D. Security Management

Jin Hong

jin.hong@uwa.edu.au

Overview

- Security requirements asks **key security questions** of the system
  - What assets to be protected?
  - Which threats can compromise/damage the assets?
  - What are the means to mitigate those threats?

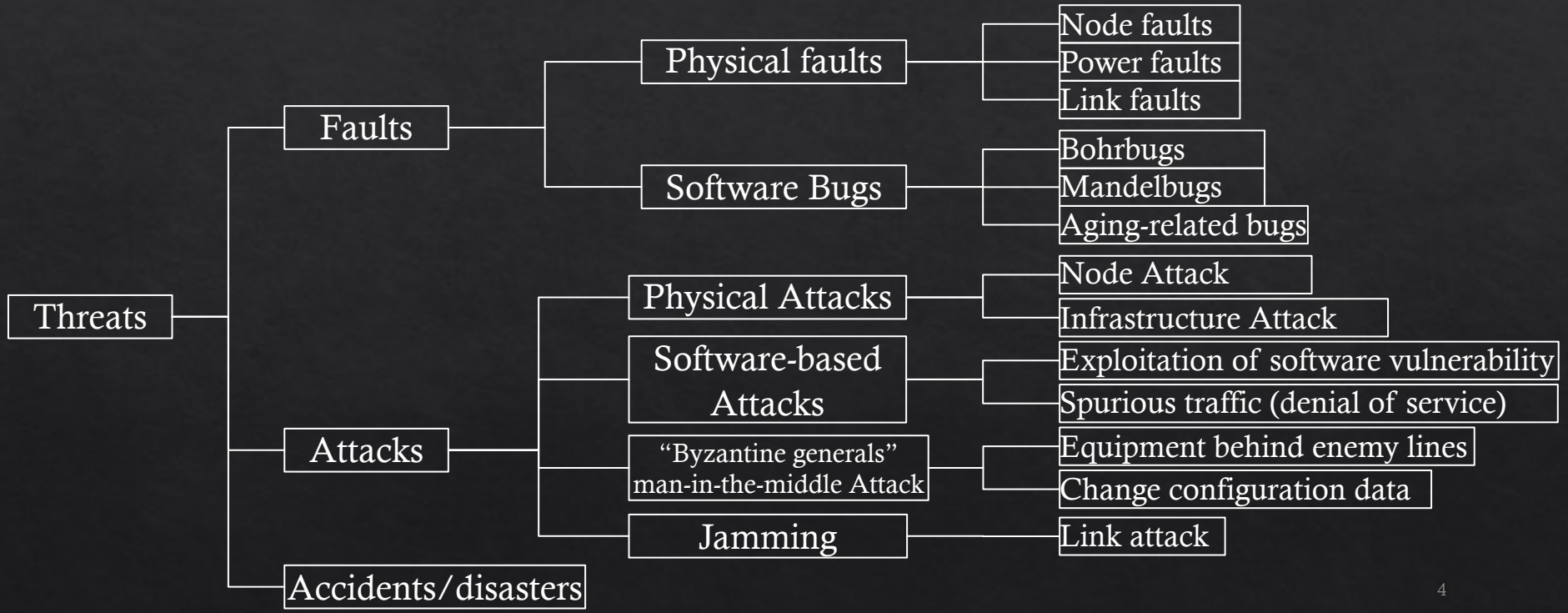
- Security management aims to **resolve those questions**
  - Define security objectives and potential threats
  - Carry out security risk assessment (w.r.t. assets)
  - Implement security solutions and monitoring

Terminology

Term	Meaning
Risk	The potential for an unwanted or adverse **outcome** resulting from an incident, event, or occurrence, as determined by the **likelihood (or the potential)** that a particular threat will exploit a particular vulnerability, with the associated consequences.
Vulnerability	A characteristic or specific **weakness** that renders an organization or asset (such as information or information system) open to exploitation by a given threat or susceptible to a given hazard.
Exploitation	A technique to breach the security of a network or information system in **violation** of security policy.
Threat	A circumstance or event (including accidental and non-human related) that has or indicates the **potential** to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
Asset	A person, structure, facility, information, and records, information technology systems and resources, materials, process, relationships, or reputation allowing entities (e.g., individuals, businesses and governments) to achieve social, economic, and other objectives of **value**.

Threats in Security

also for Dependability and Survivability



K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi, "Dependability and security models," *2009 7th International Workshop on Design of Reliable Communication Networks*, Washington, DC, 2009, pp. 11-20. doi: 10.1109/DRCN.2009.5340029

IT Security Management

- IT security management aims to achieve and maintain **appropriate levels** of confidentiality, integrity and availability of the system
- In addition, it also look at accountability, authenticity, reliability, and other security objectives

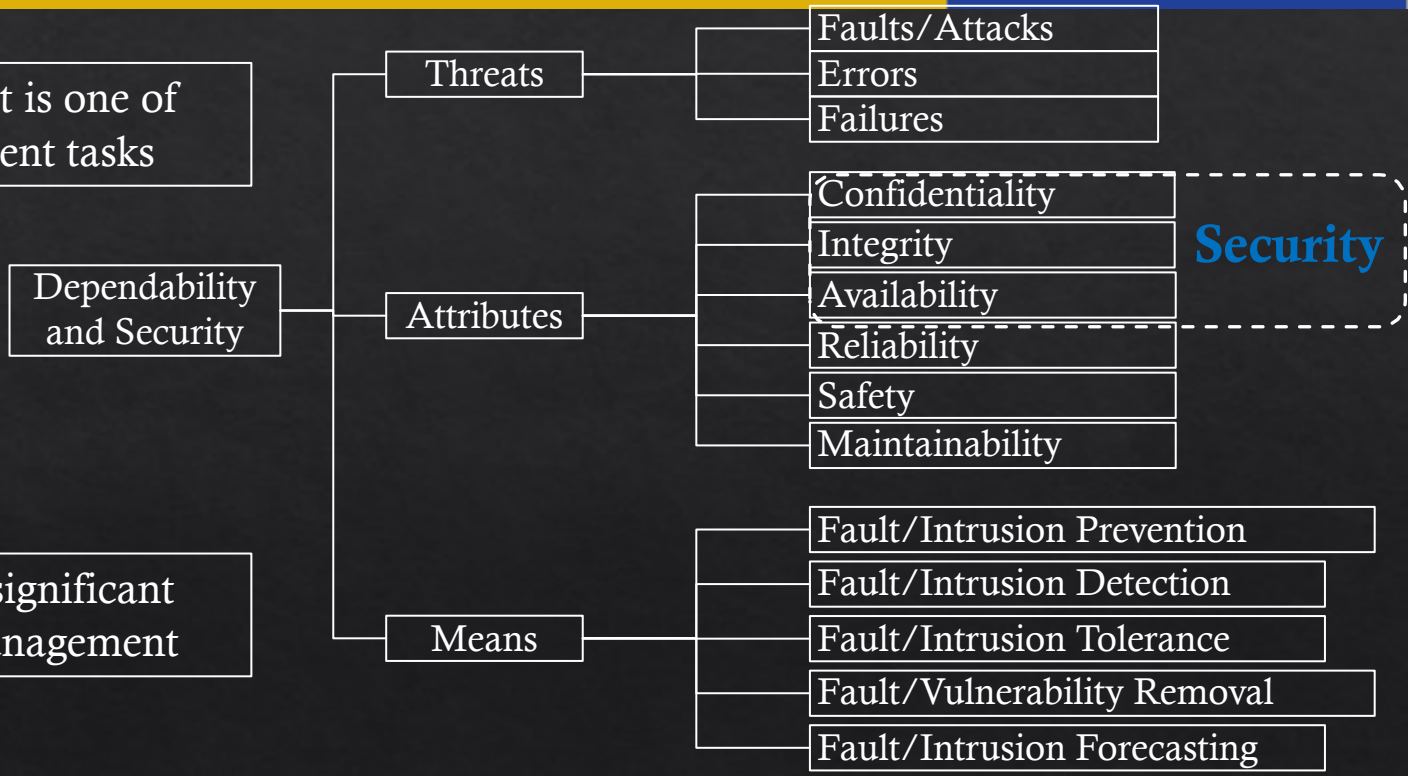
IT Security Management

- Related **tasks** for IT security management include

IT Security Management

IT Security management is one of the IT system management tasks

Dependability is also a significant aspects of IT system management



K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi, "Dependability and security models," *2009 7th International Workshop on Design of Reliable Communication Networks*, Washington, DC, 2009, pp. 11-20. doi: 10.1109/DRCN.2009.5340029

Security Standards

- ISO 27000 Security Standards
  - About 36 standards[1]
  - Widely used, but not public
- NIST Security Framework
  - Publicly available
  - Broadly reviewed by government and industry professionals
  - E.g., SP800 series
    - E.g., SP800-12: Computer security handbook
    - E.g., SP800-14: Generally accepted security principles & practices etc.

[1]http://www.iso27001security.com/index.html

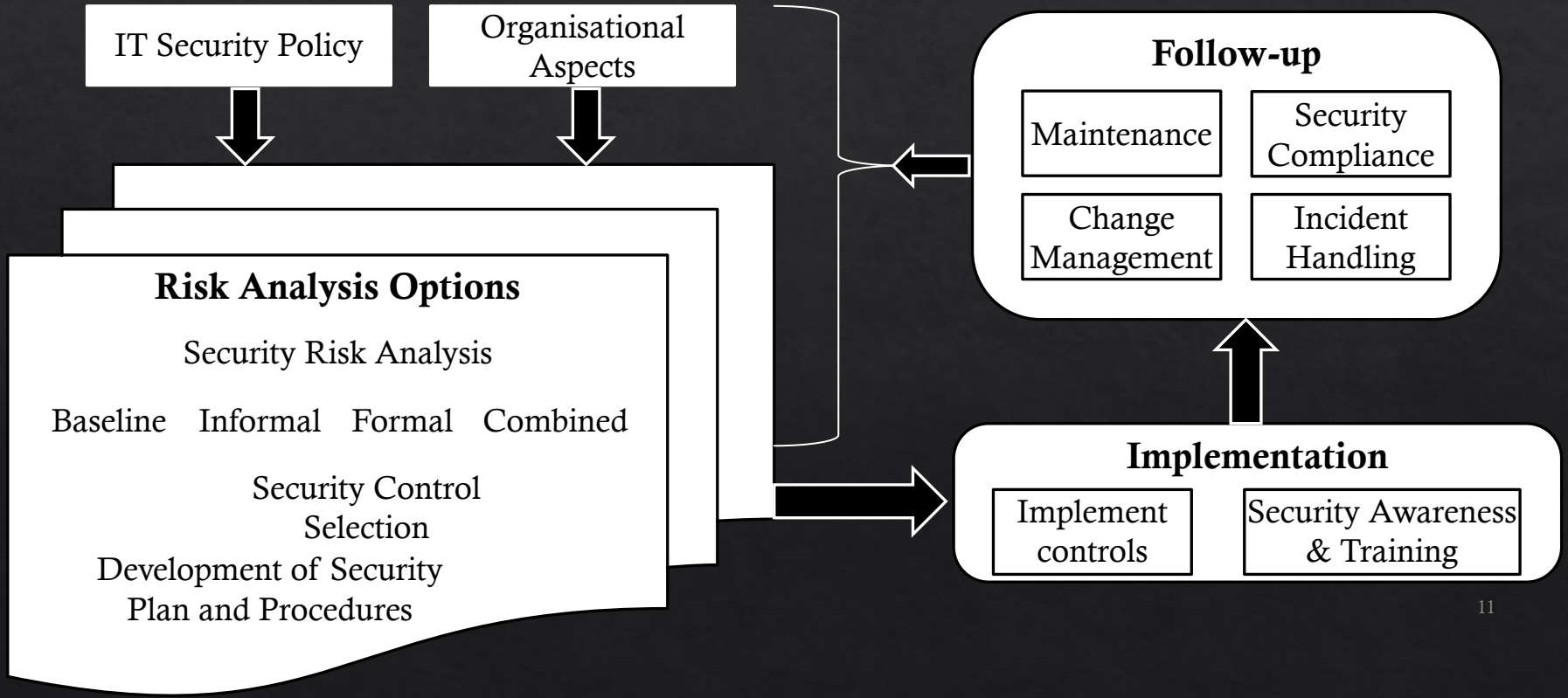
Security Standards

- IS management
  - ISO27001 – information security management systems – requirements
  - ISO27002 – Code of practice for information security management
  - ISO27003 – information security management system implementation guidance
  - ISO27007 – guidelines for information security management systems
  - SP800-14 – generally accepted principles and practices for securing IT systems
- Security measurement
  - ISO27004 – information security management – measurement
  - SP800-55 – performance measurement guide for information security

Security Standards

- Security risk management
  - ISO27005 – information security risk management
  - SP800-30 – guide for conducting risk assessments
  - SP800-37 – guide for applying the risk management framework to federal information systems: a security life cycle approach
- Incident management
  - ISO27035 – Security incident management
  - SP800-61 – computer security incident handling guide

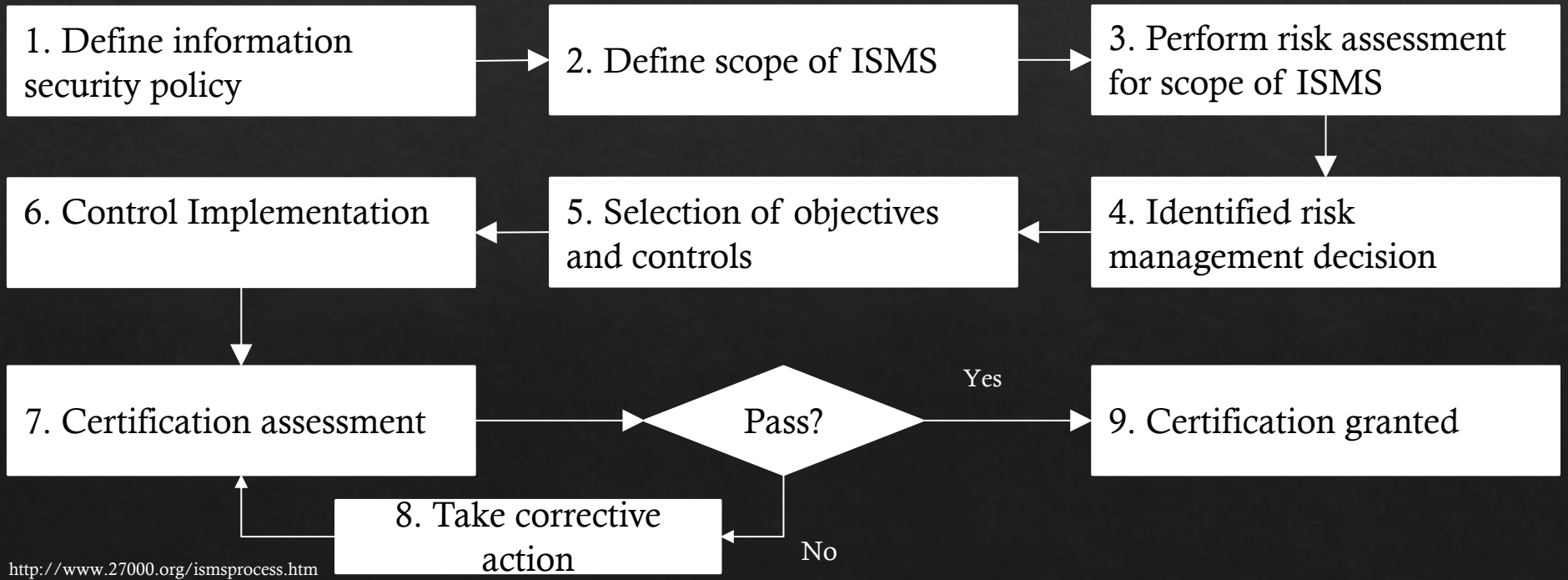
Security Management Process



Security Risk Assessment

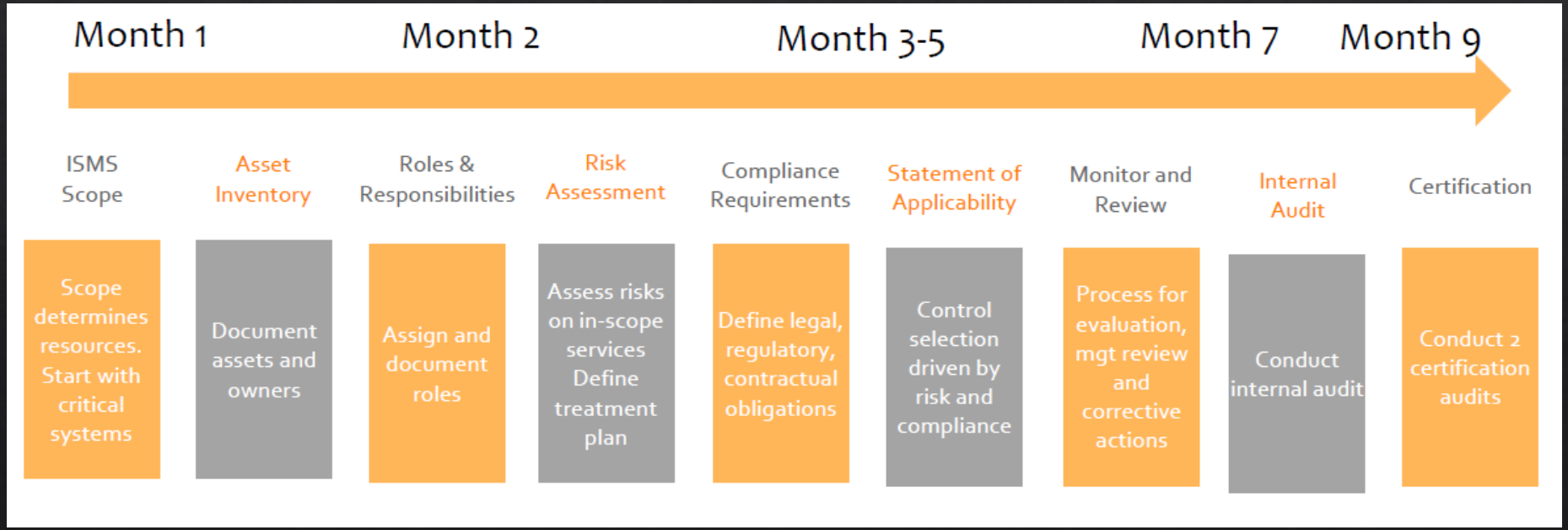
- Typical system includes many assets
  - Confidential data, user details, operational policies etc
- It is **infeasible** to examine the risk of all the assets due to *limited resources*
- To use the best security risk assessment approach given the organisation's resources
  - **Baseline**: use the "industry best practice"
    - Implementing standard security and safeguards against common threats
  - **Informal**: conduct informal, pragmatic/practical risk analysis
  - **Formal**: assess the security risk using formal structured process
  - **Combined**: combinations of other approaches

ISO27001


1. Define information security policy
2. Define scope of ISMS
3. Perform risk assessment for scope of ISMS
4. Identified risk management decision
5. Selection of objectives and controls
6. Control Implementation
7. Certification assessment
Pass?
Yes
9. Certification granted
No
8. Take corrective action
http://www.27000.org/ismsprocess.htm

ISO27001 Timeframe

- Rough estimate



NIST SP800-30

- NIST SP800-30 outlines 9 risk assessment activities

Also ISO27005, but not covered.

Risk Treatment

- Different actions can be taken for identified risks
  - **Risk acceptance**
    - Understand the risk but will not act on it
  - **Risk avoidance**
    - Take actions to prevent this risk from happening
  - **Risk transfer**
    - Shift the risk to other assets, processes or organisations
    - E.g., outsourcing to other organisations, get insurance etc
  - **Reduce consequence**
    - Implement security controls
    - E.g.,
  - **Reduce likelihood**
    - Implement security controls
    - E.g.,

Quiz

- Discuss with your peers
  1. What are some main differences between ISO27001 and NIST SP800-30?
  2. How can we say that system *A* is more secure than system *B*?
  3. What are the hurdles of automating the security risk assessment/analysis?

IT Security Management

- Related tasks for IT security management include
  - Specification of security objectives, strategies and policies
  - Determine organisational IT security requirements
  - Security threat assessments of IT assets and risks
  - Specification of appropriate security methods
  - Implementation and maintenance of security methods
  - Security awareness program and adoption
  - Detection and prevention of security incidents

Security Assessment

- Some key questions to answer in security assessment are:
  - How to represent and capture various attack scenarios?
    - What kinds of attacks are applicable?
    - How can these attacks be carried out?
    - How do we measure their impact on the system?
  - How to select the best security solutions and controls?
    - What is the best security practice for the given attack scenario?
    - What is the best security solution given these constraints?

Security Assessment

- Three main approaches
  1. Test on a real network
  2. Test on a duplicated real network
     - E.g., Emulation
  3. Model-based Security Assessment
  4. etc

Use of Security Models

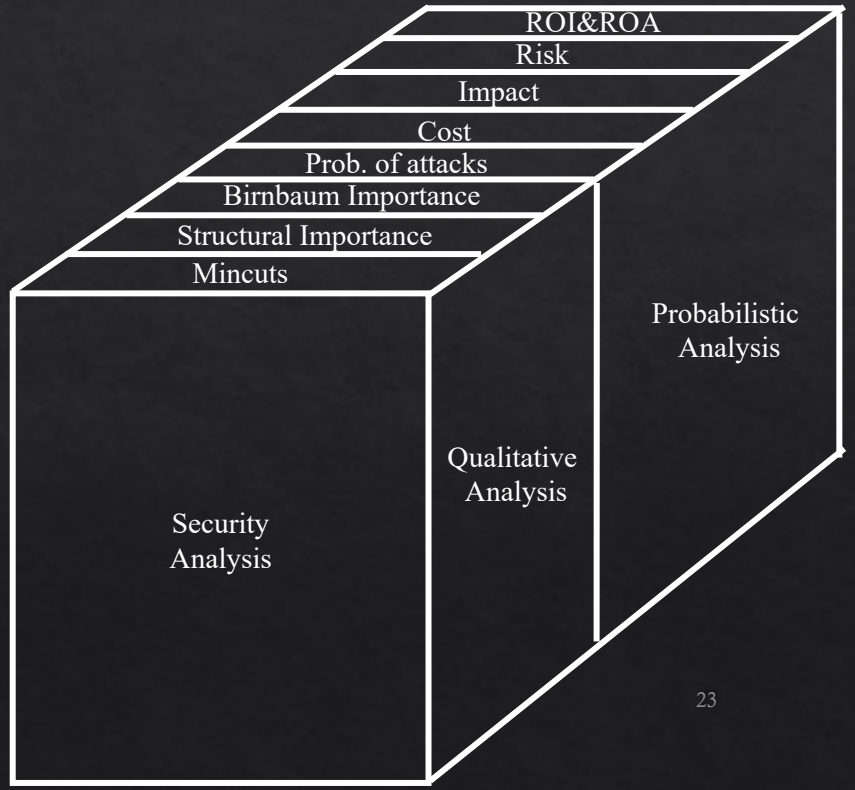
- Security models can be used to provide a **systematic approach** to assess the security of systems
- Security models are one aspect of the security assessment, which requires 3M
  - Security **M**easures : To collect required information
  - Security **M**etrics : To represent the analysis results
  - Security **M**odels : To capture security information of the system

Security Measurement

- What do we want to measure?
  - Vulnerabilities and their scores
    - Common Vulnerability and Exposures (CVE)
    - Common Vulnerability Scoring System (CVSS) Base Score (BS): e.g., 9 out of 10.
  - Reachability
    - Nmap (network mapping)
    - Network Configurations (e.g., access control by firewalls)
  - Mitigations
    - Detection (Intrusion Detection, Vulnerability Identification, …)
    - Countermeasure (Patch, firewall rules changes, …)

Security Metrics

- What can we measure?
  - Qualitative Analysis (Metrics)
    - Mincuts (Attack countermeasure scenarios)
    - Importance Measures
    - …
  - Quantitative Analysis (Metrics)
    - Probability of Attacks
    - Adversary's viewpoint
      - Cost of Attack
      - Return on Attack (ROA)
    - Defender's Viewpoint
      - Risk = Prob.*Impact
      - Security Investment Cost
      - Return on Investment (ROI)
      - …



Security Metrics

- Other way to categorise security metrics:

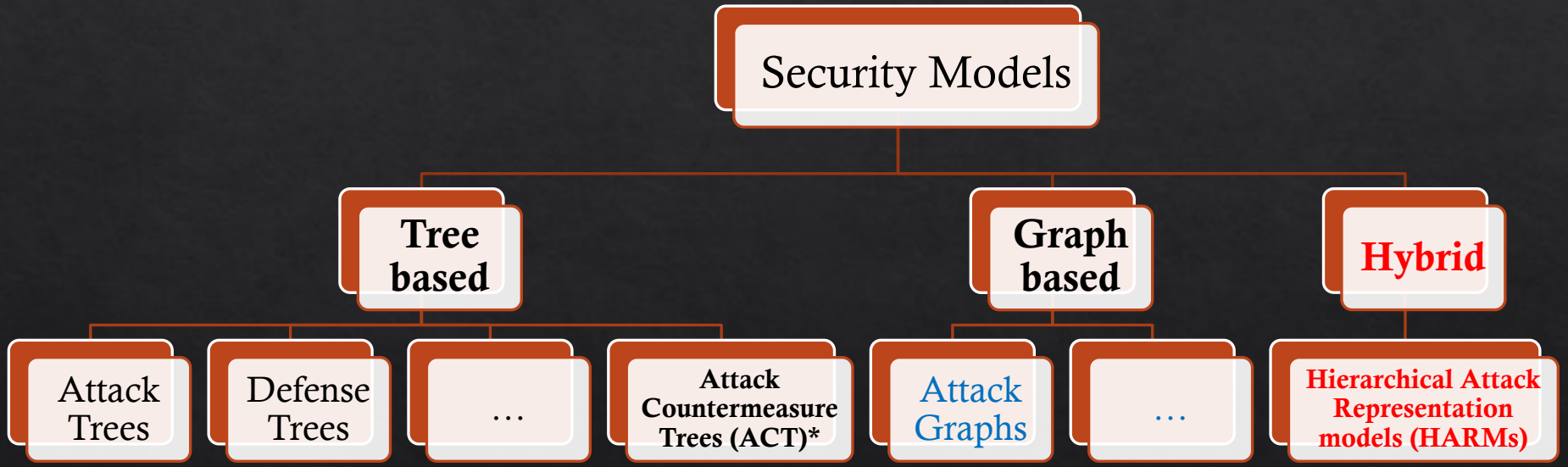
- Attack cost
- Impact analysis
- Mean time to compromise
- Mean time to recovery
- Mean time to failure
- Mean time to breach
- …

- Probability of attack success
- Probability of detection
- Probability of success of a mitigation
- …

- Shortest path
- Number of path
- Mean of path
- …

- Critical Vulnerability Set
- Network Compromise percentage
- ..

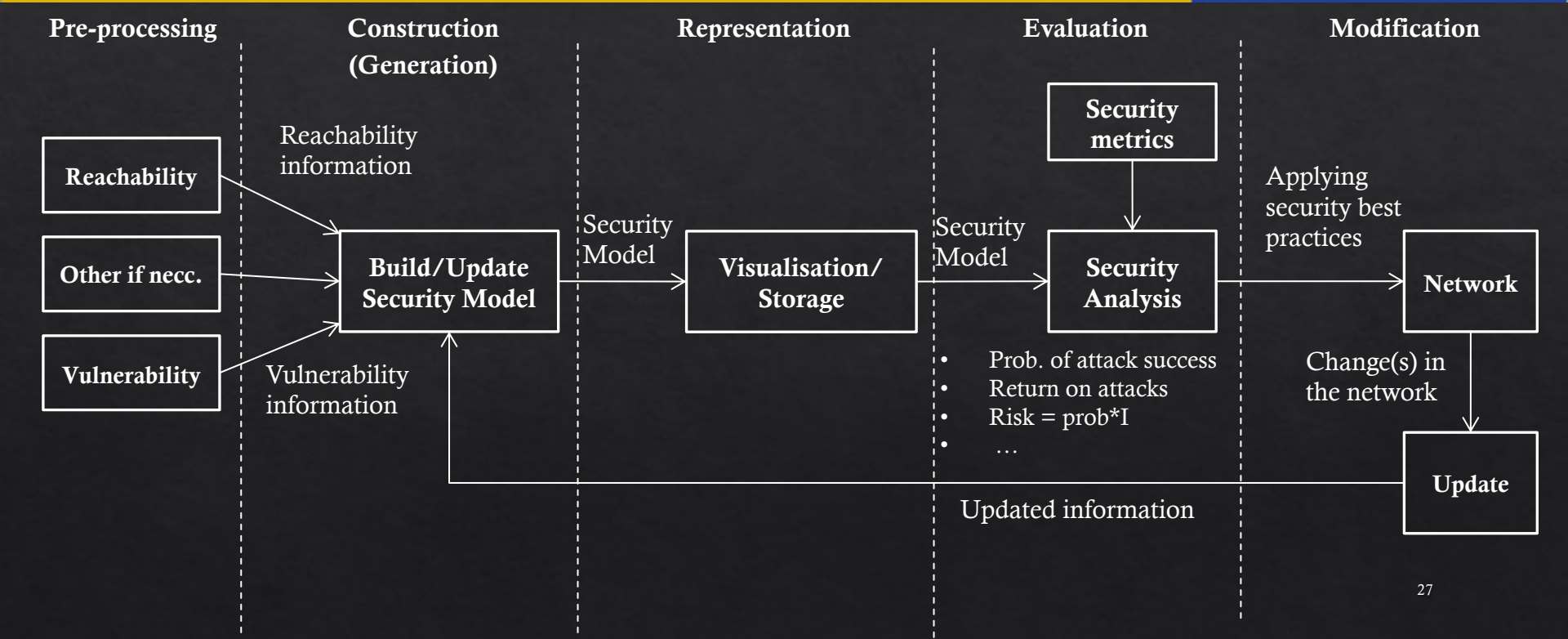
Security Models



Security Models

- Security models can…
  - Capture and analyse attack scenarios
  - Perform automated security analysis
  - Compute optimal countermeasures
  - Use various security metrics

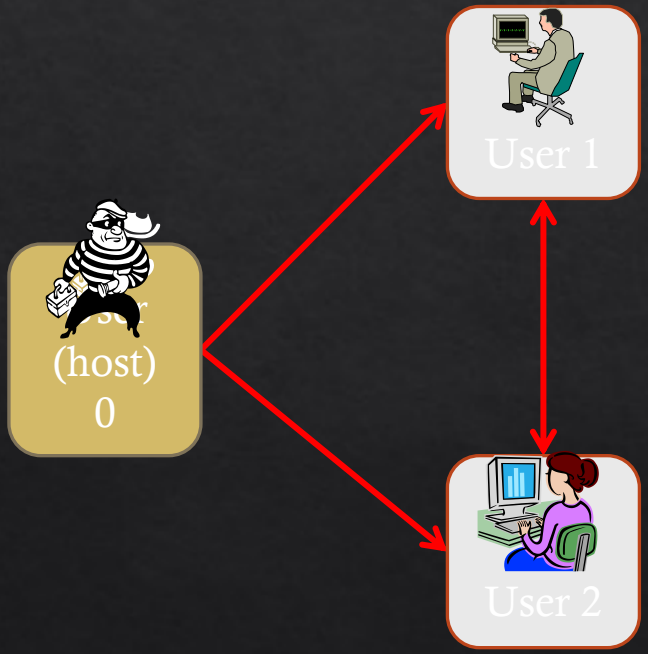
Security Model Lifecycle



Attack Graphs

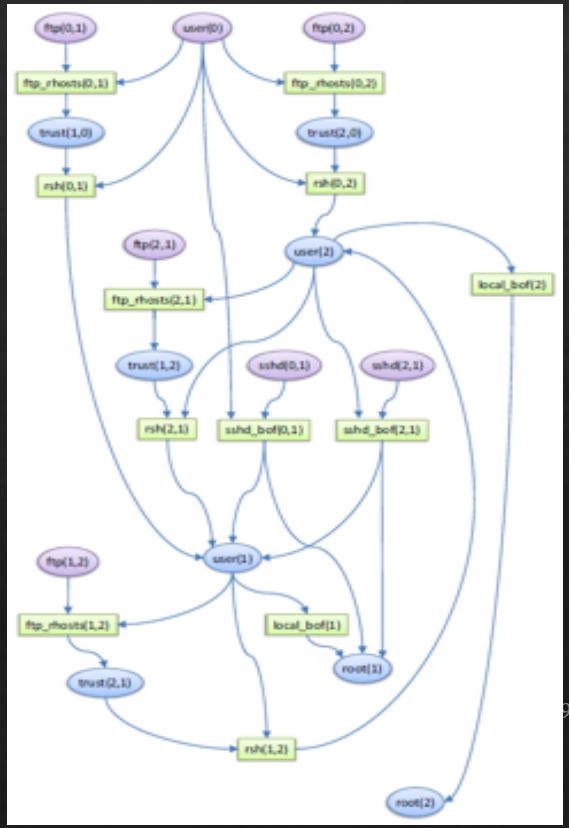
- Similar technique to Ats (covered in CITS1003)
- Unlike ATs, AGs may have cyclic dependencies or merged states
  - State transition information
  - Order of events
  - Etc.

Attack Graphs



Vulnerabilities:
- ftp_rhosts
- rsh
- sshd_BoF
- local_BoF

Vulnerabilities:
- ftp_rhosts
- rsh
- local_BoF



M. Albanese, S.Jajodia, S. Noel, "**A Time-Efficient and Cost Effective Network Hardening Using Attack Graphs**", in Proc. IEEE DSN 2012

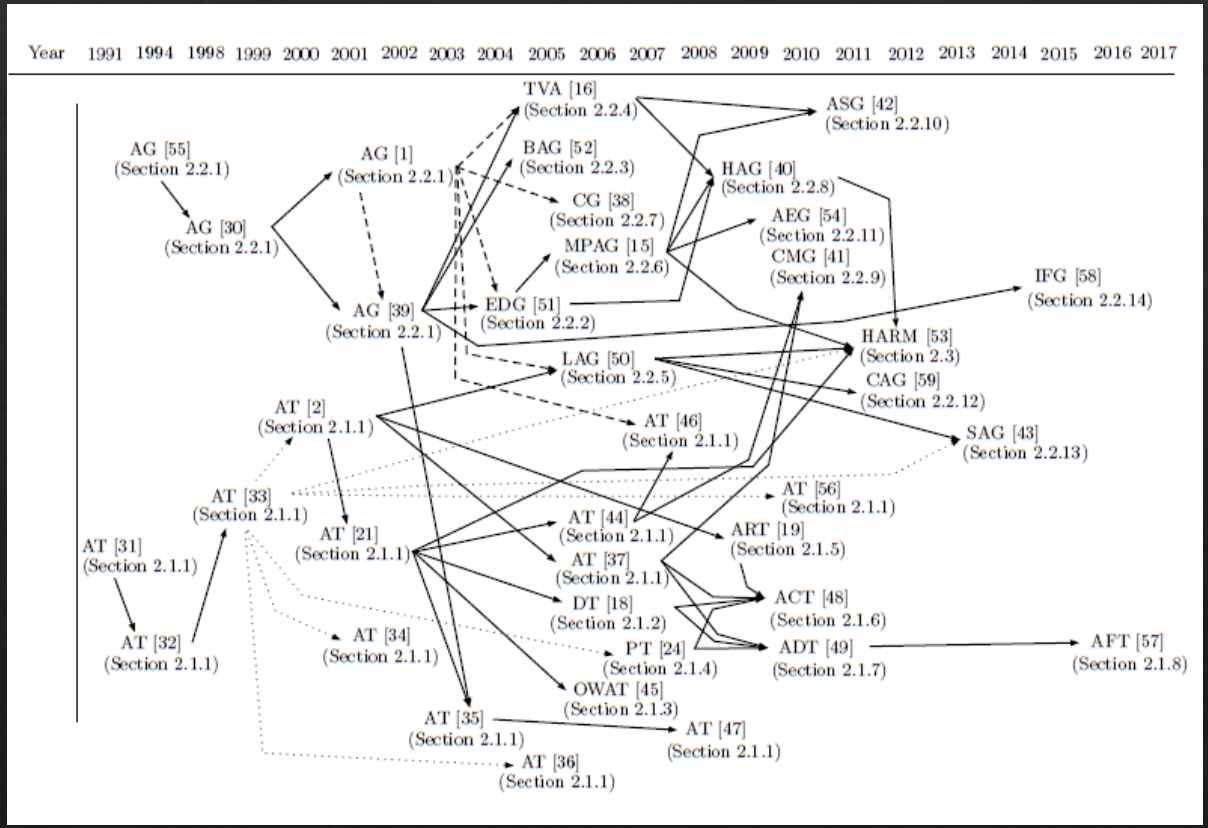
Attack Graphs

- Many variants of the AGs
  - Logical AGs, Bayesian AGs, Multiple prerequisite AGs, etc…
- There are tools available to generate AGs
  - NuSMV
  - RedSeal (commercial)
  - Skybox (commercial)
  - Cauldron (commercial)
  - CyGraph

What type do you use?

- Depends on various factors
  - What metrics can I use?
  - How efficient is the security assessment?
  - What tools are available?
  - What type of attacks can it model?
  - Which systems can I use the model?
  - Etc…

Evolution of Security Models



Limitations

- **Scalability issues**
  - The generation of full attack models and evaluation of all possible attack scenarios exhibit a **state-space explosion**
- **Dynamic adjustment (Adaptability) issues**
  - A change in the network system causes **updates** in the security model
- **Automating security decisions and countermeasure selections issues**
  - Requires intelligent security **decision making** and **real-time** adaptation and deployment of security solutions.

Limitations

- To address the scalability issues
  - Adopt new modelling techniques
    - E.g., using hierarchy, etc…
  - Implement efficient generation and evaluation algorithms
    - E.g., heuristic, dynamic programming solutions, etc…
  - Anything else?
    - E.g., subgraph evaluation, parallel computing

Limitations

- To address the dynamic adjustment issues
  - Capture dynamic changes using the model
    - E.g., use of temporal graphs
  - Real-time change detection mechanisms
    - E.g., real-time IDS, system logging etc…
  - Develop dynamic security metrics for evaluations
    - E.g., identifying persistent vulnerability etc…
  - Anything else?

Limitations

- To address the automation issues
  - Develop intelligent security analysis modules
    - E.g., use of AI, machine learning etc…
  - Pool of countermeasures for implementations
    - E.g., security awareness, easy security solution adoption methods etc…
  - Secure system architecture planning and implementation
    - E.g., security forecast, prediction, attacker profiling etc…
  - Anything else?

Summary

- There are **various** security standards and frameworks internationally accepted as a common practice
  - E.g,. ISO and NIST security standards and frameworks
- They provide detailed **procedures** for organisations to follow, in order to assess the security posture of their systems
- Many steps are involved, so security administrators should ensure that each step is done **carefully and complete**
- Use of **automated tools** can speed up the process, as well as avoiding any human errors

Additional Items

- Security standards and framework
  - ISO: http://standards.iso.org/ittf/PubliclyAvailableStandards/
  - ISO: http://www.iso27001security.com/index.html
  - NIST: https://www.nist.gov/cyberframework
- Penetration testing
  - Pentestmonkey (http://pentestmonkey.net/)
  - Metasploit (https://www.metasploit.com/)
  - Metasploit online course (https://www.offensive-security.com/metasploit-unleashed/)
- Security models
  - Kordy, Barbara, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. "DAG-based attack and defense modeling: Don't miss the forest for the attack trees." *Computer science review*13 (2014): 1-38.
  - Hong, Jin B., et al. "A survey on the usability and practical applications of graphical security models." *Computer Science Review* 26 (2017): 1-16.
  - Visualisation (note: videos are not working): https://visualisation.trespass-project.eu/