Security Models

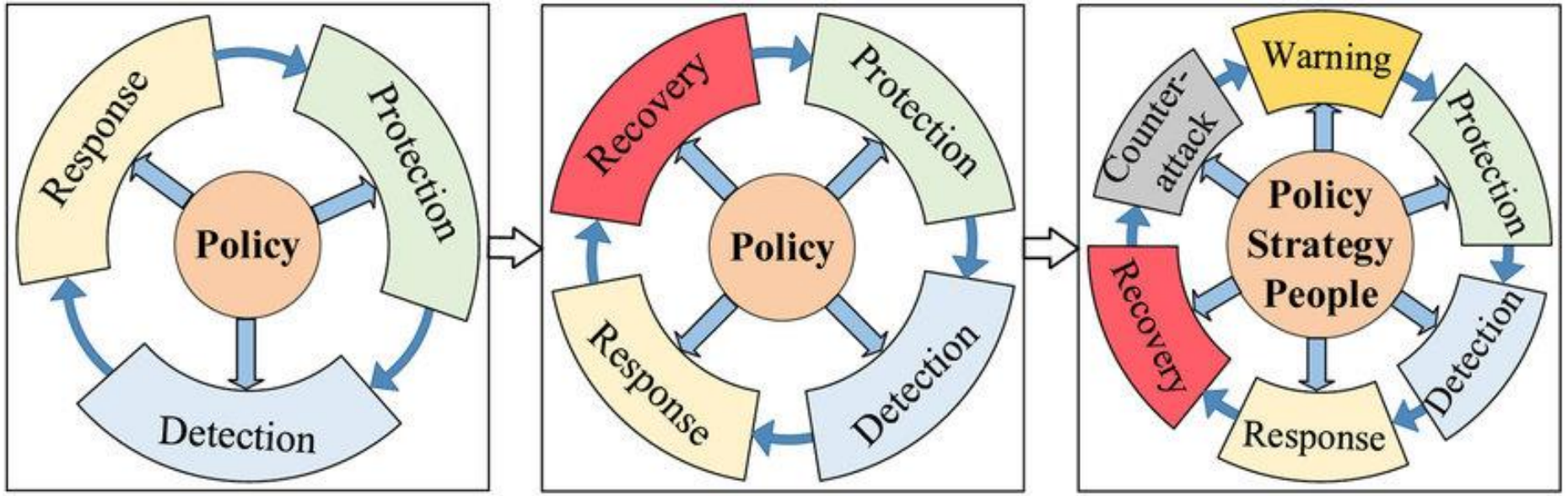
Security Models

•Security means a complete system

–Policies

–Procedures - detail how the policies are implemented

–Models



Security Policies

•Policies – the rules about what must be done.

–Policies include definitions of

- Subjects – the actors
- Objects – the information and equipment
- Actions – what can and cannot be done
- Permissions – map subjects, objects and actions together.
- Protections – rules which prevent subversion of the policy

Security Models

- A classification scheme for people, secrets, activities
- A common language used by policy makers and security administrators.
- Types of models:
  - Discretionary Access Control
  - Mandatory Access Control

Discretionary access control

- DAC
- Users have the authority to set permissions on their own files.
- Users can grant permission to other users.
- Examples – ACLs in Windows, Linux

  Assumes everyone who has permission exercises it responsibly.

Mandatory access control

- MAC
- Users have no authority to set permissions.
- Centralised policy admins set permissions.
- Each rule maps a subject (actor) to an object (resource) with a specific set of permissions
- Example – SE Linux

  Assumes no-one who has access can be trusted to exercise it responsibly.

  Even root can have no authority.

Trust management

A form of security policy:

- Actions – sensitive operations
- Principals – actors
- Policies – rules which map principals to actions.
- Credentials – digitally signed documents which map allowable actions to principals.
- Example – XACML – xml-based language for defining trust management systems.

Bell-LaPadula Model

- Ensures confidentiality
- Based on multi-levels of classification
- Levels of secrecy for documents
  - Unclassified, Confidential, Secret, Top Secret
- Levels of clearance for users
  - Public, Agent, Commander, President
  - Document at a certain level can only be read by a person with equivalent or higher clearance.

Bell-LaPadula model

Progressively more strict classifications of data

- Clearance levels assigned to individuals
- 1. User cannot read data at a higher level
- 2. User cannot write data to a lower level

- Aggregate data is more sensitive than raw

data; (only the commanders get the big picture).

- False data can move upwards and mislead decision makers.

Biba Model

- Ensures integrity
- Based on multi-levels of integrity.
- Levels of accuracy for objects
  - e.g. Document in data centre has more accuracy than document in laptop.
- Levels of integrity for users
  - Policy makers (highest), Public (lowest)
  - Document at a certain level is considered reliable by a person with equivalent or lower level.

Biba Model

Progressively less reliable classifications of data

- Integrity levels assigned to information
- 1. User cannot write data to a higher level
- 2. User cannot read data from a lower level
- Reliable data is must come from a reliable source. Low reliability data cannot be made to be reliable.
- False policy data can move downwards and misdirect workers.

More Models

- Low Watermark Model
  - Relaxed version of the Biba model.
  - Users at high levels can read low-reliability data.
- Clark-Wilson Model
  - Based on integrity of transactions.
  - Checks system state.
  - Separate auditing process which ensures that transactions are valid.

Chinese Wall Model

- Chinese Wall Model (Brewer & Nash Model)
- Prevents conflicts of interest (CoI)
- Puts resources, people into CoI Classes
- A user can only access resources from one CoI class at a time.
- CoI allocation can change with time.

Trusted Systems

- Implemented using Access Control Lists, Bell-La Padula, MAC
  - Users are authenticated, restricted access.
  - Users must be trustworthy (but have no discretion).
- Secured hardware:
  - Not on the internet (Air-gap)
  - Locked up in secure rooms
  - Isolated from power grid.
  - Rings of security/Defense in depth

Trusted Systems

- Air-Gap – what can go wrong?

NO automatic updates – Microsoft, Adobe, Oracle assume everyone is on the Internet.

Patch management is difficult to coordinate. Mission-critical systems are never shut down / re-booted.

Therefore new vulnerabilities are not patched.

Air-gapped systems are easy to compromise once the perimeter is breached (M&M security)

SWINBURNE UNIVERSITY OF TECHNOLOGY