COMP 3410 – I.T. in Electronic Commerce

eSecurity

Security of Information and IT

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...

ETS1 {.html, .ppt}

ANU RSCS, 9 October 2012

The Notion of Security

A condition
in which harm does not arise
despite the occurrence of threatening events

A set of safeguards
whose purpose is
to achieve that condition

Information Security

- **Data Secrecy**
  Prevent access by those who should not see it

Information Security

- **Data Secrecy**
  Prevent access by those who should not see it
- **Data Quality / Data Integrity**
  Prevent inappropriate change and deletion
- **Data Accessibility**
  Enable access by those who should have it

IT Security

- **Security of Service**
  - Integrity
  - Reliability
  - Robustness
  - Resilience
  - Accessibility
  - Usability
- **Security of Investment**
  - Assets
  - The Business

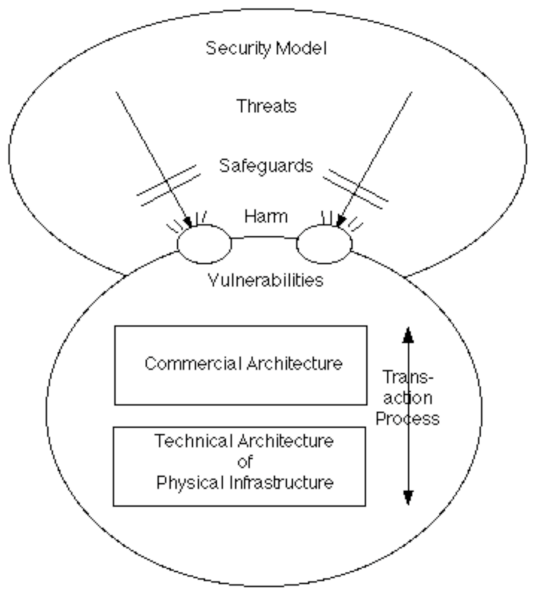
2. The Conventional Security Model

- **Threats act on Vulnerabilities resulting in Harm**
- Each Threatening Event is a Security Incident
- Safeguards are deployed to provide protection
- Countermeasures are used against Safeguards

- Safeguards have various purposes:
  - **Deterrence** of Threats
  - **Prevention** of Threatening Events
  - **Detection** of Threatening Events, Vulnerabilities
  - Support for the **Investigation** of Security Incidents
  - **Mitigation** of Harm

The Conventional IT Security Model

Threats impinge on Vulnerabilities, resulting in Harm



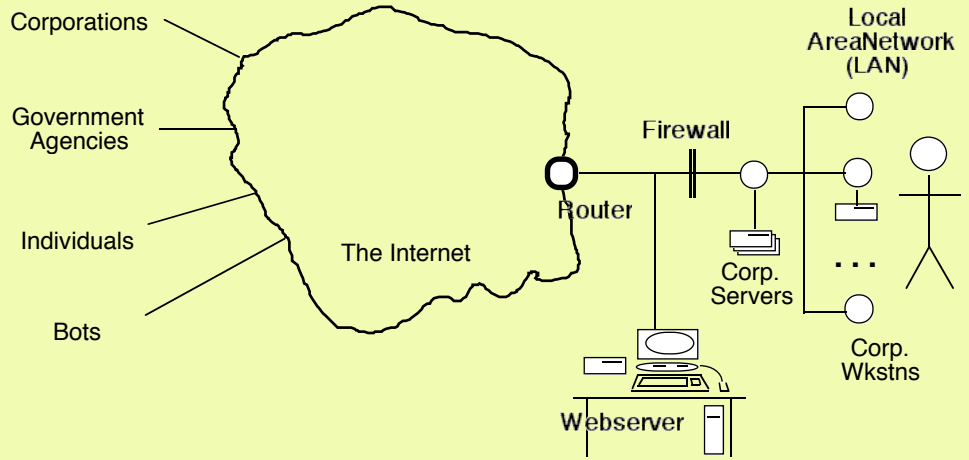
The Key Concepts

- A **Threat** is a circumstance that could result in Harm
  A **Threatening Event** is an instance of a generic Threat
  A Threat may be natural, accidental or intentional
  An intentional Threatening Event is an **Attack**
  A party that creates an Intentional Threat is an **Attacker**
- A **Vulnerability** is a susceptibility to a Threat
- **Harm** is any kind of deleterious consequence
- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard

Categories of Threat

- **Natural Threats**, i.e. Acts of God or Nature
- **Accidental Threats**:
  - By Humans who are directly involved
  - By other Humans
  - By Artefacts and their Designers
- **Intentional Threats**:
  - By Humans who are directly involved
  - By other Humans
  - By the Designers of Artefacts

Situations in Which Threats Arise



Situations in Which Threats Arise

- **Computing and Comms Facilities**, incl.
  - Data Storage
  - Software
  - Data Transmission
- of:
  - The Organisation
  - Service Providers
  - Users
  - Others
- **Physical Premises** housing relevant facilities
- **Supporting Infrastructure**, incl. data cabling, telecomms infrastructure, electrical supplies, air-conditioning, fire protection systems
- **Manual Processes, Content and Data Storage**

Intentional Threats / Attacks

By Outsider, by Insiders – Host/Server-side, User/Client-side

- **Physical Intrusion**
- **Social Engineering**
  - Confidence Tricks
  - Phishing
- **Masquerade**
- **Abuse of Privilege**
  - Hardware
  - Software
  - Data
- **Electronic Intrusion**
  - Interception
  - Cracking / 'Hacking'
    - Bugs
    - Trojans
    - Backdoors
    - Masquerade
  - Distributed Denial of Service (DDOS)
  - Infiltration by Software with a Payload

Categories of Harm

- Data Loss, Alteration, Access or Replication
- Reputation or Confidence Loss
- Asset Value Loss
- Financial Loss
- Opportunity Cost
- Personal Injury
- Property Damage

Safeguards
Measures to address Security Problems

Safeguards have various purposes:

- **Deter** Threats
- **Prevent** Threatening Events
- **Detect** Threatening Events, Vulnerabilities
- Support the **Investigation** of Security Incidents
- **Mitigate** Harm

IT and Data Security Safeguards

The Physical Site
- Physical Access Control (locks, guards, ...)
- Smoke Detectors, UPS, ...

Hardware
- Parity-checking, read-after-write
- Backup and Recovery

Network
- Channel encryption
- Firewalls
- Intrusion Detection

Software
- Authentication of data, of value, of (id)entity, and/or of attributes
- Access Control, User Authorisations

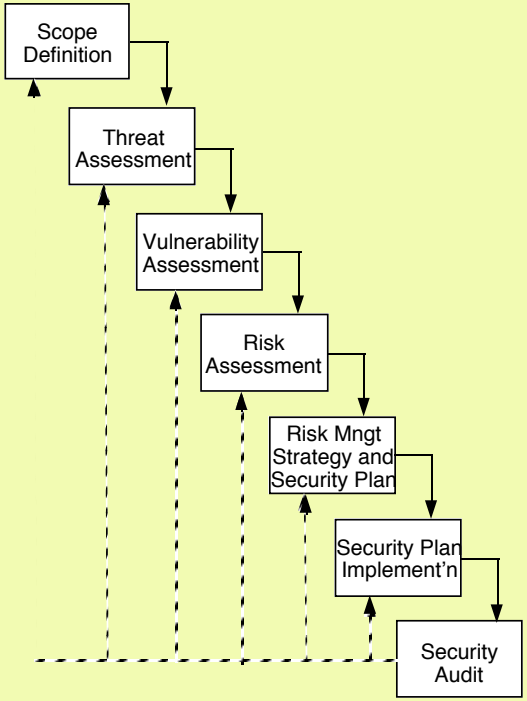
Liveware
- **Human Procedures**
  Control Totals, Reconciliations
- **Organisational**
  Respy/Authy, Separation of duties

Legal
- Duty Statements, Terms of Use, Contractual Commitments

Summary of Key Terms

- **Threat**
  A circumstance that could result in Harm
- **Vulnerability**
  A susceptibility to a Threat
- **Threatening Event**
  An occurrence of a Threat
- **Safeguard**
  A measure to prevent, to enable detection or investigation of, or to mitigate Harm from, a Threatening Event
- **Risk**
  "The likelihood of Harm arising from a Threat"
  A measure of the likelihood and/or seriousness of Harm arising from a Threatening Event impinging on a Vulnerability and not being dealt with satisfactorily by the existing Safeguards

3. The Business Processs of Risk Assessment

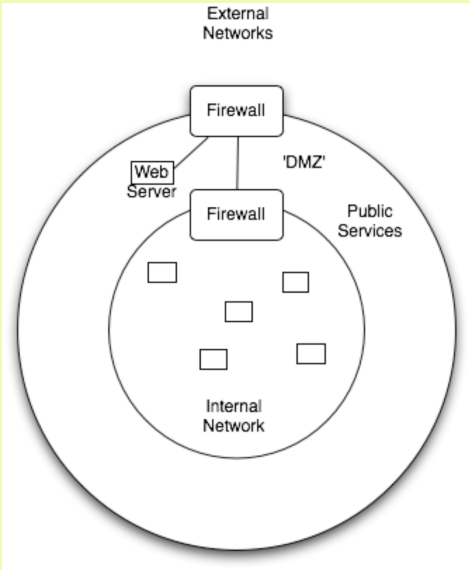


Generic Risk Management Strategies

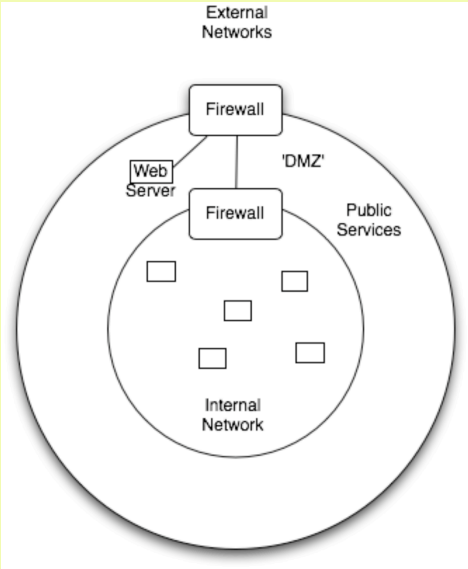
- **Proactive Strategies**
  - Avoidance
  - Deterrence
  - Prevention
- **Reactive Strategies**
  - Isolation
  - Recovery
  - Transference
  - Insurance
- **Non-Reactive Strategies**
  - Tolerance
  - Abandonment
  - Dignified Demise
  - Graceless Degradation

Costs of Risk Mitigation

- Executive Time, for assessment, planning, control
- Consultancy Time, for assessment, design
- **Operational Staff Time** for:
  - Training, Rehearsals, Incident Handling, Backups
- Computer Time for backups
- Storage costs for on-site and off-site ('fire backup') copies of software, data and log-files
- Transmission Costs for database replication
- **Loss of Service** to clients during backup time
- **Redundant Capacity** (Hardware, Networks)
- **Contracted Support** from a 'hot-site' / 'warm-site'



4. An Architecture for IT Security Safeguards



External Security

Perimeter Security

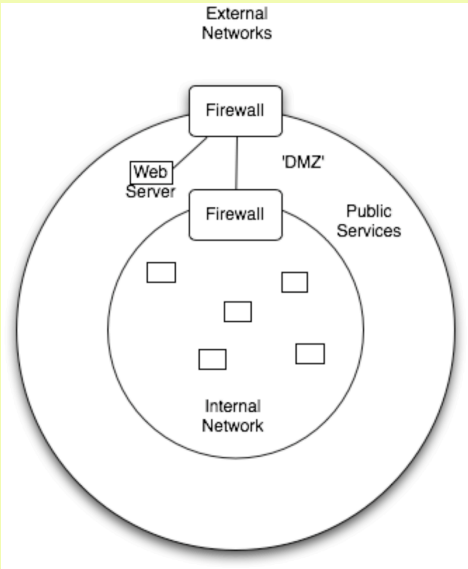
Internal Security

4. An Architecture for IT Security Safeguards

Key IT Security Safeguards Categories

External Security

- Content Transmission Security ('Confidentiality') e.g. SSL/TLS
- Authentication of Sender, Recipient, Content e.g. Dig Sigs, SSL/TLS, Tunnelling, VPNs
- 'White Hat Hacking'
- Network-Based Intrusion Detection (ID)
- ...



External Security

Perimeter Security

Internal Security

4. An Architecture for IT Security Safeguards

Key IT Security Safeguards Categories

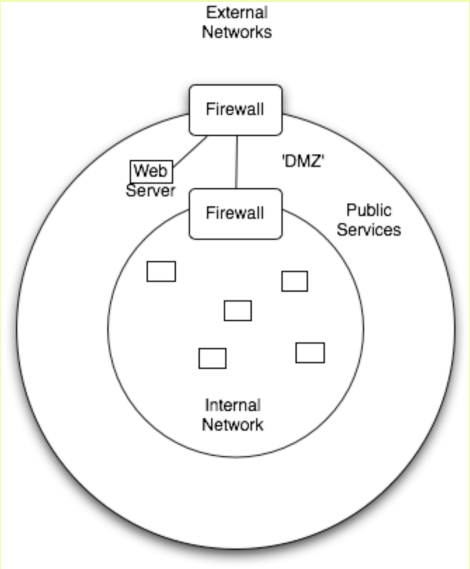
External Security

- Content Transmission Security ('Confidentiality') e.g. SSL/TLS
- Authentication of Sender, Recipient, Content e.g. Dig Sigs, SSL/TLS, Tunnelling, VPNs
- 'White Hat Hacking'
- Network-Based Intrusion Detection (ID)
- ...

Perimeter Security

Inspection and Filtering

- Traffic, i.e. 'Firewalls'
- Malcontent, Malware



External Security

Perimeter Security

Internal Security

4. An Architecture for IT Security Safeguards

Key IT Security Safeguards Categories

External Security

- Content Transmission Security ('Confidentiality') e.g. SSL/TLS
- Authentication of Sender, Recipient, Content e.g. Dig Sigs, SSL/TLS, Tunnelling, VPNs
- 'White Hat Hacking'
- Network-Based Intrusion Detection (ID)
- ...

Perimeter Security

Inspection and Filtering

- Traffic, i.e. 'Firewalls'
- Malcontent, Malware

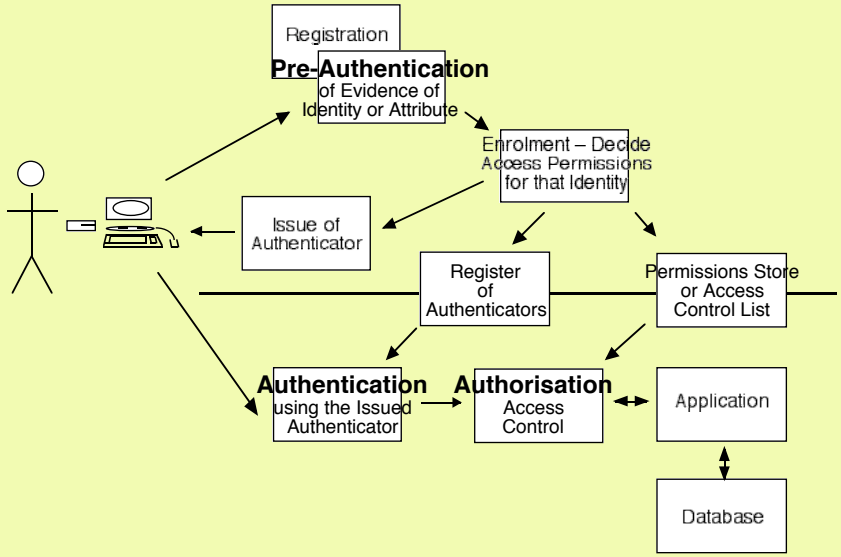
Internal Security

- Access Control
- Vulnerability Inspection
- Intrusion (Threat) Detection
- Safeguard Testing
- Backup, Recovery, 'Business Continuity Assurance', incl. 'warm-site', 'hot-site'

A Key Safeguard – Access Control

- Protect System Resources against Unauthorised Access
- Give the right people convenient access to relevant data and software capabilities, by providing User Accounts with Privileges and Restrictions
- Prevent the wrong people from achieving access to data and software capabilities
- Person-Based, or Role-Based (RBAC)

Access Control



Threats to Passwords

1. Guessing
2. 'Brute Force' Guessing
3. Visual Observation
4. Electronic Observation
5. Interception
6. Phishing
7. Use of One Password for Multiple Accounts
8. Discovery of a Password Database
9. Compromise of the Password-Reset Process
10. Continued Use of a Compromised Password
11. Compromise of a Password Stored by a Service-Provider
12. Acquisition and Hacking of the Password-Hash File

Australian Consumers' Password Practices

- When using the Internet, [do you] use **hard to guess passwords** which are changed regularly?
  Always – 18% Never – 58%

Australian Consumers' Security Practices

- When using the Internet, [do you] use hard to guess passwords which are changed regularly?
  Always – 18% Never – 58%

- [Do you] use, and change regularly, passwords on your main **mobile device**?
  Always – 37% Never – 29%

Australian Consumers' Security Practices

- When using the **Internet**, [do you] use hard to guess passwords which are changed regularly?
  Always – 18% Never – 58%

- [Do you] use, and change regularly, passwords on your main **mobile** device?
  Always – 37% Never – 29%

Unisys Security Index (October 2010)
Supplementary Questions to their standard push-poll

Ways of Strengthening Access Control

- Channel Encryption, e.g. SSL/TLS, so that even if the password is intercepted, it is not 'in clear'
- Transmission of only a hash of the password
- Server-Side Storage of only a hash of the password
- One-Time Passwords

Ways of Strengthening Access Control

- Channel Encryption, e.g. SSL/TLS, so that even if the password intercepted, it is not 'in clear'
- Transmission of only a hash of the password
- Server-Side Storage of only a hash of the password
- One-Time Passwords
- Multi-Factor Use Authentication:
  - **what you know**
    password, 'shared secrets'
  - **what you have**
    one-time password gadget, a digital signing key
  - **where you are**
    your IP-address, device-ID
  - **what you are**
    a biometric, e.g. fingerprint
  - **what you do**
    time-signature of password-typing key-strikes
  - **who or what you are**
    reputation, 'vouching'

E-Trading Security

Agenda

1. The Notion of Security
2. The Conventional Security Model
3. Conventional Security Processes
   - Risk Assessment
   - Risk Management
4. An Architecture for IT Safeguards
5. Access Control

COMP 3410 – I.T. in Electronic Commerce

eSecurity

Security of Information and IT

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...

ETS1 {.html, .ppt}

ANU RSCS, 9 October 2012