SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience / Advanced Security

Network security overview

Lecture one

Outline of Lecture

- What is security
- History and development of network security
- Security policy and implementation
- Important concepts and technologies in network security

Learning objectives

- You should be able to
  - describe what security is concerned with
  - describe (briefly) the evolution of approaches to network security in the past thirty years
  - explain the role of security policy in implementing appropriate security mechanisms
  - explain the meaning of confidentiality, integrity and availability
  - name the main technologies used in implementing a security policy

General security concepts

- Vulnerability – a weakness in a system
- Risk – a risk is a possible event that could exploit the vulnerability to cause a loss
- Threat – a threat is a method of triggering a risk event
- Countermeasure – a countermeasure is a way to stop a threat from triggering a risk event
- Assurance – assurance is the level of guarantee that a security system will behave as expected

(From wikipedia)

Information and network security

- Security involves tradeoffs
  - Security / functionality / cost
- Perfect information security is (usually) impossibly expensive
  - It is impossible to eradicate all risk
- The level of information security should be appropriate to the value of the information or loss its compromise might cause
  - Information security is about risk management
  - Is the cost of the security measures we put in place commensurate with the cost to the organisation should the system be compromised?
- Need some measure of 'cost'
  - Different approaches
  - In a later lecture we will have a quick look at two of the most common

History of network security

- Before the 80s computing services were expensive, highly centralised and arcane
  - Usually dumb terminals connected to a central mainframe or mini via RS232 links
    - IBM370, Burroughs 6700, DEC PDP-11 etc…
- Late 70s, early 80s
  - First large scale commercial networks deployed
    - Education, Gambling, Banking, Government
  - Networks secured by physical isolation
    - Physical access to networked terminals strongly restricted
    - No customer access
- Hacking mainly in the telecommunications environment
  - Phone “phreaking”

History of network security

- Phone “phreaking”
  - Unauthorised use of phone system to (primarily) make long distance calls
  - Attacks on metering, signaling, switching and configuration and end systems
  - Long distance calls expensive
- A big political element to “phreaking”
  - Telecommunications companies huge, tightly regulated, bureaucratic monopolies
  - Individual customer service not necessarily a priority
  - Telecommunications companies had a long and not always commendable relationship with Law Enforcement

History of network security

- Metering attacks
  - Earliest used “inband” signalling
    - Typically the sound of coins dropping on a metal plate then pulses
    - Could be simulated fairly easily
  - Later metering attacks included clipping phones onto an unsuspecting residential line who got hit with the bill “clip-on fraud”
- Signalling attacks
  - 2600 Hz based attacks
    - “inband” attack
    - Would call toll free 0800 number
    - 2600 Hz would clear the call at the remote end but leave the caller with a trunk (long distance) line who would then dial the number they wanted
  - 2600 Hz signal generators known as “Blue boxes”

History of network security

- Mid to late 80s
  - Some devices with limited network capabilities became available to customers
    - Automatic teller machines (ATMs)
    - AutoTote (gambling) machines
    - Very limited and very tightly controlled functionality
  - Bulletin boards and TCP/IP begin to be widely used
  - Corporate networks start to be developed
    - Financial transactions built on X.25 networks
  - Networked computers commonplace but mainly LAN services such as printing and file-server
  - email common in academic environment

History of network security

- Exploits from this time include hacking into the many insecure networks around the world usually via telnet or other insecure protocols
- Melbourne at the forefront
  - ABC documentary (available in library) “In the Realm of the Hackers”
  - Famously broke into NASA
  - Creation of first political worm (The “WANK” worm – Worms Against Nuclear Killers, complete with a quote from Midnight Oil)
- Interesting read on the topic “Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier” by Suelette Dreyfus and contributions from Julian Assange http://www.underground-book.net/download.php3

History of network security

- Early 90s
  - Internet becomes ubiquitous
    - World Wide Web and the Mosaic Browser
  - Commercial transactions still based on X.25
    - No security mechanisms for the Internet
  - Attacks on very insecure Mobile telephony systems ('scanning')
- Mid-90s
  - Work on encryption, Public key infrastructure makes commercial transactions over the Internet feasible
    - Addressed the confidentiality and integrity issues, but not the availability issues
- Late-90 / Early 2000s
  - Internet boom with many commercial ventures
  - Major denial of service attacks on commercial sites

History of network security

- Mid to late 2000s
  - Many hacking tools become available online
  - Rise of the 'script kiddies'
  - WLAN exploits
  - Lots of interesting exploits which we will look at
    - Conficker 2008
    - Stuxnet 2010
    - Athens phone tapping scandal 2004 - 2005
    - BGP outages 2010
    - News of the World voicemail hacking 2005 - 2007
    - Gemalto SIM card key compromise 2014
    - Lenovo Superfish 2015

History of network security

- Now a very different world from even five years ago
  - Cloud computing, Smart phones, Social Networks, VoIP, 3G, 4G, 5G, Many new exploits
    - Social networking exploits
  - Online bullying
  - Death of privacy
- More on these later

History of network security

- What can we make of all this?
- Has become ridiculously easy to mount attacks
  - But tools and technologies to defend against attacks are available that weren't available ten to fifteen years ago
- Systems have become much more open
  - It is possible to learn about the strengths and weaknesses of a technology in a way that wasn't possible in the days of 'closed' computing systems
    - Closed systems tended to rely on 'security by obscurity'
  - But large numbers of users of a compromised technology means resources available to fix it
  - Also, if there is a weakness it will probably be found. Not always the case with closed systems

Security management

- There is a trade-off between security / functionality / cost
- Security management is largely about managing that trade-off
- Need to work out what risks are acceptable and what are unacceptable
  - It is not possible to be connected and have no risk
  - A balance needs to be found
- Security needs to be implemented in a coherent fashion
  - A security programme (or program)
- Usually sponsored and controlled by senior management
  - Top down rather than bottom up

Security management

- Goal is to identify the security requirements, goals and assurance levels needed for different parts of the organisation
  - These are collated in the Security Policy of the organisation
- The Security Policy is then implemented through Administrative, Physical and Technical controls
  - Our interest in this unit is primarily on Technical controls but all are of equal importance and all will be used in implementing most Security Policies

Security policy

- Level of security needs to be assessed
  - Has to be appropriate to the purpose of the network, the risk associated with the enterprise
  - It is too expensive and too restrictive to make any modern network totally secure
- Need to have a methodical way of assessing risk and deciding on appropriate level of security
  - Need to develop a security policy
  - The security policy is concerned with confidentiality, integrity and availability
  - Depending on the size and nature of an organisation it will have different requirements for each of these

Confidentiality

- What information needs to be kept secret and how secret does it need to be?
- What is the appropriate level of confidentiality needed for particular information
  - Passwords, encryption keys need to be absolutely secure
  - Credit card numbers, customer lists, customer transactions probably very high
  - Stock lists probably very low
- Different ways of providing confidentiality
  - passwords on files and servers
  - physical access restrictions
  - encryption

Integrity

- Usually concerned with timeliness and accuracy
- What information must be accurate in realtime and what information is less important?
- What is an appropriate level of integrity for the particular information
  - Financial transactions probably very high
  - Personal Emails on corporate server probably quite low
- Usually some broad kind of classification
  - High, Moderate, Low
- Can be provided through passwords, physical isolation or digital signing

Availability

- Part of Business Continuity Planning
- A global online business such as Amazon.com or eBay.com will have much greater requirements for availability than a home user's blog
- Some systems within an organisation will have more stringent availability requirements than others
  - Eg. After an outage a bank will want its customer transaction processing systems to be back up and running immediately
  - Other systems such as payroll (while important) can probably tolerate more delay
- Can be provided through backup machines, alternate sites, backup power supplies, alternate ISPs etc
  - Again, key issue is how much money will it cost the organization for these systems not to be operational

Question

On a scale of 1 to 3 (1 low, 3 high) evaluate the confidentiality, integrity and availability risks of the following information

- The office footy-tipping competition
- A customer list including discount arrangements
- Emails to and from clients
- Emails between staff members
- Student academic records
- Minutes of senior management meeting
- Personal credit card number used for online purchases

Security policy implementation

- Policies are implemented through Procedures
- Procedure might be a manual procedure
  - 'Check criminal record of new recruits'
- Procedure might be a technical procedure
  - 'Block all telnet sessions on web server'
  - Use stateful firewalls at network perimeter
- Technical procedures typically implemented through Firewalls, Authentication systems, Virtual Private Networks, Intrusion Detection Systems, Intrusion Prevention Systems
- Our emphasis is on technical procedures, but manual procedures should not be neglected
  - Will often be used to supplement or in concert with technical procedures

Technologies used to implement security policy

- Firewalls
  - Used to specify who can access what information from where
  - Proxy gateways and packet filters
  - Specify what protocols are allowed through the network and what are not
- Authentication Systems and Procedures
  - How do we guarantee that we are who we claim to be?
    - Something that we know
      - Passwords, PINs
    - Something that we have
      - Tokens, ATM Card
    - Something that we are
      - Biometrics
  - Strong authentication requires Biometrics and one of the others

Technologies used to implement security policy

- Virtual Private Networks
  - Specify how private communications channels (tunnels) can be implemented across public networks
  - Makes use of many technologies
  - Proxies, IPSec, SSL/TLS, CHAP, S-HTTP
  - Tunnelling technologies
    - GRE, PPTP, L2TP
  - Authentication technologies
    - Kerberos, RADIUS, DIAMETER
  - Encryption technologies
    - RSA, AES, IKE, SHA256

Technologies used to implement security policy

- Intrusion Detection and Prevention Systems
  - How to identify when your system is under attack or has been compromised?
  - Need to differentiate between normal and damaging use
  - Made up of sensors, monitors, resolvers and controller
    - Sensors collect data
    - Monitors process the data
    - Resolver determines response
    - Controller used for configuring the IDS

Technologies used to implement security policy

- Anomaly detection
  - Technology underpinning intrusion detection but can be used in a more general setting
  - For example, BGP failures are often caused by misconfiguration
    - Can we detect anomalies in BGP behavior that might indicate an error on behalf of an ISP
    - An interesting and difficult area
  - Banking transactions in which in-store customer transactions come from a variety of overseas locations within a short time-frame

Technologies used to implement security policy

- Cryptography
  - Many security technologies are built upon cryptography
  - VPNs, passwords, other authentication systems
  - Encryption can be used to provide confidentiality and integrity
  - Different kinds of encryption
    - symmetric key (sometimes secret key encryption)
      - Examples include DES, AES, RC5
    - asymmetric key (sometimes public key encryption)
      - Examples include RSA, Elliptic Curve

Technologies used to implement security policy

- Public key infrastructure
  - How can you trust a communication through the Internet? For example:
  - An email
    - How can you be sure it is from the person it claims to be from?
  - A financial transaction
    - How can a consumer be sure that they are interacting with the real Westpac.com and not a phishing site?
  - Public key infrastructure is used to provide some assurances as to the integrity of a communication
  - Makes use of the concept of a digital signature

Technologies used to implement security policy

- Wireless and IoT specific technologies
  - Wireless communication is inherently insecure
    - Wired networks have some physical security. Wireless networks (usually) don't
    - Not possible (at a reasonable cost) to restrain a wireless signal to a specific area
    - Wireless device performance (usually) constrained by battery power and processor capacity
  - Different solutions are needed for wireless communications security than are used for wired networks
- Cloud specific technologies
  - Geographical separation of processor and user
  - Virtualisation of services
  - Introduce new issues

Conclusion

- Networks much more open than in the past
- Perfectly secure network is usually not possible
- Three facets to security
  - Confidentiality, Integrity and Availability
- Need some methodical way of assessing risk and implementing appropriate solutions
  - Security policy
- Security policy implemented using a mix of manual and technology based procedures
- Wireless and cloud introduces new security issues