



# Introduction to the System-level Elements of Network Security Systems

Lecture-7

**Dr. Rahul Banerjee**

Associate Professor: CS & IS group

Birla Institute of Technology & Science, Pilani  
(India)

E-mail: [rahul@bits-pilani.ac.in](mailto:rahul@bits-pilani.ac.in)

Home: <http://discovery.bits-pilani.ac.in/rahul/>





# Interaction Points

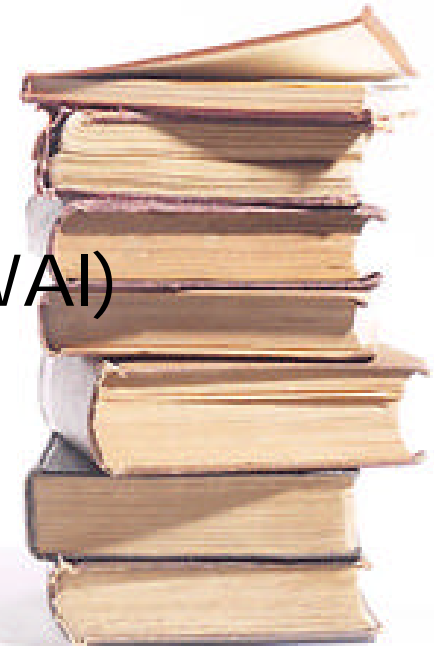
- Fundamentals of System-level elements of Network Security
  - Trusted Network
  - Untrusted Network
- Network Perimeter
- Firewalls
- Intrusion Detection Systems
- Packet Filters
- Virtual Private Networks





# Trusted versus Untrusted Networks

- **My Network** (PAN/LAN)
  - Fully Trusted
  - Partly Trusted
- **Our Network** (LAN/MAN/WAN/WAI)
  - Fully Trusted
  - Partly Trusted
  - Unsure
- **Other Networks** (LAN/MAN/WAN/WAI)
  - Partly Trusted
  - Untrusted
  - Unsure





# The Network Perimeter

- A Network / Internetwork Perimeter is a secure boundary of a network that may include some or all of the following:
  - Firewalls
  - Routers
  - IDS
  - VPN mechanisms
  - DMZ
  - Screened subnets
- DMZ is outside the Firewall
- Screened subnet is an isolated sub-network connected to a dedicated firewall interface





# Intrusion Detection System

- **Intrusion Detection System (IDS) is a system that**
  - comprises of mechanisms / devices involving one or more Intrusion Detection Sensors (traffic monitoring devices / mechanisms) placed at security-wise strategic locations; and,
  - Has been designed to detect any known or likely intrusion into the protected network.
- **Types of IDS:**
  - Network-based IDS (NIDS) : Subnet-resident
  - Host-based IDS (HIDS) : Host resident
- **Sensor reporting may involve several forms like logs, database updates, Email alerts etc.**





# Internetwork Firewall

- Firewall is an internetwork security device that
  - serves on the only access route that connects the internal network / internetwork (i.e. the segment to be protected) to the external network (s) / internetwork (s); and,
  - decides about physically allowing / denying entry / exit to / from the protected segment using a set of policies (often manifested in terms of rules) is called a Firewall.
- A Firewall may be implemented in hardware / software / firmware or a combination of these.





# Characteristics of Internet Firewalls

- Characteristically, an Internet Firewall exhibits security measures and internetwork-control-mechanisms related to but not necessarily limited to:
  - Internet services as separated from the intranet services
  - Service-based directional traffic
  - User-specific / Class-specific / Group-specific service access
  - Service-usage / deployment-behaviour
  - Origin-specific / Destination-specific service / traffic / monitoring / QoS-security bindings
  - Relaying / blocking / redirection of encapsulated and / or encrypted traffic
- A common assumption (though debatable) made is that the Firewall itself is incorruptible / impenetrable
- A firewall works under the assumption that it is solely responsible for blockade / allowance of any traffic between two or more than two networks / internetworks separated by it.





# What does a firewall do?

As part of an Internetwork Security System, a firewall:

- Allows defining exit and entry points for traffic from and to the internal protected network / intranet
- Offers a set of mechanisms and a set of locations / points for supervising security-sensitive activities / events / behaviour
- Provides network-level encapsulation, encryption, decryption, decapsulation, tunnelling services
- Permits a variable-security facility-zone's creation that may also offer some functionalities not necessarily related to the security function that is the primary function of the firewall
- Supports creation and interpretation of structured logging mechanisms and files for a variety of purposes.





# What a Firewall does not do?

## A Firewall is not meant for:

- Virus / Worm / Trojan Horse / Logic bomb detection
- Virus / Worm / Trojan Horse / Logic bomb removal
- Semantic analysis of the application-to-application messages with certain exceptions
- Protecting a network / internetwork from a trusted entity (client / server / user) or an internal authorized user with adequate privileges
- Protecting from power, link or protocol failure
- Monitoring processes at individual workstations / servers / switches that are of local significance to that machine or network segment except for certain explicitly registered classes of processes / systems / users / patterns
- Guarding against traffic that bypasses the Firewall itself





# Constituents & Types of a Firewall

- **Firewall Constituents:** (some of these can serve as firewalls as well)
  - Application-level Gateways and Proxies
  - Transport-level / Circuit-level Gateways and Proxies
  - Network-level Gateways / Routers
  - Packet filters (also known as Static Packet Filtering Firewalls)
  - Bastion Host
  - Screened Host
- **Types of Firewalls:**
  - Stateless Firewalls
  - Stateful Inspection-based Firewalls
  - Perimeter Firewalls
  - Screened Host Firewalls
  - Intranet Firewalls
  - Internet Firewalls
  - Extranet Firewalls





# Examples of Commercial Firewalls

- Static Packet Filtering Firewall  
*(implemented on a Router):*

*Example:*

*Nortel's Accellar Router Firewall*

- Proxy Firewall:

*Example:*

*Secure Computing's  
Sidewinder Firewall*

- Stateful Inspection-based Firewall:

*Example:*

*Cisco's PIX Firewall*





# Virtual Private Networks

- A *Virtual Private Network* (VPN) is a **mechanism** that allows establishment of a *protected session* between *two network nodes / services* located in / on *two different protected networks / internetworks* separated by unprotected / untrusted / insecure (often public) networks / channels / infrastructure.
- **Example:** Nortel's Contivity, Cisco's VPN 3000 Concatenator
- **Another perspective:** SSH, TLS, SSL, IPsec, L2TP, PPTP are choices providing different types of security at different layers.
- **Although, all of these could be reused in an appropriately designed VPN mechanism, often the L-3 and L-2 mechanisms are preferred by many VPN designers.**
- Often, people refer to a VPN as a security device / mechanism on the perimeter of the protected network / internetwork that allows encrypted sessions.





# Advantages of VPNs

- Capability to access remote network as if there exists a private channel to that network
- Several security options available to provide a range of security
- Adequacy of lower-strength encryption schemes on certain occasions
- Cost-effective if well-designed, well-implemented and well-configured
- Can be quickly implemented





# Disadvantages of VPNs

- Requirement of encryption, decryption, encapsulation and decapsulation induce a sizeable processing overhead, packet overhead and storage overheads and may introduce latency as well as increase cost of service
- In some cases, if designed ad-hoc, certain network installations may pose additional challenges in adding the VPN functionality due to the added overhead in packet processing.
- Intricate design issues, unless handled carefully, may actually serve to lower the network performance without really bring corresponding increase in the security level of the network.
- Implementation issues include VPN pass through issues, NAT-specific issues and MTU-size related issues
- Troubleshooting becomes tricky.





# Defining the Relevant Terms

- The Control Zone:

- Consider a typical electronically controlled device like a tape drive, hard disk drive or other gadget that operates in an unshielded environment. Each such device emits signals that can be sensed within a zone called Control Zone.

- For security reasons, it is important that:

- No important information about any device operation leaks out of the target environment

- No external body should be able to make use of control or data signals related to this device





# The Concept of Security Services

- Authentication Service
- Access Control Service
- Availability Service
- Confidentiality Service
- Integrity Service
- Identification: Author, Authorization, Endorsement, Approval, Access, Concurrence, Licensing, Certification, Signature, Witness, Validation, Timestamps, Authenticity, Ownership, Registration, Privacy / Confidentiality / Secrecy
- Non-Repudiation Service





# Internet-based E-mail Security Principles

E-mail Security Architectures should allow varying degree of security and privacy options including:

- Optional Authentication
- Optional Encryption
- Optional facility to use the Non-Repudiation check
- Privacy





# Internet-based E-mail Security Principles ...

- Choice of encryption algorithms
- Compatibility with other de-facto architectures and standards
- Interoperability of services with competing architectures
- Defining any attachment type with associated security parameters
- Compliance with one or more standard protocol stacks used in the Internet
- Security audit provision
- Route tracking facility
- Version management with embedded security information embedding





# Attacks revisited

- Active attacks involve *active attempts on security leading to modification, redirection, blockage or destruction of data, devices or links.*
- Passive attacks involve *simply getting access to link or device and consequently data.*





# Case-Studies

- University Network
  - Hypothetical specification <PDF version>
- Corporate Network
  - Hypothetical specification <PDF version>
- Government Network
  - Hypothetical specification <PDF version>
- Also visit:
  - [http://www.intel.com/design/network/casestudies/dt\\_04.htm](http://www.intel.com/design/network/casestudies/dt_04.htm) <an Intel™ case-study paper>
  - <http://itresearch.forbes.com/detail/RES/1092160685251.html> <a Cisco™ whitepaper>
  - <http://itresearch.forbes.com/rlist/term/Network-Security-Software.html> <list>
  - <http://www.itpapers.com/SECURITY/Intrusion++Tampering/Network+Security/> <list>
  - [http://www.networkworld.com/topics/links/all\\_security\\_security\\_casestudies.html](http://www.networkworld.com/topics/links/all_security_security_casestudies.html) <another list>





Any Questions?

*Thank You!*

