Distributed Systems Security

Operating Systems and Enterprise Systems

Prof. Steve Wilbur
s.wilbur@cs.ucl.ac.uk

Z08

Lecture Objectives

- Identify potential security weaknesses in Operating Systems
- Review assurance criteria from standards bodies
- Review BS7799 Enterprise security policy framework

Z08

Trusted Operating Systems

- We place our trust in OSs to enforce/mediate security policy on our behalf
- Generally we do not write our own OS - buy from vendor
- How do we know that its security claims are justified?

Z08

Non-Assurance Methods!

- Emphatic Assertion
  - Claim by vendor that it is "designed to a certain security level"
  - Need independent validation of claims
- Security Through Obscurity
  - Security by hiding functionality or data - "needle in a haystack"
  - Open Design allows public examination and analysis
- "I Couldn't Find any Flaws"
  - Designer/vendor not best placed to find flaws because of constrained mind-set
  - Users may discover weaknesses by doing the unexpected

Z08

Non-Assurance Methods! - 2

- Challenging users to find flaws for a reward
  - User may benefit more from exploiting flaw than the reward
  - Vendor may find it too expensive to fix flaw - e.g. major re-design
- Careful design, organised testing and professional, independent assessment needed

Z08

Secure OS Principles
Saltzer and Schroeder (1974, 1975)

- Least Privilege: minimise indvertent damage by using fewest possible privileges
- Economy of Mechanism: Protection system should be small, simple and straightforward. Allows analysi, testing and perhaps, verification
- Open Design: Allows independent confirmation of the design
- Complete Mediation: Every access attempt must be checked - must not be possible to circxumevent mediation

Z08

Secure OS Principles - 2
Saltzer and Schroeder (1974, 1975)

- Permission-based: Default condition must be denial of access
- Separation of privilege: Access to objects should depend on more than one thing, eg. user identity plus encryption key ("belt and braces")
- Least common mechanism: Keep sharing of objects to minimum - provide potential channels. Use physical or logical separation where possible
- Easy to Use: Complex mechanisms are circumvented if possible or perhaps used incorrectly

Z08

General Purpose OS Security

- Authentication of users
- Protection of memory
  - r, w, x access to different segments by hardware/OS
- File and I/O device access control
  - access matrix, ACL
- Access control of general objects
  - concurrency and sync primitives

Z08

General Purpose OS Security - 2

- Enforcement of sharing
  - integrity and consistency Fair service guarantee
- Fair Service guarantee
- Inter-process Communication and Sync
  - OS provides support
- Protection of OS protection data
  - information related to security enforcement must be protected by OS
  - eg. capabilities, page tables, file protection info, etc.
  - use separation, encryption, etc.

Z08

Trusted OS Security

- User identification and authentication
- Mandatory access control
- Discretionary access control
- Object re-use protection
- Complete mediation
- Audit
- Audit log reduction
- Trusted path
- Intrusion detection

Z08

Trusted OS Security - 2

- Object Re-use Protection
  - When memory and disk space are freed up GPOS usually leaves the pages "dirty"
  - Security weakness - new user could read before write to "scavenge" for data from another process
  - TOS needs to clear object space before re-issue (preferably on release)
- Complete Mediation
  - All accesses must be controlled, not just file accesses
  - Includes network, memory etc.

Z08

Trusted OS Security - 3

- Trusted Path
  - Need to be sure that security interface is not beeing spoofed, eg. logging in or changing access permissions
  - Trust path provides this
  - Arranged by unique key sequence designed to only get to security part of OS, or done at start-up before any other processes run
  - Windows NT-4 Ctrl-Alt-Del to login ensures not Trojan Horse

Z08

Trusted OS Security - 4

- Accountability and Audit
  - Need to keep log (***audit log*** or ***audit trail***) of all security related events
  - Such events: access to a file, change access permission, etc.
  - Audit trail must be protected from outsiders
- Audit Log Reduction
  - Balance between logging everything and acceptable volume eg. log only opening and closing of files (WP may open many files)
  - Some apps continually read/write to single file, so these operations may need to be logged
  - Some systems do ***audit reduction*** from comprehensive log for most analyses - full log still available if needed

Z08

Trusted OS Security - 5

- Intrusion Detection
  - Software to analyse audit logs to detect anomalies
  - Intrusion and fraud detection
  - "Intelligent System" techniques
- See Pfleeger pp 292 foll. For trusted OS design principles

Z08

Assurance Methods
Testing

- detects existence *not absence* of flaws and weaknesses
- combinatorial explosion of cases means poor coverage of cases
- *black-box testing* cannot exercise all pathways in the design
- *white-box testing* needs addition of code to expose internal state - may later be source of vulnerability
- penetration or *tiger team* analysis uses experts to try to break into system knowing likely weak points from experience - but still only exposes flaws, not correctness (DO NOT try this!)

Z08

Assurance Methods - 2
Formal Verification

- Use of *theorem provers*
- Very time consuming:
  - assertions need to be stated for each step of algorithm and logical flow verified
- Complex:
  - generally only feasible for limited algorithms, not whole OSs.
  - use on ***reference monitor*** or ***security kernel*** at most
  - ideally, designed with formal verification in mind

Z08

Assurance Methods - 3
Validation

- Includes verification, but more general
- Requirements checking
  - cross-check each requirement against source code or execution behaviour
  - demonstrates that system does what it should in at least one situation
  - may not demonstrate that it ***does not do*** anything adverse
- Design and Code Reviews
  - success depends on rigour of reviewer

Z08

Assurance Methods - 4
Validation

- Module and System Testing
  - independent team selects data to test correctness
  - data must be methodically chosen to test all paths
  - usual problems of combinatorial explosions etc.

Z08

Evaluation

- Most consumers do not have skills to evaluate a system for security
- Independent third-party evaluation required
- Need standard schemes for users' assurance
- Many schemes exist:
  - US Orange Book Criteria
  - German Green Book
  - UK Criteria
  - European IT Security Evaluation Criteria (ITSEC)
  - Others ...
  - Eventual harmonised international criteria?

Z08

US Orange Book

- Trusted Computer System Evaluation Criteria (TCSEC)
- Class D
  - no requirements - may or not be secure
- Class C1, C2, B1
  - need security features common to many commercial OSs
- Class B2
  - requiring proof of security of underlying model
  - also specification of trusted computing base
- Class B3, A1
  - more stringent proof of design

Z08

US Orange Book - 2

- Class C and B1 may be obtainable by adding features to existing OS
- But, for B2 security must be included in the design
- And for B3, A1 the OS must start with proof of the formal model of security

Z08

US Orange Book - 3

- C1: Discretionary Access Control
  - separates users from data
  - but granularity may be > single user
  - must be controls that appear sufficient for this
  - may not be stringently evaluated
- C2: Controlled Access Protection
  - Still discretionary, but granularity finer
  - audit trail capable of tracking attempted accesses to individual objects

Z08

US Orange Book - 4

- B1: Labeled Security Protection
  - all B-level include non-discretionary access control
  - for B1 it does not need to control every object
  - controlled objects labeled with security level
  - labels used for access control
  - hierarchical and non-hierarchical categories
  - Bell-LaPadula implemented

Z08

US Orange Book - 5

- B2: Structured Protection
  - design and implementation must permit more thorough testing and review
  - verifiable top-level design and confirmation through testing
  - internal structure in "well-defined largely independent modules"
  - principle of least privilege enforced in design
  - analysis of covert channels required

Z08

US Orange Book - 6

- B3: Security Domains
  - security functions small enough for extensive testing
  - more stringent design and argument that implementation matches it
  - security functions must be tamperproof
  - system audit facility able to identify when a security violation is imminent!

Z08

US Orange Book - 7

- A1: Verified Design
  - formal model of protection and proof of consistency and adequacy
  - formal spec of protection and demonstration that this matches model
  - implementation "informally" shown consistent with specification
  - formal analysis of covert channels

Z08

German Green Book

- Eight basic functions suitable for range of policies
  - identification and authentication
  - administration of rights
  - verification of rights
  - audit
  - object re-use
  - error recovery
    - identification when recovery is necessary
  - continuity of service
    - degree of delay or loss that can be tolerated
  - data communications security
    - peer authentication, data confidentiality, integrity, origin authentication, non-repudiation

Z08

German Green Book - 2

- Separates quality from functionality
- Ten functional levels F1 to F10
  - F1 to F5 similar in functionality to US C1 to B3
  - F6 high data and program integrity
  - F7 high availability
  - F8 to F10 data comms situations
- Eight quality levels Q0 to Q7
  - Q1 implementation more or less ok - no major errors
  - Q3 largely resistant to simple penetration attempts
  - Q6 formally proven that high level spec meets all requirements of policy and source code analysed
  - Q7 beyond US A1

Z08

ITSEC

- European scheme started in 1991 to harmonise
- Combines German and UK (claims based) approaches
- Retains German functionality classes

- Vendor defines Target of Evaluation (TOE)
  - considered in context of operational environment (threats)
  - and enforcement requirements

Z08

ITSEC - 2

- Vendor states:
  - system security policy/rationale
  - security enforcing function
  - mechanisms in the product
  - claim of strength of mechanisms
  - target evaluation level (***functionality*** and ***effectiveness***)
- Evaluation determines:
  - suitability of function
  - binding of functionality - work together?
  - vulnerabilities
  - ease of use
  - strength of mechanism

Z08

Enterprise Security Policy BS7799

- BS7799 defines process and framework of controls for this
- Management framework established by:
  - defining policy
  - defining scope of Information Security Management System
  - undertaking risk assessment
  - managing the risk
  - selecting control objectives and controls to be implemented
  - Preparing statement of applicability - "critique of the objectives and controls applicable to the needs of the organisation"

Z08

BS 7799

- Requires documentation of evidence of actions taken, procedures, management framework
- Documentation readily available under version control
- Records kept to demonstrate compliance, eg. visitors' book, audit records

Z08

BS7799 Controls

- Security Policy
  - policy document approved by management, reviewed regularly
- Security Organisation
  - ***Infrastructure:*** manage information security within organisation - involvement of managers, identification of responsibilities, authorisation processes, specialist advice
  - ***Third Party Access:*** risk assessment and procedures
  - ***Outsourcing:*** security requirements for outsourcing management and control of info systems, networks etc

Z08

BS7799 Controls - 2

- Asset Classification and Control
  - ***Inventory of assets***
  - ***Information classification:*** classification for sharing/restricting information, procedures for labelling such information
- Personnel Security
  - ***Job definition:*** reduce risks from human error; screening, confidentiality agreements
  - ***Training:*** information security education and training
  - ***Responding to incidents:*** minimise damage from incidents and learn from experience: reporting weaknesses and malfunctions; disciplinary action

Z08

BS7799 Controls - 3

- Physical and Environmental Security
  - ***Secure areas:*** prevent unauthorised access: security perimiter; control of loading bays etc
  - ***Equipment security:*** prevent loss or compromise to assets: siting of equipment, power supplies, cabling, maintenance, off-premises use, disposal of equipment
- General Controls
  - Prevent compromise or theft of information and IP facilities (IPF): clear desk/clear screen policy, removal policy

Z08

BS7799 Controls - 4

- Comms and Operations Management
  - ***Operational Procedures:*** ensure correct and secure operation of IPF: separation of duties, documented procedures, change control
  - ***System Planning and Acceptance:*** capacity planning, acceptance criteria for new systems
  - ***Malicious Software:*** user awareness plus tools
  - ***Housekeeping:*** integrity and availability of IP and comms services, back-ups, fault logs
  - ***Network Management:*** safeguard information in network - firewalls etc
  - ***Media Handling:*** handling of removable media, disposal of all media - disclosure and misuse, protection of system documentation

Z08

BS7799 Controls - 5

- Comms and Operations Management
  - ***Exchange of Information and Software:*** prevent loss or misuse of info passed between organisations: agreements, e-mail security, formal authorisation for release
- Access Control
  - Definition of business requirements for access control policy
  - ***User Access Management:*** registration, privilege management, password management, access rights
  - ***User Responsibilities:*** password use, unattended equipment
  - ***Network Access Control:*** routing control, enforced path, limited use

Z08

BS7799 Controls - 6

- Access Control
  - ***OS Access Control:*** terminal identification, log-on procedures, use of system utilities, duress alarms, limits to connection time
  - ***Application Access Control:*** restriction of access to information, sensitive system isolation
  - ***Monitoring System Access and Use:*** to detect unauthorised activities: event logging, clock synchronisation
  - ***Mobile Computing and Tele-working:*** policy for working in unprotected environments

Z08

BS7799 Controls - 7

- Systems Development and Maintenance
  - ***Security Requirements:*** to ensure that security is built in to new systems and any modifications
  - ***Security in Applications Systems:*** to prevent misuse of loss of data in applications: input data validation, internal checks on consistency and integrity of data
  - ***Cryptographic Controls:*** protect confidentiality, authenticity, integrity of information: policy on crypto-controls, digital signatures, key management, non-repudiation services
  - ***Security of System Files:*** ensure support activities conducted securely: control of operational software, protection of system test data, access control of source code

Z08

BS7799 Controls - 8

- Systems Development and Maintenance
  - ***Development and support:*** use of change control procedures, restriction on changes to software, covert channels, outsourced software development
- Business Continuity Management
  - ***Interruptions due to major failures and disasters:*** process, impact analysis, contingency plans, testing these plans

Z08

BS7799 Controls - 9

- Compliance
  - ***Legal requirements:*** avoid breaches of law and contracts: Data Protection Act and personal information, regulation of cryptographic controls, collection of evidence
  - ***Review of policy and technical compliance:*** managers responsible for their areas and systems regularly checked for compliance
  - ***Systems Audit:*** audits planned to minimise disruption, access to tools limited to prevent misuse

Z08

Further Reading

- Pfleeger C, "Security in Computing", 2ed, Prentice Hall, 1997, 0-13-185794-0
  - **Trusted Operating Systems:** pp 287-331
  - **ITSEC/Orange Book:** pp 313-324
- BS7799 parts 1 and 2 1999

Z08