

Enterprise Security Architecture

Technology Components

The required security services to protect the state's information infrastructure will be discussed in this chapter as technical topics. They include:

- Identification** - the process of distinguishing one user from all others.
- Authentication** - the process of verifying the identity of the user.
- Authorization and access control** - the means of establishing and enforcing rights and privileges allowed to users.
- Administration** - the functions required to establish, manage, and maintain security.
- Audit** - the process of reviewing system activities that enables the reconstruction and examination of events to determine if proper procedures have been followed.
- Directory Services** - a database that provides a mechanism to inventory, administer, and access resources in the network.

Figure 12-3 shows the relationship between security services and the technologies required.

Authentication

Cryptography - A technology that scrambles data to prevent unauthorized individuals from reading the data. A cryptographic key is a sequence of numbers and characters used in scrambling and unscrambling the data.

Public Key / Private Key Cryptography - A cryptography technique that gives a user a 'public' key for others to communicate with the user, and a 'private' key which is used as a digital signature.

Public Key Certificate - An electronic document that contains a user's public key. It is made available to anyone wanting to verify a digital signature or communicate confidentially with a certified user.

Message Digest - A method to ensure information cannot be modified without detection. It is used in the digital signature process.

Digital Signature - A process by which a private key is used to scramble information. Since only the signer's public key is able to unscramble the information, this is considered sufficient proof of the signer's identity.

Public Key Infrastructure - The functions required to issue and manage the public key certificates needed for authentication.

Access control

The technology used to protect the enterprise from unauthorized internal and external access and ensure the integrity and confidentiality of information used by the enterprise includes:

Cryptography - A technology that scrambles data to prevent unauthorized individuals from reading the data. A cryptographic key is a sequence of numbers and characters used in scrambling and unscrambling the data.

Secret key cryptography - A cryptography technique which uses a single key for both scrambling and unscrambling data. Since only a single key is used both parties must share this secret.

Security protocols - Protocols are well-defined message formats that can be applied at useful places in a software or communications architecture. A protocol can be used at the application level and below. Where a protocol is applied has particular advantages and disadvantages.

Firewalls - A term used for software or devices used to control access from one network, usually external, to another internal network.

Virtual Private Networks - A technique to provide secured access from one network to another across an intervening untrusted network.

Administration

Security Policy Domains Security domains are areas within the enterprise, which adhere to a specific security policy and its enforcement. These could be administrative domains (such as departments) or resource-based (computing environments) or even geographic domains.

Sign-on Administration

Certificate Authority (CA) Public Key Certificates are used to authenticate users and establish non-repudiation of sender or recipients of information. A Certificate Authority (CA) performs the management of certificates in a Public Key Infrastructure.

Registration Authority Certificate Authorities are usually centralized and hierarchical. A typical centralization would be to have a CA for the enterprise, one or more CAs at a regional or state level and so on. Since individuals requiring certificates are local, the function of verifying the validity of a certificate request is often localized. This local function is referred to as a Registration Authority (RA).

Key Recovery/Escrow Information that is encrypted must be able to be recovered should the original encryptor's keys no longer be available. A key recovery or key escrow mechanism should be in place. Keys may need to be escrowed for future verification of digital signatures.

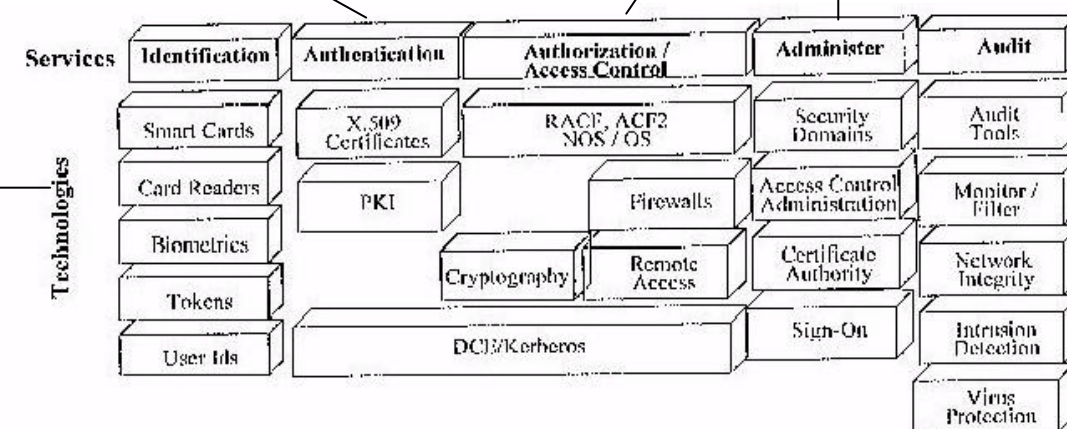
Standards

Identification

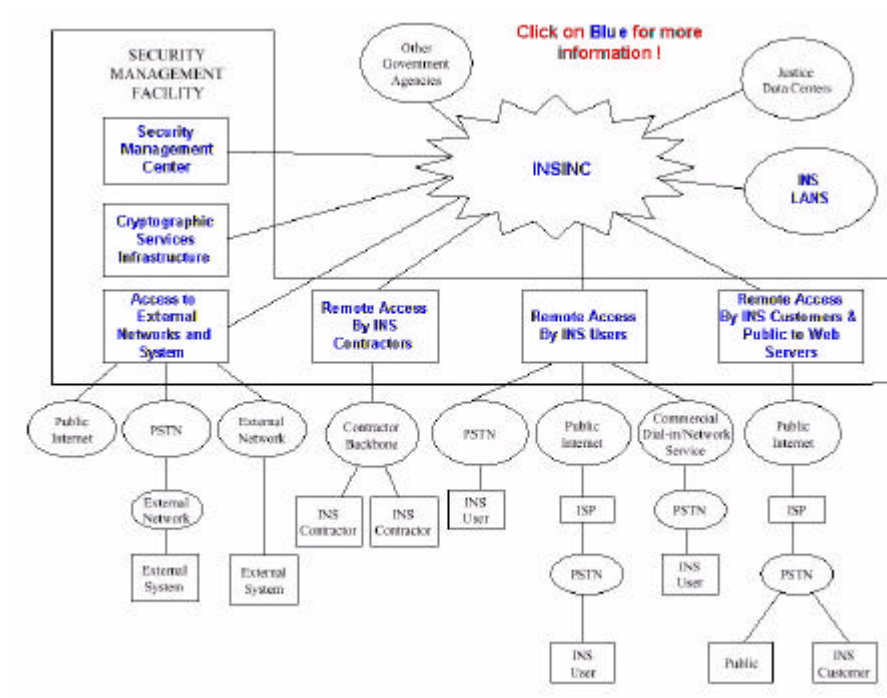
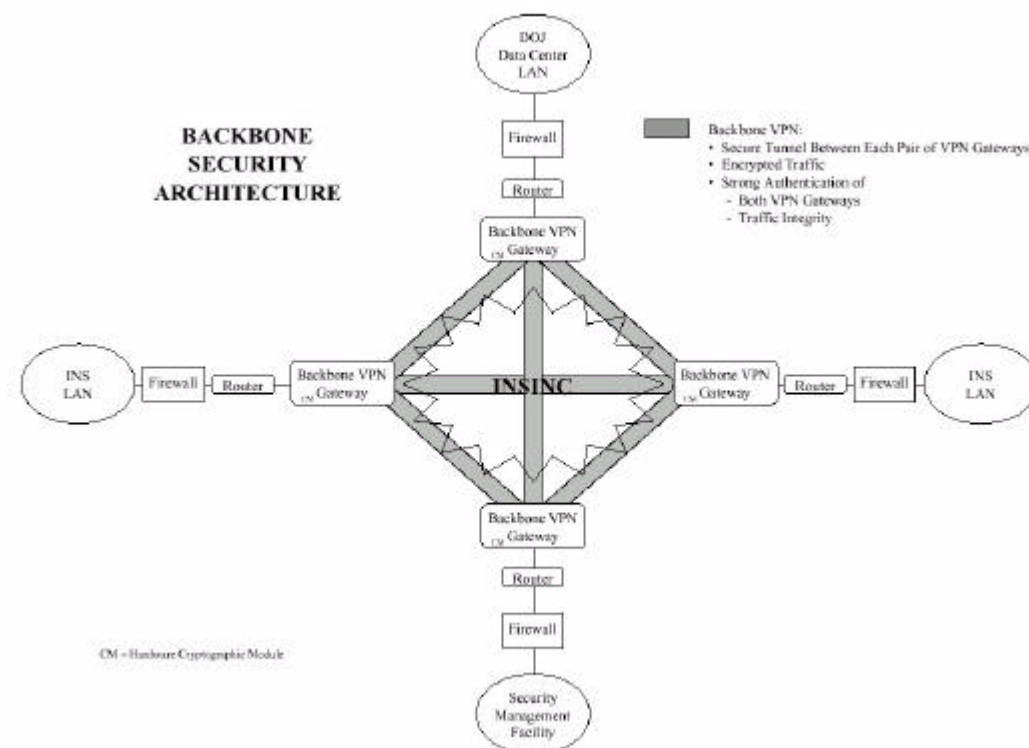
Userids User-ids and associated passwords for authentication are inexpensive and widely integrated into today's systems.

Proprietary Tokens Tokens are physical cards similar to credit cards that work in conjunction with a user id to identify a user to the system. T

Biometrics A biometric is a unique, measurable physical or behavioral characteristic of a human being for automatically recognizing or verifying identity. Biometric characteristics can include fingerprints, iris data, hand and face geometry, signature, voice and DNA.



Enterprise Architecture



Products

Security Domain Standards				
<i>Entries in Italics are suggestions for items missing or not yet identified.</i>				
COMPONENT	Obsolete	Transitional	Strategic	Research
Firewall				
Cisco PIX				
BorderManager				
Checkpoint				
Proxy				
WebTrack SMARTFILTER				
NZHR				
Admin Tools				
Intrusion				
ISS RealSecure				
Protocol Analysis				
NAI Sniffer Pro				
Scanning/Penetration				
ISS Internet Scanner				
LophCrack				
Lan/Wan Management				
Landesk				
Managewise				
ZenWorks				
Tivoli				
CA-Uncenter TNG				
Virus/Content Filtering				
Content Technologies MimeSweeper				
TrendMicro				

Enterprise Service Architecture	Technology Architecture			
	Security Architecture			
	SIDE	FSCM ND	DWGNQ	REV
	John Wu		SFEE	QF 13