SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience

Formulating and implementing the security policy

Lecture eight

Outline of Lecture

- Formulation and implementation of security programme
  - Emphasis on formulating network related security policy
- Risk assessment
- Development of procedures from policy
- Example of implementing policy with a firewall

Learning objectives

- You should be able to
  - Quantify the risk associated with an attack
  - Be able to explain how controls are derived from policy
  - Explain what a firewall is including a brief discussion of its three network interfaces

Process of formulating security policy

- Identify assets
- Carry out risk analysis
  - Estimate risk
  - Prioritise risk
- Formulate policy to address risk
- Implement policy

Risk assessment

- Each asset has a risk associated with it
  - risk is a multi-factor measure
- Factors to consider are
  - internal or external threat
  - accidental or deliberate damage
  - logical or physical damage
  - active or passive damage
- These risks need to normalised by their likelihood and the damage to the organisation if they were to happen

Risk management and analysis

- A major part of developing a security programme is analysing and managing risk
- Major risk categories are:
  - Physical damage
    - Fire, water, vandalism, power loss, natural disasters
  - Human interaction
    - Accidental or deliberate action or inaction than can disrupt operations
  - Equipment malfunction
  - Internal and external attacks
    - Hacking, cracking, attacking
  - Misuse or loss of data
  - System errors

Risk analysis

- Goals of risk analysis
  - Identify assets and their values
  - Identify vulnerabilities and threats
  - Quantify the probability and impact on the organisation of threats
  - Provide an economic balance between the impact of the threat and the cost of the countermeasure
- Risk analysis results in a cost/benefit comparison
  - For example, if an organisational asset is worth $100,000 per annum then there is no point in spending $150,000 per annum to protect it

Value of information and assets

- Costs to consider
  - Cost to acquire or develop the asset
  - Cost to maintain and protect the asset
  - Value of the asset to owners and users
  - Value of the asset to competitors
  - Value of intellectual property inherent in the asset
  - Price others are willing to pay for the asset
  - Cost to replace the asset if destroyed
  - Operational and production activities affected if the asset is compromised
  - Liability issues if the asset is compromised
  - Usefulness and role of the asset in the organisation

Information classification

- Part of risk analysis is identifying the assets of the organisation and their value to it
- Information assets need to be identified and classified as well
- Classification is usually based on Confidentiality, Integrity and Availability
  - How important is the confidentiality of this information? Its integrity? Its availability?

Quantitative risk assessments

- Assign value to assets
- Estimate potential loss per threat
- Perform a threat analysis
  - Determine likelihood of each threat
  - Calculate the annualised rate of occurrence
- Combine potential loss and probability of loss
- Reduce, transfer or accept the risk
  - Reduce
    - Security systems and procedures
  - Transfer
    - Insurance

Example of quantitative risk assessment (from Harris)

Asset	Threat	Single loss expectancy	Annualised rate of occurrence	Annual loss expectancy
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card information	Stolen	$300,000	3.0	$900,000

Question

- On average we can expect a particular attack to occur once every 18 months. The cost to our organisation when it occurs is estimated at $75,000. We have two proposed solutions.
  - A new VPN with a capital cost of $250,000 written off over five years and an annual cost of $10,000
  - An IDS that has a capital cost of $100,000 written off over 5 years and annual cost of $20,000
- What is the Single Loss Expectancy (SLE)?
- What is the Annualised Rate of Occurrence (ARO) of the attack?
- What is the Annual Loss Expectancy (ALE)?
- What is the annual cost of each solution? Which one is worth considering?

Qualitative risk assessment

- Often too difficult, too slow or too expensive to carry out a comprehensive quantitative risk assessment
- Often quicker and just as effective to do a qualitative risk assessment
- Goal of qualitative risk assessment is to rank threats and the validity of different countermeasures
- Commonly used method is ‘Delphi method’ requiring a risk analysis team consisting of domain and security experts

Risk assessment

- The Delphi method
  - Security and domain experts write an anonymous short (one page) scenario for each significant possible threat and identify possible countermeasures
  - Team attempts to rank each of the following on a 1 to 5 (or sometimes 1 to 10) point scale
    - Severity of threat
    - Likelihood of threat taking place
    - Effectiveness of proposed countermeasure
    - Relative cost of proposed countermeasure

Risk assessment

- Example: a communications company
  - A terrorist attack on a central exchange
    - Damage? It would be devastating 5 / 5
    - Likelihood ? Moderately low 2 / 5
    - Risk on a scale of 1 to 25 is 5 x 2 = 10
  - Countermeasures
    - Encase exchange in 10 foot thick concrete
      - Would prevent some attacks but not all (3)
      - Would be very expensive (1)
      - Effectiveness 1 x 3 = 3
    - Appoint 24 hour guards
      - Would prevent most attacks (4)
      - Moderately expensive (2)
      - Effectiveness 4 x 2 = 8

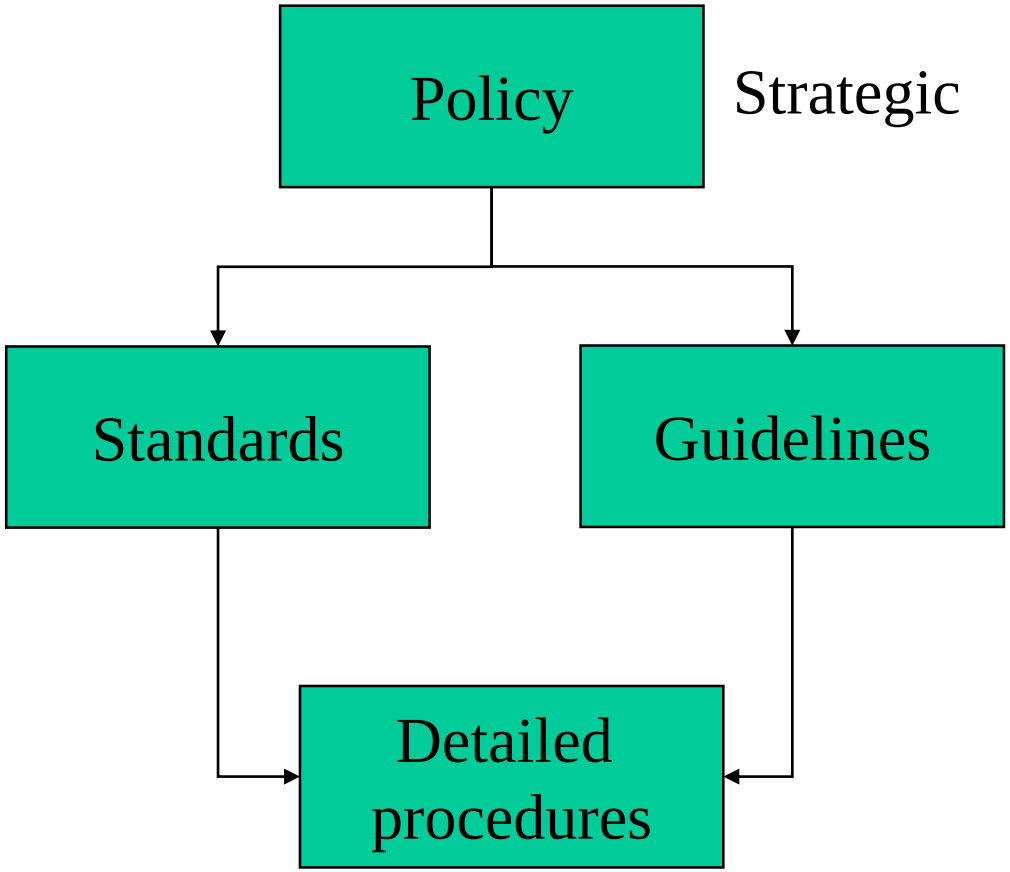
Question

- We run a small web-based company with a high volume of low value transactions
- What is the risk associated with the following events?
  - Hacker gains write access to our cloud based webserver?
  - Customer database is hacked?
  - ISP failure?
- How might you deal with the risk?

Formulating the policy

- Policies, standards, guidelines and procedures
- Security policies
  - State what needs to be done
- Standards
  - Specify mandatory activities, actions, rules, regulations
- Guidelines
  - Recommended approaches to implementing standards
  - Often many options
- Detailed procedures and controls
  - Derived from standards and guidelines

Policies, standards, guidelines and procedures



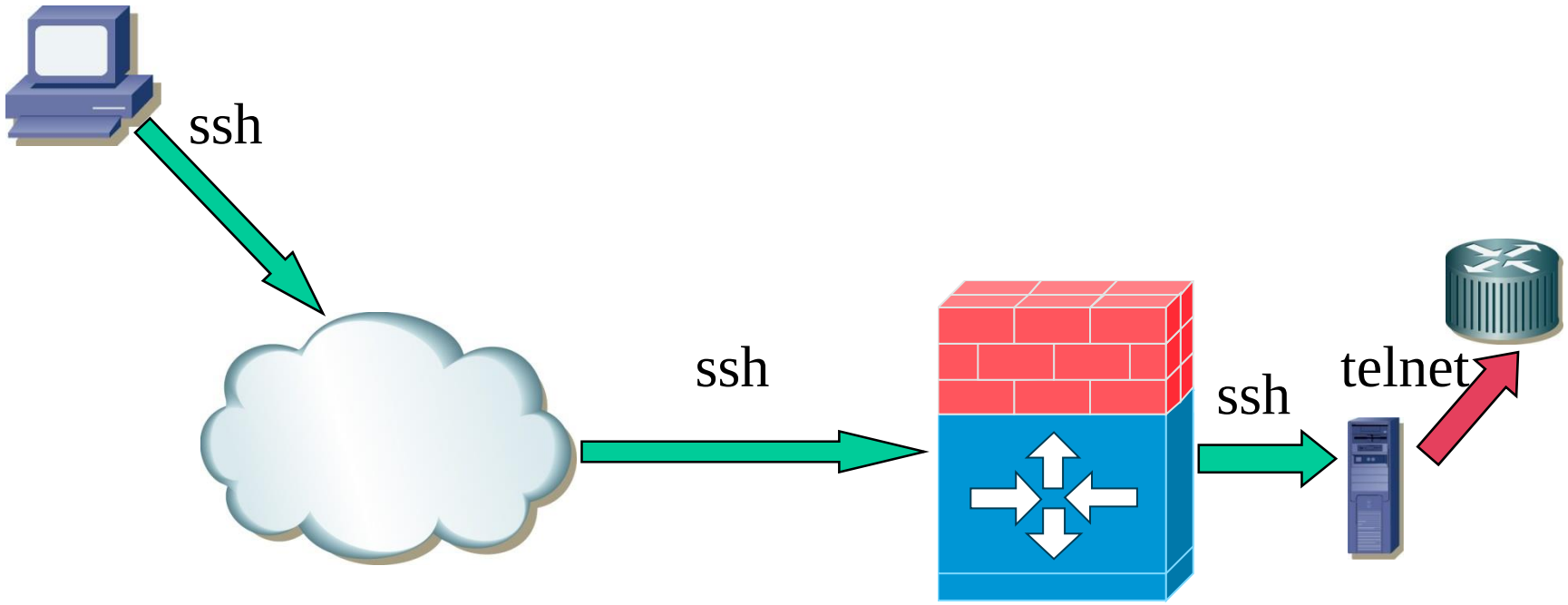
Example of implementation of policy

- Policy
  - A policy states what is to be achieved
    - “Remote access to our routers is to be encrypted”
- Standards
  - Spell out what must be done
    - “Telnet must not be used across a firewall”
    - “Only SSH can be used for remote access across a firewall”

Example of implementation of policy

- Guidelines
  - Specify preferred approaches to common situations
  - We might have guidelines regarding “Remote access to routers”
    - Suppose we are using routers that do not support ssh
    - “Our older routers do not support encrypted communications, so they should be accessed from a host local to the router from where telnet can be safely done”
    - “Remote access should be either ssh or VPN”
- Detailed implementation
  - Firewall configuration, host local to the router that can be ssh’d to

Example (continued)



General guidelines on developing procedures from policy

- Once the risk associated with a policy item has been assessed procedures can be developed to implement the policy
  - Deal with the riskiest issues first
  - Complexity and cost of procedure or control should be appropriate to the risk
- Procedures implement policy
- Procedures and controls will be either
  - manual
  - electronic
  - a combination of both
- Main mechanism for implementing network policy is a firewall
  - A lot more on firewalls in the next two lectures

Policy and procedures

- Policy specifies what is to be done and the general intention of the organisation
- Procedures are derived from policy and specify how policy goals are to be achieved
- Sometimes (CISCO) see reference to two levels of security policy
  - Requirements level
  - Implementation level
- Regardless of what it is called, there is a distinction between what we want to achieve (Policy or Requirements) and how we achieve it (Implementation)
- We now show how policy decisions might be implemented with a Firewall

Introduction to firewalls

- A firewall is a **system** for allowing secure communication between **trusted** and **untrusted** networks
  - Responsible for securing the perimeter of the network
  - System
    - hardware
      - routers and packet filters, possibly integrated in the one box
    - software
    - packet filtering, proxy services, NAT/NAPT translation
  - trusted network
      - usually internal
      - doesn't mean users are necessarily trusted but traffic is controlled by the organisation
  - untrusted network
    - networks over which we have no control

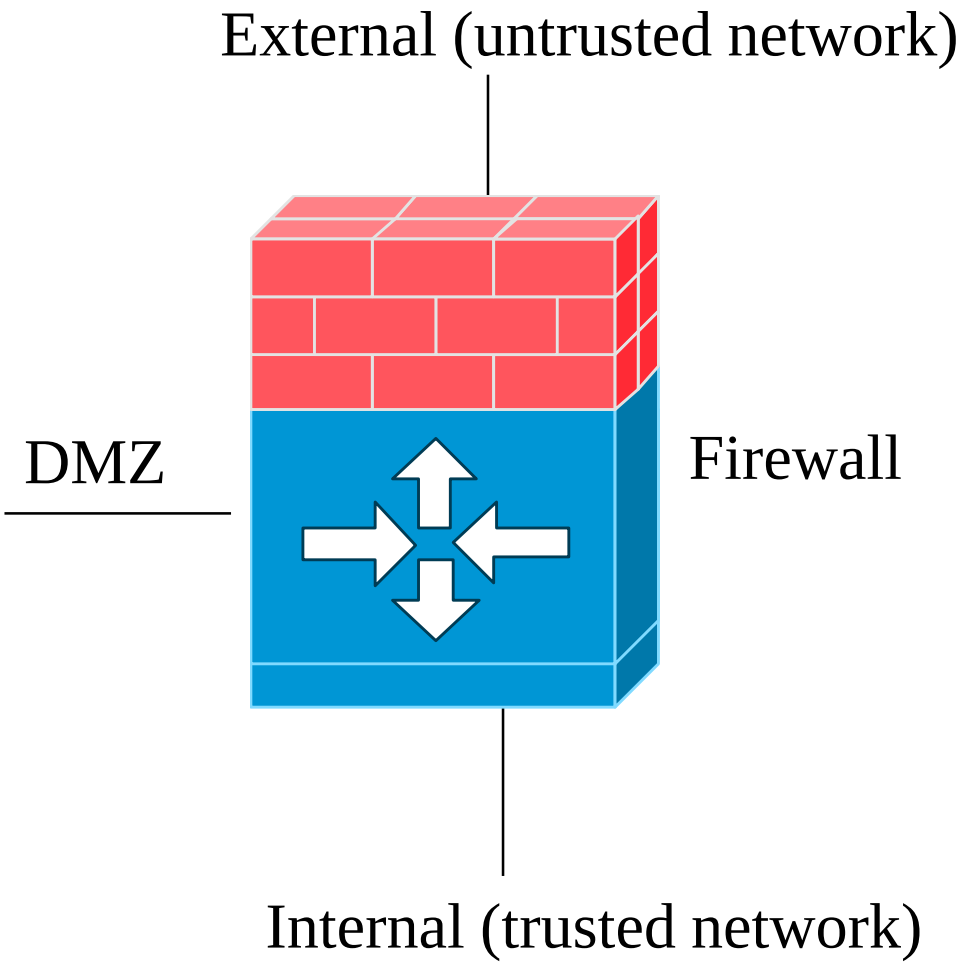
Introduction to firewalls

- Corporate firewalls need to be reliable and secure
  - a natural target for hackers
- Corporate firewall operating systems are usually simple and hardened
  - typically a stripped down version of unix
- Corporate firewall hardware is usually reliable
  - multiple power supplies
  - built-in battery backup etc
- Using a standard router or workstation as a corporate firewall is probably not a good idea
- More on firewalls in later lectures

Firewall overview

- A minimum of two interfaces
  - Trusted (internal) network
  - External network
- Often a third interface (two firewall devices configured to provide an effective third interface)
  - DeMilitarized Zone (DMZ)
- “Defence in depth”
- Internal hosts can connect to hosts in the DMZ and (subject to security policy) to the external network
- External hosts can only connect to hosts in the DMZ
- Hosts in the DMZ can only connect to the external network
  - provides protection against internal hosts being compromised

Firewall overview



Firewall overview

- Hosts that will normally be in the internal network are
  - internal web server
    - corporate information not accessible to outside world
  - internal mail server
  - internal DNS server
    - specifics of inner hosts
- Hosts that will be in the DMZ are
  - external web server
  - external DNS server
    - will only have reference to well known host names
  - external mail server

Implementing policy with a firewall

- A firewall implements some of the security policy
  - not all of it!
  - a firewall is used for just one part of the implementation of the security policy
- Firewall selection, configuration and operation are all defined by the policy
- Policy specifies what services are allowed or denied between the trusted and untrusted networks
  - eg telnets? DNS?
  - do we allow them at all?
  - do we allow them in?
  - do we allow them out?

Question

- Why might we prohibit DNS queries into our trusted network?

Firewall policy

- Two aspects to implementing policy on a firewall
  - What is our network service access policy?
  - How can we make sure the device implementing the policy is secure?
- The firewall itself is a probable target for hacking
- Following firewall issues need to be dealt with in security policy
  - Who is responsible for verifying that the firewall operates as required?
  - Who is responsible for firewall maintenance?
  - Who is responsible for firewall updates?

Issues not included in the Security Policy

- When using a firewall to implement policy, what do we do about issues not included in the security policy?
- Three approaches
  - Open security policy
  - Restrictive security policy
  - Closed security policy
- Open security policy
  - Permit everything not explicitly denied
  - (really should not be adopted)
- Restrictive security policy
  - Some things that the security policy does not mention are denied
- Closed security policy
  - Deny everything not explicitly permitted

Network services access policy

- As part of the policy formulation, questions like the following need to be answered
  - What internet services will we use?
  - Where will these services be allowed to be used from?
  - What additional security features do we need to make sure the services are used securely?
    - usually authentication
- There needs to be a balance between usability and security
  - System can be very secure but completely unusable
  - Need to formulate a satisfactory balance as part of the policy formulation
    - Based on risk analysis

Example implementation of policy

- We now show how some parts of a security policy can be implemented on a firewall
- We consider
  - Domain Name Services
  - SNMP
  - Routing protocols
  - electronic mail
  - remote access
  - file transfer

Domain Name Services

- As part of the information asset classification and risk assessment we will probably have the policy that our internal network structure remains confidential and that the nodes (routers, switches, servers) have high level of integrity
  - The policy may state that “information as to internal server names and addresses is to be confidential”
  - There will probably be some measure of risk and level of confidentiality needed
- How does this policy get translated into a (firewall) procedure?
  - A number of different firewall procedures relating to these services
    - DNS, SNMP and routing protocols

Domain Name Services

- Common implementation is to use two domain name servers
- Inner DNS is connected to the trusted network
  - it is used by hosts in the internal network for resolving queries about internal domain names
- Outer DNS is connected to the DMZ
  - it is used by the internal DMZ in the internal network for resolving queries about domain names on the untrusted network (the Internet)
- A host has a DNS query about an external network
- The query goes to the inner DNS
- It doesn't recognise the domain name
- It sends it to the outer DNS which then resolves the domain name

Domain Name Services

- Inner DNS knows internal host names
- Outer DNS does not know internal host names
  - Must prohibit transfer of zone files
    - contain DNS information

SNMP

- DNS implementation has helped make our internal network structure confidential.
- But other services can be used to determine internal network structure
- One threat is from the simple network management protocol (SNMP)
- SNMP allows nodes to report their state to, and have their state modified by a network management system
  - Threats to confidentiality, integrity and availability
- Our policy will probably be that external management systems should not be able to control our network
  - Firewall should block all SNMP messages

Routing protocols

- Routing protocols exchange information about network structure with their neighbours
- Our policy is usually that we do not want anyone outside our firewall receiving information about what our internal network looks like
- The firewall should prevent routing protocols from crossing from the internal to the external network
  - routing between DMZ and external network should use static routes

Electronic mail

- Email headers contain lots of information about the internal network structure
  - email server and relay IP addresses
- Our policy may be that email messages do not expose internal network information
- May decide to implement two SMTP servers
  - Similar implementation to DNS
  - An inner SMTP host on the trusted network
  - An outer SMTP host on the DMZ
- Outer mail host is a point of contact for all Internet users
- Inner mail host hides the structure of the network

Remote access

- Access control section of the security policy may state that ‘remote users are to be properly authenticated and their communications, including passwords, must be encrypted’
- Will usually mean that externally initiated telnet, rsh etc should be blocked by the firewall
- ssh may be permitted

WWW

- WWW is vulnerable
  - client can execute code on server
  - highly privileged scripts may be executed by exec or cgi commands
  - can obtain information about directory structure of web server
  - WWW author list may be compromised
  - WWW configuration files may be compromised
  - Server child processes may be run as user *nobody*

WWW

- Need to make lots of policy decisions regarding WWW
  - Policy might be no direct access to internal systems from publicly available web server
- Implementation might be
  - Run proxy WWW Server in the DMZ
- Other WWW security procedures may include
  - disabling directory information
  - prohibiting symbolic links
  - preventing execution of cgi-bin and other script files
  - limit WWW group membership
  - make configuration files writable by web administrator only

Firewall policy

- Firewall should be rebuilt before deployment
  - remove any trapdoors or trojans that may have been installed between ordering it and its delivery
- Firewall audits should be monitored
  - usually done as part of an intrusion detection system (IDS)
- Firewall patches and upgrades should be installed regularly

Conclusion

- Policy needs to be translated to procedures
- An important tool in that translation is the firewall
- Firewall typically has three interfaces
  - internal, external and DMZ with restrictions as to traffic between them
- Seen how a firewall is used to implement policy