need to be able to:
  1. Identify the subject
     - Who are you claiming to be?
  2. Authenticate the subject
     - Provide evidence that you are who you claim to be
  3. Verify that the subject is authorized for the requested mode of access
     - Check that you are permitted to access resource in the manner requested
- Consider control mechanisms to enforce the access control policy for the resource being protected
  - Just having a policy doesn't mean users will abide by it

Outline

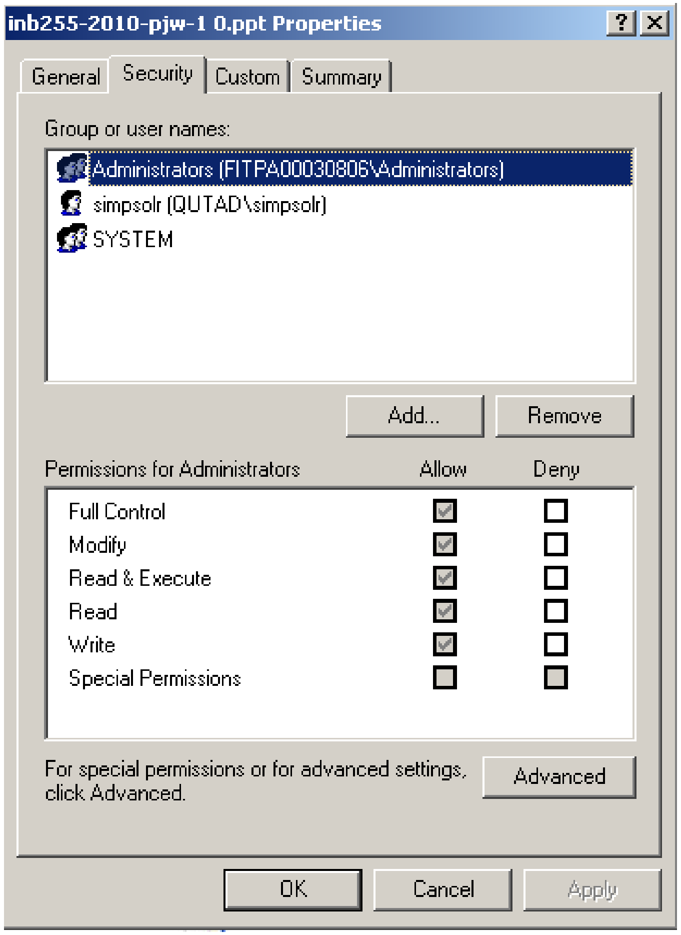
- Introduction to access control
- <u>Major access control approaches</u>
  - Discretionary
  - Mandatory
  - Role-based
- Implementing access control
- User authentication mechanisms
  - Knowledge based
  - Object based
  - ID-based

Major access control approaches

- **Discretionary access control**
  - Access rights to an object or resource are granted at the discretion of the owner
    - For example, the security administrator, the owner of the resource, or the person who created the asset
  - DAC is discretionary in the sense that a subject with a certain access authorization is capable of passing that authorization (directly or indirectly) to any other subject.
  - Often implemented access control lists or matrices
  - Popular operating systems use DAC.

Major access control approaches

- DAC in Windows XP:
  - For a particular object,
    - check Properties
    - then Security
  - The DACL lists
    - groups and users with access permissions, and
    - the type of permissions



inb255-2010-pjw-1 0.ppt Properties

Group or user names:

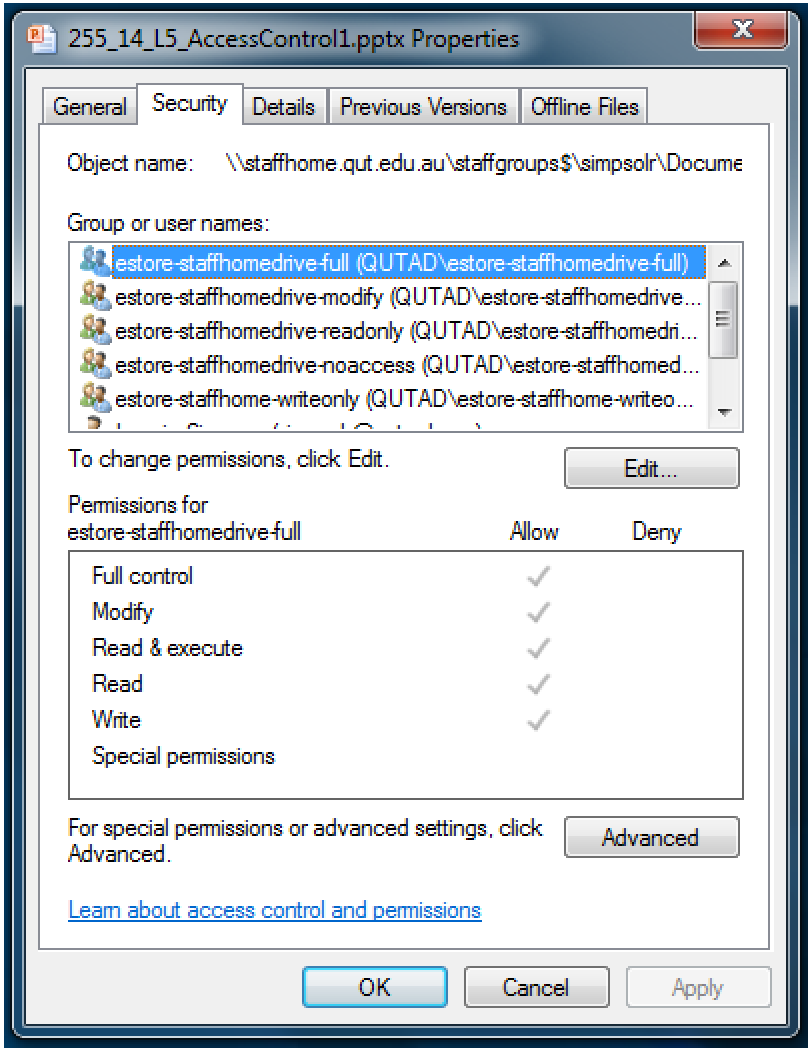
- Administrators (FITPA00030806\Administrators)
- simpsolr (QUTAD\simpsolr)
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Major access control approaches

- DAC in Windows 7:
  - For a particular object,
    - check Properties
    - then Security
  - The DACL lists
    - groups and users with access permissions, and
    - the type of permissions



Object name: \\staffhome.qut.edu.au\staffgroups$\simpsolr\Docume

Group or user names:

estore-staffhomedrive-full (QUTAD\estore-staffhomedrive-full)
estore-staffhomedrive-modify (QUTAD\estore-staffhomedrive...
estore-staffhomedrive-readonly (QUTAD\estore-staffhomedri...
estore-staffhomedrive-noaccess (QUTAD\estore-staffhomed...
estore-staffhome-writeonly (QUTAD\estore-staffhome-writeo...

To change permissions, click Edit.

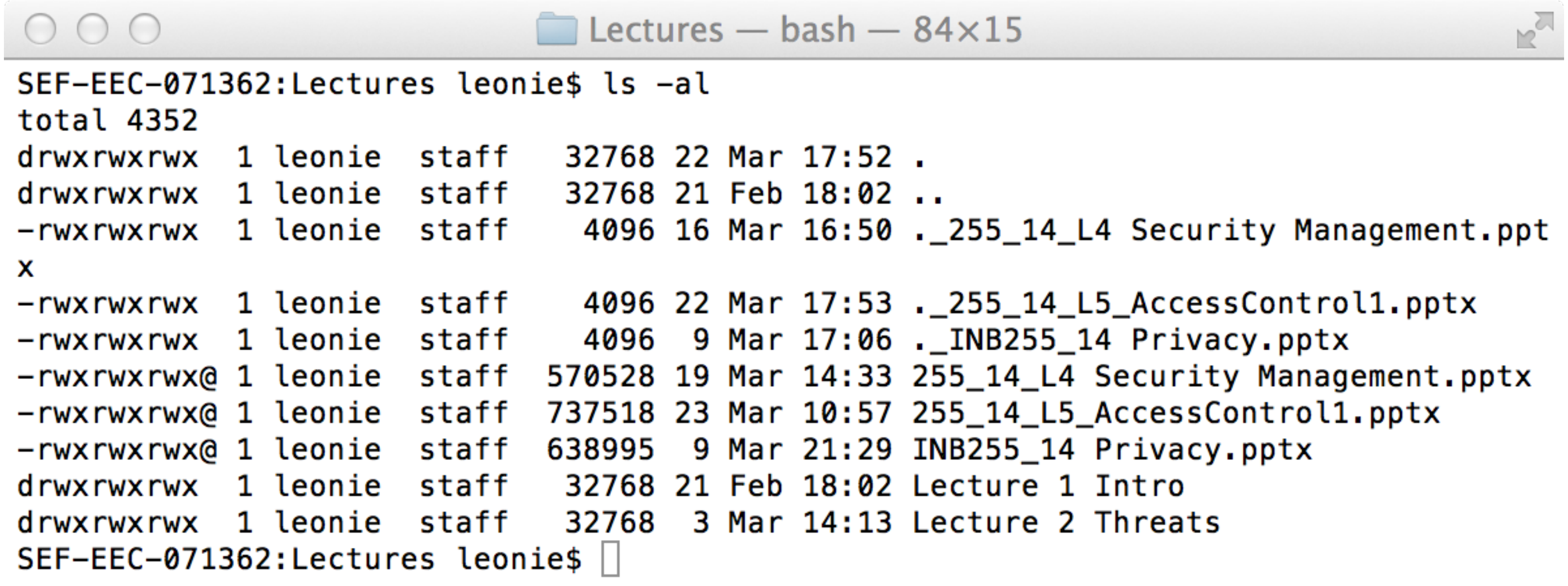
Permissions for estore-staffhomedrive-full	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Major access control approaches

- DAC in Apple OS X:
  - Object on each line
  - Permissions indicated for: Owner, Group and Other
  - Type of permissions: r read, w write and x execute



```
SEF-EEC-071362:Lectures leonie$ ls -al
total 4352
drwxrwxrwx  1 leonie  staff   32768 22 Mar 17:52 .
drwxrwxrwx  1 leonie  staff   32768 21 Feb 18:02 ..
-rwxrwxrwx  1 leonie  staff    4096 16 Mar 16:50 ._255_14_L4 Security Management.ppt
x
-rwxrwxrwx  1 leonie  staff    4096 22 Mar 17:53 ._255_14_L5_AccessControl1.pptx
-rwxrwxrwx  1 leonie  staff    4096  9 Mar 17:06 ._INB255_14 Privacy.pptx
-rwxrwxrwx@ 1 leonie  staff  570528 19 Mar 14:33 255_14_L4 Security Management.pptx
-rwxrwxrwx@ 1 leonie  staff  737518 23 Mar 10:57 255_14_L5_AccessControl1.pptx
-rwxrwxrwx@ 1 leonie  staff  638995  9 Mar 21:29 INB255_14 Privacy.pptx
drwxrwxrwx  1 leonie  staff   32768 21 Feb 18:02 Lecture 1 Intro
drwxrwxrwx  1 leonie  staff   32768  3 Mar 14:13 Lecture 2 Threats
SEF-EEC-071362:Lectures leonie$ 
```

Major access control approaches

- **Mandatory access control**
  - A central authority assigns attributes to objects and to subjects
    - For example:
      - subjects – clearance levels,
      - objects -classification levels
  - Have a system-wide **set of rules** relating attributes of the objects and subjects to the modes of access that are permitted
  - MAC is mandatory in the sense that entities are not able to decide which other entities they want to allow to access resources, the system rules apply
    - the system denies users full control over access to the resources they create

Major access control approaches

Example – BLP model security level hierarchy

Top Secret

↓

Secret

↓

Confidential

↓

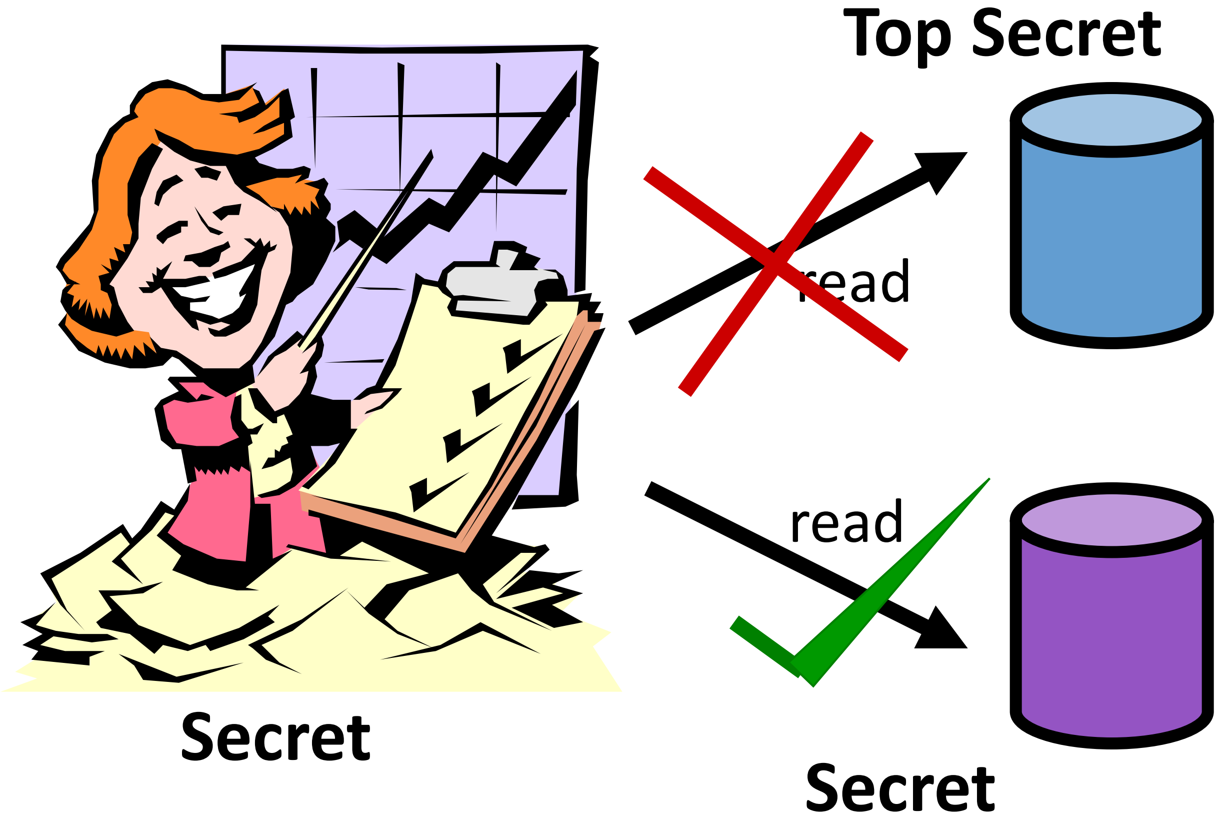
Classified

↓

Unclassified

Major access control approaches

Example: BLP model - mandatory access control



Top Secret

read

read

Secret

Secret

Major access control approaches

- **Role based access control**
  - Access rights are based on the role of the subject, rather than the subject' s individual identity
    - A role is a collection of procedures or jobs that the subject performs
      - Examples: user, administrator, student, etc
    - A subject could have more than one role
      - Example: Mr Kush is a student and a staff member
    - More than one subject could have the same role
      - Example: Lots of students!

Major access control approaches

- Combinations of access control approaches are often used:
  - Combining mandatory and discretionary access control approaches:
    - Mandatory access control is applied first:
    - If access is granted by the mandatory access control rules, then the discretionary system is invoked
    - Access granted only if both of the approaches permit access

Major access control approaches

- Combining mandatory and discretionary access control approaches ensures that:
    - no owner can make sensitive information available to unauthorized users, and
    - ‘need to know’ can be applied to limit access that would otherwise be granted under mandatory rules

- Other combinations possible:
    - combine RBAC with DAC and/or MAC

Outline

- Introduction to access control
- Major access control approaches
  - Discretionary
  - Mandatory
  - Role-based
- <u>Implementing access control</u>
- User authentication mechanisms
  - Knowledge based
  - Object based
  - ID-based

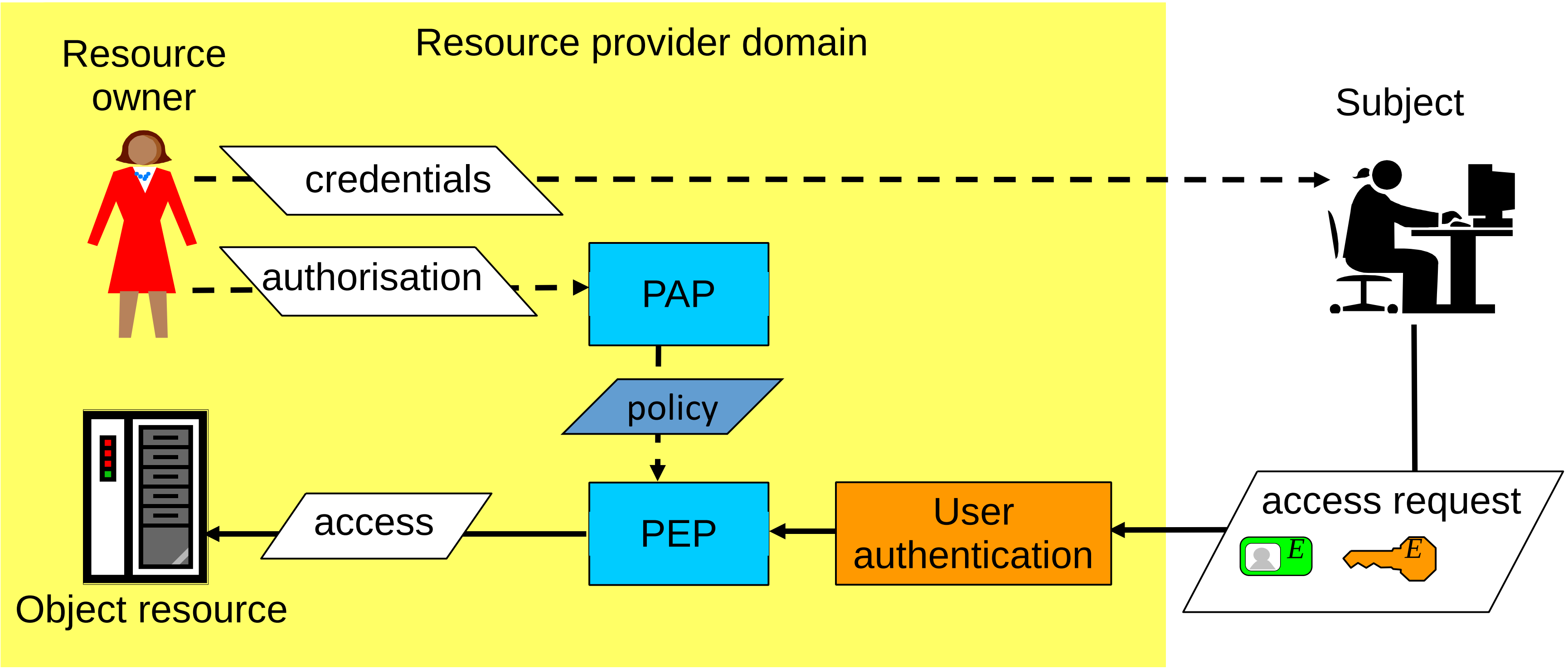
Implementing access control

- Two phases of access control:
  1. Policy definition (authorisation) phase where privilege is allocated and administered
     a. Authorise subject by defining the AC policy
     b. Distribute access credentials/token to subject
     c. Change/revoke authorisation whenever necessary
  2. Policy enforcement (grant access) phase* where privilege is required to gain access
     a. Authenticate subject
     b. Grant access as authorised by policy
     c. Monitor access

     * **(note: sometimes the term "authorisation" is used for this phase)**

Implementing access control

Access control conceptual diagram



Legend PAP: Policy Administration Point

PEP: Policy Enforcement Point

- - - - ▸ AC policy definition phase

◂——— AC policy enforcement phase

Implementing access control

- Phase 1 - Administration of privileges
  - How are users informed of
    - their access privileges?
    - their responsibilities w.r.t. these privileges?
  - How do you
    - give users the means to exercise their privileges (credentials)?
    - revoke (take back the means to exercise) their privileges?
  - Who keeps track of who has what?
    - Recording privileges

Implementing access control

- Phase 1- Administration of privileges
- **Need mechanisms in place to inform users of the privileges they have:**
  - Which assets does the user have access to?
    - Physical assets – buildings, rooms, photocopier, telephone
    - Electronic assets – files, systems
  - What sort of access does the user have?
    - Limitations of their access privilege:
      - Access limited to certain rooms, certain times, may have restricted access e.g. local phone calls only
      - Restriction on type of access: read-only access, etc

Implementing access control

- Phase 1- Administration of privileges
- **Need mechanisms in place to inform users of the conditions of use of their privileges:**
  - limitations on disclosure of protected data
  - how to handle unauthorized requests for access
  - disciplinary consequences of violation of privileges
  - action to be taken if a security incident occurs and
  - reporting procedures for security incidents

Implementing access control

- Phase 1- Administration of privileges

- **Need mechanisms in place to securely hand over the means to exercise the privileges:**
  - to the intended recipient
    - Check identity
  - only to the intended recipient
    - Security of handover phase
- **The access control measure may be**
  - physical
    - ID badge, uniform, door key, magnetic swipe card
  - logical
    - password, PIN

Implementing access control

- Phase 1- Administration of privileges
- **Need mechanisms in place to record details of users and their privileges:**
  - How are privileges recorded?
    - Are the records of privileges secure from illicit disclosure or modification?
    - Would the records of privileges be acceptable in a legal challenge?
  - Can you easily identify privileges associated with
    - a particular user?
    - a particular resource?

Implementing access control

- Phase 1- Administration of privileges
- **Need mechanisms in place to revoke the privileges when required:**
  - Is there an expiry time of the privilege?
  - Is there a procedure for automatic revocation of the privilege under certain conditions?
    - Example: on termination of employment
  - Who needs to be informed of the withdrawal of a privilege?
    - User
    - Administration
    - Security

Implementing access control

- Phase 1- Administration of privileges
- **Need mechanisms in place to revoke the privileges when required:**
  - Are there procedures for:
    - the user to hand back the privilege?
    - the privilege be withdrawn without the cooperation of the user?
      - Often harder to revoke physical access control than logical access control
  - Can the user prove that the privilege had been withdrawn or handed back?

Implementing access control

- Phase 1- Administration of privileges
- **AS/NZS 27002:2006** deals with this in Clause 11- Access control:
  - 11.2 User access management
  - *Objective: To prevent unauthorized access to information systems.*

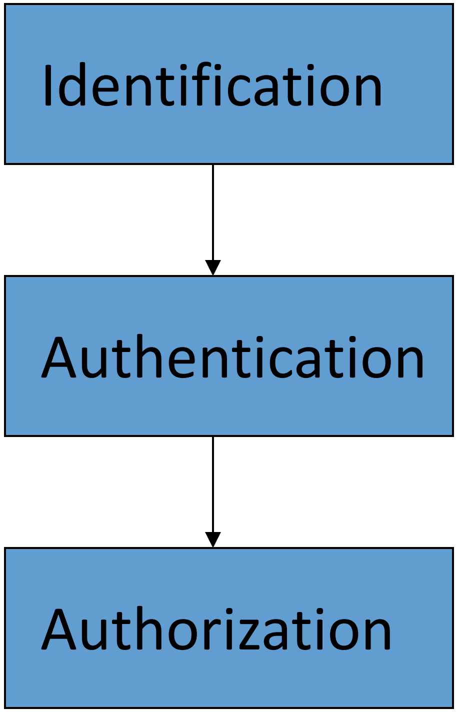
    Formal procedures in place to control allocation of access rights ... to cover all stages … from initial registration of new users to the final deregistration of users who no longer require access ...
  - *11.2.1 User registration*
  - *11.2.2 Privilege management*
  - *11.2.3 User password management*
  - *11.2.4 Review of user access rights*

Implementing access control

- Phase 2 - Policy enforcement
- To gain access to a resource, users should be authenticated and authorised
  - Authentication permits the system to verify you are the identity you claim to be
    - Identification: the process of claiming an identity
    - (Entity) Authentication: the process of proving (validating or verifying) the claimed identity
  - Examples:
    - You announce who you are, and show your ID card
    - You provide a user ID, and the corresponding password
  - The system checks if you are authorised for the requested access (from Phase 1) before granting access

Implementing access control

- Phase 2 - Policy enforcement
- Identification, authentication and authorization



Who are you?

Is it really you?

Are you allowed to access this resource? In what mode?

Implementing access control

- Phase 2 - Policy enforcement
- Identification and authentication of users is important because:
  - User identity is used to make access control decisions
  - User identity is recorded in logs of events in an audit trail
- The system needs to be assured that
  - attackers cannot masquerade as legitimate users
- Users need to be assured that:
  - they are communicating with legitimate systems
  - the system does not allow masquerade attacks (which could result in their being held responsible for the actions of an attacker), and
  - the system itself cannot subsequently masquerade as the user

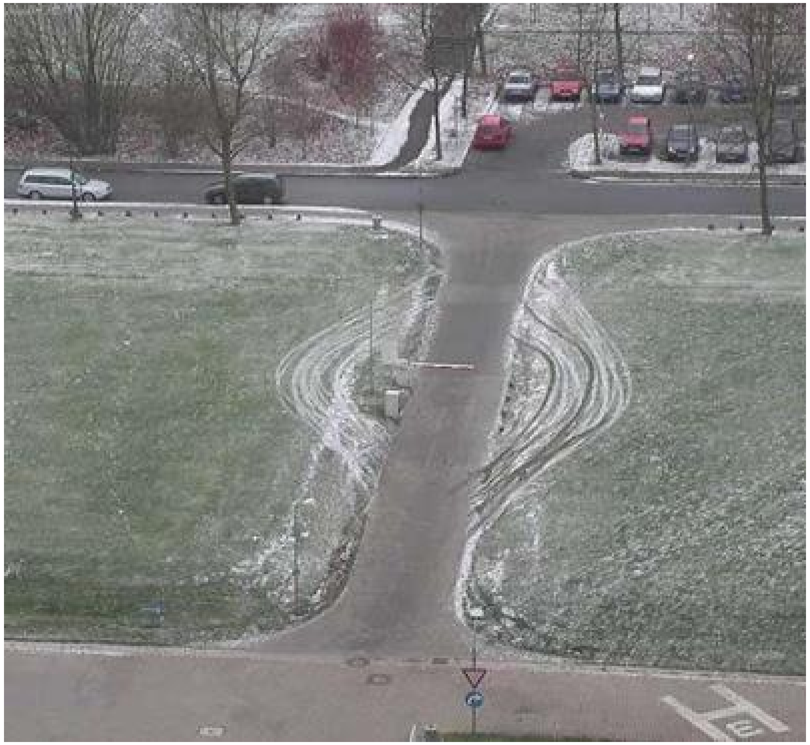
Implementing access control

- Phase 2 - Policy enforcement
- **Monitoring access**
- This is important for
  - detecting unauthorized activities
    - detecting access control loopholes
    - identifying security incidents
  - providing evidence of security incidents,

  and
  - providing a model of normal system behaviour
    - Used for detecting some attacks (Intrusion Detection Systems)

Implementing access control

- Monitoring can help detect access control loopholes permitting unauthorised accesses



- Picture from http://www.syslog.com/~jwilson/pics-i-like/kurios119.jpg

Implementing access control

- Phase 2 - Policy enforcement
- **Monitoring access**
- **AS/NZS 27002:2006** deals with this in Clause 10 – Communications and operations management:
  - 10.10 Monitoring
  - *Objective: Detect unauthorized information processing activities*
    - 10.10.1 Audit logging
    - 10.10.2 Monitoring system use
    - 10.10.3 Protection of log information
    - 10.10.4 Administrator and operator logs
    - 10.10.5 Fault logging
    - 10.10.6 Clock synchronization

Outline

- Introduction to access control
- Major access control approaches
  - Discretionary
  - Mandatory
  - Role-based
- Implementing access control
- User authentication
  - Knowledge based
  - Object based
  - ID-based

User authentication

- Authenticators can be categorised as:
  - Knowledge-Based (Something you know)
  - Object-Based (Something you have)
  - ID-Based (Something you are)
  - Location-based (Somewhere you are)

- Multi-factor authentication uses combinations of the above categories of authenticators

User authentication

- Knowledge-Based (Something you know):
  - Characterized by secrecy or obscurity
    - something only you would know
  - Examples:
    - memorized passwords
    - responses to questions:
      - your birthdate,
      - Mother' s maiden name,
      - or your pet' s name

User authentication

- Knowledge-Based (Something you know):
  - Advantages include:
    - Readily accepted method
    - Easily implemented
  - Disadvantages include:
    - Can be shared with others by user
    - User may forget password
    - May be compromised without user knowledge
      - Others may know or be able to guess
      - Difficult for user to know if compromised

User authentication

- Object-Based (Something you have):
  - Characterized by physical possession of a token.
  - Examples:
    - Physical key
    - Magnetic swipe card
    - Token used for generating access codes

RSA SecurID SID700

User authentication

- Object-Based (Something you have):
  - Advantages include:
    - Difficult to share (effort required to make a copy)
    - If lost, the owner may realise - sees evidence of the loss
  - Disadvantages include:
    - If lost, the finder can make use of the token
    - May be difficult or expensive to recall without cooperation of user

User authentication

- ID-Based (Something you are):
  - Characterized by uniqueness to one person.
  - Examples include:
    - fingerprint,
    - eye scan (iris or retina),
    - voiceprint,
    - physical signature

User authentication

- ID-Based (Something you are):
  - Advantages include:
    - Characteristic can't be forgotten or lost
    - May be difficult to copy, share or distribute
    - Should require the person being authenticated to be present at the time and point of authentication
  - Disadvantages include:
    - System to implement this may be complex
    - Characteristic may not be 'secret': others may be able to produce sample
    - Harder to replace a compromised biometric authenticator, than to replace passwords or tokens

User authentication

- Location-based (Somewhere you are):
  - Characterized by your location
    - space and/or time
  - Examples:
    - Use of location and tracking technologies
      - triangulation of cell-phone signals, or global positioning systems (GPS).
    - Machine IP address and DNS name
    - Link location to time

User authentication

- Location-based (Somewhere you are):
  - Advantages include:
    - Can improve network security, if access locations are (relatively) local
  - Disadvantages include:
    - Privacy issues
      - who should know where you are, when?

User authentication

- Multi-factor authentication
  - Combines two or more authentication techniques
  - Aim is to obtain a stronger and more reliable level of authentication
- Typical example:
  - Two-factor authentication is commonly based on
    - something a user knows (factor one), plus
    - something the user has (factor two).
  - Common combination is a token and a password
    - Example: ATM card and PIN

Summary

- Access control is important for information security
- Need to consider how to:
  - Make access control policy decisions
  - Enforce access control policy using control measures
    - Monitoring required
- Major access control approaches:
  - Discretionary
  - Mandatory
  - Role-based
- User authentication is important:
  - In preventing unauthorised access to resources

Things to note:

- This is Week 5 and Lecture 5
- In Week 6:
  - Workshops/tutorials will be held as usual
  - No lecture
  - Quiz 1 (mid-semester exam) will be held in the lecture timeslot:
    - For room allocations check Blackboard (look under Assessment)
    - Details on what to bring, what to expect, how to prepare, etc on BB
    - Covers lectures 1 - 5 and associated workshops/tutorials
- In Week 7:
  - Security news log first submission due on Friday