



Seminar Lecture to UNSW
Computer Security Course
October 16, 2003

EXPERIENCE. RESULTS.

Kim Valois
Director, Global Information Security Services
Computer Sciences Corporation, Australia

General Discussion on Security Architecture

Security Risks: General Categories

- Outsider Threats
- Insider Abuses and Misuses
- Design Flaws, Configuration Errors, Poor Controls
- Errors, Mistakes, Accidents, Disasters

Top sources of risk today--security professionals estimate that 90% of exposures are due to:

- Software configuration, especially default installations
- Exposures in software that could be closed with available patches...but have not

IT environments change frequently

- Changes may occur in an IT environment every day, or even every hour !
- It is very difficult to manage these changes, to even know about them
- Managing the risks they introduce to the environment is difficult

AND...

- Most organizations DO NOT have good asset management information, basically the inventory of information assets and their configuration, and most important: their business value !!!
- Fewer still have ways to verify the true security state of their enterprise on a day-to-day basis



- **Typical commercial network security defenses still focus on protecting the perimeter of the network.**
- **The true risks of connecting to the Internet are not well understood.**
- **The cost of deploying defenses is perceived to be higher than expected loss due to security breaches.**
- **Many security defense strategies remain simple at best.**



- **Changes in the nature of the threat environment have illuminated the need for better defenses.**
- **It is too easy for an intruder to get through a single line of defense, often a firewall or a simple DMZ/TMZ.**
- **As the costs of recovering from attacks have grown, so has interest in deploying preventative and protective measures.**

- **Address many vulnerabilities, especially in component, software, and application configuration**
- **Keep up with frequently changing environments and threats**
- **Deal with technical complexity—closing exposures requires deep technical skill and insight that cannot be abstracted**

Relationship between Security Policy and Architecture

- **Security policy provides the fundamental rules for the business or enterprise**
- **Security policy as a foundation is a high level statement that does not change frequently**
- **Given policy, it is possible to develop:**
 - **Security Standards**
 - **Security Guidelines**
 - **Implementation solutions of the security policy**

- **Confidentiality**
- **Integrity**
- **Availability**



- **Confidentiality**
 - Encryption services, to provide confidentiality of data and transactions in transit
 - Encryption services to protect data in stored state
- **Integrity**
 - Authentication services, to identify and/or identify users or transactions, or provide access control services
 - Controls to prevent or detect unauthorised changes to data, transactions, or system configuration
 - Digital or electronic signature services, to verify the time and source of a transaction
- **Availability**
 - Network defence services, including gateway defences
 - Anti-Virus services to protect availability of IT services and systems
 - Monitoring and alerting, to identify and prevent intrusions, denials-of-service, and other attacks



- **A good security architecture should support and help implement the security policy.**
- **A good understanding of the security policy is one of the essential inputs to developing a security architecture that meets the enterprise's needs**
- **While it is possible to come up with a solution or architecture without knowing the policy, it may not provide or meet the security needs of the organisation**

Defence-in-Depth Security Architecture

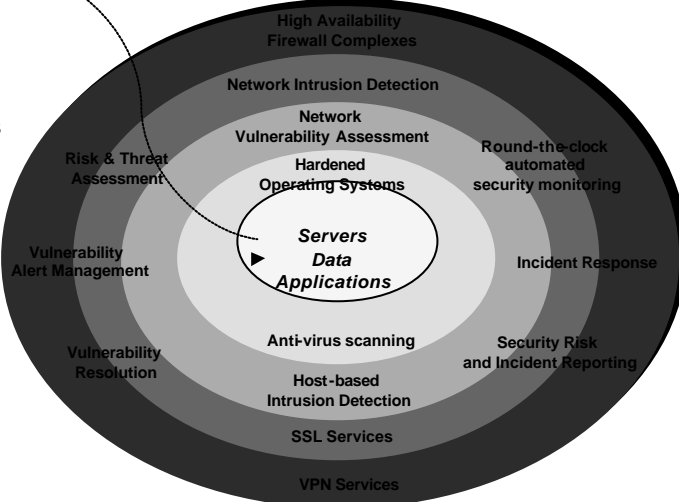
What is Defence-in-Depth ?

- **Defence-in-Depth is a security construct by which defenses are layered around assets, enhancing the overall protection of them**
- **The objective of Defence-in-Depth is to layer defenses in such a way as to thwart or discourage foes, by making their work more difficult**

- Does not rely on a single security control or on a single security boundary for protection
- Combines security controls and mechanisms to complement each other, strengthening defences

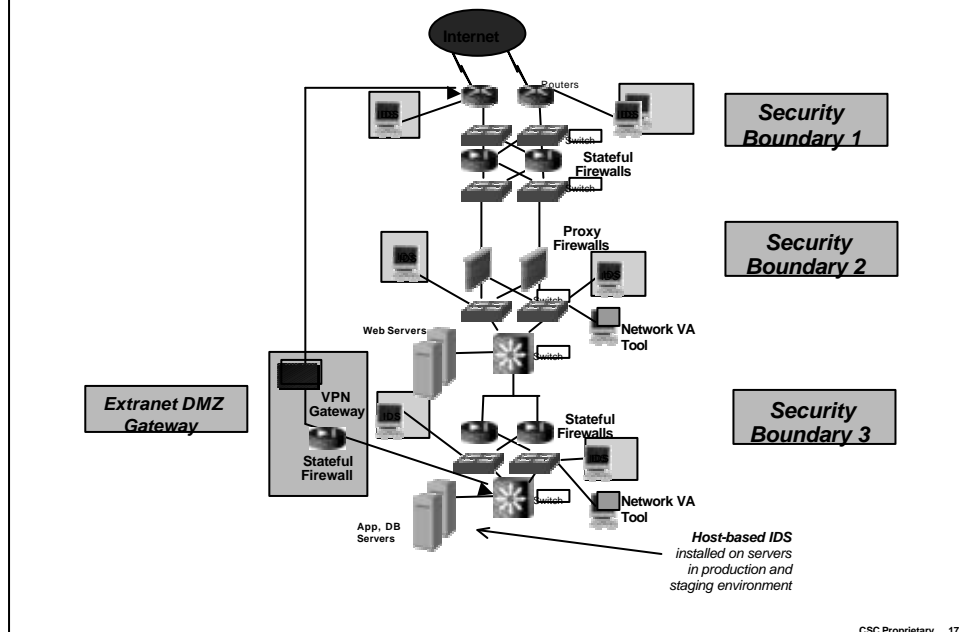
Defence-in-Depth

- Combines multiple layers of protective controls and practices
- Protects systems from known attack methodologies and exploits
- Provides security enforcement services to match needs
- Adapts in response to constantly changing threat environment





Example: Logical Defence-in-Depth Security Architecture



CSC Proprietary 17



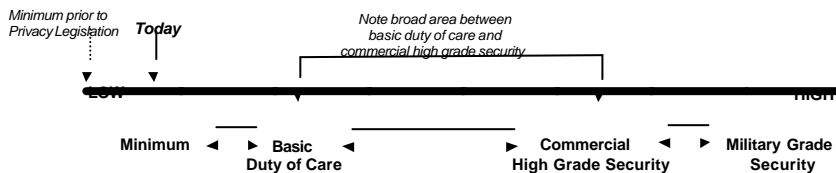
Characteristics of Defence-in-Depth

- Multiple security controls
- Complementary controls
- Layered control array or schema
- Uses topology and security architecture and design as features to enhance defences and layered schema
- Can include both automated (tools) and process controls
- Should include controls to address human factors & behavior

CSC Proprietary 18

<i>Some Risks to Web-based e-commerce providers:</i>	<i>Some Defensive countermeasures:</i>
Defacement of web sites	File integrity checking, access controls, user authentication, incident response, hardened OSs
Denial-of-service/availability problems	Perimeter firewalls & routers, network IDS, incident response, anti-virus scanning
Intrusions and damage to web sites and web infrastructure	access controls, user authentication, incident response, hardened OSs, vulnerability assessment
Unauthorized disclosure of data transmitted between web site and users/browsers.	SSL services, VPN services, file encryption, PKI services
Unauthorized access to web site data	User authentication controls, host-based IDS,
Unauthorized modification of web site data	File integrity checking, host-based IDS

<i>Some Risks to Web-based e-commerce users:</i>	<i>Some Defensive countermeasures:</i>
Disclosure to third parties of personal or sensitive data	SSL services, VPN services, file encryption, access controls
Denial of service of e-commerce data and transactions	Perimeter firewalls & routers, network IDS, incident response
Unauthorized modification of user's data	File integrity checking, user authentication, access controls
Virus threat	Anti-virus scanning and eradication



- **Today's Minimum:** legislative duty to safeguard privacy of *personal and sensitive* information
- **Basic Duty of Care:** encompasses a rather broad range of *reasonable and expected efforts to prevent or manage security risks* using appropriate controls, mechanisms, and processes
- **Commercial High Grade Security:** *very secure systems and applications to assure availability, integrity, and confidentiality* of systems, information, and transactions, such as those used in the finance industry
- **Military Grade Security:** *very strong grade security suitable to protect national assets and interests*

	Minimum	Basic Duty of Care	Commercial High Grade Security
	Minimum	Moderate	Strong
Outsider Threat	Basic perimeter defence (e.g., firewall at external gateway)	Transaction/DeMilitarised Zone (TMZ/DMZ) architecture, multiple perimeter controls, such as firewall, VPN, etc	Layered security architecture with multiple boundaries featuring complementary controls, including firewall, IDS, VPN, virtual switching, incident response, etc
Insider Misuse and Abuse	Ability to track transactions to user or application that generated them (e.g., individual user accounts, basic authentication)	<i>Minimum level plus:</i> occasional audits if system access and transactions, occasional user security awareness initiatives	Strong two factor authentication (token or PKI based) for signing of transactions; regular compliance monitoring, logging and analysis, regular and ongoing user security awareness program
Design Flaw, Config Error, Poor Control	Basic anti-virus defences, ability to patch if required, aperiodic vulnerability assessment	<i>Minimum level plus:</i> basic vulnerability alert review, occasional vulnerability assessment, may have process oriented change management,	Robust closed loop process vulnerability alerting, proactive patching, regular vulnerability assessments, security configuration controls, standard builds and automated roll-backs or re-builds (tools based), data integrity and file checking controls, Change Management (with tools-based or automated verification)
Mistake, Accident, Disaster	Basic business continuity using system backups, etc (cold system/process at best)	Disaster recovery and business continuity plan with some infrastructure to support business during a short or extended outage (perhaps warm or cold site)	Formal and possibly integrated disaster recovery and business continuity infrastructure and planning. Use of hot or warm sites for back ups with aperiodic operational testing (min. annual)

Practical Problems/Exercises



Problem Exercise #1: Basic Internet Gateway Security

- You work for a company that is responding to a Request for Proposal (RFP) that has been released to the market. Your firm will be competing against other service providers and needs to design an Internet Gateway solution that meets the client's needs and can be developed into a competitive market solution. You have been assigned to the bid team as the Security Solutions Architect and need to develop a suitable solution.
- Draw a logical diagram of the solution you propose showing the functional components and logical configuration required, annotating it with the security features and services you recommend. (Make sure you include infrastructure you need to manage the gateway complex)
- **The basic requirements your solution needs to meet are:**
 - Support outgoing Internet browsing by 1000 corporate users
 - Support incoming Internet browsing of the corporation's Internet web sites, one of which needs to support secure web protocols (e.g., HTTPS)
 - Provide Internet mail services
 - Provide basic firewall and gateway security appropriate for this infrastructure
 - Basic Anti-Virus scanning for Internet gateway and mail
- **Bonus:**
 - Add fail over and redundant features to the gateway solution
 - What other security features could you add ? Why would you add them ? (what security benefits do they provide ?)



Exercise #1 Interactive Discussion

Discussion about the Questions in Exercise #1

Question & Answer Session



- Your company is designing a gateway refresh for an existing client that already has a basic Internet gateway supporting outbound and inbound web browsing, basic Internet mail and a basic gateway security complex (firewalls). If you like, you can use the diagram from Exercise one as the client's existing gateway.
- The following features need to be added in the refresh project. Draw these in a logical diagram of your recommended solution, annotating the diagram with the security solution features you propose.
 - Provide (host) Intranet Services for the corporation, including corporate Intranet portal and some workflow applications for corporate procurement, travel requests, and timekeeping
 - Provide a remote access gateway, for remote users to access the corporate Intranet when working from home or while traveling.
 - All Intranet services require two-factor authentication
 - Anti-virus scanning for Intranet services and access
- **Bonus Question:**
 - The client wants to ensure that unauthorised users cannot view or conduct transactions involving the Intranet related resources. However, the gateway complex needs to accommodate external Internet browsing to the client's publicly viewable Internet sites as well. Describe what controls or solution features will allow you to provide this.



Discussion about the Questions in Exercise #2

Question & Answer Session

- **A client has come to your firm and wants to implement security monitoring, to respond to a finding of a security assessment recently conducted on their infrastructure. Using one of the gateway solutions you have designed in Exercise #1 or #2, design a security monitoring solution with the following features:**
 - Ability to detect intrusions or attacks in the environment
 - Ability to detect unauthorised access or transactions on critical servers or applications
 - Identify vulnerabilities on systems in the environment
 - Ability to detect inappropriate activities by users conducted from corporate resource and/or during work hours
 - Record keeping and retention of suspicious transactions or inappropriate activities.
 - Ability to support investigations and legal prosecution

- **Identify the security monitoring solutions, components, or systems that will satisfy each of the feature statements above.**

- **Draw a security monitoring solution that meets all the feature requirements. Include the components and configuration to allow the solution to be centrally managed.**

Discussion about the Questions in Exercise #3

Question & Answer Session

- **The next solution you need to design must be able to provide secure and high integrity transaction processing for an Internet site that will be handling transactions of value. Taking a basic Internet gateway solution, describe what additional components and systems you need to add to include the following features in the secure transaction solution.**
 - Secure web browsing from the Internet
 - Secure web transactions that involve reading and writing data from a database or involving an application layer
 - Strong authentication, to assure you have some confidence that users are who they claim to be
 - Auditing functions to protect the business offering the secure services, in the event there is a dispute or a complaint that needs to be investigated
- **Bonus Question:**
 - Security monitoring is required for this solution. What special considerations or problems are there to do security monitoring for this solution? Describe a solution that will provide security monitoring in this case.

Discussion about the Questions in Exercise #4

Question & Answer Session

*For More Information,
E-Mail or Call Us....*

Kim Valois
CSC Australia
kvalois@csc.com.au
+61 (0)2 9464 4244

EXPERIENCE. RESULTS.