SWINBURNE UNIVERSITY OF TECHNOLOGY

Firewalls

Lecture ten

Outline of Lecture

- Rules for stateful firewalls
- Problems with firewalls
- Firewall certification
- Example firewalls

Learning objectives

- Should be able to
  - Develop access rules for simple stateful firewalls
  - State some of the potential weaknesses of firewalls
  - Describe the main firewall certification schemes and their goals

ipfilter stateful firewall

- Stateful firewalls closely examine TCP three-way handshake
- State of connection is either NEW or ESTABLISHED
- When a client initiates a new connection, it sends a packet with the SYN bit set in the packet header.
  - All packets with the SYN bit set are considered by the firewall as NEW connections
- The service will reply to the SYN packet with a packet in which both the SYN and the ACK bit are set.
  - State is still NEW (UNREPLIED)
- The client will then respond with a packet in which only the ACK bit is set, and the connection will enter the ESTABLISHED state

ipfilter stateful firewall

- Rules regarding the SYN and ACK bits
  - For NEW connections
    - SYN bit is set
    - ACK bit is reset
  - For NEW UNREPLIED connections
    - SYN bit is set
    - ACK bit set
  - For ESTABLISHED connections
    - SYN bit is reset
    - ACK bit is set

Problems with firewalls

- Some problems with firewalls
  - New technologies may make old rules redundant
    - Eg webmail over port 80 may make rules regarding SMTP ports irrelevant
  - Firewalls can be incorrectly configured
    - Eg large rulesets can easily cause problems
    - Poorly documented rulesets
      - Is it ok to remove a particular rule?
      - What is the effect on this rule if we move the firewall?
    - Network can be incorrectly configured
      - Eg web server in the DMZ not in the trusted network
    - Someone opens a temporary hole in the firewall and forgets to close it

Problems with firewalls

- Large organisations may have hundreds of firewall appliances
  - distributed organisations
  - sensitive internal information
- How do you audit the collective behaviour of 100 or more firewalls?
- How can we be sure the security policy is correctly implemented on these firewalls?
- How do we know what combination of failures or compromised hosts will cause the internal network to be exposed?

Testing firewalls

- Rule inspection
  - How many rules?
    - Lots of rules is usually risky
    - Often administrators are reluctant to change what previous administrators have done
      - Will add new rules
    - Need some version control software annotating why a rule was added or changed
  - Manual inspection a good start
    - Can identify obvious flaws
    - Can identify if the ruleset is clear and unambiguous

Testing firewalls

- Computer assisted inspection
  - Can test firewalls in similar ways to testing software
    - Test scripts
    - Regression tests
- Tiger teams / PenTests
  - Attempt to break into the firewall
  - Needs to be done with great care
- General testing guidelines
  - Rules with wildcards can cause trouble
  - So can rules that partially overlap.

Threats to firewalls and other security devices

- Tunneling
- Covert channels
- Time of check / time of use attack
- Buffer overflow

Tunnels through a firewall

- Tunneling
  - Encapsulation of a message from one protocol inside another
  - Using the facilities of the second protocol to traverse some network hops (possibly including a firewall)
  - At the destination the encapsulating protocol is removed and the original message recovered and possibly transmitted further
- Good uses of tunneling
  - Encryption of links
  - Connecting multiple branches of an office in a seamless fashion
  - Mobile IP
  - VPNs

Tunnels through a firewall

- IP packets can be tunneled in many ways
  - Often encapsulated within other IP packets
    - Layer2 Tunnelling Protocol
    - Generic Route Encapsulation
    - More when we talk about VPNs
  - Can be tunnelled through other IP protocols
    - Usually not so good
      - Compromise firewall security
        - » Restrictive firewall policy
        - » Malice or economic gain
    - http tunnelling
    - telnet, DNS and ftp have all been used as successful tunnels

Dealing with unauthorised tunnels

- Difficult to deal with by packet filtering
- Can be detected with deep inspection
- Often a people issue
  - Needs someone inside the network to set up the interior side of the tunnel
  - A good illustration of many security issues being personnel issues.

Covert channels

- Hidden channel embedded in an overt channel
- Goal of covert channel is to hide the existence of communication
- Can be used to leak information from a high security source to a low security source
- Many different kinds of covert channels
  - Unused header bits
  - Header extenstion fields
  - TCP Initial Sequence Number fields
  - IP fields including time to live, timestamp, address
  - Packet rate, packet loss, timing channels
  - DNS caching channels

Covert channels

- Usually require complicit insiders
- Identification very difficult
- When identified, response is one of
  - Eliminate the channel
  - Limit the bandwidth of the channel
  - Audit the channel
  - Document the channel

Time of check / time of use attack

- Exploits time dependency of actions
- Process 1 validates the authorisation of a user to access a non-critical file and passes the result to process 2 which carries out the file opening
- An attack might be to change the file from a non-critical one to a password file once process 1 has completed but before process 2 starts
- Problem can be avoided by some locking mechanism of the resource between check and use

Buffer overflow

- Poor programming practice and poor array bounds checking
- Particularly important to avoid on firewall systems
  - A popular firewall appliance will be a popular target
- Best dealt with by keeping patches up to date and implementing good programming practice

Firewall certification

- Lots of firewall products
  - not necessarily a self-contained box
  - can be software that runs on a standard host
  - can be a router with a sophisticated ACL
- Lots of variations in performance, features and quality
- Security policy issue as to which is appropriate
- Security certification and accreditation schemes
  - Any products that might be security related including operating systems, applications as well as network devices including firewalls,
  - Purpose is to provide independent evaluation of security related products

Security product evaluation

- Usually based on some kind of state machine model
  - Mathematical description of behaviour
  - Sometimes ‘Formal Models’
- Goal is to ensure that there are no mechanisms that can ‘leak’ information (probably via a covert channel)
- Bell-LaPadula and derivatives most commonly used
  - Multilevel security system
  - Each level has its own handling procedures
  - Specifies ways in which subjects (such as users) can access and write to objects (such as databases)
  - Bell-LaPadula is “no read up, no write down.”

Security product evaluation

- Government certification
  - Trusted Computer System Evaluation Criteria (Orange Book)
  - Information Technology Security Evaluation Criteria (ITSEC)
  - Common Criteria
- Commercial certification
  - International Computer Security Association (ICSA)
  - Firewall Product Developer's Consortium (FWPDC) Criteria

Government certification

- TSEC, ITSEC and Common Criteria
- In Australia administered by Australian Signals Directorate (ASD)
  - Actually done by commercial firms
- Australasian Information Security Evaluation Program
  - https://acsc.gov.au/infosec/aisep/
  - Lots of mutual recognition
  - Canada, France, Germany, United Kingdom, United States, Australia and New Zealand
- Not just firewalls
  - Any security product can be evaluated
    - biometrics, VPN, IDS,

TSEC

- Developed by Department of Defense (US)
- Largely replaced by CC
- Has four broad levels of classification with sublevels
  - A: Verified protection
  - B: Mandatory protection
  - C: Discretionary protection
  - D: Minimal security
  - Also allows subdivisions eg B1, B2
- Based on four main topics
  - Security policy
  - Accountability
  - Assurance
  - Documentation

Information Technology Security Evaluation Criteria

- Largely superseded by Common Criteria
- Primarily a European scheme
- Separates Functionality and Assurance
  - Functionality
    - What the product does
  - Assurance
    - How well the functionality is implemented
- ITSEC rates functionality and assurance separately unlike TSEC which aggregates them
- ITSEC functionality rating scale
  - F1 to F10
- ITSEC assurance rating scale
  - E0 to E6

ITSEC Functional Requirements

- Identification and authentication
- Audit
- Resource utilization
- Trusted paths/channels
- User data protection
- Security management
- Product access
- Communications
- Privacy
- Cryptographic support

ITSEC Functional levels

- D: non-secure system.
- C1: Requires user login, but allows group ID.
- C2: Requires individual user login with password and an audit mechanism.
- B1: (US) Department of Defense clearance levels
- B2: Provides assurances that system can be tested and clearances cannot be downgraded.
- B3: System is characterized by a mathematical model
- A1: System is characterized by a mathematical model that can be proven. Highest security.

ITSEC Assurance Requirements

- Documentation and manuals
- Configuration management
- Vulnerability assessment
- Delivery and operation
- Life-cycle support
- Assurance maintenance
- Development
- Testing

ITSEC Assurance Levels

- E0 Failed
- E1 Informal architectural design
- E2 Detailed design and penetration testing. An informal detailed design, and test documentation must be produced.
- E3 Source code or hardware drawings to be produced. Correspondence must be shown between source code and detailed design.
- E4 Formal model of security and semi-formal specification of security enforcing functions, architecture and detailed design to be produced
- E5 Architectural design explains the inter-relationship between security enforcing components.
- E6 Formal description of architecture and security enforcing functions to be produced.

Common criteria

- Weakness of ITSEC is that it provides too many options
  - 10 functional rankings and 6 assurance ratings = 60 possible classifications
- Common criteria uses **protection profiles**
  - Describes the problem that the product is attempting to deal with
  - Specifies security requirements for specific situations that the product addresses
  - EG there are protection profiles for
    - Biometric products
    - Firewall products

Common Criteria Assurance Levels

- EAL0 Inadequate
- EAL1 Functionally Tested.
  - Black box tested. Provides analysis of the security functions, using a functional and interface specification of the device, to understand the security behaviour
- EAL2 Structurally Tested.
  - Anaysis of the security functions using a functional and interface specification and the high level design of the subsystems of the device.
- EAL3 Methodically Tested and Checked.
  - The analysis is supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities.

Common Criteria Assurance Levels

- EAL4 Methodically Designed, Tested and Reviewed.
  - Analysis is supported by the low-level design of the modules of the device, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.
- EAL5 Semiformally Designed and Tested.
  - Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required

Common Criteria Assurance Levels

- EAL6 Semiformally Verified Design and Tested.
  - Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.
- EAL7 Formally Verified Design and Tested.
  - The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

Problems with ITSEC and CC certification

- Expensive
  - can cost $200,000 to have a firewall evaluated
- Slow
  - Evaluation up toE3 can take two years
- Firewall certification can only evaluate a product at the time it was submitted for certification
  - Environment can change dramatically in two years
- Consequently, very few firewalls certified beyond E3 and none (that I'm aware of) beyond E4

Commercial certification

- Verizon Cybertrust offers industry product certifications
  - International Computer Security Association (now ICSA Labs)
- ICSA Evaluates firewalls on specific criteria
  - issues ‘certificates’ for various capabilities
    - virus
    - cryptography
    - filtering
    - biometrics
- Much easier to obtain than ITSEC or CC but not as stringent

Conclusion

- Examined firewalls in some depth, including stateful firewalls
- Attacks on firewalls
- Firewall certification