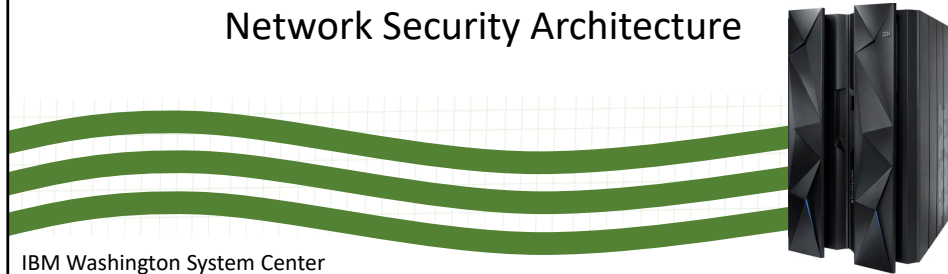


Securing and Encrypting Network Traffic
with z/OS Communications Server and
Policy Agent

Security Workshop

Network Security Architecture



IBM Washington System Center
IBM Technical Sales Support

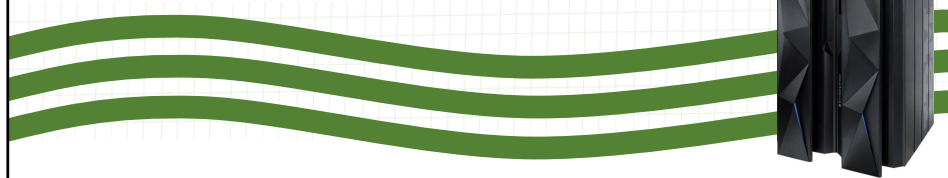
Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
- **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
- All other products may be trademarks or registered trademarks of their respective companies.
- Refer to www.ibm.com/legal for further legal information.
- OSA-Express Features
- There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

Agenda

- Why Do We Care about Security?
- Where to Protect Data
- Security Landscape: Security Architectures in General
- Security Architectures in IT Networking
- Cryptographic Landscape: One piece of the Security Landscape

Why Do We Care About Security?



001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 4

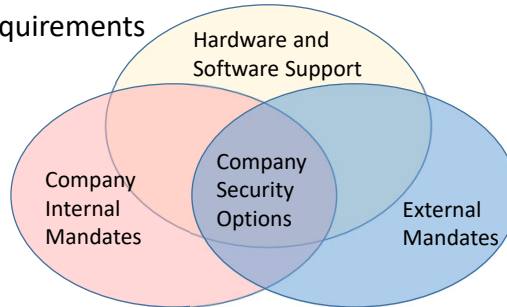
Data Breach

- Costly:
 - Penalties
 - Loss of Trust
 - Loss of Business
 - Loss of Data

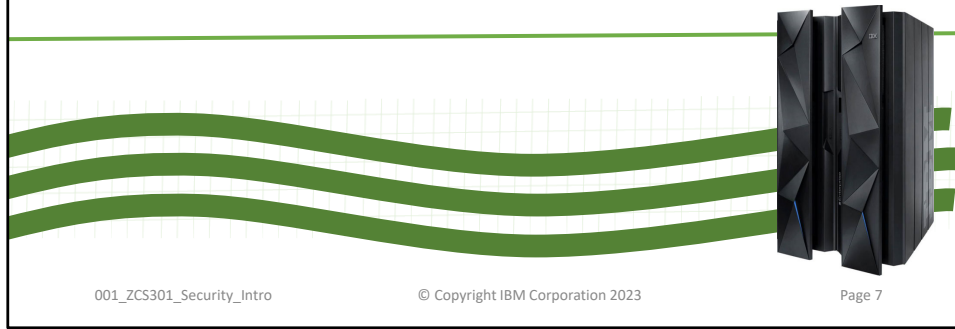
Security Mandates

- Internal and External Requirements

- Encryption Protocols
 - IPsec IKEv1, IKEv2
 - TLS V1.0, V1.1, V1.2
 - OpenSSL
- Encryption Algorithms
 - 3DES, AES
- Hash Algorithms
 - SHA1, SHA2
- Key Sizes
 - 1024, 2048
- External Mandates
 - GDPR – General Data Protection Regulation
 - PCI – Payment Card Industry
 - FIPS – Federal Information Processing Standards
 - HIPA – Health Insurance Portability and Accountability Act



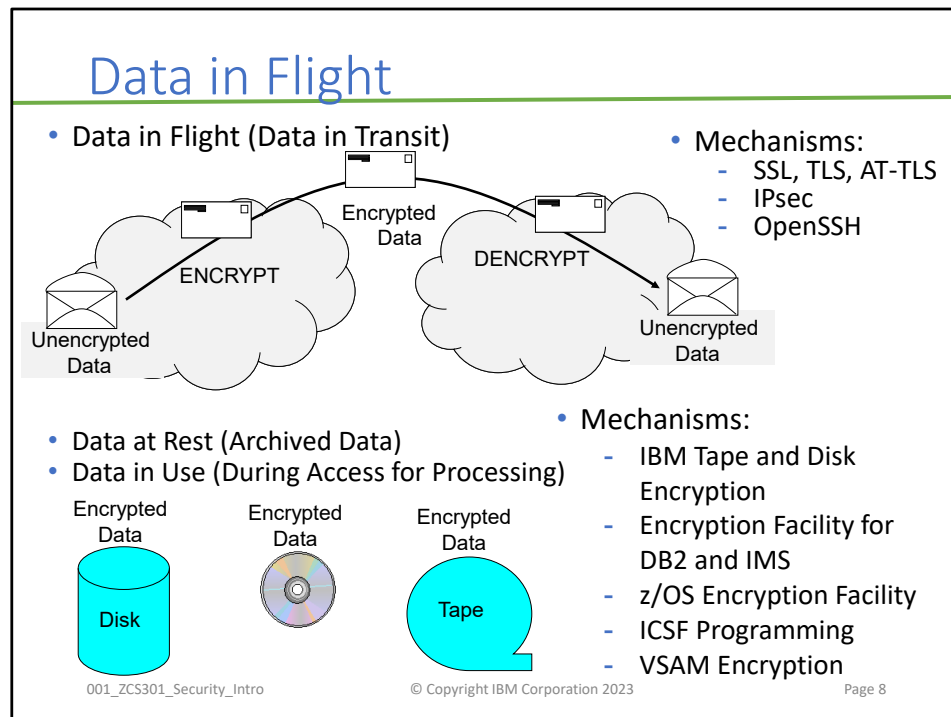
Where to Protect Data



001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 7



In taking steps to protect data, you must decide where and when you need to protect it. This page shows you that it may be necessary to protect the data while it traverses the network. This is called "protecting the data in flight." Protecting the data in flight usually involves providing for:

- Authentication of the connection partners.
- Verification that the data has not been altered in flight.
- Encryption of the data prior to transmission and decryption at the end of the transmission.

There are a number of mechanisms that can be used to encrypt and decrypt the data while working with it for transmission across a network.

- Secured Sockets Layer (the Netscape version)
- Transport Layer Security (TLS - IETF Standardized version of SSL)
- AT-TLS (IBM z/OS Exclusive TLS)
- IPSec (standard for building a Virtual Private Network -- VPN)
- Open Secured Shell (OpenSSH)

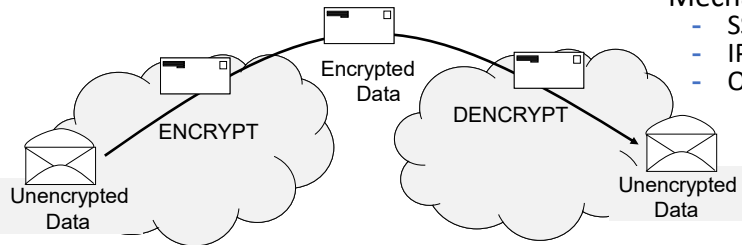
The visual also shows you that you may need to protect data that has been stored on disk or tape for archiving purposes. Alternatively you may be encrypting the data as you store it onto the storage medium during application processing and then decrypting it as you extract the data from storage during processing. The latter is called "Data in Use."

There are a number of mechanisms that can be used to encrypt and decrypt the data while storing and working with it

- If you use the IBM Tape and Disk Encryption, you can use it to archive data or to manipulate it while application programs process it.
- DB2 and IMS data can be encrypted and decrypted for USE with the Encryption Facility for DB2 and IMS
- You may invoke your own encryption calls with the Integrated Crypto Security Feature (ICSF) program of z/OS; this can be used for data that you will store or data that you want to process ("in use")
- You may deploy VSAM encryption and then store the data in encrypted format.

Security Checks Performed for Data in Flight

- Data in Flight (Data in Transit)



- Mechanisms:

- SSL, TLS, AT-TLS
- IPsec
- OpenSSH

- Authenticate the partner in the connection
 - Is this the connection partner we are supposed to be communicating with?
- Verify the integrity of the transmission
 - Has the data been altered in transit?
- Encrypt the data in transit
 - Is anyone unauthorized able to intercept the transmission and understand the contents?
 - Have we made the contents of the transmission private while it is traversing the network?

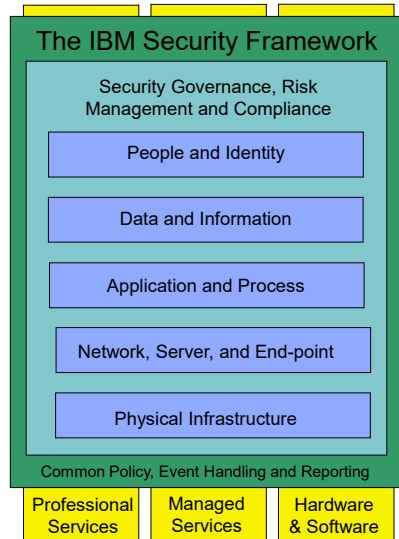
The Security Landscape: Security Architecture in General

Questions for Planning Security:

- **What** needs protecting?
- **How** should you protect?
- **Which** mechanisms or technologies should you use to protect?



The IBM Security Framework: What to Protect



• IBM Solutions:

- Security Compliance
 - Demonstrate policy enforcement aligned to regulations
- Identity and Access
 - Controlled and secure access to information, applications, and assets
- Data Security
 - Protect and secure data and assets
- Application Security
 - Manage, monitor, audit
- Infrastructure Security
 - Threat management across networks, servers, end-points

001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 11

Here is a list of "Essential Questions for Planning Security":

- What needs protecting?
- How should you protect?
- Which mechanisms or technologies should you use to protect?

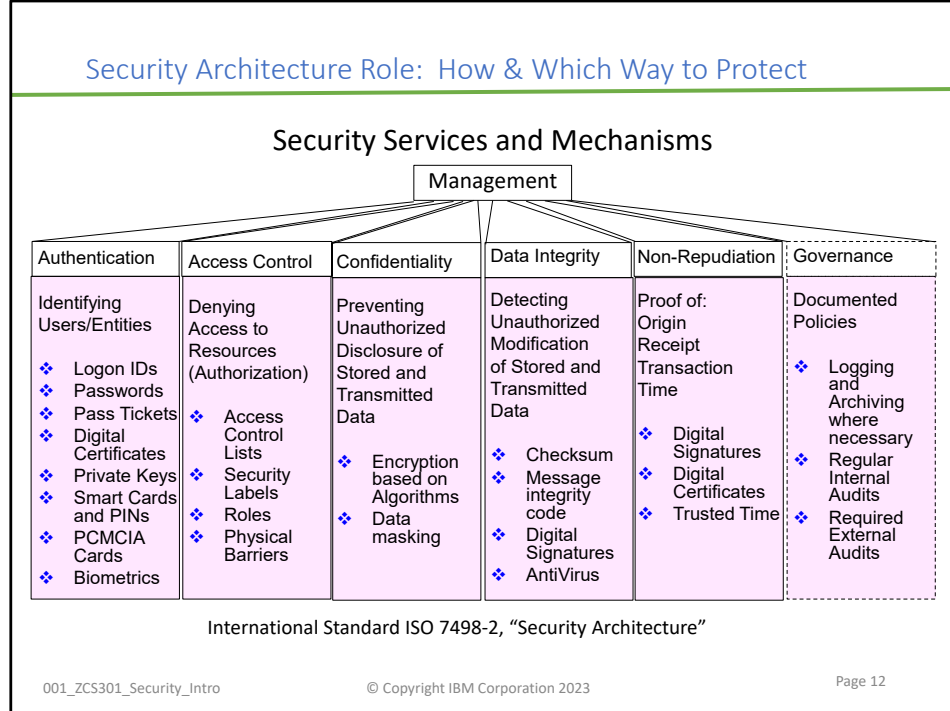
The IBM Security Framework -- depicted here -- addresses the first sub-bullet above: "What needs protecting".

The IBM Security Framework provides a model for selecting, designing, and monitoring technologies to protect all aspects of an IT organization.

IBM provides the professional services to assess an organization's needs for security with regard to compliance mandates and general security requirements. These services can design, implement, and manage security technologies and can recommend hardware and software solutions for an organization.

More information: Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security; IBM RedGuide REDP-4528-00, July 2009

Security Architecture Role: How & Which Way to Protect



You have seen the "Essential Questions for Planning Security":

- What needs protecting?
- How should you protect?
- Which mechanisms or technologies should you use to protect?

The ISO 7498-2 model -- depicted here -- addresses the second and third sub-bullets above: "How should you protect," and "Which mechanisms or technologies should you use to protect?"

This is an older version of the ISO security model. Note the entry for "Governance" and "Logging." This is not part of the ISO model, but it is nevertheless integral for any security implementation. We have added it here to show its importance.

SUMMARY: You have now seen a couple of architectures for security. What is the difference?

- The IBM Security Framework describes WHAT needs to be protected in an IP installation.
- This ISO Security architecture describes:
 - HOW to protect the data (i.e., which Services should be used to protect data and resources)
 - WHICH ways to protect the data (i.e., which security mechanisms could be used to protect the data and resources)

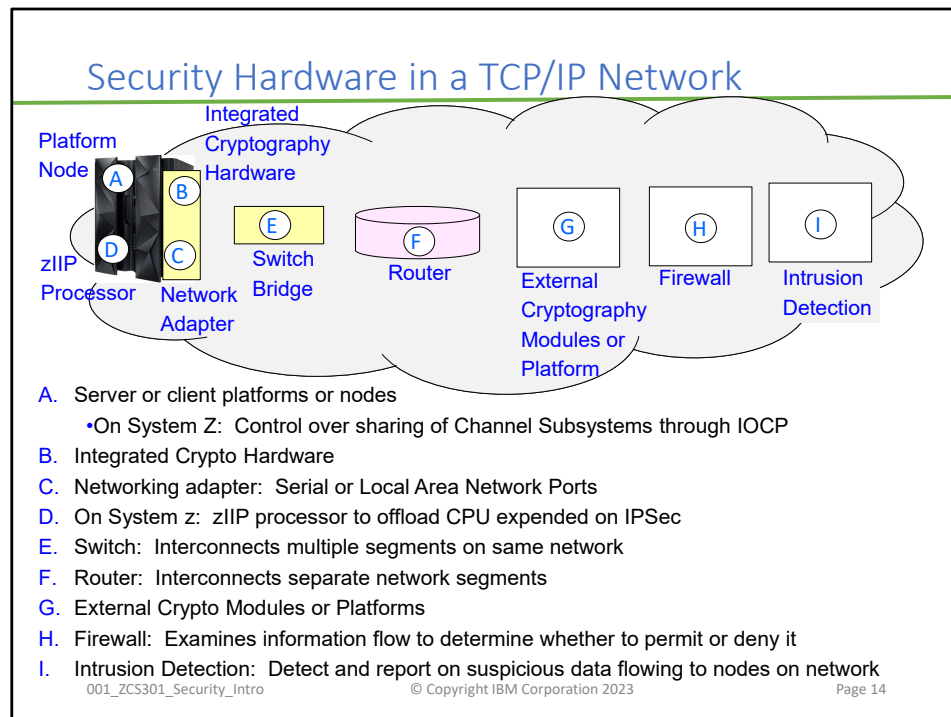
Network Security Components



001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 13



This visual depicts many types of security hardware available to protect or assist in protection of the systems and the network..

A. Often overlooked is the platform or the node itself as part of the security hardware. On system z the most overlooked part of security is probably how the sharing of channel subsystems is controlled across secure and non-secured LPARs through the IO definitions generated by the Input Output Control Program (IOCP) based upon entries in the Hardware Console Definitions (HCD) or an Input Output Data File (IODF).

B. Integrated Cryptography hardware can also provide encryption assistance. On System z this includes a hardware instruction area called CPACF (CP Assist for Cryptographic Function), and cryptographic cards or adapters.

C. Network Adapters can be configured with attributes that may be used for security filtering. On System z the network adapters are also under the control of the IODF. (Revisit Bullet A above.)

D. The zIIP processor on System z can provide performance improvements if certain IPSec Encryption calls are passed to this specialty processor.

E. Switches and Bridges can be configured with attributes that may be used for security filtering.

F. Routers can be configured with attributes that may be used for security filtering.

G. External Cryptography Modules are available to provide encryption external to the processor platform (described in A).

H. FIREWALL: A firewall is an implementation (or extension) of an organization's security policies. Any large organization has (or should have) a formal document explaining the classification of company data, as well as the classification of company networks. A firewall controls and limits access between networks of different security classifications, and sometimes even within a network that is already protected by a firewall. Firewalls can filter based upon port numbers and IP addresses (or networks).

- Firewalls also often function as endpoints for secure communications across a non-secure network. Data travelling from the secure network outward will be secured as it crosses the non-secure network (a requirement of the organization's security policy, no doubt). Data travelling into this firewall would likewise be secured.

I. INTRUSION DETECTION: A host such as z/OS includes intrusion detection services (IDS) that allow the host to detect and react to malicious activities coming from the network. Some IDS is built into TCP/IP on z/OS itself, while other aspects of IDS are configurable. IDS can be an integral part of host availability.

RACF

- IBM Resource Access Control Facility (RACF)
 - Uses z/OS System Authorization Facility (SAF) to control access to resources:
 - Data Sets, MVS Commands, Networks, Network Services
 - SAF = high level MVS interface for plugging into any SAF-compatible security product.
 - Keeps a record of all the resources that it protects in the RACF database.
 - A resource can be a data set, a program, and even a subnetwork.
 - Identification of users and Authentication of user IDs and passwords
 - When a user tries to access a resource, RACF checks its database for User ID and password and permits or denies access to the resource.
 - It displays an ICH408I message if the access is denied.


```
ICH408I  USER(UTSM)  GROUP(MTSM)  NAME(TSOMON  STC=USERID)
EZB.PORTACCESS.SX00.TCP2.SAPSYS  CL (SERVAUTH)
INSUFFICIENT ACCESS AUTHORITY FROM EZB.PORTACCESS.*.*.SAPSYS (G)
```
 - Protection of Application Programs
 - Robust protection of its programs from unauthorized alteration.
 - Makes the z/OS platform effectively immune to computer viruses.
 - Protection of Network Resources with SERVAUTH resource class
 - Uses the SERVAUTH resource class to protect most TCP/IP resources:
 - Ports, Networks, IP Stacks.
 - Protection of Network Resources with Multi-level Security (MLS)
 - Uses Security Labels (SECLABELs)
 - A security category such as PAYROLL, PERSONNEL, or RESEARCH
 - A security level such as CONFIDENTIAL, SENSITIVE, or TOP-SECRET
 - Access to Resource is permitted only if User's SECLABEL is greater than or equal to the SECLABEL of resource

001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 15

IBM Resource Access Control Facility (RACF)

Using the z/OS System Authorization Facility (SAF), controls access to resources such as data set and MVS commands. In a networking context, RACF resources can include networks and network services.

- SAF is the high level MVS interface that allows you to plug into any SAF-compatible security product.

The RACF concept is very simple: it keeps a record of all the resources that it protects in the RACF database.

A resource can be a data set, a program, and even a subnetwork.

Identification of users and Authentication of user IDs and passwords

- When a user tries to access a resource, RACF checks its database for User ID and password. Then, based upon the information that it finds in the database, RACF either allows or denies the access request. It displays an ICH408I message if the access is denied.

Protection of Application Programs

- Robust protection of its programs from unauthorized alteration.
- Makes the z/OS platform effectively immune to computer viruses.
- RACF uses the following mechanisms to secure programs from unauthorized access:
 - Authorized Program Facility (APF)
 - Program Protection by RACF resource class PROGRAM
 - Program Access Control
 - Controlling program access by SYSID
 - The sticky bit in the UNIX environment

Protection of Network Resources

- Most TCP/IP resources are protected by profiles defined in the SERVAUTH resource class.

Protection of Network Resources with Multi-level Security (MLS) using Security Labels (SECLABELs); a SECLABEL consists of two entities:

- A security category such as PAYROLL, PERSONNEL, or RESEARCH
- A security level such as CONFIDENTIAL, SENSITIVE, or TOP-SECRET

The security administrator sets security labels for each user and each resource. When a user tries to access a resource, RACF allows access only if the security level in the user's SECLABEL is higher or equal to the security level specified in the resource's SECLABEL for the security category being accessed.

Hardware and Software on System z

- z/OS Cryptographic Services
 - CP Assist for Cryptographic Function (CPACF)
 - IBM Z hardware feature 3863
 - No cost feature that is enabled by default in most countries (no Started Procedure)
 - Provides APIs to encrypt or decrypt user data
 - Integrated Cryptographic Service Facility (ICSF)
 - z/OS component that provides secure, high-speed crypto services (Started Procedure must be up)
 - A variety of cryptographic primitives
 - Application access to z/OS hardware crypto features (CPACF, Crypto Coprocessor card, and Crypto Accelerator card)
- System SSL
 - z/OS component that provides SSL, TLS implementations (Started Procedure available but not required)
 - Also provides certificate-related APIs, including RSA signature generation and validation
 - Contains own software implementations of all crypto algorithms
 - Makes use of hardware crypto facilities to varying degrees
- z/OS Communications Server
 - TCP/IP stack implements
 - Application Transparent - TLS and IPSec including Internet Key Exchange daemon (IKED)
 - Both contain software implementations of most cryptographic algorithms
 - Both use hardware crypto facilities to varying degrees
 - Intrusion Detection Services
- OpenSSH
 - Uses OpenSSL for cryptographic algorithms
 - Uses hardware crypto facilities to varying degrees

001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 16

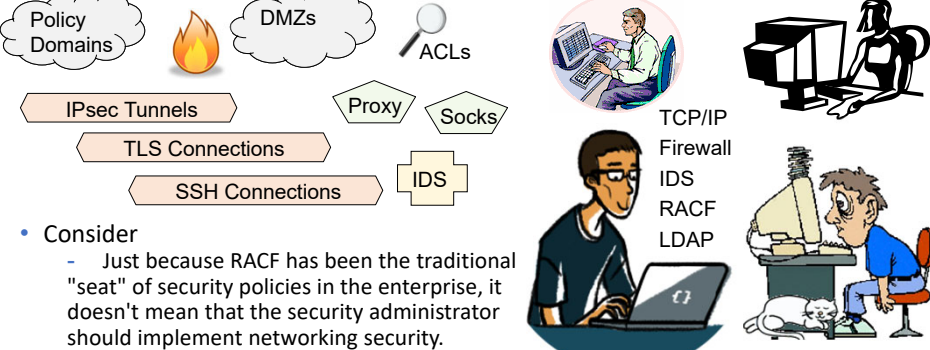
Cryptographic algorithms are regulated by ISO (International Standards Organization).

Other System z

- Selected Other Software Offerings:
 - z/OS Encryption Facility, Encryption Facility for IMS and DB2, etc.
 - OPTIM Data Privacy Solution
 - Rational APPScan
 - Tivoli Identity Management, etc.
 - Proventia Firewall for Linux on z
 - IBM zSecure
 - <https://www.ibm.com/security/mainframe-security/zsecure>

Cryptographic algorithms are regulated by ISO (International Standards Organization).

Best Practices: Security Teaming – Multiple Departments



- Consider
 - Just because RACF has been the traditional "seat" of security policies in the enterprise, it doesn't mean that the security administrator should implement networking security.
 - Requires TCP/IP knowledge.
 - Requires understanding of the IDS options and parameters that are meaningful for your environment.
 - Requires analysis of what the samples (Idif and xml) provide you and what you may want to change in them.
 - Advise the Firewall and the external IDS technical crew of all your findings.
 - Work with them to enhance their policies and rules.
 - Always use Internal IDS as a second or third line of defense.

001_ZCS301_Security_Intro © Copyright IBM Corporation 2023 Page 18

IPSec, IP Filtering, AT-TLS, and IDS need to be implemented by one or more persons knowledgeable in TCP/IP networking on the mainframe. At the very least, the lead implementer should be a "networker." However the skills required are complex, so it makes sense to include the other security implementers in the process. That includes

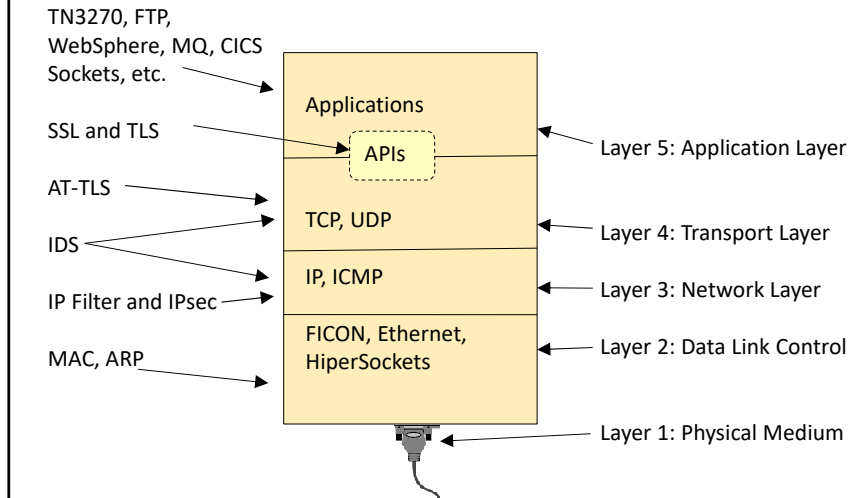
personnel with Firewall, outboard IDS, and RACF and LDAP experience, for example.

The TCP/IP person needs to understand what is and is not supported in the samples in order to make informed decisions about what to add, change, delete.

If not already in place, ensure that the system has more than this one "line of defense."

- Front-end production systems and networks with Firewall Filtering
- Front-end production systems and networks with other platforms offering Intrusion Detection Systems
- Implement SSL/TLS and/or IPSec where required
- Exploit application security controls where appropriate: exits, parameters, etc.

Security and Other Protocols in a TCP/IP Network



001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 19

Each level of any security architecture can implement security functions. For example, certain applications have implemented their own security by enabling calls to RACF, enabling Access Control Lists, specifying which data sets MUST be used, etc.

For example, many of the other layers of the TCP/IP stack implement the types of security that Policy Agent policies can exploit: SSL/TLS (AT-TLS), IDS, IPsec, IP Filtering, etc. It is possible at the DLC layer to invoke MAC filtering for the purposes of security.

One should not think of security only in terms of encryption -- there are many layers of security that can be implemented.

PHYSICAL: This is the actual hardware ... adapter and cabling ... that connects the TCP/IP node with the external network.

LINK: Layer 2 is the data link layer. This layer is also called simply the link layer. The actual protocols encompassed in the link layer are numerous, and the implementation details can be found in various documents throughout the Internet and in trade texts. The foremost data link layer protocol is the Ethernet protocol.

MAC: Ethernet designates the frame format and the speed of the data travelling over the physical network. However, there is still a need for controlling how individual hosts (workstations) attached to the physical network locate each other. The answer is the media access control (MAC) address. Every host connected to the network has a unique MAC address associated with its NIC.

ARP: The Address Resolution Protocol is a layer 2 protocol used to map MAC addresses to IP addresses. All hosts on a network are located by their IP address, but NICs do not have IP addresses, they have MAC addresses. ARP is the protocol used to associate the IP address to a MAC address.

IP: The most significant protocol at layer 3 (also called the network layer) is the Internet Protocol, or IP. IP is the standard for routing packets across interconnected networks -- hence, the name internet. It is an encapsulating protocol. The format of an IP packet is documented in RFC 791. The most significant aspect of the IP protocol is the addressing: every IP packet includes the IP source address (where the packet is coming from) and the IP destination address (where the packet is heading to).

ICMP: ICMP is actually a user of the IP protocol -- in other words, ICMP messages must be encapsulated within IP packets. ICMP is implemented as part of the IP layer. So ICMP processing can be viewed as occurring parallel to, or as part of, IP processing.

TRANSPORT LAYER: This layer deals with the actual delivery of a packet to an application.

Two protocols available at Layer 4: TCP and UDP. They know about the port numbers of applications they are to deliver data to.

TCP: TCP is always referred to as a connection-oriented protocol. What this entails is that prior to any communication occurring between two endpoints, a connection must be established. During the communications (which can last for seconds or for days) the state of the connection is continually tracked. And, when the connection is no longer needed, the connection must be ended.

UDP: A UDP header containing an IP address and a port number is wrapped around whatever data needs to be sent, and the packet is handed over to the IP layer. As long as the lower layers do their jobs correctly, the remote end should receive the datagram as expected. There are no acknowledgement counters and no connection states.

SOCKETS: The term socket in a TCP or UDP context fully describes the endpoint of a connection. The socket is consequently a combination of an IP address, a port number, and the protocol being used.

APPLICATIONS: Sitting above layer 4 are the applications. Applications are recognized by their port numbers. Port numbers are TCP's method of knowing which application should receive a packet. Applications can use either TCP or UDP to communicate.

Because of its inherent reliability, TCP tends to be used more often. Examples of applications running on z/OS using TCP include sendmail, Web servers, FTP and telnet. Applications using UDP on z/OS are Traceroute, and Enterprise Extender.

End of Topic



001_ZCS301_Security_Intro

© Copyright IBM Corporation 2023

Page 20