What is Layered security

- **Layered security**, also known as **layered defense**, describes the practice of combining multiple mitigating security controls to protect resources and data.
- The term bears some similarity to defense in depth,
- A term adopted from a military strategy that involves multiple layers of defense that resist rapid penetration by an attacker but yield rather than exhaust themselves by too-rigid tactics.

What is Layered security(Contd…)

- Because potential Internet security risks can occur at a variety of levels, you need to set up security measures that provide multiple layers of defense against these risks.
- In general, when you connect to the Internet, you should not wonder if you will experience intrusion attempts or denial of service attacks.
- Instead, you should assume that you will experience a security problem.
- Consequently, your best defense is a thoughtful and proactive offense.

What is Layered security(Contd…)

- Using a layered approach when you plan your Internet security strategy ensures that an attacker who penetrates one layer of defense will be stopped by a subsequent layer.
- Your security strategy must include measures that provide protection across the following layers of the traditional network computing model.
- Generally, you need to plan your security from the most basic (system level security) through the most complex (transaction level security).

Customer Layered security

- Consumer(Application) level security measures control how users can interact with specific applications.
- In general, you must configure security settings for each application that you use.
- However, you need to take special care to set up security for those applications and services that you will use from or provide to the Internet.
- These applications and services are vulnerable to misuse by unauthorized users looking for a way to gain access to your network systems.
- The security measures that you use need to include both server-side and client-side security exposures.

Various consumer layered security strategies

- Extended validation (EV) SSL certificates
- Multifactor authentication (also sometimes known as versatile or two-factor authentication)
- Single sign-on (SSO)
- Fraud detection and risk-based authentication
- Transaction signing and encryption
- Secure Web and e-mail
- Open fraud intelligence network

Various consumer layered security strategies(contd...)

Extended Validation Certificate (EV)

- It is an X.509 public key certificate
- Issued according to a specific set of identity verification criteria.
- These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued.
- Certificates issued by a CA under the EV guidelines
- They are not structurally different from other certificates (and hence provide no stronger cryptography than other, cheaper certificates), but are designated with a CA-specific policy identifier so that EV-aware software can recognize them.

Various consumer layered security strategies(contd…)

- The criteria for issuing EV certificates are defined by the Guidelines for Extended Validation Certificates, currently (as of May 2012) at version 1.4
- The guidelines are produced by the CA/Browser Forum- a voluntary organization whose members include leading CAs and vendors of Internet software, as well as representatives from the legal and audit professions.
-

Multifactor authentication (versatile or two-factor authentication)

- Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction.
- The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network.
- It is an approach to authentication which requires the presentation of two or more of the three authentication factors:
  - a *knowledge* factor ("something the user *knows*"),
  - a *possession* factor ("something the user *has*"), and
  - an *inherence* factor ("something the user *is*").

Multifactor authentication (versatile or two-factor authentication) contd...

- Knowledge factors: "something the user knows"
  - 1 Password
  - 2 PIN
  - 3 Pattern
- Possession factors: "something the user has"
  - 1 Tokens with a display (disconnected tokens)
  - 2 Connected tokens
    - 2.1 USB tokens
    - 2.2 Smartcards
    - 2.3 Audio Port tokens
  - 3 One-time pads
  - 4 Mobile phones

- Inherence factors: "something the user is"
  - Biometrics

Single sign-on (SSO)

- **Single sign-on** (**SSO**) is a property of access control of multiple related, but independent software systems.
- With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.
- Conversely, **Single sign-off** is the property whereby a single action of signing out terminates access to multiple software systems.
- As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication.

Fraud detection and risk-based authentication

- Fraud detection would be a critical security layer
- Includes Risk-based Authentication as a mechanism for fraud detection
- Risk-based authentication is a technique that uses both contextual and historical user information, along with data supplied during Internet transaction, to assess the probability of whether a user interaction is authentic or not.

Fraud detection and risk-based authentication contd...

- Contextual information includes the username and password, who the user is, their IP addresses, location information, what kind of device they are using.
- Historical user data includes specific attributes provided from the session as well as user behavior and transaction patterns.
- This information represents an additional authentication factor that supplements the username and password, making this an enticing multifactor authentication technique.

Transaction signing and encryption

- Eliminating information piracy, data theft, etc. and ensuring security of information transmitted online is even more necessary as e-payments are fast becoming the norm than the exception.
- Example: A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Transaction signing and encryption contd...

- A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).
- Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Secure email & Web

- **Email security** includes a combination of email encryption, digital signatures, content monitoring and policy compliance capabilities that are automatic and invisible to everyday users.
- use of antivirus also helps in web & email security
- advanced threat dashboards, forensic reporting and data capture, sandbox analysis of malware, and data-aware defenses that provide containment of sensitive information.

Open fraud intelligence network

- Open Fraud Intelligence Network represents a powerful new weapon on fraud.
- by consolidating information from a variety of sources, including fraud patterns that have been experienced by leading global financial services organizations.
- The combination of fraud data and the ability to share fraud experiences promises to be a significant advancement in the way fraud can be detected and addressed.

Enterprise Layered Security Strategy

- Workstation application whitelisting
- Workstation system restore solution
- Workstation and network authentication
- File, disk and removable media encryption
- Remote access authentication
- Network folder encryption
- Secure boundary and end-to-end messaging
- Content control and policy-based encryption

Workstation application whitelisting

- Whitelisting-listing the allowed users
- Application Whitelisting is one of the latest tools offered to enhance your “Defense in Depth” security strategy.
- With increasing numbers of attempted intrusions, cautionary tales of security breaches and the potential for resulting damages at your site,
- Application Whitelisting can be an important addition to your security arsenal.

Authentication

Prove continuity in relationship

- Basis of trust
- Identification

Who you are (biometrics)

Physical authentication: where you are

What you have (tokens)

What you know

Password: snoopy1

Mother's maiden name: jones

Pets name: snoopy

Network Authentication

- Password
- One-time Passwords (ex. tokens)
- Network address
  - Caller-id - credit card
  - IP address
  - MAC address – banks
- Cryptographic protocols

File, disk and removable media encryption

- Develop and test appropriate a Data Recovery Plan
- Use compliant encryption algorithm and tools when creating a password, follow strong password requirements
- Do NOT use the same password from other systems.

File, disk and removable media encryption contd...

- Use a secure password management tool to store sensitive information such as passwords and recovery keys
  - Where passwords need to be shared with other users, ensure that passwords are sent separately from the encrypted file. E.g. call the person to verbally communicate the password.
  - Do NOT write down the password and store it at the same location as the storage media (e.g. post-it note with the password next to the encrypted USB drive)

File, disk and removable media encryption contd…

- After the covered data is copied to a removable media,
  - Verify that the removable media works by following instructions to read the encrypted covered data
  - If applicable, securely delete unencrypted covered data following secure deletion guidelines
- Removable media (e.g. CD, hard disks) should be labeled with the following information:
  - Title. For example "Project XYZ Data"
  - Data owner (researcher or research unit name)
  - Encryption date

File, disk and removable media encryption contd…

- When unattended, the removable media should be stored in a secured and locked location (e.g. cabinets, lock boxes, etc) where access is limited to users on a need-to-know basis.
- Document the physical location of removable media, along with the label information (specified above) for tracking and future reference.

Remote Access Authentication

- The ability to verify identity (authentication) is even more important for remote users than for those who are on-site
- Without a secure authentication scheme anyone could get into the network and view, copy, change or even destroy important data
- Remote access servers can be configured as dial-in servers or VPN servers. Dial-in servers use the Point-to-Point Protocol (PPP) or in the case of some older servers, the Serial Line Internet Protocol (SLIP) as the link layer protocol.

Remote Access Authentication contd...

- VPN servers can use the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), or IPSec tunnel mode to establish a secure "tunnel" over the Internet.
- Windows remote access servers support the following set of authentication methods:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft's implementation of CHAP (MS-CHAP)
  - Updated version of MS-CHAP (MS-CHAP2)
  - Extensible Authentication Protocol/Transport Layer Security (EAP/TLS)

Network folder encryption

- With PGP NetShare, organizations can protect their intellectual property and other sensitive information as required by partner and regulatory mandates for information security and privacy.
- Persistent File Encryption on Network ServersPGP NetShare Protected Files & Directories With PGP NetShare, authorized users can save and share files on file servers and use all applications as they currently do while benefiting from the comprehensive protection offered by PGP encryption.
- Content such as documents, spreadsheets, presentations, video, audio, and Web materials is automatically encrypted when saved to a PGP NetShare–protected folder.

- The end-to-end principle is the core architectural guideline of the Internet

Content control and policy-based encryption

- Policy-based Encryption service allow customers to set up filters based on the content of a message, if the message meets the set criteria it will be encrypted.
- Once signed up for this service, all messages sent from MS Exchange mailboxes to external recipients are processed according to configured policies and encrypted, if required.