Corporate Computer Security, 4th Edition

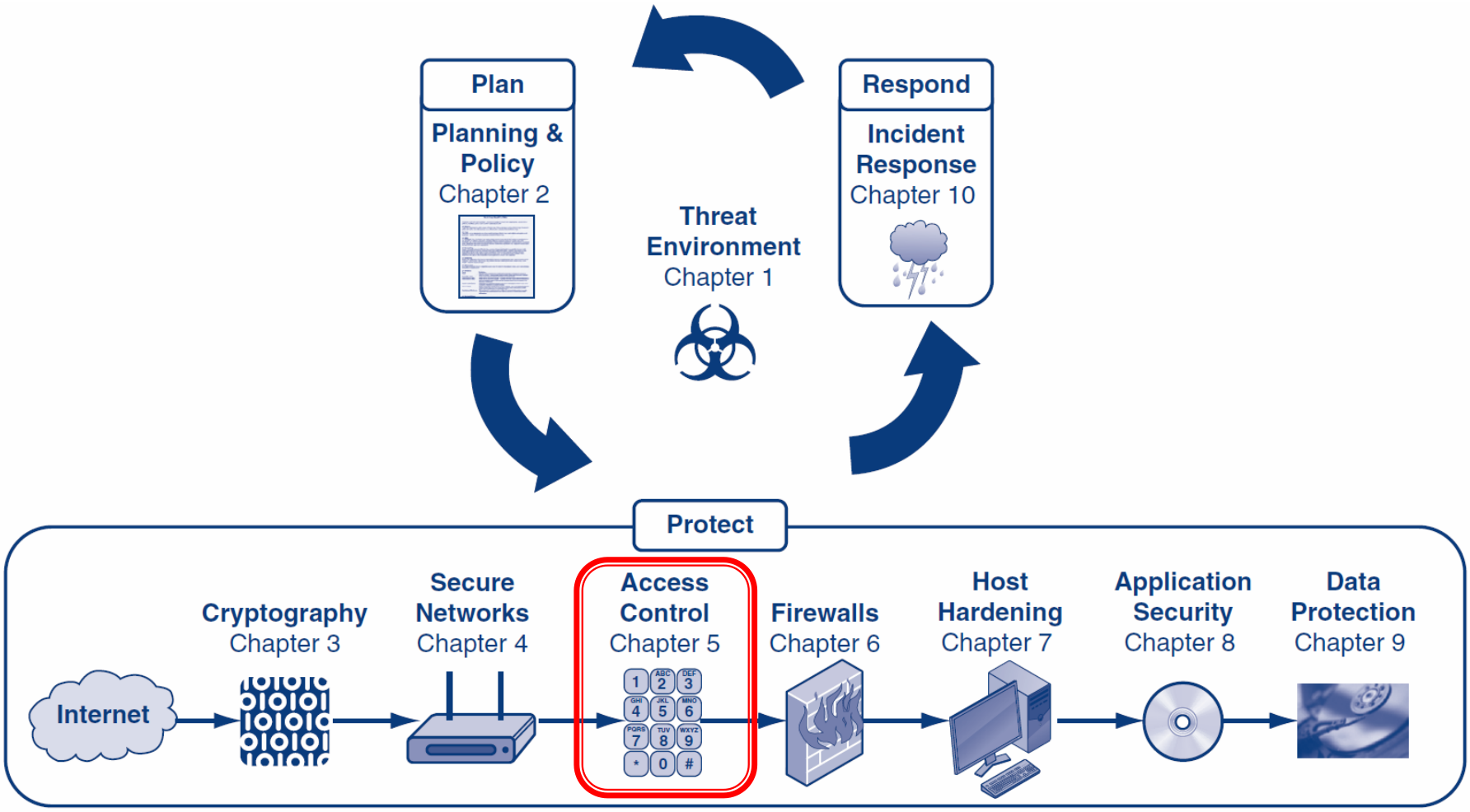
Randall J. Boyle & Raymond R. Panko

Access Control

Chapter 5

Learning Objectives

- Define basic access control terminology.
- Describe physical building and computer security.
- Explain reusable passwords.
- Explain how access cards and tokens work.
- Describe biometric authentication, including verification and identification.
- Explain authorizations.
- Explain auditing.
- Describe how central authentication servers work.
- Describe how directory servers work.
- Define full identity management.



Orientation

- If attackers cannot get access to your resources, they cannot attack them
- This chapter presents a number of important access control tools, such as reusable passwords and biometrics
- We covered crypto before access controls because many access controls use cryptography
- However, not all access controls use crypto, and those that do usually use it for only part of their process

What's Next?

- 5.1 Introduction
- 5.2 Physical Access and Security
- 5.3 Passwords
- 5.4 Access Cards and Tokens
- 5.5 Biometric Authentication
- 5.6 Cryptographic Authentication
- 5.7 Authorization
- 5.8 Auditing
- 5.9 Central Authentication Servers
- 5.10 Directory Servers and Identity Management

5.1: Access Control

- **Access Controls**
  - Firms must limit access to physical and electronic resources
  - Access control is the policy-driven control of access to systems, data, and dialogues
- **Cryptography**
  - Many access control tools use cryptography to some extent
  - However, cryptography is only part of what they do and how they work

5.1: Access Control

- **The AAA Protections**
  - Authentication—supplicant sends credentials to verifier to authenticate the supplicant
  - Authorization—what permissions the authenticated user will have
    - What resources he or she can get to at all
    - What he or she can do with these resources
  - Auditing—recording what people do in log files
    - Detecting attacks
    - Identifying breakdowns in implementation

5.1: Access Control

- **Beyond Passwords**
  - Passwords used to be sufficiently strong
  - This is no longer true thanks to increasing computer speeds available to hackers
  - Companies must move to better authentication options

5.1: Access Control

- **Credentials Are Based On**
  - What you know (e.g., a password)
  - What you have (e.g., an access card)
  - What you are (e.g., your fingerprint) or
  - What you do (e.g., speaking a passphrase)

5.1: Access Control

- **Two-Factor Authentication**
  - Use two forms of authentication for defense in depth
  - Example: access card and personal identification number (PIN)
  - Multifactor authentication: two or more types of authentication
  - Can be defeated by a Trojan horse on the user's PC
  - Can also be defeated by a man-in-the-middle attack by a fake website

5.1: Access Control

- **Individual and Role-Based Access Control**
  - Individual access control: bases access rules on individual accounts
  - Role-based access control (RBAC)
    - Bases access rules on organizational roles (e.g., buyer, member of a team, etc.)
    - Assigns individual accounts to roles to give them access to each role's resources
    - Cheaper and less error-prone than basing access rules on individual accounts

5.1: Access Control

- **Human and Organizational Controls**
  - People and organizational forces may circumvent access protections

5.1: Military and National Security Organization Access Controls

- **Mandatory and Discretionary Access Control**
  - Mandatory access control (MAC)
    - No departmental or personal ability to alter access control rules set by higher authorities
  - Discretionary access control (DAC)
    - Departmental or personal ability to alter access control rules set by higher authorities
  - MAC gives stronger security but is very difficult to implement

5.1: Military and National Security Organization Access Controls

- **Multilevel Security**
  - Resources are rated by security level
    - Public
    - Sensitive but unclassified
    - Secret
    - Top secret
  - People are given the same clearance level

5.1: Military and National Security Organization Access Controls

- **Multilevel Security**
  - Some rules are simple
    - People with a secret clearance cannot read top secret documents
  - Some rules are complex
    - What if a paragraph from a top secret document is placed in a secret document?
  - Access control models have been created to address multilevel security
    - Will not discuss because not pertinent to corporations

What's Next?

- 5.1 Introduction
- 5.2 Physical Access and Security
- 5.3 Passwords
- 5.4 Access Cards and Tokens
- 5.5 Biometric Authentication
- 5.6 Cryptographic Authentication
- 5.7 Authorization
- 5.8 Auditing
- 5.9 Central Authentication Servers
- 5.10 Directory Servers and Identity Management

5.2: ISO/IEC 27002:2005 Physical and Environmental Security

- **ISO/IEC 27002's Security Clause 9, Physical and Environmental Security**
- **Risk Analysis Must Be Done First**
- **ISO/IEC 9.1: Secure Areas**
  - Securing the building's physical perimeter (e.g., single point of entry, emergency exits, etc.)
  - Implementing physical entry controls
    - Access should be justified, authorized, logged, and monitored

5.2: ISO/IEC 27002:2005 Physical and Environmental Security

- **ISO/IEC 9.1: Secure Areas**
  - Securing public access, delivery, and loading areas
  - Securing offices, rooms, and facilities
  - Protecting against external and environmental threats
  - Creating rules for working in secure areas
    - Limit unsupervised work, forbid data recording devices, etc.

5.2: ISO/IEC 27002:2005 Physical and Environmental Security

- **9.2 Equipment Security**
  - Equipment siting and protection
    - Siting means locating or placing (same root as *site*)
  - Supporting utilities (e.g., electricity, water, HVAC)
    - Uninterruptible power supplies, electrical generators
    - Frequent testing

5.2: ISO/IEC 27002:2005 Physical and Environmental Security

- **9.2 Equipment Security**
  - Cabling security (e.g., conduits, underground wiring, etc.)
  - Security during offsite equipment maintenance
    - Permission for taking offsite
    - Removal of sensitive information

5.2: ISO/IEC 27002:2005 Physical and Environmental Security

- **9.2 Equipment Security**
  - Security of equipment off-premises
    - Constant attendance except when locked securely
    - Insurance
  - Secure disposal or reuse of equipment
    - Removal of all sensitive information
  - Rules for the removal of property

5.2: Other Physical Security Issues

- **Terrorism**
  - Building set back from street
  - Armed guards
  - Bullet-proof glass
- **Piggybacking**
  - Following an authorized user through a door
  - Also called tailgating
  - Psychologically difficult to prevent
  - Piggybacking is worth the effort to prevent

5.2: Other Physical Security Issues

- **Monitoring Equipment**
  - CCTV
  - Tapes wear out
  - High-resolution cameras are expensive and consume a great deal of disk space
  - Low-resolution cameras may be insufficient for recognition needs
  - To reduce storage, use motion sensing

5.2: Other Physical Security Issues

- **Dumpster[TM] Diving**
  - Protect building trash bins that may contain sensitive information
  - Maintain trash inside the corporate premises and monitor until removed
- **Desktop PC Security**
  - Locks that connect the computer to an immovable object
  - Login screens with strong passwords

What's Next?

5.1 Introduction

5.2 Physical Access and Security

5.3 Passwords

5.4 Access Cards and Tokens

5.5 Biometric Authentication

5.6 Cryptographic Authentication

5.7 Authorization

5.8 Auditing

5.9 Central Authentication Servers

5.10 Directory Servers and Identity Management

5.3: Server Password Cracking

- **Reusable Passwords**
  - A password that is used multiple times
  - Almost all passwords are reusable passwords
  - A one-time password is used only once

5.3: Server Password Cracking

- **Difficulty of Cracking Passwords by Guessing Remotely**
  - Account is usually locked after a few login failures
- **Password-Cracking Programs**
  - Password-cracking programs exist
    - Run on a computer to crack its passwords or
    - Run on a downloaded password file

5.3: Password Policies

- **Password Policies**
  - Regularly test the strength of internal passwords
  - Not using the same password at multiple sites
  - Use password management programs
  - Password duration policies
  - Shared password policies (makes auditing impossible)
  - Disabling passwords that are no longer valid

5.3: Password Policies

- **Other Password Policies**
  - Lost passwords (password resets)
    - Opportunities for social engineering attacks
    - Automated password resets use secret questions (i.e., Where were you born?)
      - Many can be guessed with a little research, rendering passwords useless
      - Some questions may violate security policies

5.3: Password Policies

- **Password Strength Policies**
  - Password policies must be long and complex
    - At least 8 characters long
    - Change of case, not at beginning
    - Digit (0 through 9), not at end
    - Other keyboard character, not at end
    - Example: tri6#Vial
  - Completely random passwords are best but usually are written down

RockYou.com			Gawker.com			Hotmail.com		
Rank	Count	Password	Rank	Count	Password	Rank	Count	Password
1	290,731	123456	1	2,516	123456	1	64	123456
2	79,078	12345	2	2,188	password	2	18	123456789
3	76,790	123456789	3	1,205	12345678	3	11	alejandra
4	61,958	Password	4	696	qwerty	4	10	111111
5	51,622	iloveyou	5	498	abc123	5	9	alberto
6	35,231	princess	6	459	12345	6	9	tequiero
7	22,588	rockyou	7	441	monkey	7	9	alejandro
8	21,726	1234567	8	413	111111	8	9	12345678
9	20,553	12345678	9	385	consumer	9	8	1234567
10	17,542	abc123	10	376	letmein	10	7	estrella
11	17,168	Nicole	11	351	1234	11	7	iloveyou
12	16,409	Daniel	12	318	dragon	12	7	daniel
13	16,094	babygirl	13	307	trustno1	13	7	0
14	15,294	monkey	14	303	baseball	14	7	roberto
15	15,162	Jessica	15	302	gizmodo	15	6	654321
16	14,950	Lovely	16	300	whatever	16	6	bonita
17	14,898	michael	17	297	superman	17	6	sebastian
18	14,329	Ashley	18	276	1234567	18	6	beatriz
19	13,984	654321	19	266	sunshine	19	5	mariposa
20	13,856	Qwerty	20	266	iloveyou	20	5	america

FIGURE 5-6 Common Passwords (Study Figure)

5.3: Password Policies

- **The End of Passwords?**
  - Many firms want to eliminate passwords because of their weaknesses
  - Quite a few firms have already largely phased them out

What's Next?

5.1 Introduction

5.2 Physical Access and Security

5.3 Passwords

5.4 Access Cards and Tokens

5.5 Biometric Authentication

5.6 Cryptographic Authentication

5.7 Authorization

5.8 Auditing

5.9 Central Authentication Servers

5.10 Directory Servers and Identity Management

5.4: Access Cards and Tokens

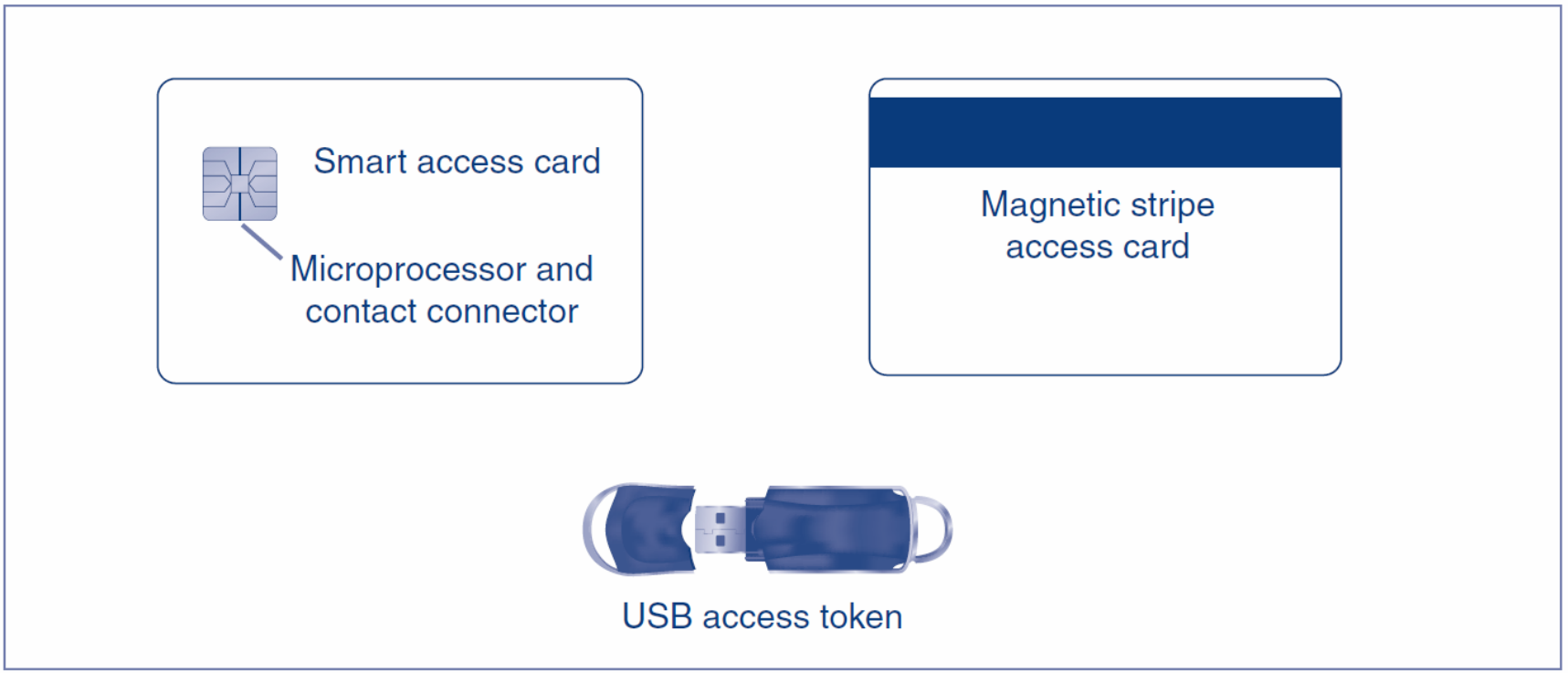


FIGURE 5-8 Access Cards and Tokens

5.4: Access Cards and Tokens

- **Access Cards**
  - Magnetic stripe cards
  - Smart cards
    - Have a microprocessor and RAM
    - Can implement public key encryption for challenge/response authentication
  - In selection decision, must consider cost and availability of card readers

5.4: Access Cards and Tokens

- **Tokens**
  - One-Time-Password Tokens:

A one-time-password token is a small device with a display that has a number that changes frequently.

Users must type the current number into key locks or into their computers.

Using a one-time password avoids the need for reusable passwords, which, as we saw earlier, often are easy to defeat.

5.4: Access Cards and Tokens

- **Tokens**
  - USB tokens

A USB token is simply a small device that plugs into a computer's USB port to identify the owner.

USB tokens give many of the protections of smart cards without requiring the cost of installing a smart card reader on each PC.

5.4: Access Cards and Tokens

- **Proximity Access Tokens**
  - Use Radio Frequency ID (RFID) technology
  - Supplicant only has to be near a door or computer to be recognized
- **Addressing Loss and Theft**
  - Both are frequent
  - Card cancellation
    - Requires a wired network for cancellation speed
    - Must cancel quickly if risks are considerable

5.4: Access Cards and Tokens

- **Two-Factor Authentication Needed because of Ease of Loss and Theft**
  - PINs (Personal Identification Numbers) for the second factor
    - Short: 4 to 6 digits
    - Can be short because attempts are manual
    - Should not choose obvious combinations (e.g., 1111, 1234) or important dates
  - Other forms of two-factor authentication
    - Store fingerprint template on device; check supplicant with a fingerprint reader

What's Next?

5.1 Introduction

5.2 Physical Access and Security

5.3 Passwords

5.4 Access Cards and Tokens

5.5 Biometric Authentication

5.6 Cryptographic Authentication

5.7 Authorization

5.8 Auditing

5.9 Central Authentication Servers

5.10 Directory Servers and Identity Management

5.5: Biometric Authentication

- **Biometric Authentication**
  - Authentication based on biological (bio) measurements (metrics)
    - Biometric authentication is based on something you are (e.g., your fingerprint, iris pattern, face, hand geometry, and so forth)
    - Or something you do (e.g., write, type, and so forth)
  - The major promise of biometrics is to make reusable passwords obsolete

5.5: Biometric Authentication System

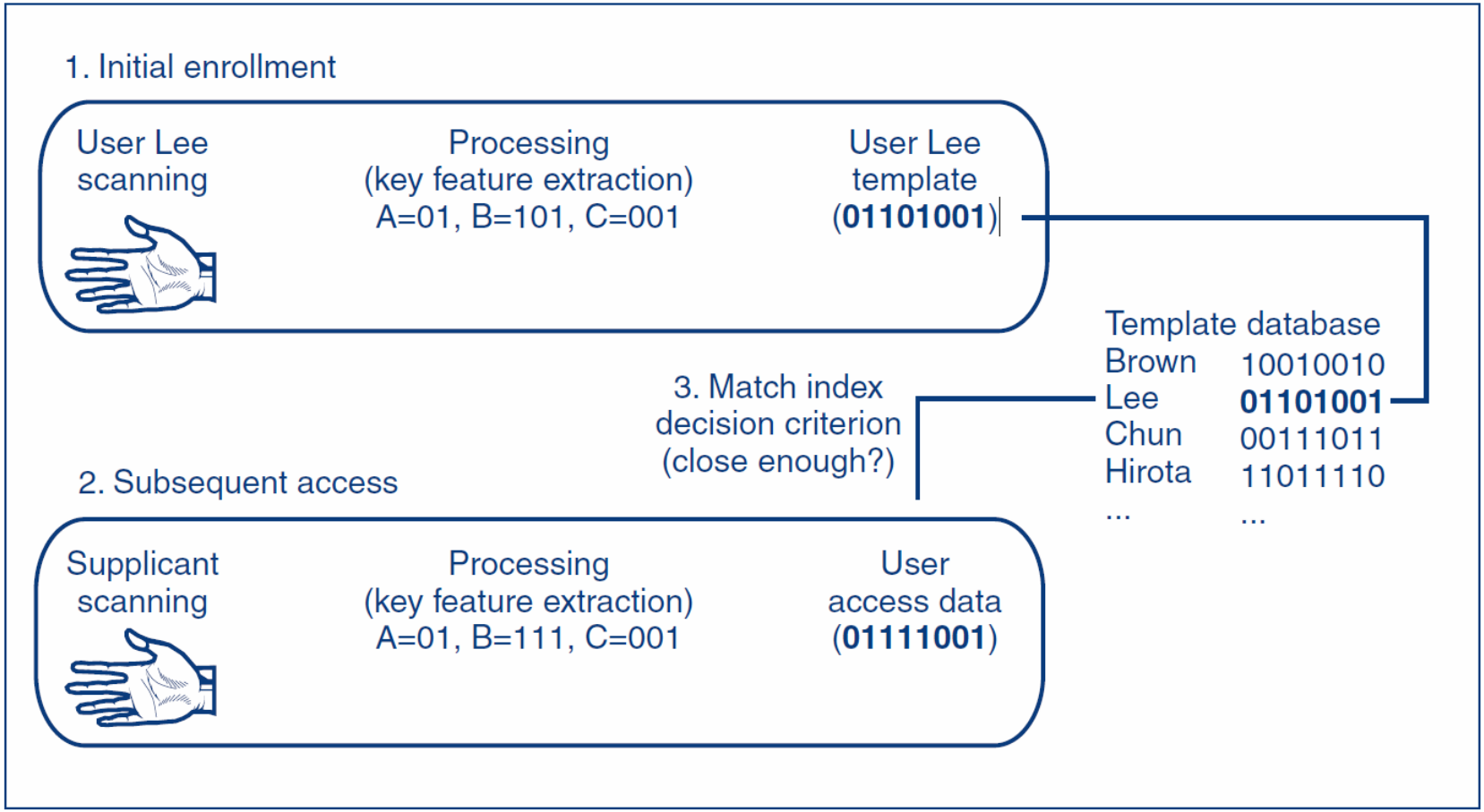


FIGURE 5-10 Biometric Authentication System

5.5: Biometric Authentication

- **Biometric Systems (Figure 5-10)**
  - Enrollment (enrollment scan, process for key features, store template)
    - Scan data is variable (scan fingerprint differently each time)
    - Key features extracted from the scan should be nearly the same
  - Later access attempts provide access data, which will be turned into key feature data for comparison with the template

5.5: Biometric Authentication

- **Biometric Systems (Figure 5-10)**
- Why not use entire scans instead of key features?
- The problem is that entire scans are not very useful in raw form. If a person swipes his or her finger at different angles, raw scan files will be very different, but key features such as the relative locations of loops, arches, and whorls in fingerprints will be the same or almost the same no matter how a finger is scanned.

5.5: Biometric Authentication

- **Biometric Systems (Figure 5-11)**
- Figure 5-11 shows the enrollment process for a fingerprint reader on a Transcend® JetFlash®.
- The process is user-friendly and takes about three minutes.
- To complete the process, a user is required to swipe the same finger four times and enter a password.

5.5: Biometric Authentication

- **Biometric Systems (Figure 5-11)**
  - Biometric access key features will never be exactly the same as the template
  - There must be configurable decision criteria for deciding how close a match to require (match index)
    - Requiring an overly exact match index will cause many false rejections
    - Requiring too loose a match index will cause more false acceptances

5.5: Biometric Enrollment

5.5: Subsequent Access

5.5: Biometric Errors and Deception

- **Errors versus Deception**
- **False Acceptance Rates (FARs)**
  - Percentage of people who are identified or verified as matched to a template but should not be
- **False Rejection Rates (FRRs)**
  - Percentage of people who should be identified or verified as matches to a template but are not

5.5: Biometric Errors and Deception

- **Which is Worse?**
  - **It depends on the situation**

Situation	False acceptance	False rejection
Identification for computer access	Security Violation	Inconvenience
Verification for computer access	Security Violation	Inconvenience
Watch list for door access	Security Violation	Inconvenience
Watch list for terrorists	Inconvenience	Security Violation

5.5: Biometric Errors and Deception

- **Vendor Claims for FARs and FRRs**
  - Tend to be exaggerated through tests under ideal conditions
- **Failure to Enroll (FTE)**
  - Subject cannot enroll in system
  - E.g., poor fingerprints due to construction work, clerical work, age, etc.

5.5: Biometric Errors and Deception

- **Deception**
  - Errors: when subject is not trying to fool the system
  - Deception: when subject *is* trying to fool the system
    - Hide face from cameras used for face identification
    - Impersonate someone by using a gelatin finger on a fingerprint scanner
    - Etc.

5.5: Biometric Errors and Deception

- **Deception**
  - Many biometric methods are highly vulnerable to deception
    - Fingerprint scanners should only be used when the threat of deception is very low
    - Fingerprint scanners are better than passwords because there is nothing to forget
    - Fingerprint scanners are good for convenience rather than security

5.5: Biometric Verification, Identification, and Watch Lists

- **Verification**
  - Supplicant claims to be a particular person
  - Is the supplicant who he or she claims to be?
  - Compare access data to a single template (the claimed identity)
  - Verification is good to replace passwords in logins
  - If the probability of a false acceptance (false match) probability is 1/1000 per template match,
    - The probability of a false acceptance is 1/1000 (0.1%)

5.5: Biometric Verification, Identification, and Watch Lists

- **Identification**
  - Supplicant does not state his or her identity
  - System must compare supplicant data to *all* templates to find the correct template
  - If the probability of a false acceptance (false match) probability is 1/1000 per template match,
    - and if there are 500 templates in the database, then
    - the probability of a false acceptance is 500 * 1/1000 (50%)
  - Good for door access

5.5: Biometric Verification, Identification, and Watch Lists

- **Watch Lists**
  - Subset of identification
  - Goal is to identify members of a group
    - Terrorists
    - People who should be given access to an equipment room

5.5: Biometric Verification, Identification, and Watch Lists

- **Watch Lists**
  - More comparisons than validation but fewer than identification, so the risk of a false acceptance is intermediate
  - If the probability of a false acceptance (false match) probability is 1/1000 per template match,
    - And if there are 10 templates in the watch list, then
    - the probability of a false acceptance is 10 * 1/1000 (1%)

5.5: Biometric Methods

- **Fingerprint Recognition**
  - Simple, inexpensive, well proven
  - Most biometrics today are fingerprint recognition
  - Often can be defeated with latent fingerprints on glass copied to gelatin fingers
  - Fingerprint recognition can take the place of reusable passwords for low-risk applications

5.5: Use of HIIDE™ in Correctional Facilities

5.5: Military Use of HIIDE™

5.5: Biometric Methods

- **Iris Recognition**
  - Pattern in colored part of eye
  - Uses a camera (no light is shined into eye, as in Hollywood movies)
  - Very low FARs
  - Very expensive

5.5: HIIDE™ Eye Scan

5.5: Biometric Methods

- **Face Recognition**
  - Surreptitious identification is possible (in airports, etc.)
  - Surreptitious means *without the subject's knowledge*
  - High error rates, even without deception
- **Hand Geometry for Door Access**
  - Shape of hand
  - Reader is very large, so usually used for door access

5.5: HIIDE™ Face Capture

5.5: Biometric Methods

- **Voice Recognition**
  - High error rates
  - Easily deceived by recordings
- **Other Forms of Biometric Authentication**
  - Veins in the hand
  - Keystroke recognition (pace in typing password)
  - Signature recognition (hand-written signature)
  - Gait (way the person walks) recognition

What's Next?

5.1 Introduction

5.2 Physical Access and Security

5.3 Passwords

5.4 Access Cards and Tokens

5.5 Biometric Authentication

5.6 Cryptographic Authentication

5.7 Authorization

5.8 Auditing

5.9 Central Authentication Servers

5.10 Directory Servers and Identity Management

5.6: Cryptographic Authentication

- **Key Points from Chapter 3**
  - Cryptographic systems have initial and message-by-message authentication
  - MS-CHAP uses passwords for initial authentication
  - Electronic signatures provide message-by-message authentication
    - Key-Hashed Message Authentication Codes (HMACs) are fast and inexpensive
    - Digital signatures with digital certificates are extremely strong but slow
  - Chapter 3 did not mention that public key authentication with digital certificates are also good for initial authentication

5.6: Cryptographic Authentication

- **Public Key Infrastructures (PKIs) (Figure 5-18)**
  - Firms can be their own certificate authorities (CAs)
  - Requires a great deal of labor
  - Provisioning
    - Giving the user access credentials

5.6: Functions of a Public Key Infrastructure (PKI)

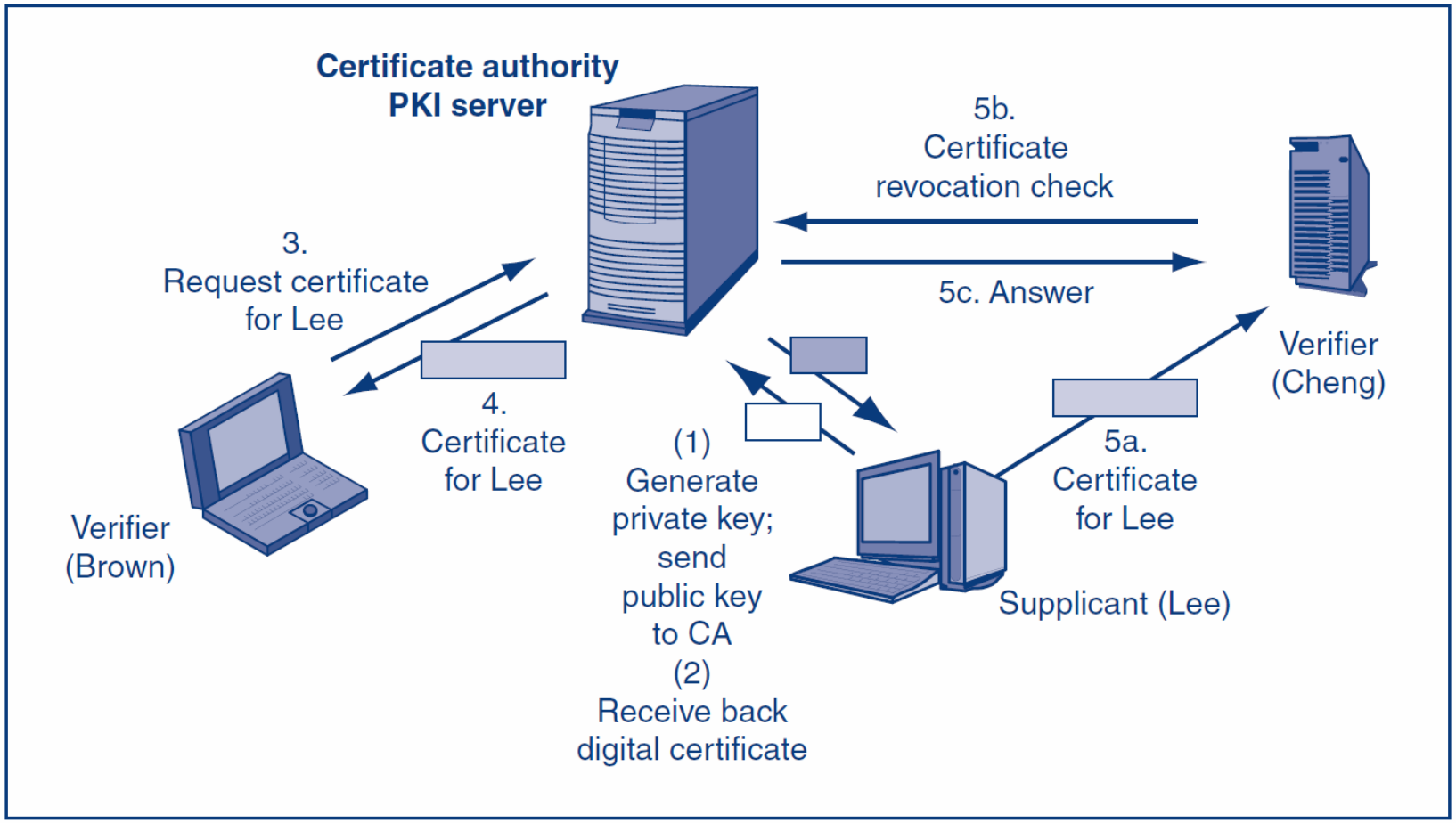


FIGURE 5-18 Functions of a Public Key Infrastructure (PKI)

5.6: Cryptographic Authentication

- **Public Key Infrastructures (PKIs) (Figure 5-18)**
  - Provisioning
    - Human registration is often the weakest link
      - If an impostor is given credentials, no technology access controls will work
      - Limit who can submit names for registration
      - Limit who can authorize registration
      - Have rules for exceptions
    - Must have effective terminating procedures
    - Supervisors and Human Resources department must assist

What's Next?

5.1 Introduction
5.2 Physical Access and Security
5.3 Passwords
5.4 Access Cards and Tokens
5.5 Biometric Authentication
5.6 Cryptographic Authentication
5.7 Authorization
5.8 Auditing
5.9 Central Authentication Servers
5.10 Directory Servers and Identity Management

5.7: Principle of Least Permissions

- **Authorizations**
  - Authentication: Proof of identity
  - Authorization: The assignment of permissions (specific authorizations) to individuals or roles
  - Just because you are authenticated does not mean that you should be able to do everything

5.7: Principle of Least Permissions

- **Principle of Least Permissions**
  - Initially give people only the permissions a person absolutely needs to do his or her job
  - If assignment is too narrow, additional permissions may be given
    - If assignment is too narrow, the system fails safely

5.7: Principle of Least Permissions

- **Principle of Least Permissions**
  - System has permissions A, B, C, D, E, and F
    - Person needs A, C, and E
    - If only given A and C, can add E later although user will be inconvenienced
    - Errors tend not to create security problems
    - Fails safely
  - This will frustrate users somewhat

5.7: Principle of Least Permissions

- **Giving Extensive or Full Permissions Initially Is Bad**
  - User will almost always have the permissions to do his or her job
  - System has permissions A, B, C, D, E, and F
    - Person needs A, C, and E
    - If given all, but take away B and D, still has F
    - Errors tend to create security problems

5.7: Principle of Least Permissions

- **Giving Extensive or Full Permissions Initially Is Bad**
  - Assignments can be taken away, but this is subject to errors
  - Such errors could give excessive permissions to the user
  - This could allow the user to take actions contrary to security policy
  - Giving all or extensive permissions and taking some away does not fail safely

What's Next?

5.1 Introduction
5.2 Physical Access and Security
5.3 Passwords
5.4 Access Cards and Tokens
5.5 Biometric Authentication
5.6 Cryptographic Authentication
5.7 Authorization
5.8 Auditing
5.9 Central Authentication Servers
5.10 Directory Servers and Identity Management

5.8: Auditing

- **Auditing**
  - Authentication: Who a person is
  - Authorization: What a person may do with a resource
  - Auditing: What the person *actually did*

5.8: Auditing

- **Logging**
  - Events
  - On a server, logins, failed login attempts, file deletions, and so forth
  - Events are stored in a log file

5.8: Auditing

- **Log Reading**
  - Regular log reading is crucial or the log becomes a useless write-only memory
  - Periodic external audits of log file entries and reading practices
  - Automatic alerts for strong threats

What's Next?

5.1 Introduction
5.2 Physical Access and Security
5.3 Passwords
5.4 Access Cards and Tokens
5.5 Biometric Authentication
5.6 Cryptographic Authentication
5.7 Authorization
5.8 Auditing
5.9 Central Authentication Servers
5.10 Directory Servers and Identity Management

5.9: Need of Central Authentication Server

- Most firms have hundreds or thousands of servers. Individual employees may need access and authorizations for a dozen or more servers. Companies address this need by using central authentication servers.
- Central authentication servers reduce costs, give consistency in authentication no matter where a user or attacker comes into the network, and allow company-wide changes to be made instantly.
- The most widely used standard for central authentication servers is RADIUS.

5.9: RADIUS Central Authentication Server

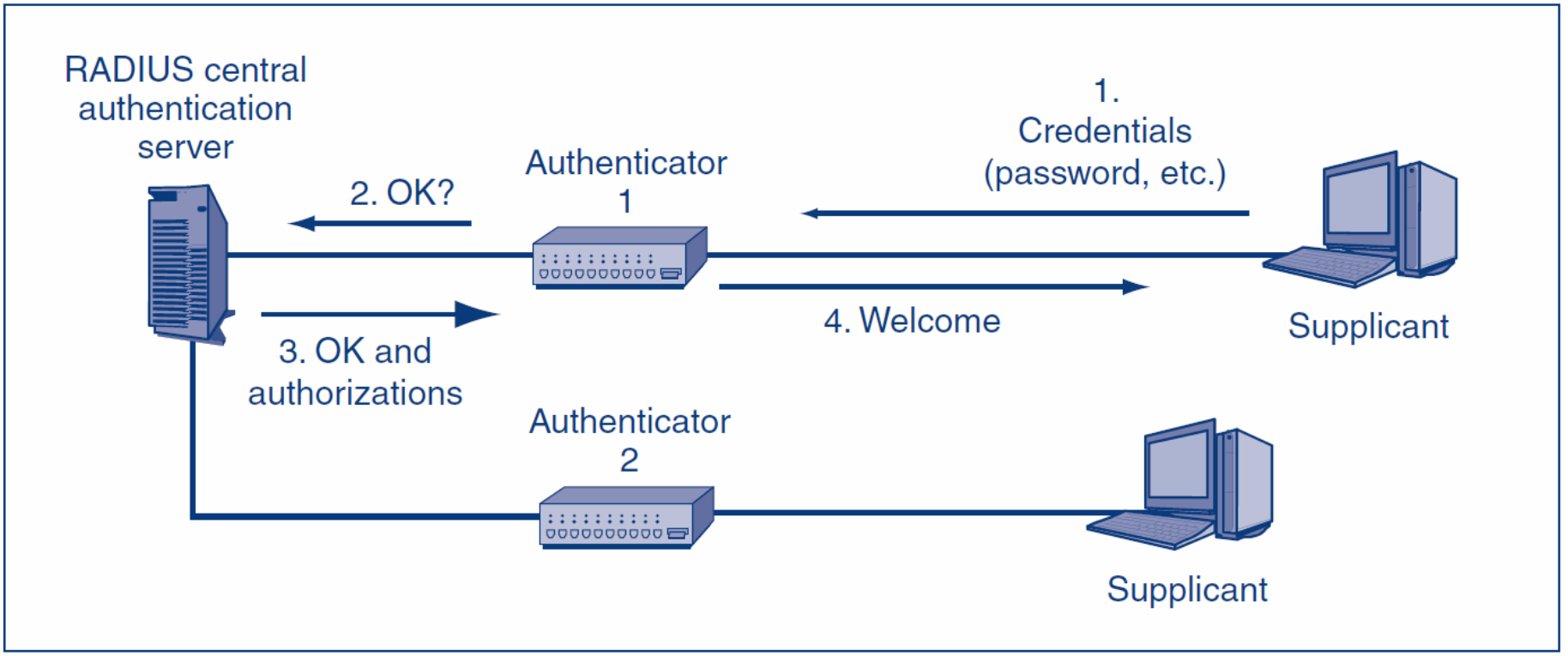


FIGURE 5-21 RADIUS Central Authentication Server

5.9: RADIUS Central Authentication Server

- Figure 5-21 recaps the basic elements in RADIUS central authentication.
- When a central authentication server is used, the device to which the supplicant connects is called the authenticator.
- When a supplicant sends credentials to any authenticator, the authenticator passes the credentials on to the central authentication server.

5.9: RADIUS Central Authentication Server

- The authentication server checks the credentials and sends a message back to the authenticator.
- This message tells the authenticator whether or not the supplicant's credentials were verified.
- Based on this information, the authenticator will either accept or reject the supplicant.

5.9: Kerberos Central Authentication Server

- Although RADIUS is arguably the most popular central authentication server standard, Kerberos is also important, in large part because Microsoft uses it to link hosts together.
- Actually, Kerberos is more than a central authentication server. It also provides keying information to parties that need to communicate with one another, and it can provide authorization information as well. (RADIUS can also do this.)

5.9: Kerberos Initial Login

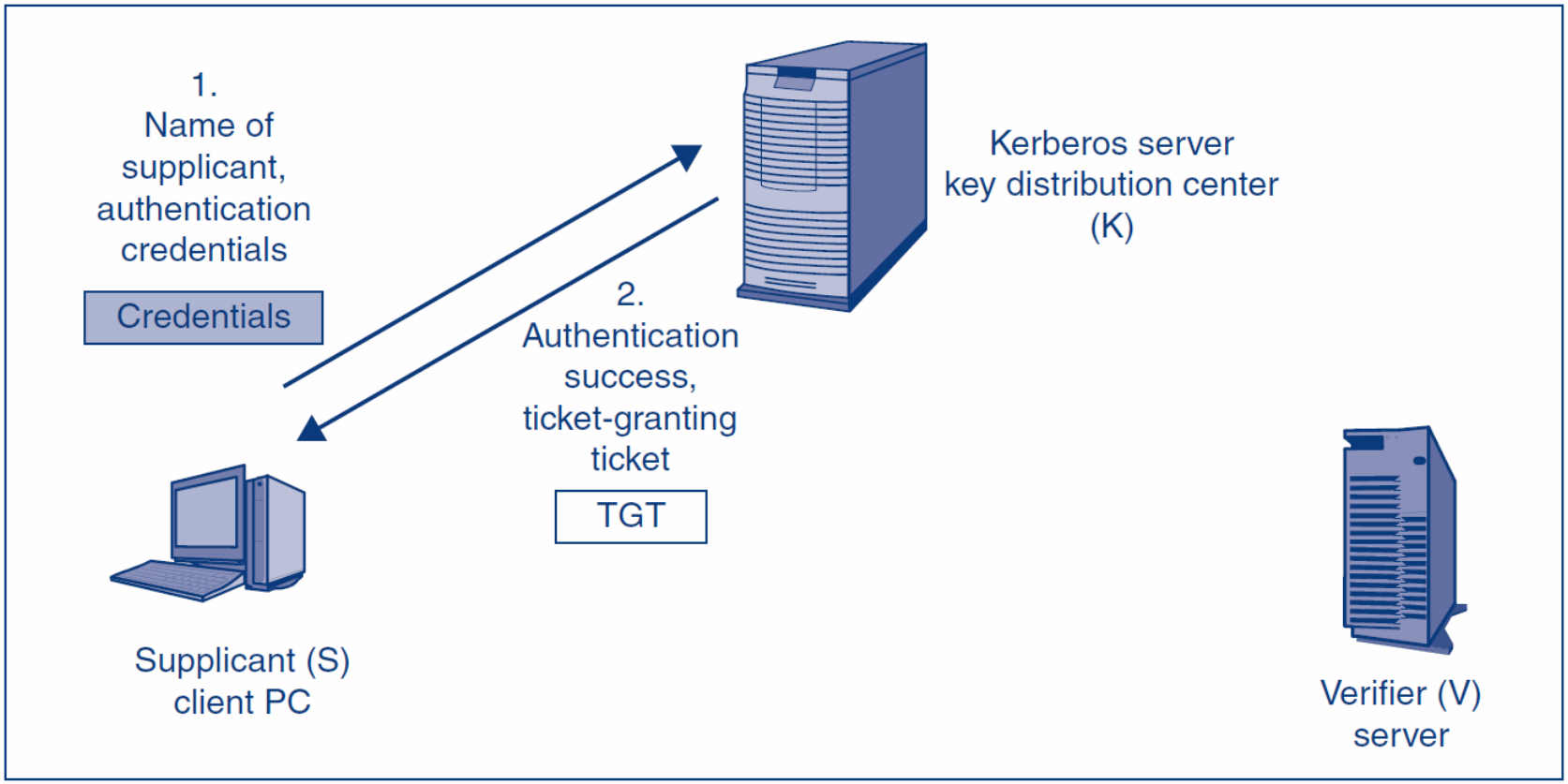


FIGURE 5-22 Kerberos Initial Login

5.9: Kerberos Initial Login

- Figure 5-22 shows that when a host wishes to connect to another host, it first logs into a Kerberos server. If it succeeds in logging in, it gets a ticket granting ticket (TGT).
- This is like getting a wrist bracelet when you enter a concert or sports event. It gets you back in later without having to show your original authentication credentials.

5.9: Kerberos Ticket Granting Service

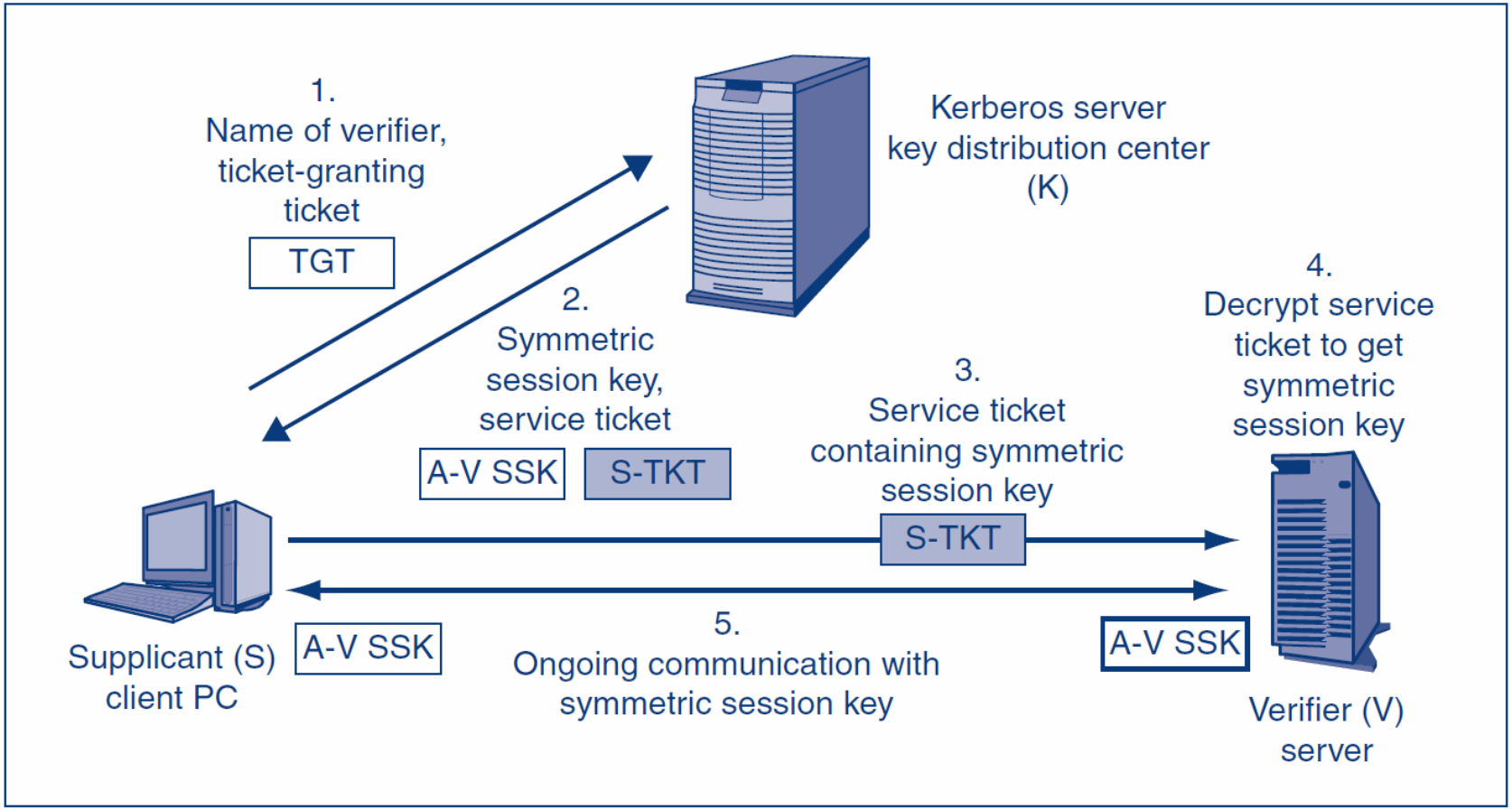


FIGURE 5-23 Kerberos Ticket Granting Service

5.9: Kerberos Ticket Granting Service

- Figure 5-23 shows that Supplicant S contacts the Kerberos server. In the process, Supplicant S sends its ticket granting ticket to the Kerberos server to prove that it has already been authenticated.
- If the Kerberos server permits the connection to the verifier V, it sends a service ticket to Supplicant S, which sends the service ticket on to verifier V.
- The verifier V has a symmetric key that it only shares with the Kerberos server.

5.9: Kerberos Ticket Granting Service

- It uses this shared key to decrypt the service ticket sent by the Kerberos server.
- The decrypted service ticket contains a session key for Supplicant S to use to talk to verifier V. It may also list permissions that Supplicant S should have on verifier V.
- When the Kerberos server sends the service ticket to Supplicant S, it also sends the session key with verifier V encrypted with a key that only the supplicant and the Kerberos server share. Supplicant S uses this shared key to decrypt the symmetric session key with verifier V.

5.9: Kerberos Ticket Granting Service

- Now that both hosts have the same symmetric session key, they can begin communicating back and forth, encrypting their transmission for confidentiality with the session key.

What's Next?

5.1 Introduction

5.2 Physical Access and Security

5.3 Passwords

5.4 Access Cards and Tokens

5.5 Biometric Authentication

5.6 Cryptographic Authentication

5.7 Authorization

5.8 Auditing

5.9 Central Authentication Servers

5.10 Directory Servers and Identity Management

5.10: Directory Server

RADIUS, Kerberos, and other central authentication servers improve centralization, but two problems remain in most large firms.

- First, most large firms find themselves with multiple RADIUS, Kerberos, and other central authentication servers.

- In addition, most large companies have made a strategic decision to use directory servers as their place to store data centrally in the firm.

5.10: Directory Server

- Directory servers are central repositories for information about people, equipment, software, and databases. Directory servers store authentication, authorization, and auditing information required for security.
- However, directory servers are not limited to security information. They store information about host configurations, employee contact information such as telephone numbers, and a great deal of general information.

5.10: Directory Server Organization

- Database courses usually focus on relational databases. Relational databases are good when there are about an equal numbers of accesses and updates.
- When there are many more accesses than updates, as there are with directory servers, a hierarchical database organization may be better.
- Directory servers use a hierarchical database organization.
- The directory server database schema is a hierarchical collection of objects (nodes).

5.10: Directory Server Organization

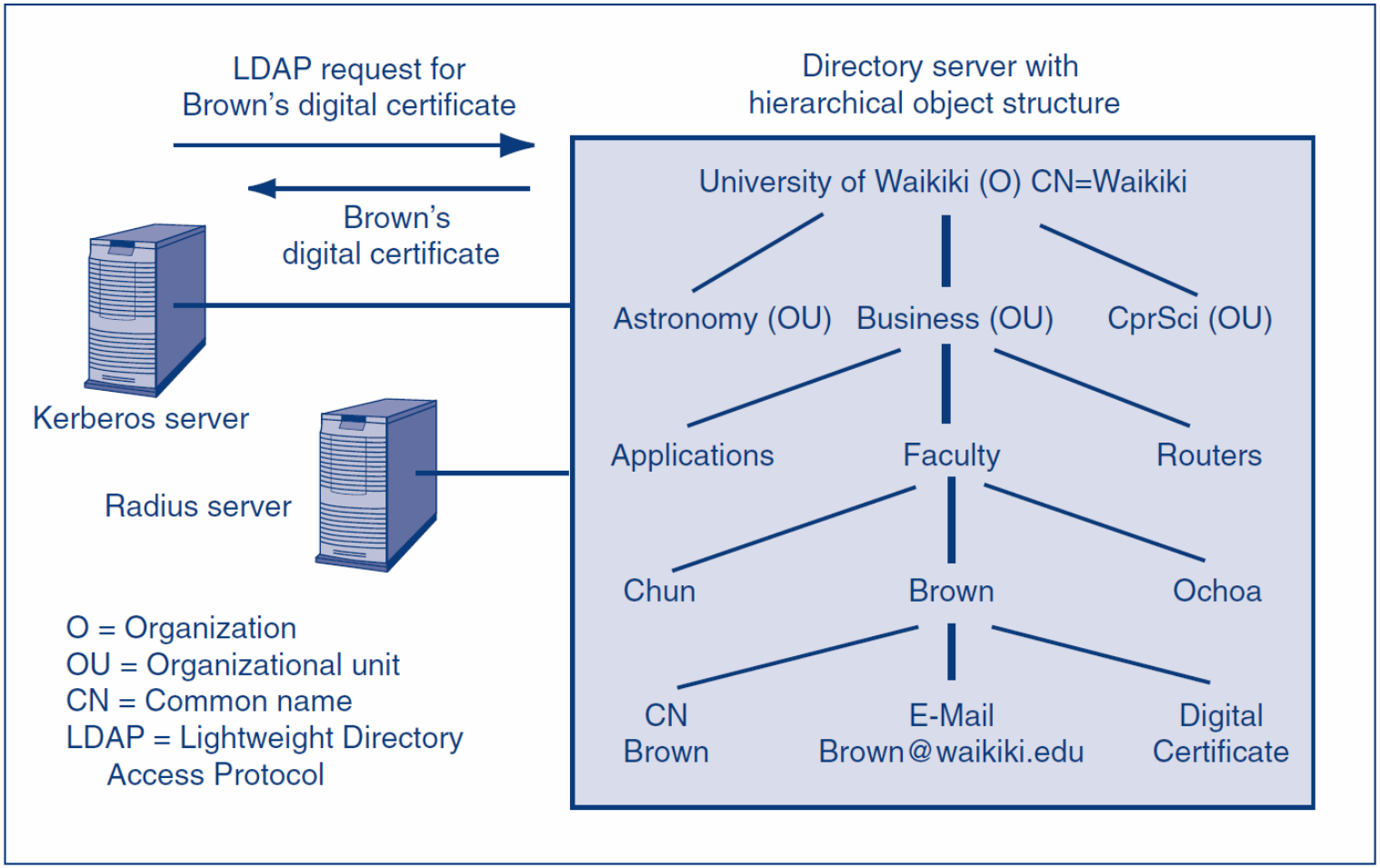


FIGURE 5-24 Directory Server Organization

5.10: Directory Server Organization

Lightweight Directory Access Protocol (LDAP)

- Authentication servers communicate with directory servers using the LDAP. Mostly, LDAP is used to retrieve data from the directory server.
- It can also be used to update information in the directory server. Nearly all directory servers support LDAP.
- Note that LDAP does not govern the internal operations of the directory server.

5.10: Using a Directory Server to Centralize Authentication Information

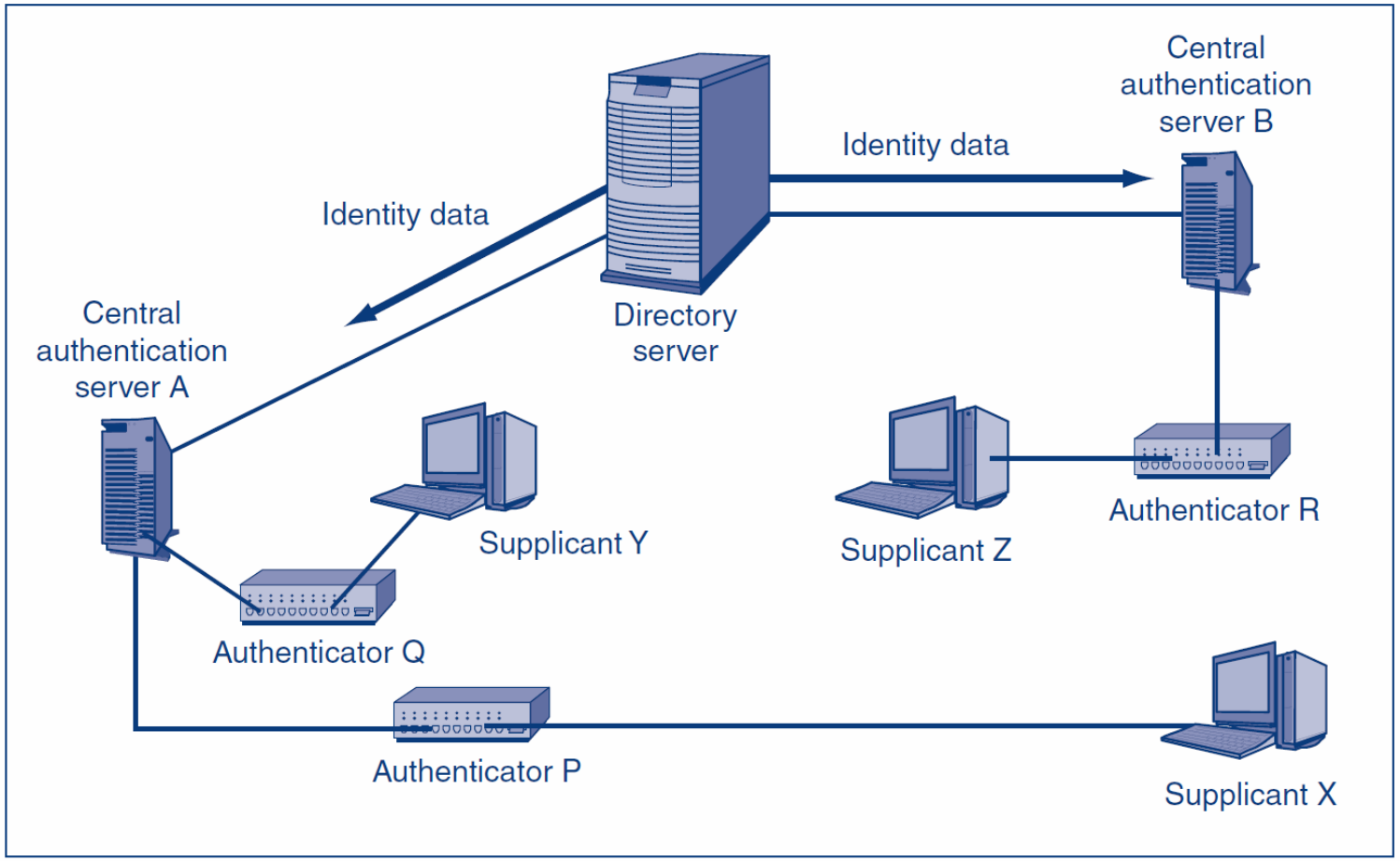


FIGURE 5-25 Using a Directory Server to Centralize Authentication Information

5.10: Using a Directory Server to Centralize Authentication Information

- In security, directory servers are important because they are used by central authentication servers such as RADIUS servers and Kerberos servers.
- Figure 5-25 shows that a directory server can provide authentication information to many authentication servers. Just as authentication servers are valuable because they centralize authentication information, directories provide a higher level of centralization for firms that have many central authentication servers.

5.10: Active Directory

- Microsoft's directory server product is called active directory (AD). Given the widespread use of Microsoft products in corporations, security professionals should understand AD.
- Figure 5-26 shows a firm with several active directory servers. Companies usually divide their resources into multiple **active directory domains**. AD domains usually are organizational units.

5.10: Active Directory

- For instance, in a university, an individual school or college may be a domain. The resources of the domain typically are managed by the organizational unit. AD domains may correspond to DNS domains, but they do not have to.

5.10: Active Directory Domains and Tree

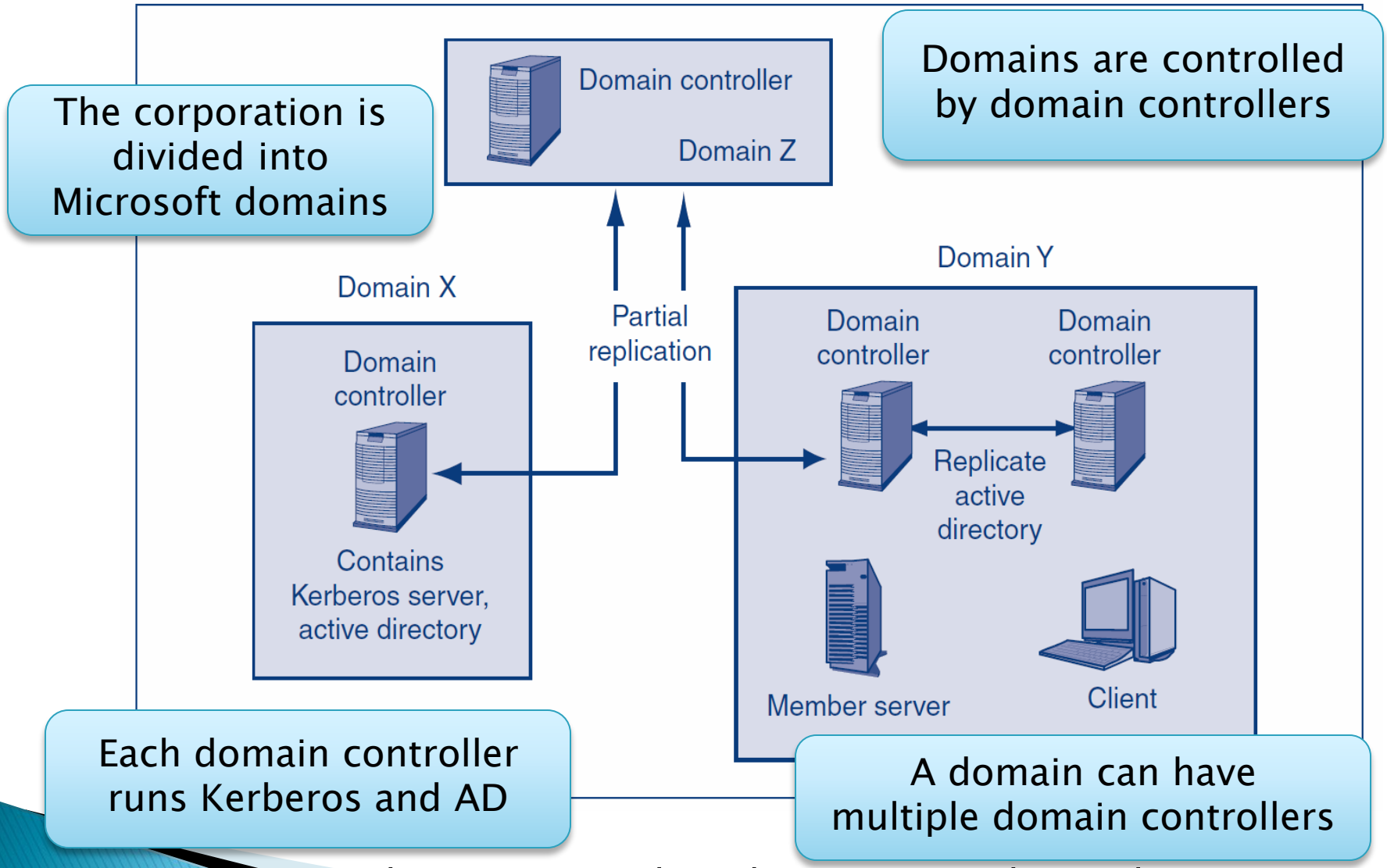


Figure 5-26: Active Directory Domains and Tree

5.10: Active Directory Domains and Tree

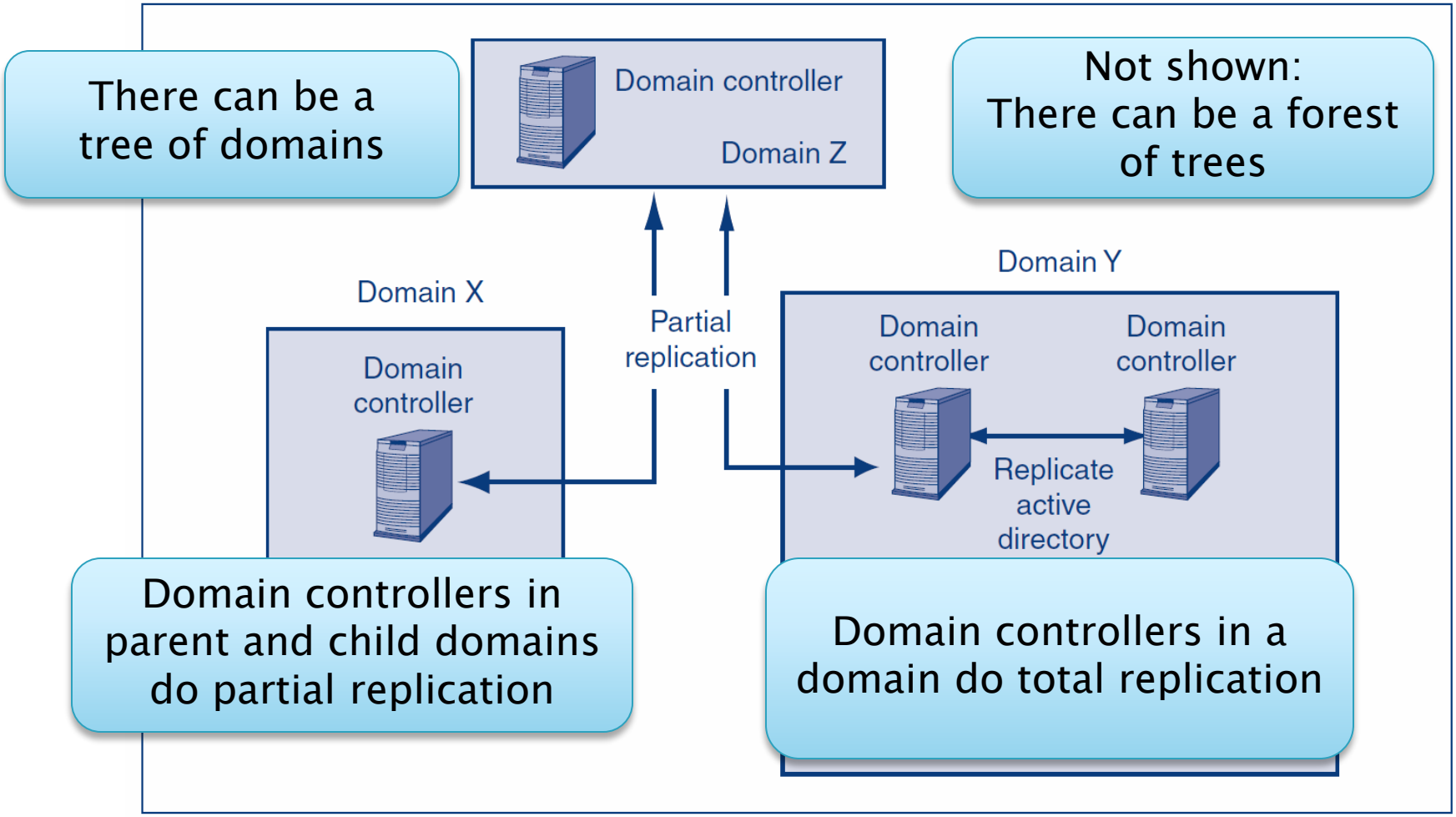


Figure 5-26: Active Directory Domains and Tree

5.10: Trust Directionality and Transitivity

- **Trust**
  - One directory server will accept information from another
- **Trust Directionality**
  - Mutual
    - A trusts B and B trusts A
  - One-Way
    - A trusts B or B trusts A, but not both

5.10: Trust Directionality and Transitivity

- **Trust Transitivity**
  - Transitive Trust
    - If A trusts B
      - and B trusts C,
        - then A trusts C automatically
  - Intransitive Trust
    - If A trusts B
      - and B trusts C,
        - this does NOT mean that A trusts C automatically

5.10: Multiple Directory Servers and Metadirectory Server

- In an ideal world, a company would only have a single family of directory servers. Instead, companies typically have several types of directory servers, as Figure 5-28 shows.
- Other common types of directory servers are Novell eDirectory and Sun ONE directory servers for Solaris(Sun's version of Unix).
- To connect these disparate directory servers together, the company in the figure has a metadirectory server.

5.10: Multiple Directory Servers and Metadirectory Server

- The **metadirectory server** gets the directory servers to exchange information and to synchronize services in a variety of ways.
- Unfortunately, these exchanges and synchronizations are limited today. Most commonly, when a user resets a password on one directory servers, the metadirectory server passes the password reset to other directory servers.

5.10: Multiple Directory Servers and Metadirectory Server

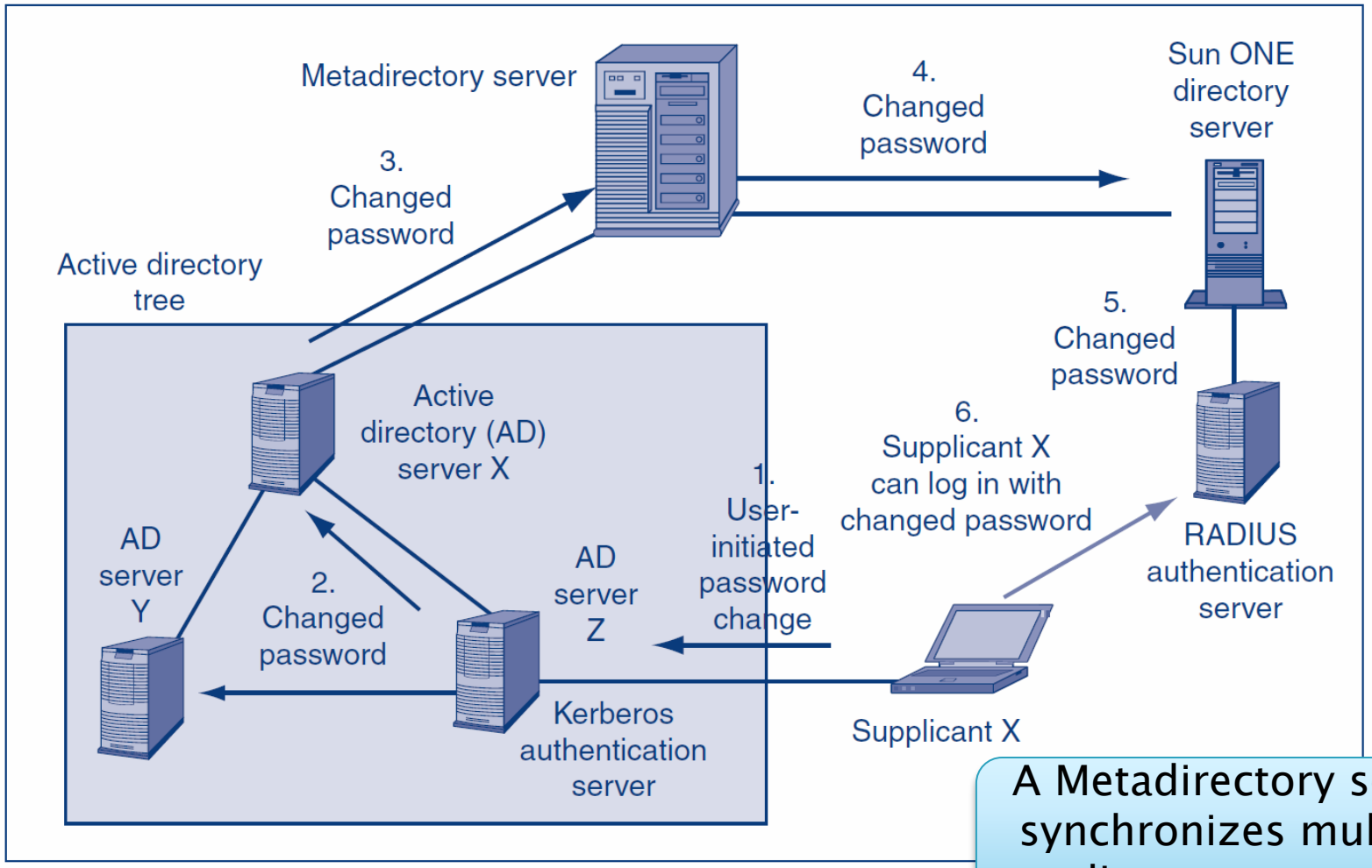


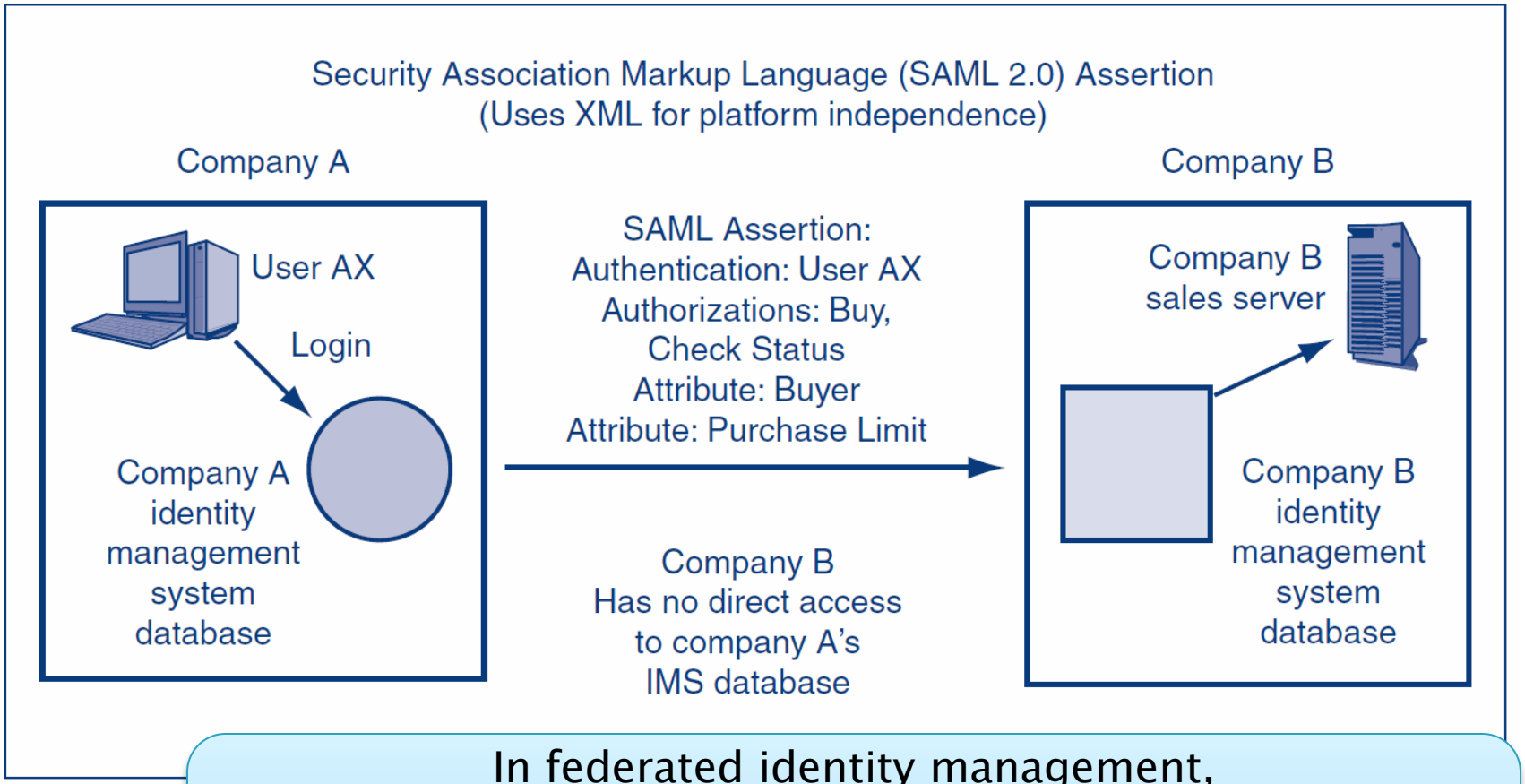
FIGURE 5-28 Multiple Directory Servers and Metadirectory Server

A Metadirectory server synchronizes multiple directory servers

5.10: Federated Identity Management

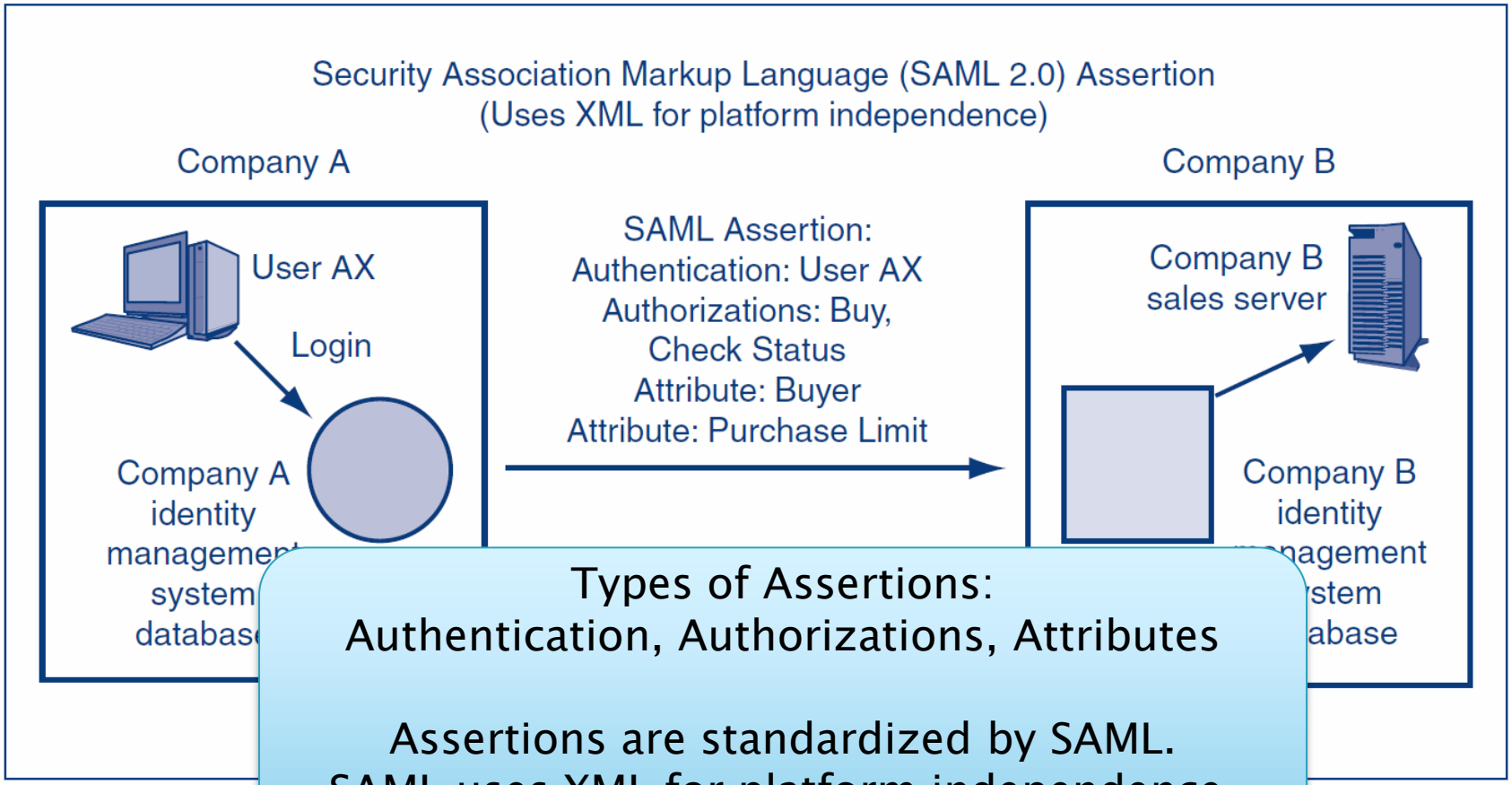
- Within companies, trust is complex. The situation is even more complex *between* companies.
- Between companies, we talk about federated authentication, authorization, and auditing or, more commonly, **federated identity management**.
- In federated identity management, business partners do not access each other's databases. Instead, they send assertions about a person. The receiver trusts the assertions.

5.10: Federated Identity Management



In federated identity management,
business partners do not access each other's databases.
Instead, they send assertions about a person.
The receiver trusts the assertions.

5.10: Federated Identity Management



5.10: Federated Identity Management

- In this case, Employee Dave first logs into Firm A's identity management server and is authenticated in the process.
- Employee Dave is a buyer in Firm A. He has a $10,000 purchase limit.
- Dave asks the federated identity management server in Firm A to contact the sales server in Firm B so that he can purchase supplies from Firm B.

5.10: Federated Identity Management

- The federated identity management server in Firm A sends an assertion to its counterpart in Firm B. An **assertion** is a statement that Firm B should accept as true if Firm B trusts Firm A.
- The assertion may have three major elements.
  - Authentication
  - Authorizations
  - Attributes

5.10: Federated Identity Management

- First, the assertion may contain **authenticity** information, namely that Dave is an employee by that name and has been authenticated at Firm A.

- The assertion may also contain an **authorization**, in this case that Firm B should allow Dave to access Firm B's sales server.

- Third, the assertion may contain **attributes** that describe the party being described, for instance, stating that Dave is a buyer and that Employee AX has a maximum purchase limit of $10,000.

5.10: Federated Identity Management

The Security Assertion Markup Language

- The dominant standard for sending security assertions today is the Security Assertion Markup Language (SAML).
- This standard uses XML to structure messages. Consequently, the interacting identity management systems do not have to use the same software technology.

5.10: Federated Identity Management

The Security Assertion Markup Language

- Thanks to XML, SAML is platform-independent.
- It does not matter what programming language the two partners use to program their systems. This is the key to SAML interoperability across firms.

5.10: Identity Management

- **Definition**
  - Identity management is the centralized policy-based management of all information required for access to corporate systems by a person, machine, program, or other resource.

5.10: Identity Management

- **Benefits of Identity Management**
  - Reduction in the redundant work needed to manage identity information
  - Consistency in information
  - Rapid changes
  - Central auditing
  - Single sign-on
  - Increasingly required to meet compliance requirements
  - At least reduced sign-on when SSO is impossible

5.10: Identity Management

- **Identity**
  - The set of attributes about a person or nonhuman resource that must be revealed *in a particular context*
    - Subordinate to a particular person
    - Manager of a department
    - Buyer dealing with another company
    - Manager responsible for a database
  - Principle of minimum identity data: only reveal the information necessary *in a particular context*

5.10: Identity Management

- **Identity Management**
  - Initial credential checking
  - Defining identities (pieces of information to be divulged)
  - Managing trust relationships
  - Provisioning, reprovisioning if changes, and deprovisioning

5.10: Identity Management

- **Identity Management**
  - Implementing controlled decentralization
    - Do as much administration as possible locally
    - Requires tight policy controls to avoid problems
  - Providing self-service functions for non-sensitive information
    - Marital status, etc.

The End