Distributed Systems Security

Security Policy and Models

Prof. Steve Wilbur
s.wilbur@cs.ucl.ac.uk

Z08

Lecture Objectives

- Identify broad security policy approaches in operating systems
- Examine standard approaches
- Examine formal models for data security and integrity

Z08

Security Policy

- Security requirements as a *set of rules* which are:
  - well-defined
  - consistent
  - implementable
- System based on such *Policy* will meet user's expectations
- A policy is a statement of the security we expect the system to enforce

Z08

Security Models

- Designer must have confidence that proposed system will meet requirements
- Need to be modelled to study ways of enforcing security
- We will study some of these

Z08

Trust

- Need some basis for believing OS will meet our expectations
- *Features/functionality* to enforce security policy
- *Assurance* that it has been implemented to enforce the policy

Z08

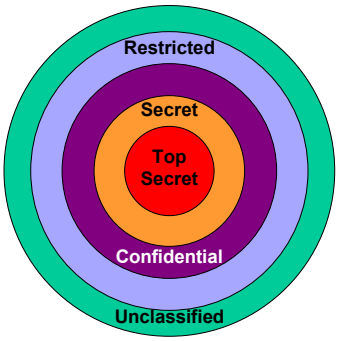
Terminology

- Secure
  - Something either is or is not secure
  - Absolute - not qualified by who, when, where etc
  - A goal
- Trusted
  - ∴Generally talk of trusted systems
  - Graded: degrees of trustedness
  - Judged: based on evidence and analysis
  - Relative to use
  - A characteristic of a system

Z08

Military Security Policies

- Information ranked by sensitivity level, eg.:
  - unclassified
  - restricted
  - confidential
  - secret
  - top secret
- Sensitivity denoted by rank in this list

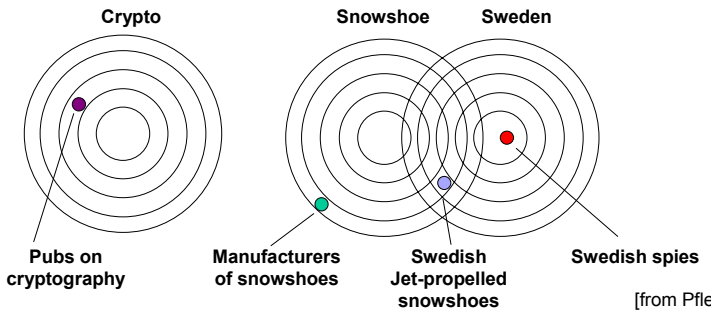


- Access limited by need-to-know rule - only to those needing it for their jobs

Z08

Military Security Policies - 2

- Information is associated with one or more projects or compartments - helps enforce need-to-know



[from Pfleeger]

Z08

Military Security Policies - 3

- Compartments = list of compartments in which info classified
- Classification = <rank; compartments> for (data) object
- Clearance = rank up to which someone is cleared and needs to know information in certain categories
  = <rank; compartments> for subject

Z08

Military Security Policies - 4

- Subject can only read information if:
  - clearance level of subject is at least as high as info
  - the subject has a need to know in all compartments
- Appropriate to rigidly controlled environment - with centralised control
- Mandatory access control - data users, even if they originated the material, do not control who accesses it

Z08

Bell-LaPadula Model

- Military (and some other) approaches can be critically analysed by building formal models of them
- Bell-LaPadula (BLP) model captures important properties of military *confidentiality* model
- Does not model integrity - Biba models *integrity* independently of confidentiality
- See later for names of other well-known models

Z08

Simplified BLP Model

- S is set of subjects
- O is set of objects
- Security levels L partially ordered:
  - $L0 \leq L1 \leq L2 \leq \ldots$
- C(s) denotes clearance level of subject s
- C(o) denotes classification level of object o

ss-property
- Simple Security Property
- A subject s may have read access to an object o only if $C(o) \leq C(s)$
- The "No read-up" policy

Z08

Simplified BLP Model - 2

- Not sufficient for confidentiality of information
- A subject could copy high level object contents to low level object
- ∴ Need to control write access

*-property
- Star Property
- A subject s who has read access to an object o may have write access to object p only if C(o) ≤ C(p)
- The "No write-down" policy

Z08

Simplified BLP Model - 3

- High clearance subject can never send messages to low clearance subjects
- Possible solutions:
  - Temporarily downgrade high clearance subject
  - Modelled by notion of subject's ***current security level*** (fc) and ***maximal security level*** (fs), where fc ≤ fs
  - Assumes s forgets all it knew when fc < fs
  - Not reasonable for human domain but reasonable for programs because only info at fc can be accessed
- or:
  - Identify set of subjects who can violate the *-property
  - ***Trusted Subjects***
  - Actually you hope ***trustworthy*** because such subjects can damage you

Z08

Simplified BLP Model - 4

Basic Security Theorem

If all state transitions in a system are secure and if the initial state of the system is secure, then every subsequent state will be secure, no matter what inputs occur

- Proof would be by induction over input sequences
- Relies on each state transition preserving security properties
- Not specific to BLP

Z08

Tranquility

- McLean considered state transition:
  - downgrade all subjects to lowest level
  - downgrade all objects to lowest level
- State reached is secure according to BLP
- Is BLP flawed?
- Two opinions:
  - McLean: BLP intuitively not secure if system can be moved to a state where everyone can read everything
  - Bell: If user requirements need such a transition then it should be implemented, otherwise not. Need to correctly capture user requirements

Z08

Tranquility - 2

- Problem is a state transition which changes access rights
- Possible within BLP
- But they were really considering cases where access rights are tranquil or fixed
- Property of security levels and access rights never changing is called tranquility

Z08

Commercial Security Policies

- Less rigid than military environment, but some similarities
- Items may have different degrees of sensitivity: eg. *public, proprietary, internal*
- No formal clearance mechanism
- Ownership of data is often *delegated*
- Delegates can use discretion to decide who should be allowed to access information and in what way

- Discretionary access control

Z08

Commercial Security Policies - 2

Mechanisms include:

- Access control lists:
  - list of those allowed to perform function
  - functions may be eg. read, write, append, delete, change permissions
- Set based:
  - specific functions permitted for owner, containing group, world
  - Unix etc. as examples

Z08

Commercial Security Policies - 3

Security needed to ensure that:

- transactions occur in proper order - *Integrity*
- fraud by employees is minimised - *Separation of Duty*
- client's interests not disclosed to competitors - *Conflicts of Interest*

Z08

Commercial Integrity

- Clark-Wilson Integrity model
- Notion of *well-formed transactions*
- Integrity managed by means of *transformation procedures* on *constrained data items*
- In following diagram:
  - GoodsIn Clerk's transaction can only generate delivery receipt (2) if goods arrive which match an order - to ensure only quantities delivered are authorised for payment and were those ordered
  - Payments clerk transaction checks price and terms (1, 3) with original order and that they have been delivered (2) before issuing cheque (4)

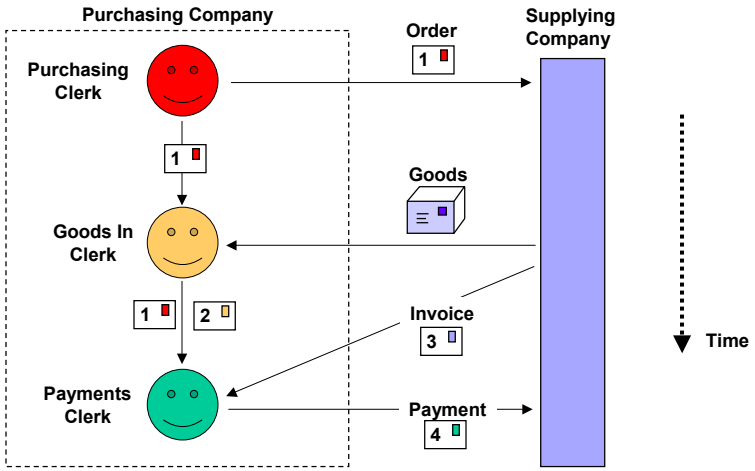
Z08

Commercial Integrity - 2

- Can be cast as access triples:
  - authorised user
  - constrained data items
  - transformation procedure
- Access Triple ::= <userID, TPi, {CDIx, CDIq, …}>

Z08

Commercial Security Policies- 4



Z08

Separation of Duty

- Several people may be authorised to perform specific transformations
- Potential for fraud/abuse if same person executes all transformations
- Policy may specify that different people must be responsible for the different TPs - *Separation of Duty*
- Usually accomplished by *dual/multiple signatures*
- *Clark-Wilson model* does not describe relationships between triples but can be extended to cover this

Z08

Conflicts of Interest

- Legal, advertising, IT consultancy and other companies may work for many clients
- Some of these clients may compete with each other
- Need to ensure clients' commercial secrets do not leak via consultants
- *Conflict of Interest* when a person can obtain sensitive information on competing companies
- *Chinese Walls* security policy (Brewer and Nash) to handle this

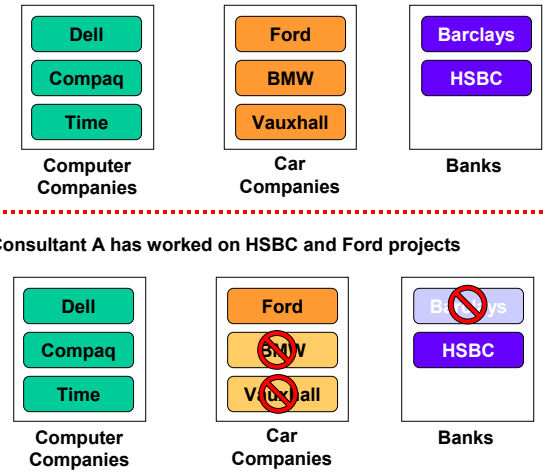
Z08

Chinese Walls

- Objects: Each elementary object, such as a file, contains information relating to only one company
- Company Groups: All objects relating to each company are grouped together
- Conflict Classes: Classes identified relating to areas of business with company groups clustered accordingly

Z08

Chinese Walls - 2



Z08

Chinese Walls - 3

- Access rule to enforce confidentiality policy is:

"A consultant can access information provided they have never accessed information from a different company in the same conflict class"

- Access restrictions thus change dynamically
- Relies on proper classification of conflict classes
- Such classes may change over time with takeovers, mergers etc. - flawed?

Z08

Security Models

- We have dealt with security policies informally
- In practice need formal models which can be used for precisely documenting, and validating policies
- Several such models - see Pfleeger
  - Lattice
  - Bell-LaPadula
  - Harrison-Ruzzo-Ullman
  - Chinese Wall
  - Graham-Denning
  - Biba
  - Clark-Wilson
  - Information Flow

Z08

Security Models - 2

- Why so many?
- Deal with different aspects or policies, eg.
  - mandatory vs. discretionary
  - confidentiality vs. integrity
  - information flow
  - conflict of interest

Z08

Further Reading

- Pfleeger C, "Security in Computing", 2ed, Prentice Hall, 1997, 0-13-185794-0
  - **Trusted Operating Systems:** pp 269-331
- Gollman D, "Computer Security", Wiley, 1999, 0-471-97844-2
  - **Security Models:** pp 46-60
- McCarthy L, "Intranet Security: Stories from the Trenches", Prentice Hall, 1998, 0-13-894759-7

Z08

Further Reading - 2

- Clark D, Wilson D, "A Comparison of Commercial and Military Security Policies", Proc. IEEE Symp Security & Privacy, 1987, pp 184-194
- Brewer D, Nash M, "The Chinese Walls Security Policy", Proc. IEEE Symp Security & Privacy, 1989, pp 289-303
- Bell D, LaPadula L, "Mitre Technical Report 2547 (Secure Computer System): Volume II", Journal of Computer Security, pp 239-263, 1996 (re-publication of original paper)

Z08