Contents

Topic 1: Scenario

Authentication at Deposit Trust

Authentication
CSEC 630 – Module 4

Authentication at Deposit Trust
Deposit Trust's Cincinnati branch is one of the best-performing privately managed trust fund companies in the country. The branch boasts $400 million in assets and attracts an international clientele.

Deposit Trust takes customer confidentiality extremely seriously. To ensure that customer information is secure, the company has initiated a plan to implement the Federal Financial Institutions Examination Council's (FFIEC) *Authentication in an Internet Banking Environment* guidelines.

Ben Shilling, the CEO of this branch, has hired Harold Martin, an online banking security specialist, to help implement the guidelines.

The names and companies used in the scenario and throughout the rest of the module are fictitious; any similarities to actual individuals or companies are coincidental.

Scenario
The FFIEC guidelines mandate that financial organizations, including Deposit Trust, have a multifactor authentication system put in place for clients. The guidelines allow for complying entities to choose between types of authentication mechanisms, such as biometric systems and tokens.

Harold Martin decides to interview stakeholders at Deposit Trust to gain an understanding of the current authentication system.

Harold speaks with CEO Ben Shilling to gauge Deposit Trust's commitment to improving its authentication system.

The conversation between Harold Martin and Ben Shilling, the CEO of Deposit Trust, is reproduced below.

Harold: Hello, Ben! I requested this meeting to get your views on how the FFIEC guidelines will impact Deposit Trust's handling of authentication.

Ben: Harold, our employees, clients, and brokers face online threats every day. Implementing the FFIEC guidelines is a good opportunity for us to upgrade our current authentication processes to make them more secure.

Harold: What do you believe is the single biggest security challenge for Deposit Trust concerning authentication?

Ben: Well, Deposit Trust is an organization with over 300 employees. Most of our employees and even some of the brokers have to remember at least three or four different passwords.

Ben: Our clients, on the other hand, need to remember only one password, which makes it simple for them but also makes it fairly insecure.

Harold: Yes, that is something that organizations that deal with electronic transactions often find at odds.

Harold: Multiple passwords establish increased security because individual passwords can be cracked given enough time and effort, yet the users often find it difficult to remember all of them.

Ben: Exactly. I feel that almost any security system that depends on users to maintain security, such as with Deposit Trust's clients, is bound to fail.

Harold: That's true. In your opinion, is cost an important consideration in determining which authentication technology Deposit Trust should be using?

Ben: Not really. We have to consider how much it would cost us in terms of our reputation and liability if a data breach occurs.

Harold: You raise an excellent point.

Ben: Well, we constantly run the figures through a cost-benefit analysis, and found that it is almost always more cost-effective to have the necessary security controls in place than to risk compromising our sensitive data.

Harold: Excellent. Thank you, Ben.

After speaking with Ben, Harold Martin talks to Thomas Pence, Deposit Trust's chief information security officer, to get an idea of Deposit Trust's authentication requirements.

The conversation between Harold Martin and Thomas Pence is reproduced below.

Harold: Hello, Thomas. As you are aware, I have been hired to assist Deposit Trust select an appropriate authentication method. I believe I have some understanding of the current practices and controls, and I would like your perspective.

Thomas: Harold, I view this review process as an opportunity rather than a task; it will allow us to maintain up-to-date standards, which will ultimately result in direct benefits to our organization and our clients.

Harold: OK, so what authentication method is currently being used, and what are its critical requirements?

Thomas: Right now, we're very dependent on the use of passwords, which has proven to be relatively susceptible to hackers and not very secure.

Thomas: It also relies heavily on our users to follow the various password policies, and that has been a tough sell.

Thomas: What I envision is creating an authentication system and process that is both scalable and client-friendly.

Harold: How about two-factor authentication?

Thomas: I've heard conflicting views about two-factor authentication. I'm concerned that two-factor authentication may not be enough to meet our security requirements and in the end not justify its costs.

Next, Harold Martin speaks to Janice Pearce, a help desk supervisor with Deposit Trust, to understand the practical issues both internal and external users encounter with the company's existing authentication processes.

The conversation between Harold Martin and Janice Pearce is reproduced below.

Harold: Hi, Janice. I'm an information security consultant who has been hired to help Deposit Trust improve authentication processes. I understand you find that many employees and clients have problems with passwords?

Janice: Constantly! Passwords give us a lot of trouble. Looking at the statistics from our ticket system, I find that most of the issues we deal with are from clients who lose their passwords or get locked out of their accounts.

Harold: What is the usual procedure you follow when clients are locked out of their accounts? Can you give me an example?

Janice: Well, recently one of our clients called the help desk after being locked out for entering invalid passwords 10 times in a row within a five-minute timespan.

Janice: We asked for his account number and provided him a temporary password. After he logged in, he was prompted to change his password.

Harold: OK. So anyone who knows a client's account number can call the help desk, pretend to be that client, and ask for a password?

Janice: Well...yes, I suppose. We have no foolproof way to identify a client, so we send the temporary password to the e-mail address.

Harold: Thank you, Janice.

Topic 2: Module Introduction

Authentication is the process of validating a user's identity by asking users to provide proof that they are who they say they are. This occurs in at least one of three forms—by proving "something you know," "something you have," or "something you are." The number of electronic transactions is increasing, driving the need for strong identity verification measures.

In Deposit Trust's case, weak authentication created security vulnerabilities, eventually leading to increased IT costs, client frustration, and potential security violations. This module covers strong authentication methods, including multifactor authentication. The module also covers authentication strategies for enterprise security.

Topic 3: Enterprise Security and Authentication

Modern Enterprise Security

The enterprise security environment has evolved over the past few decades. Years ago, enterprise security was much less of a challenge—a network firewall provided enough security to prevent most unauthorized access into the enterprise network.

Today, enterprise networks need to comply with stringent regulations and requirements for protecting sensitive data. This is coinciding with the need to provide secure access to those authorized to access critical business applications. Extensive business travel yields increased telecommuting and employees attempting to access company assets from unsecure locations, such as wireless Internet connections from hotel rooms or coffee shops.

While firewalls still have an important place as an information-security control, they are just one of the many building blocks of enterprise security. For effective implementation of security, modern enterprises must use a layered approach.

Risk Involved in Using Simple Passwords
The most commonly used form of authentication employs issuing a set of user credentials, which are a username and a password. Users should employ strong passwords of eight characters in length or greater, containing a mix of lowercase and uppercase letters, numbers, and special characters. Many password-cracking tools are capable of performing brute-force, dictionary, and hybrid attacks, which can be used to crack simple passwords.

Attackers often use social engineering to get users to reveal their logon credentials, providing them with access to an enterprise network.

Here are some views about security risks by experts Peter Clifton and Anthony Bernadi.

Peter Clifton, CEO, RBNet, Inc.
Finding undocumented, unexploited vulnerabilities is a major threat to organizations, especially software vendors. It is a vendor's responsibility to issue a patch to fix such vulnerabilities quickly, so that end-users and corporations alike do not incur additional risk of exploitation.

Because it is not possible for vendors to anticipate all possible vulnerabilities, the mantra in the information security profession is that an attacker has to get it right once, while security teams need to get it right every time. Multifactor authentication adds complexity to the amount of layers an attacker must breach before gaining access to a network. Therefore, the reliance on password authentication should be only one level of defense.

Anthony Bernadi, Director, Product Marketing, NetSecure
The security market is flooded with products addressing different types of security issues. Enterprises often suffer from the fallacy of implement then evaluate, where they subscribe to putting a particular security tool into use before properly assessing the risks it poses on a corporate network. It is imperative that all security tools and software being used in an enterprise setting first be properly tested to ensure that their functionality falls within an acceptable risk level.

Topic 3: Enterprise Security and Authentication

Implementing a Layered Security Strategy

Introduction

To strengthen enterprise security, organizations should adopt a layered security approach, including multifactor authentication.

Strong authentication is a term used to describe applying two or more factors to validate someone's identity. This is usually used in conjunction with an enterprise access-management architecture to provide secure access to enterprise applications and data storage. Additional strength in the layered access-management approach comes from data segmentation, which classifies more sensitive data at a higher, more restricted accessibility level.

An investment bank has implemented a layered security strategy. The diagram depicts the layers of the bank's enterprise network. Each layer shows a specific resource of the bank.

Activity

Study the authentication credentials of each user group in the first column. Then, match the user group with the correct layer of security in the second column.

User Group Credentials	Resources
A. **Banking Customer** Two-factor authentication: user credentials and security tokens	1. Proprietary Corporate Research
B. **Payroll Manager** Two-factor authentication: user credentials and smart card RFID badge access	2. Enterprise Server
C. **Senior System Administrator** Two-factor authentication: user credentials and a biometric fingerprint scanner	3. Financial Transactions
D. **C-Level Executives** Three-factor authentication: user credentials, smart card RFID badge access, and a biometrics fingerprint scanner	4. Intranet Transaction

Correct Answer: A-3, B-4, C-2, D-1

Feedback:

You have matched the investments bank's users to the resources they can access based on their authentication credentials.

An organization that follows a layered identity strategy will ensure that its internal and external customers can access only what they are permitted to access. The layered identity strategy not only authenticates users, but adds complexity to attackers trying to access the network, remediating the risk of a data breach. Additional security controls can be put into place to aid in the authentication process, such as anomaly detection, prompting the user to provide additional information before being authenticated to the network.

For example, a bank can use transaction-security software for its customers' confidentiality, which keeps track of the behavioral patterns such as the geographical locations from which they log on, the types of computers they use, and the average frequency of logons within a particular time span. If a customer who usually logs on from the same PC in Seattle every day suddenly logs on from Romania, then an extra identity verification check may be required. Another approach is to restrict user access as users attempt to access more sensitive, restricted data and applications.

Therefore, as the user tries to access increasingly high-risk applications and systems, the level of authentication will increase correspondingly.

A layered identity strategy also ensures that users who hold crucial positions in the organization, such as senior system administrators and CFOs, need much stronger authentication.

Topic 3: Enterprise Security and Authentication

Enterprise Layered Security Strategy: Potential Weak Spots

Any identity validation strategy is only as effective as its enforcement. Any weakness in the system, such as the underlying protocols used, can be exploited by hackers or other malicious users. Therefore, organizations must be aware of these considerations when implementing a layered security approach.

The potential vulnerabilities in a layered identity validation continuum are listed below.

Initial Registration
Organizations must ensure their identity-registration and verification process is foolproof, as it is the premise for user trust. Only after identity verification has been accepted by the enterprise does authentication become significant.

For example, with respect to Deposit Trust, according to FFIEC guidance,

> "[C]ustomer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons."

Reference: FFIEC (2001, August 8). *Authentication in an Internet banking environment*. Retrieved from http://www.ffiec.gov/pdf/authentication_guidance.pdf

Identity Provisioning
A layered identity security system can be endangered if authentication and access controls are not properly configured. For example, when a manufacturing company issues building access to employees and vendors, it should ensure that vendors are not authenticated to enter employee-only areas.

Central Management Model
For an enterprise's layered security strategy to work, a centrally managed enterprise security system model is crucial. The system should have a policy that outlines proper use and the risk associated with each component in the system. It should also specify who can access these components, standard definitions, and contact information for asset owners.

Policy Enforcement
Policies are meaningless if employees are unaware of their existence and are not enforced. It is management's responsibility to ensure that end-users are aware of policies, are trained in how to properly adhere to policy, and to enforce the policy. A layered identity management strategy may prove to be ineffective if any of these established processes are interrupted.

End-to-End Audit

Finally, a good layered security management policy will build in an end-to-end audit of processes. This process includes soliciting feedback from the enterprise's systems and applications owners and stakeholders, as well as information from historical audits. Organizations can identify past mistakes and potential weak spots by performing audits. They can then incorporate appropriate changes in the process.

Integrated Physical and Logical Security

In most organizations, there is a lack of integration between physical security (systems that control physical access to premises and work areas) and logical security (systems that control access to IT resources). This lack of integration allows attackers to circumvent the holistic security of the system by exploiting one of the two components. For example, terminated employees should have their physical access to the premises restricted, and any access to the corporate network, including remote access, terminated as well.

Topic 4: Authentication Basics

Single Sign-On Authentication

In today's corporate environment, users require access to multiple resources to perform their routine job functions. To access each of these resources, users interact with a number of authentication mechanisms. Popular user-identity authentication mechanisms include multifactor authentication and single sign-on authentication.

Single sign-on (SSO) authentication helps to overcome the drawbacks of having to use and administer multiple logons for accessing multiple systems. SSO enables each employee to use a single username and password to access multiple accounts for systems and applications.

SSO makes password management much easier for a company's IT security team. However, it also exposes an organization to additional threats. If an intruder gains access to a user's credentials, the intruder can access all the systems for which that user has access rights.

Strong Authentication with SSO
SSO enables the user of a network to access all applications by using a single login. There are multiple advantages to this, including providing more user-friendly authentication since the user is not required to remember multiple passwords. Yet it is relatively secure since this typically requires the use of strong passwords.

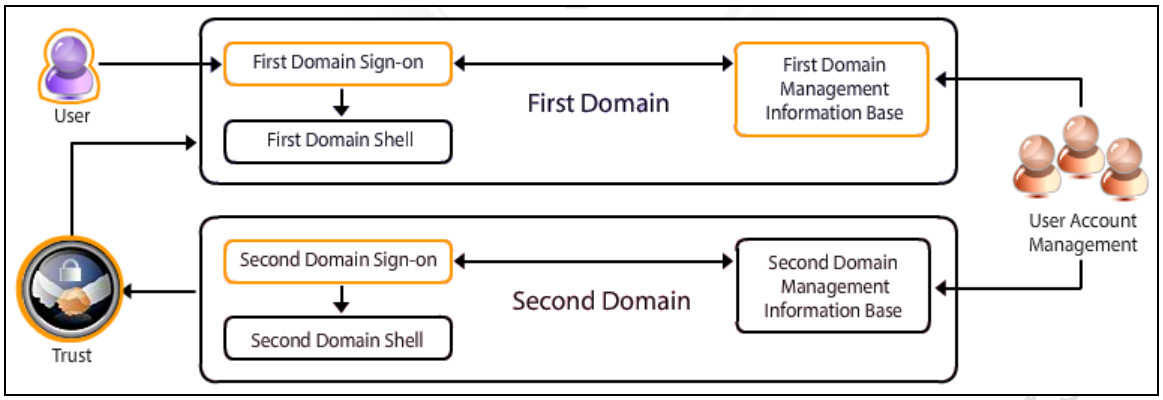
Another advantage for SSO is that it potentially reduces the amount of administration required when users forget passwords and need to have them reset.
SSO does require some preventative measures, such as instituting a session timeout policy based on user inactivity.

Reference: Imprivata. (2009). *A more secure front door: SSO and strong authentication.*

How SSO Works
Here is a brief overview of how SSO works.

User
Users need to sign in to a primary domain, such as Windows LDAP, for authentication.

First Domain Sign-On
After users have signed in, they can access other secondary domains, such as applications or resources, from the primary domain, such as Microsoft SQL server. Without SSO, each domain would otherwise require a unique set of user credentials to authenticate. This authentication establishes a trust relationship between applications and resources configured within the SSO implementation. When a user logs on to any SSO object, it becomes the primary domain, since all applications share the centralized user database.



First Domain Management Information Base
The user credentials authentication database is stored here. User passwords should be stored as hash values to preserve the integrity of this database in the event of a data breach.

Second Domain Sign-On
User credentials that have been provided during primary domain sign-on are used to establish access to secondary and tertiary domains.

Trust
Secondary domains trust the primary domain's authentication, so when a user attempts to access a secondary domain, the active logons within the primary domain are queried. If a user is not actively logged on to the primary domain, he or she will need to log on.

Try This Activity

Question: Identify the possible benefits to a large multi-location company of implementing SSO.

a. Increase in productivity and efficiency as employees do not have to remember multiple usernames and passwords while accessing different applications
b. Support for conventional authentication generally used by clients, such as Windows username and password
c. Reduction in IT costs due to lower number of IT help-desk calls regarding passwords
d. Security on all levels of entry, exit, and access to systems without the inconvenience of reprompting users
e. Centralized reporting

Correct options: All options are correct

Feedback:
The benefits of implementing SSO include an increase in productivity, support for conventional authentication methods, and reduction in IT costs. SSO also offers security on all levels of access to systems without the inconvenience of reprompting users.

However, SSO authentication is not suited for critical systems that need to be accessible at all times, such as shop-floor or security systems. In the event of failure of authentications systems, access to all systems unified under the SSO will shut down.

Topic 4: Authentication Basics

The Kerberos Authentication Protocol

Kerberos is a server-based protocol that runs as a service on Windows, UNIX, and most operating systems. Kerberos uses symmetric encryption keys or shared master keys to encrypt and decrypt messages.

Reference: Stallings, W. (2008). User authentication. In *Cryptography and Network Security*, 5th edition. Upper Saddle River, NY: Prentice Hall.

Kerberos-Based Authentication

Kerberos authentication uses the following:

- Clients requesting access to specific resources
- A key distribution center (KDC) that issues ticket granting tickets (TGTs)
- A ticket granting server (TGS) that issues service tickets

The KDC and the TGS are usually located on the same server and have access to the same database. The KDC is a trusted third-party arbitrator and a repository of its clients' secret master keys and authentication information. Each client in the KDC's domain has a secret master key that it shares only with the KDC. If a client wishes to communicate with another client in the same domain, it cannot do so without involving the KDC.

When a user logs on, an authentication request is sent to the KDC. The authentication server validates the identity of the user and sends a ticket encrypted with the user's master key.

If a user wants to communicate with another client or access another resource, it sends the initial ticket to the KDC. There are two types of tickets used by the Kerberos protocol: a ticket granting ticket (TGT) used to access the ticket granting service (TGS) and a service ticket used to access a service.

Kerberos Authentication Process

Here is an example of how the Kerberos authentication process works. Alice wants to open a file she is authorized to access from the company's network.

Step 1
Alice sends a request to the KDC for a ticket granting ticket (TGT).

Step 2
The KDC sends a TGT to Alice's computer.

Step 3
Alice decrypts the TGT with her password hash and sends it back to the KDC. She now requests a service ticket from the KDC.

Step 4
The KDC sends a service ticket to Alice.

Step 5

Alice sends her service ticket to the company's network services and requests authentication.

Step 6
Network services authenticates Alice and a client/server session is established.

Topic 4: Authentication Basics

Attacks on Kerberos: Replay Attacks

The KDC is the most critical component in the Kerberos authentication process because it has access to all shared master keys and authentication information of all the clients in the domain. Therefore, it is essential to ensure that the KDC is protected at all times.

Although Kerberos is considered to be more secure than simple password authentication, it, too, is vulnerable to various attacks, such as replay attacks.

Replay Attack
In a replay attack, tickets sent over a network can be hijacked or copied by "sniffing" specific packets that contain session information. These tickets can then be replayed at a later time. For example, Alice wants to access a shared file on Bob's computer. An intruder can intercept Alice's ticket when she accesses a file on Bob's computer and replay it.

Authenticator caching makes a replay attack slightly more difficult to execute. When users try to access a network, they need to authenticate themselves. Once the authentication is complete, the user session is cached until the user ends the session. However, if the user's PC is left unlocked, and a time out is not specified, then attackers can access the connection. Kerberos authenticators include time stamps so that authenticators are valid only for a short period.

If an attacker tries to replay a used authenticator and the authenticator's time stamp is off by more than the clock skew—usually set to a few minutes—the request is rejected.

However, authentication caching is not a foolproof protective mechanism for preventing replay attacks.

The security of Kerberos depends in large part on synchronized time, which in turn depends on the security of the time synchronization protocols used.

Example
Here is an example of how an attacker, Peter, executes a replay attack during Alice's communication with Bob.

Step 1
An attacker, Peter, copies the ticket that Alice's computer sends to Bob's computer.

Step 2
Peter takes Alice's computer off the network by using a denial of service (DoS) attack.

Step 3
Then, Peter impersonates Alice's computer's IP address and replays the ticket to access the folder on Bob's computer.

Solve This

Question: How can an information security officer prevent a replay attack on Bob's computer?

a. Reduce the maximum clock synchronization tolerance from the default setting of five minutes.
b. Maintain maximum clock synchronization tolerance.
c. Use cleartext for transmitting messages.

Reference: Microsoft Technet, Windows Server. (2003, March 28). Setting clock synchronization tolerance to prevent relay attacks. Retrieved from http://technet.microsoft.com/en-us/library/cc784130%28WS.10%29.aspx.

Correct Answer: Option a

Feedback:
A replay attack can be detected by comparing the current time on Bob's computer with the time stamp in the authenticator sent by Alice's computer. If the clock synchronization tolerance is low, the server will reject replayed messages for which time is off by more than the allowable time skew.

The maximum clock synchronization tolerance is usually five minutes. However, the time span may be too long in some cases to prevent replay attacks. Therefore, maintaining maximum clock synchronization tolerance is not a good idea.

Sending messages in cleartext makes them more susceptible to interception.

Topic 4: Authentication Basics

Password-Stealing Attacks

The secrecy of a user's session, tickets, and keys are essential to the security of Kerberos. Password stealing occurs in either an offline attack or an online attack. If an intruder can get hold of a user's encrypted credentials, then he or she can attack it offline. Otherwise, an intruder must attack a system in real time. Attackers can use brute-force attacks, dictionary attacks, or hybrid attacks to decrypt session keys.

Kerberos version 4 had serious protocol flaws that allowed unauthenticated requests to access a user's encrypted credentials. To mitigate these flaws, Kerberos 5 introduced the preauthentication option. This option allows the client to encrypt the current time with its secret key. Other advantages of Kerberos version 5 include support for strong encryption, extensibility, and better cross-vendor interoperability.

Example
Here is an example of how a password attack can be executed.

Step 1
An attacker, Peter, monitors the traffic between Alice's computer and the KDC.

Step 2
Then, Peter performs a dictionary attack to find a valid password.

Step 3
Peter can also run a brute-force attack to decrypt the session key.

Solve This

Question: How can an information security officer prevent a password-stealing attack on Bob's computer?
a. Ensure that users employ simple passwords to enable easy recall.
b. Employ passive network monitoring.
c. Encrypt the network traffic.

Correct Answer: Option c

Feedback:
Encrypting network traffic helps prevent password-stealing attacks.

Attackers steal passwords by passively observing the network traffic between the target computer and the Kerberos KDC. Therefore, passively monitoring the network will not help detect attackers. In addition, setting simple password requirements makes passwords easier to crack using dictionary and brute-force attacks.

Topic 5: 802.1X Authentication

802.1X Network Authentication

Another area of concern for organizations is the security of wireless local area networks (LANs).

802.1X is a standard used to authenticate users or devices before allowing them to access wired and wireless networks. 802.1X protects networks by not allowing computers to join wireless networks without presenting valid credentials.

In the case of wired networks, if a user tries to connect a computer to an Ethernet network, the Ethernet switch will require the computer to authenticate to the network. The network will allow traffic to flow between the network and the client computer only if the authentication requirements are met.

Organizations can centrally control both wired and wireless access to their network by combining 802.1X authentication with a Remote Authentication Dial-In User Service (RADIUS)-equipped server. As a result, if an attacker manages to get access to an organization's internal network, he or she will be prevented from connecting to an Ethernet port.

802.1X authentication can be used to restrict access to a wired network and apply user-specific bandwidth.

Network Access
Step 1
When a computer tries to connect to a network, the network switch detects the connection. Then, the switch initiates the authentication process.

Step 2
The switch sends an authentication request to the configured RADIUS server.

Step 3
The switch uses the server's response to determine whether the computer should be given access to resources, such as the private intranet, or another virtual LAN.

Applying User-Specific Bandwidth
Step 1
802.1X can be used to apply user-specific bandwidth or quality of service (QoS) policies. These policies are used for the classification and queuing of high-priority traffic.

Step 2
The user's computer tries to connect to an available Ethernet port.

Step 3
The 802.1X switch starts authentication by passing the computer's request to the RADIUS server.

Step 4
The RADIUS server authenticates the computer that is trying to access the Ethernet port and sends a message to the switch.

Step 5
The 802.1X switch allows Intranet access to the Ethernet port and enforces required restrictions or QoS policies.

Topic 6: Secure Sockets Layer

Secure Sockets Layer Overview

Kerberos is a protocol that establishes authentication, whereas Secure Sockets Layer (SSL) is a security protocol based on public key cryptography that provides secure transmission of data.

SSL can be used with the HTTP Web protocol, FTP protocol, and the SMTP e-mail protocol. SSL creates an encrypted link between a Web server and a client's Web browser to ensure that all the data passed between the two is in obfuscated ciphertext. This protects the integrity of data from interception during transit.

During an SSL session, the data transmission will remain encrypted until the session is terminated by either the client or the server. Connection termination occurs through an agreed-upon termination, as in the case of an FIN command, or by the server sending an RST command. Before engaging in a session, the client and server must perform a three-way handshake, called an SSL handshake, to establish trust between parties.

Topic 6: Secure Sockets Layer

Transport Layer Security

The next evolution of the SSL protocol is the Transport Layer Security (TLS) protocol.

Introduction to Transport Layer Security
The TLS protocol is used to protect data in transit. SSL connections begin with security and proceed directly to secured communications.

With TLS, the initial "Hello" connection request is not secured. The TLS protocol requires a completed handshake between client and server before it enters secure mode. Therefore, if the handshake process is not completed, a connection is never established.

TLS uses symmetric encryption and a message authentication code (MAC) to ensure reliability of data.

During the three-way handshake, the client and server agree on acceptable parameters for the transmission. Upon establishing a connection, a client machine presents a list of ciphers it supports; the server then chooses the strongest cipher and hash function to use and informs the client of its decision.

The server sends its digital certificate to prove its identity. In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key and sends the result to the server. The server uses its private key to decrypt the message, using the random number to exchange key material during the transmission.

Transport Layer Security Handshake
Step 1
Consider the example of Hannah Avery, who wants to use her bank's online service to transfer money. In the first step, Hannah's client computer sends a ClientHello message specifying the highest TLS protocol version it supports.

The client computer also sends a random number, a list of suggested cipher settings, and compression methods.

Step 2
The bank's server responds with a ServerHello message to the client. The message contains the chosen protocol version, a random number, cipher settings, and compression method from the choices offered by Hannah's computer.

Step 3
The bank's server sends its certificate message to the client. However, the server may omit this step, depending on the selected cipher settings. The bank's server then uses a CertificateRequest message to ask for a certificate from the client so that the connection can be mutually authenticated.

Step 4
The bank's server sends a ServerHelloDone message, indicating that its part of the handshake negotiation is over.

Step 5
The client then sends a Certificate message to the bank's server, which contains the client's certificate. The computer sends a ClientKeyExchange message, which may contain an encrypted premaster secret, public key, or nothing at all. This depends on the cipher that has been selected. The public key of the server certificate is used to encrypt the premaster secret.

Step 6
The client computer sends a CertificateVerify message to the bank's server. This message can be verified by using the public key embedded in the computer's certificate. The verification lets the bank's server know that Hannah's computer has access to the private key of the certificate and therefore owns the certificate.

Step 7
The client and the bank's server then employ the random numbers and premaster secret to create a shared secret, referred to as the master secret.

Step 8
Hannah's client computer now sends a ChangeCipherSpec record to the bank's server. This communicates that everything the computer now sends will be authenticated and encrypted, if encryption was negotiated.

Step 9
Finally, the client sends an encrypted Finished message that contains a hash and MAC over the handshake messages sent earlier.

The server tries to decrypt the computer's Finished message and verify the hash and MAC contained in the message.

In the event that the decryption or verification fails, the handshake will fail and the connection will be broken.

Step 10
In this step, the server sends a ChangeCipherSpec to Hannah's computer. This message indicates that any information the server sends to the client will be authenticated or encrypted, if encryption was part of the negotiation. Then, the server sends its own encrypted Finished message.

Step 11
Hannah's computer performs the same decryption and verification that the server had performed earlier with the computer's Finished message. At this point, the TLS handshake is considered complete and the application protocol is enabled.

After this, application messages exchanged between Hannah's computer and the bank's server will also be encrypted as the Finished message was.

Topic 7: Multifactor Authentication

Multifactor Authentication Overview

Often, passwords alone do not provide adequate protection. One way of strengthening security is to deploy more than one authentication method before users are allowed to access a system. The process of using more than one means of authentication for added security is known as multifactor or strong authentication.

The most commonly used form of multifactor authentication is two-factor authentication, in which a combination of two separate security elements are used in tandem before access is granted.

In general, authentication is based on three factor types:

- Type 1: “Something you know”
- Type 2: “Something you have”
- Type 3: “Something you are”

For organizations that need to guard mission-critical data, additional factors should be evaluated.

Two-Factor Authentication
Three-factor authentication combines three security elements before allowing access to an asset. Security elements may include a password, authentication tokens or digital certificates, and physical characteristics such as fingerprints. A three-factor authentication is useful in safeguarding extremely sensitive information such as a confidential customer data.

An extra layer of authentication can prevent unauthorized access to data.

Three-Factor Authentication
Three-factor authentication combines three security elements before allowing access to an asset. Security elements may include a password, authentication tokens or digital certificates, and physical characteristics such as fingerprints. A three-factor authentication is useful in safeguarding extremely sensitive information such as confidential customer data.

The use of three factors can drastically reduce incidents involving phishing, Trojan attacks, and identity theft.

Topic 7: Multifactor Authentication

Security Tokens

Security tokens are a commonly used multifactor authentication mechanism. A token is a piece of hardware or a physical device that generates one-time security passwords composed of strings of random numbers and characters, set to sync with the server. Tokens are typically set to expire in one minute, so if the password is not entered in that time, a new password will be generated by the token. It is important that passwords are completely random to ensure the security of this method.

Scenario 1: How Do Security Tokens Work?
Take the example of Hannah Avery, who wants to access her Internet banking account to pay her bills. Hannah's bank uses a two-factor authentication mechanism. To access her account, Hannah requires a username and password, and a unique security code generated by a security token provided by the bank.

Step 1
Hannah clicks on her banking Web page and enters her username and password.

Step 2
Hannah then clicks the button on her security device. A six-digit number appears on the screen of the device. The numbers on the device randomly change about every minute. They are generated by a mathematical algorithm that is known only to the bank's server.

Step 3
Hannah types the random number generated by the security device in the security code field.

Step 4
The information Hannah enters is encrypted and sent to the bank's validation server. If the password is correct and the number from the security device matches the number on the device, which is synced with the bank's server, Hannah will be authenticated. Hannah can then access her bank account online.

Analyze This Scenario

Security tokens provide much stronger authentication than traditional passwords. Unlike passwords that are changed every 60 to 90 days or on the discretion of users, a security token's one-time password changes every minute or so, providing much higher security.

In addition, security tokens are preprogrammed for use and are made to be tamper-proof.

Scenario 2: Security Token Weaknesses
While security tokens go a long way in providing online security, they are not foolproof. There are many points in the process at which security can be compromised. Take the example of Erica Gomez, who has just been hired by a construction company, Niall & Co.

Step 1
At the time of joining the company, Erica is asked to fill out forms with her personal information and to provide proof of identity.

Step 2
Niall & Co.'s HR department accepts Erica's identity information and enters it into the company's systems. The HR department provides Erica with authentication mechanisms, such as a username, a temporary password, and a security token. In addition, the HR department asks the IT department to generate a digital certificate for Erica and e-mail it to her.

Step 3
Erica sometimes logs on to the office network from coffee shops and public libraries. She always carries her security token in her purse.

Analyze This Scenario
Based on the entire sequence of events described above, identify two weak links where Niall & Co.'s security could be compromised.

Correct answer: Steps 1 and 3

Feedback:
The authentication process at Niall & Co. depends entirely on the identity-validation details Erica provided. If Erica gave false identity information, then she would still be positively authenticated because the information was not double-checked. In this case, authentication is not enough. Niall & Co. should have run a background check on Erica before issuing authentication mechanisms.

The other weak link arises from Erica's use of the authentication mechanisms. She accesses the company's systems from public computers and over unsecured networks. A person who obtains her username and password and steals her security device would be able to gain unauthorized access to the company's systems.

Scenario 3: Cost Associated with Security Tokens
Security tokens have costs associated with them, including the cost of the physical tokens, the infrastructure to manage tokens, the software, and the cost of personnel to handle any security token issues and management. One such management issue is token distribution, which involves determining who gets a security token and ensuring that tokens are returned by employees upon termination.

Topic 7: Multifactor Authentication

Smart Cards

Many organizations use smart cards to provide multifactor authentication mechanisms. A smart card differs from a computer memory card in that it can read, store, and process data. They can be created with programmable magnetic strips to allow the user to swipe the card for access.

References: Smart Card Alliance. (2004). Logical access security: The role of smart cards in strong authentication. Retrieved from http://www.library.ca.gov/crb/rfidap/docs/SCA Smart_Cards_and_Logical_Access_Report.pdf

Imprivata. (2009). *A more secure front door: SSO and strong authentication*.

Smart Cards
Smart cards are designed to support a variety of authentication approaches, including one-time passwords, public key infrastructure certificates, generation of key pairs, and biometric technologies. A smart card is often combined with one or more authentication techniques as part of a two-factor or multifactor approach to provide stronger security. Smart cards provide the capability to include all the required authentication factors, thereby ensuring the security and privacy of the authentication process.

Frequently, companies issue smart cards that can be used not only for access control, but also to digitally sign e-mail messages, files, or other content to prove authenticity.

Passive Proximity Cards
Passive proximity cards provide authentication information using radio frequency (RF) technology. The proximity technology is very flexible and can be embedded in electronic badges and other types of electronic access devices. These cards do not have a battery or active power source.

Active Proximity Cards
Active proximity cards, sometimes thicker than the passive cards, are equipped with a wireless transceiver typically attached to a user that maintains constant communications with a paired device connected to a workstation or other computing device. Such cards are useful in maintaining security when a user temporarily leaves a computer or workstation. Whenever the communications link is interrupted, the user device is locked.

Topic 7: Multifactor Authentication

Biometrics

Identity theft and data fraud are huge security challenges for organizations around the world. With the increase in online financial transactions, identity theft is also on the rise. Even as organizations step up efforts to mitigate security threats, criminals find new ways of breaching security.

Because identity theft is so prevalent and breaches are occurring at a higher frequency, organizations are gravitating toward increased use of multifactor authentication mechanisms. Biometrics is an attractive option because it offers a way of uniquely identifying individuals based on physical and behavioral traits that do not change.

Biometric devices are designed to provide authentication by verifying a unique physiological or behavioral characteristic that belongs to the user.

How Fingerprint Biometrics Works

A biometric fingerprint identity authentication system determines whether the scanned fingerprints match that of a user. System components include acquisition, template representation, the extraction of features, and the matching process. The matching process defines a metric of the similarity between that of a stored fingerprint representation of the user.

Reference: Jain, A., Hong, L., Pankanti, S., & Bolle, R. (1997*).* An identity-authentication system using fingerprints. Retrieved from http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf

Finger Biometric Devices

Finger biometric devices are appearing in a growing range of forms, from scanners and area readers to USB devices, and built into laptops, PCs, and mobile phones. As the reliability of these devices increases and their cost declines, more organizations are expected to adopt finger biometrics as an effective, affordable, and easy-to-use form of strong authentication.

Fingerprint Verification

Fingerprint verification is one mode of fingerprint authentication and matches the fingerprint to the user after the user has provided a username, thereby establishing a one-to-one match.

Fingerprint Identification

The second mode of fingerprint authentication, known as fingerprint identification, tends to be more appealing because of its simplicity. The user presents a finger and is authenticated, which is considered a one-to-many match. Fingerprint identification offers a much more streamlined workflow for the user and is generally better received.

Topic 7: Multifactor Authentication

Evaluating Biometrics

Biometric authentication is a physical access control based on “something you are”— a physical or behavioral characteristic. It is used to validate identity by performing a one-to-one database search for matching records. The database that stores biometric images is referred to as a corpus.

Most biometric authentication methods can help prevent unauthorized access to corporate information systems. There are, however, other aspects to consider, including the specific benefits of each method for users, IT departments, ease of implementation and acceptance, and regulatory compliance, as well as purchase and deployment costs.

Before selecting biometrics as an authentication mechanism, organizations should consider various factors and performance measures.

Evaluation Factors
In evaluating a biometric system, three factors must be considered.

Enrollment Time
Enrollment time is the time it takes the system to enroll someone by evaluating the samples provided. An acceptable time is two minutes or less.

Throughput Rate
The throughput rate refers to the rate at which people, once enrolled in the system, can be processed, identified, and eventually authenticated. An acceptable rate is 10 persons per minute.

Acceptability
Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, changes in retinal patterns can reveal private health-related information, such as the onset of diabetes or high blood pressure.

Biometrics Performance Measures
There are three main performance measures involved with biometrics authentication, which must be considered before choosing which system should be put into place in an organization.

Type 1 Error
Type 1 error is the false rejection rate (FRR). The FRR is the percentage of valid subjects that are falsely rejected, such as someone who should have been authenticated but was not granted access. If sensitivity levels are increased within the biometric reader, the FRR increases. An example of this might be a voice-recognition reader trying to identify someone who has laryngitis.

Type 2 Error
Type 2 error is the false acceptance rate (FAR). Unlike the FRR, the FAR is the percentage of invalid persons that are falsely accepted, such as someone who should not be granted access to the system but is authenticated anyway.

Biometric systems can operate in one sensitivity setting at a time, so that when system sensitivity is set to minimize false acceptance, closely matching data will be rejected, and the false rejection rate will go up significantly. Conversely, when system sensitivity is set to minimize false rejects, the false acceptance rate will go up. It is impossible to minimize false acceptance rates and false rejection rates simultaneously.

Crossover Error Rate
The final performance measure is the crossover error rate (CER). CER is considered the most important measure in biometrics because it is fair and impartial in comparing the performance of the various systems. CER, also known as equal error rate (EER), is the rate at which both accept and reject errors are equal.

In general, the sensitivity setting that produces equal error will be close to the setting that will be optimal for field operation of the system. A biometric system that delivers a CER of 2 percent will be more accurate than a system with a CER of 5 percent.

Reference: CISSP Open Study Guide. (n.d.). Characteristics of biometric systems. Retrieved from http://www.ccert.edu.cn/education/cissp/hism/039-041.html

Topic 7: Multifactor Authentication

Selecting Strong Authentication Methods

In addition to considering an organization's unique security requirements, it is important to weigh the benefits and costs of various strong authentication choices.

Cost
When considering total cost of ownership, there are two primary considerations: the initial cost and the operating cost. It is also important to consider the types of incremental costs with adding users to expanding the authentication model to other aspects of the organization's enterprise.

Usability
Authentication methods should be as transparent as possible and not negatively affect the way users are able to carry out their jobs.

Manageability
The application of authentication along with the management of user accounts and the monitoring of their use plays an important part in the overall security of information resources. The authentication method should provide centralized management along with advanced capabilities including tracking events, auditing, and reporting capabilities.

Flexibility
Where there are differing requirements, an organization may deploy alternative authentication methods. The authentication method should be capable of addressing multiple functional requirements while also matching the risk profile of user groups.

Integration
The authentication mechanism should be capable of integrating with existing enterprise applications such as single sign-on (SSO), virtual private network (VPN), Internet protocol security (IPsec) and public key infrastructure (PKI) authentication, and Remote Authentication Dial-In User Process (RADIUS).

Topic 7: Multifactor Authentication

Follow-Up on Deposit Trust

Introduction
After analyzing Deposit Trust's authentication processes, Harold Martin realizes the company's online security depends entirely on customers protecting their own passwords. He recognizes that for Deposit Trust to comply with the FFIEC guidelines, the company needs to adopt a strong authentication approach.

Harold wants to add a second layer of authentication—for Deposit Trust's retail customers—that balances security, cost, and user acceptability.

In addition, Harold wants to provide secure authorized access to critical information and applications to employees and partners from different locations. Harold needs a solution that will allow different users to access the bank's systems with different levels of authentication.

Workspace
Authentication Options
Harold has identified authentication options Deposit Trust can deploy.

Security Tokens

Advantages	Disadvantages
• Reduce risks associated with ordinary passwords • Offer security codes that change every 60 seconds • Are usually tamper-proof	• Come with high management costs • Can be stolen by attackers who can masquerade as the user if they have the user's ID and password • Need to be physically issued to users • Increases burden on staff to deal with replacing lost tokens

Biometrics

Advantages	Disadvantages
• Based on unique characteristics of individuals • Cannot be duplicated or shared because the biometric used is an intrinsic part of an individual	• Relatively expensive compared to other authentication methods • Cannot be erased or replaced if compromised or stolen • Can be invasive

Smart Cards

Advantages	Disadvantages
• Can perform multiple functions	• May require a special reader • Prone to damage and may need to be replaced often • Unencrypted, making it easy to read information from the card

Digital Certificates

Advantages	Disadvantages
• Validate user identity and are signed by a trusted party • Can be stored on computers, USB, and smart cards	• Require a PKI infrastructure • Have high support costs

Activity 1: Selecting Multifactor Authentication

Question: Harold has identified four crucial criteria for selecting an authentication mechanism for Deposit Trust: user acceptability, operational management time, security, and total costs.

Based on these criteria, select the most suitable authentication mechanism for Deposit Trust.

a. Security tokens
b. Digital certificates
c. Biometrics
d. Smart cards

Correct answer: Option a

Feedback:
A security token provides comparatively high security and higher user acceptability. The cost of deploying tokens is also not high. On the other hand, security tokens can be stolen and can increase the burden on support staff who handle token replacement.

However, Deposit Trust's fundamental problem is the lack of a second layer of authentication. Biometrics is not a sufficient solution because there is no way to validate biometrics in an online setting. Smart cards may require a physical reader, so they, too, are not a good solution. Digital certificates are one way to integrate security online; however, the chance of forgery would be much higher with digital certificates than with security tokens, which use a random number generator.

Security tokens are the most suitable option for Deposit Trust.

Activity 2: Authentication Solutions

Question 1: An employee of Deposit Trust logs on to the bank's network in the morning. Select an appropriate authentication mechanism to allow the user to complete this task.
a. Password
b. Digital certificate
c. Security token
d. Biometrics

Correct answer: Option a

Feedback:
In this case, a password would serve as the second layer of authentication since employees usually require a RFID badge to gain access to corporate premises.

Because the user needs only generalized access to the enterprise portal, a password would be a good enough authentication mechanism for this task.

Question 2: One of Deposit Trust's vendors offers business-consulting services in areas such as risk and trading. The vendor needs to access some generic company data while putting together a report for Deposit Trust.

The company allows access to its systems to vendors only from its corporate premises, where the vendors are provided with RFID badges. Deposit Trust wants to ensure that vendors have limited access to their systems. Select an appropriate authentication mechanism for this situation.
a. Digital certificates
b. Security tokens
c. Biometrics
d. Username and password

Correct answer: Option d

Feedback:
The company already has a first layer of authentication in place for vendors in the form of RFID badges. In this case, a username and password would be sufficient for the vendor to complete the task.

Review
After studying various options, Harold Martin has recommended an authentication solution for Deposit Trust's online operations.

Based on cost, risk, and user acceptability, Harold has recommended using security tokens as a stronger form of authentication that complies with FFIEC guidelines for secure online transactions.

Customers of Deposit Trust will now need to use both passwords and security tokens to complete online transactions.

Further Challenges
Create a report that addresses the following questions:

1. Should versatile authentication—being able to change authentication mechanisms—be employed, and if so, where?

2. Could there be some approaches of two- and three-factor authentication that do not rely on seeds and secret algorithms?

3. Which authentication methods are suited for simpler approaches, such as using soft tokens?

4. Why is it critical to build flexibility when investing in authentication?

Reference: Kuppinger, M. (2010, November 3). Versatile authentication—break-through for mass adoption of strong authentication [Blog post]. Retrieved from http://blogs.kuppingercole.com/kuppinger/2010/03/11/versatile-authentication-break-through-for-mass-adoption-of-strong-authentication/?eont2=museo

Topic 8: Summary

We have come to the end of Module 4. The key concepts covered in this module are listed below.

- Organizations can use the single sign-on (SSO) authentication system to enable users to log on only once to access multiple, related, and independent software systems.
- Kerberos is a server-based protocol that provides secure authentication. It has been implemented within multiple operating systems, most notably Windows.
- Secure Sockets Layer (SSL) is a standard security protocol based on public key encryption. SSL creates an encrypted session between a client and a server. SSL can be used in conjunction with the HTTP, FTP, and SMTP protocols.
- Transport Layer Security (TLS) is the next evolution of SSL, which improves upon some of its predecessor's weaknesses.
- Authentication is based on three factor types: something you know, something you have, and something you are.
- Multifactor authentication is the process of using more than one means of authentication for added security. The most commonly used form of multifactor authentication is two-factor authentication.
- Two-factor authentication involves combining something a user knows, such as a password, along with something a user has, such as a security token, smart card, digital certificate, retinal scan, facial scan, voice print, iris scan, fingerprint, palm scan, or hand geometry.

Glossary

Term	Definition
Authentication	Authentication is the process of verifying the identity of an individual.
Authenticator Caching	When a user is authenticated to access a network, the session is cached until the user ends the session. This process is known as authenticator caching.
Biometrics	Biometrics is the science of identifying unique physical and behavioral traits of individuals. Biometric techniques include facial recognition, voice recognition, fingerprinting, iris recognition, and retinal scanning.
Digital Certificates	Digital certificates are pieces of software that are digitally signed by a trusted certification authority. Digital certificates are used to authenticate users during online transactions.
Federal Financial Institutions Examination Council (FFIEC)	The FFIEC is an interagency group that provides guidelines, principles, and standards for U.S. banking institutions.
Kab	In the Kerberos protocol, Kab refers to a secret key that will be shared between the client and the server so they can securely communicate.
Kerberos	Kerberos is a server-based protocol that provides secure authentication over open Windows, UNIX, and Macintosh networks. Kerberos uses symmetric encryption keys or shared master keys to decrypt and encrypt messages.
Key Distribution Center (KDC)	The KDC is a trusted third-party arbitrator and a repository of its clients' secret master keys and authentication information.
Multifactor Authentication	The process of using more than one means of authentication for added security is known as multifactor authentication.
Public Key Infrastructure (PKI)	A PKI offers secure message exchange based on public key cryptography.
Quality of Service (QoS)	QoS is the process for classifying and queuing high-priority traffic. This requirement varies on a case-by-case basis.
Ticket Granting Server (TGS)	A TGS is a component of a KDC that sends encrypted keys known as tickets to a client.
Token	A token is a piece of hardware or a physical device that generates one-time security passwords composed of random numbers.
Transport Layer Security (TLS)	TLS is a security and authentication protocol used in Web servers and browsers. It is similar to the Secure Sockets Layer protocol.

Term	Definition
Two-Factor Authentication	Two-factor authentication involves combining something a user knows, such as a password, along with something a user has, such as a security token.
Secure Sockets Layer (SSL)	SSL is a standard security protocol that creates an encrypted link between a Web server and a Web browser to secure all data that passes between a Web site and a customer.
Single Sign-On (SSO) Authentication	The SSO authentication method enables users to log on only once to access multiple, related, and independent software systems.
Universal Series Bus (USB) Token	A USB token is a hardware security device that is used with the USB of a PC or laptop for authentication purposes.
Wireless Authentication	Wireless authentication uses various protocols to secure access to networks from wireless devices.