Lecture 2
Basics of Security

References:

1. Wikipedia, https://en.wikipedia.org/wiki/Main_Page
2. C. P. Pfleeger and S. L Pfleeger, "Security in Computer," 4th edition, Prentice Hall, 2006.

1

1

Security Assets

- (Security) Assets
  - Any data, device, or components to support sensitive activities
    - in information, computer, and network security
- Include
  - Hardware (e.g., servers, routers)
  - Software (e.g., mission critical applications)
  - Sensitive information (data)
- Protected from
  - Illicit access and use, disclose, alteration, destruction, theft

2

Security Goals

- Security Goals (CIA Triad)
  - Confidentiality, Integrity, and Availability
- Confidentiality
  - Assets accessed by authorized parties
  - Read type access
    - Read, view, print, or just know existence of object
- Integrity
  - Assets modified by authorized parties or in authorized ways
  - Modification - write, change, delete, or create

3

Security Goals

- Availability
  - Assets must be available when needed
  - Timely response, fair allocation, fault tolerance
  - Preventing denial-of-service (DoS) attacks
    - Flood of incoming messages to system
- Outside CIA Triad
  - Privacy
  - Non-repudiation

4

Privacy

- Privacy
  - Any rights you must control personal information and how it is used, e.g.,
    - Privacy policies when visiting doctor office
- Privacy vs confidentiality (secrecy), e.g.,
  - Privacy and confidentiality maintained
    - Clinic uses your information to treat your illness
  - Privacy compromised and confidentiality maintained
    - Clinic sells your information to a marketer without agreeing with privacy disclosure
  - Both privacy and confidentiality (secrecy) compromised
    - Your information exposed and sold on a dark web
    - Due to breach of clinic data by cybercriminals

5

Non-repudiation

- Non-repudiation
  - Assurance that someone cannot deny something
  - Ability to ensure that
    - A party to a contract cannot deny the authenticity of its signature, e.g.,
      - Check issued by Alex with signature, but deny it later
    - A party to a communication cannot deny the sending of a message that it originated, e.g.,
      - Purchase order made by Steve online, but deny it later

6

Authentication or Authorization

- Are they a security goal?
  - May be not
  - But they are means to realize security goals?
  - May break the confidentiality, integrity, and availability of assets

7

Security Services (Security Techniques or Security Measure)

- Confidentiality service
  - Protect against information being disclosed to any unauthorized entities
  - Secret key or public key cryptosystem, secure socket layer (SSL)
- Integrity services
  - Protect against unauthorized changes to data
  - Message Digest (MD), or Message Authentication Code (MAC)

8

Security Services (Techniques or Security Measure)

- Non-repudiation service
  - Protect against one party to a transaction or communication activity later falsely denying that the activity occurred
  - Digital signature
- Availability Service (Denial of Service)
  - Occurs when an authorized party is prevented from accessing a system to which it has legitimate access
  - Analysis of network data

9

Security Services (Techniques or Security Measure)

- Authentication service
  - Allow an entity (a user or system) to identify itself positively to another entity
  - Password, personal identification number (PIN), challenge/response, digital certificate, smart card, or biometrics
- Access Control service
  - Protect against unauthorized access to resources based on security policies
  - Attribute-based access control (ABAC), Role-based access control (RBAC), Mandatory access control (MAC), discretionary access control (DAC)

10

Confidentiality Service

- Cryptosystem
- Symmetric Cryptosystem
  - DES, AES
- Asymmetric Cryptosystem
  - Diffie Hellman, RSA
- Key Establishment
- Public Key Certificate

11

Cryptosystem

- Encryption
  - Message encoded to not obvious message
  - Encrypt, encipher, encode
- Decryption
  - Encrypted message transformed into normal form
  - Decrypt, decipher, decode

- Cryptography
  - Practice of using encryption to conceal text
- Cryptanalysis
  - Finding hidden meanings of messages

12

Cryptosystem

- Cryptosystem
  - System for encryption and decryption
  - Plaintext P = (p1, p2, …., pn): original form of a message
  - Ciphertext C = (c1, c2, …., Cm): encrypted form
  - Transformation between P and C
    - C=E(P) and P = D(C)
  - Cryptosystem: P = D(E(P))

13

Cryptanalysis

- Ciphertext only
  - Only Knows ciphertext
- Known plaintext
  - Knows some plaintext-ciphertext pairs
- Chosen plaintext
  - Knows some plaintext-ciphertext pairs for plaintext of the cryptanalyst' choice
- Chosen ciphertext
  - Knows some plaintext-ciphertext pairs for ciphertext of the cryptanalyst's choice

14

Attacks

- Passive attacks
  - Observe but do not modify assets
  - Threat for confidentiality
- Active attacks
  - Delete/add assets, and reply traffic
  - Threat for confidentiality, integrity, availability, authentication, and non-repudiation

15

Basic Encryption Techniques

- Substitution
  - Substitute a letter with another
  - E.g., Caesar cipher
    - $C_i = E(p_i) = p_i + 3$
    - Plaintext A B C D E F G H I J K L …
    - Ciphertext d e f g h i j k l m n o …

16

Basic Encryption Techniques

- Transposition (Permutation)
  - Letters of message are rearranged
  - E.g.,
    - E = (1,2,3,4) → (4,3,1,2)
    - D = (1,2,3,4) → (3,4,2,1)
    - G E O R G E b M A S O N
    - R O G E M b G E N O A S

17

Confusion

- Confusion
  - Degree of prediction of what will happen to ciphertext by change in key
  - Hides the relationship between ciphertext and key
  - E.g., Caesar cipher – not good for confusion
  - E.g., One-time pad – good confusion

18

Diffusion

- Diffusion
  - Degree of prediction of what will happen to ciphertext by change in plaintext
  - Hides the relationship between the ciphertext and the plaintext

19

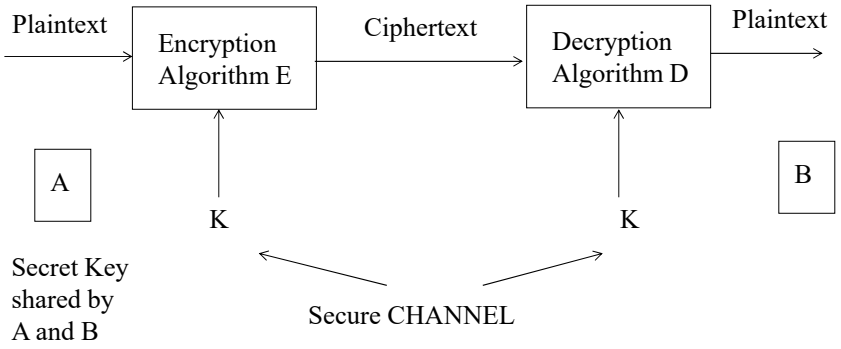
Stream and Block Ciphers

- Stream Cipher
  - Convert one symbol of plaintext to a symbol of ciphertext
  - E.g., Caesar cipher
  - Advantages
    - Speed of transformation
- Block Cipher
  - Encrypts a group of plaintext symbols as one block
  - E.g., Transposition cipher
  - Advantages
    - High diffusion

20

Symmetric Cryptosystem

- Secret Key Cryptosystem (Single Key)
  - Encryption and decryption keys are the same
  - P = D(K, C) where C = E(K, P)
  - P = D(K, E(K, P))



21

Symmetric Cryptosystem

- Confidentiality depends only on secrecy of the key
- Attacker is assumed to know E and D
- Secret key systems do not scale well
  - With N parties we need to generate and distribute N*(N-1)/2 keys
- A and B can be people and computers

22

Data Encryption Standard (DES)

- Developed for the U.S. government
  - Accepted as a cryptographic standard in US and abroad (1976)
- DES
  - 56 bits long key; 64-bit block size; E and D are public
  - Has not been broken by sustained public cryptanalysis since 1977
  - Different modes
    - Electronic Code Book, Ciphertext Block Chaining, Cipher FeedBack, Output Feedback modes
  - Adequacy questioned – Not secure

23

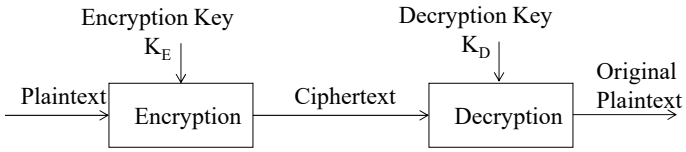
Advanced Encryption Standard (AES)

- NIST selected AES in 2001
- Symmetric key cryptography as a block cipher
  - Block sizes of 128 bits
  - Key sizes of 128, 192, and 256 bits
- E.g., Program

24

Asymmetric Cryptosystem

- Asymmetric Encryption (known as Public Key, Two Keys)
  - A pair of keys for encryption and decryption
  - $P = D(K_D, E(K_E, P))$



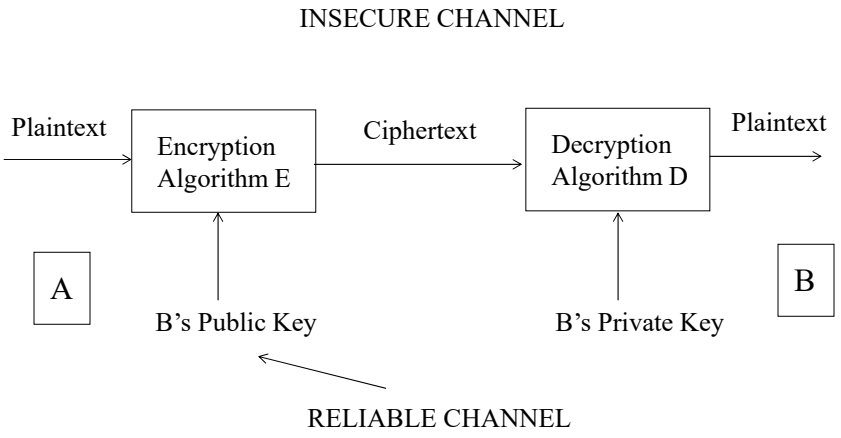
25

Public Key (Asymmetric) Encryption

- Diffie and Hellman [1976]
  - Motivation – n*(n-1)/2 for secret keys among n-users
  - Proposed a public key encryption system
  - Each user has two keys – a public key and a private key
  - $P = D(K_{PRIV}, E(K_{PUB}, P))$
    - Alice encrypts messages with Bob's public key
  - $P = D(K_{PUB}, E(K_{PRIV}, P))$
    - Bob encrypts a message with a private key and the message can be revealed with his public key

26

Public Key Encryption



27

Public Key Cryptosystem

- Solve the key distribution problem
  - Need a reliable channel for communication of public keys
- Scales well for large-scale systems
- Confidentiality based on infeasibility of computing B's private key from B's public key
- Key sizes are large (512 bits and above) to make this computation infeasible

28

RSA (Rivest-Shamir-Adelman)

- Introduced in 1978
  - To date remains secure
- Public key is (n, e)
- Private key is d
- Encrypt: $C = M^e \bmod n$
- Decrypt: $M = C^d \bmod n$
- Key size of RSA is selected by the user
  - Casual 384 bits
  - Commercial 512 bits
  - Military 1024 bits
- E.g., Program

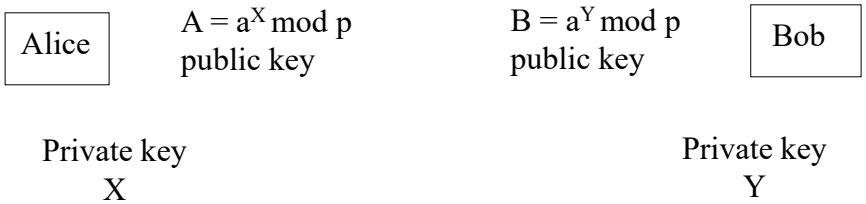
29

RSA Versus DES

- RSA encrypts at kilobits/second
- DES encrypts at megabits/second
- This 1000-fold difference in speed is likely to remain independent of technology advances
  - Due to key size and algorithm
- Public key algorithms are useful for special tasks

30

Diffie-Hellman Key Establishment



$K = B^X \bmod p = A^Y \bmod p = a^{XY} \bmod p$

- System constants
  - p: prime number, a: integer

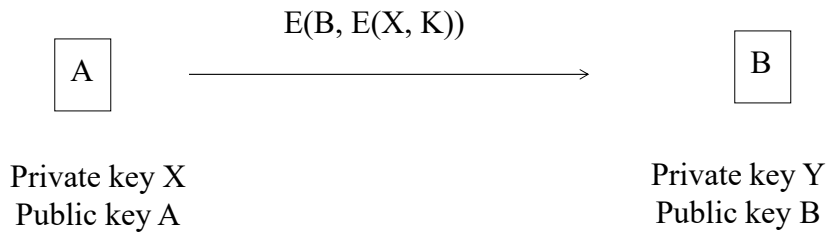
31

Diffie-Hellman Key Establishment

- Proposed in 1976
- First public key algorithm
- Allows a group of users to agree on a secret key over an insecure channel
- Requires no prior communication between A and B

32

Secret Key Exchange using Public Key



- Suppose Alice and Bob want to derive a shared symmetric key
  - Alice and Bob have public keys for a common encryption algorithm
  - Resolved authenticity for both

33

Applications for Public-Key Cryptosystems

- Encryption/decryption
- Digital signature
- Key exchange
- Some algorithms suitable for all three
  - Whereas others can be used for one or two of these applications

34

Public-Key Certificates

- Reliable distribution of public keys
- Public-key encryption
  - Sender needs public key of receiver
- Public-key digital signatures
  - Receiver needs public key of sender
- Public-key key agreement
  - Both need each other public keys
  - Strong point: scalability
  - Weakness: acquire public key of issuer

35

X.509 Certificate

Version
Serial Number
Signature Algorithm
Issuer
Validity
Subject
Subject Public Key Info
Signature

36

36

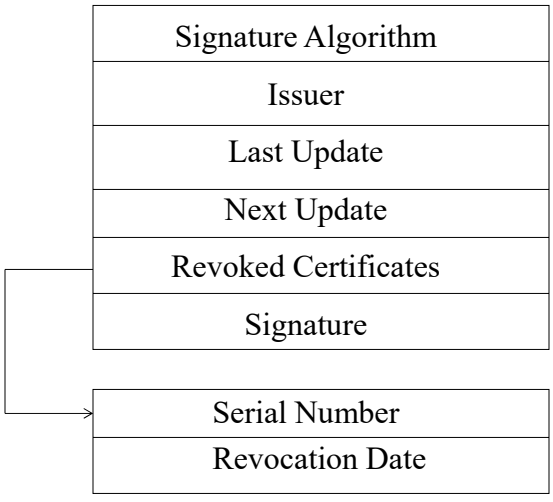
X.509 Certificate

0
1234567891011121314
RSA+MD5, 512
C=US, S=TX, O=TTU, OU=CS
1/1/20-3/1/20
C=US, S=TX, O=TTU, OU=CS, CN=Michael Shin
RSA, 1024, xxxxxxxxxxxxxxxxxxx
Signature

37

37

CRL (Certification Revocation List) Format



38

38

Public-Key Certificates

- How to acquire public key of the issuer to verify signature
- Whether or not to trust certificates signed by the issuer for this subject
- Trusted Certificate authority

39

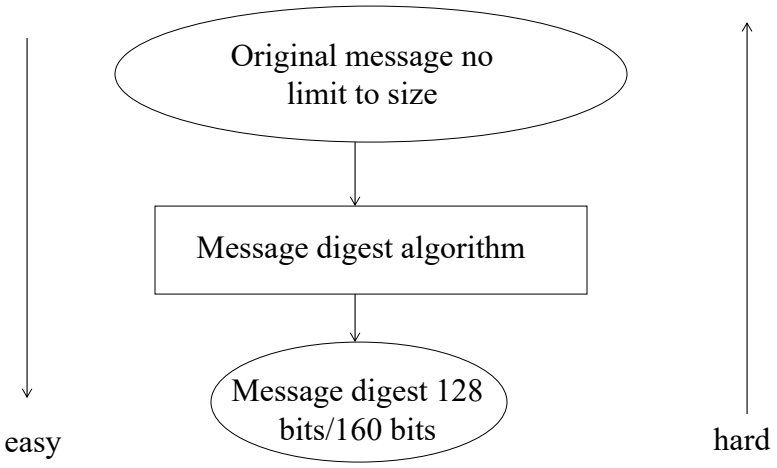
Integrity Service

- Protect against unauthorized changes to data
- One technique for integrity
  - Seal message
- Message digest (MD) or message authentication code (MAC)

40

Message Digest

- One-way function
  - m = H(M) is easy to compute
  - M = H^{-1}(m) is hard to compute



41

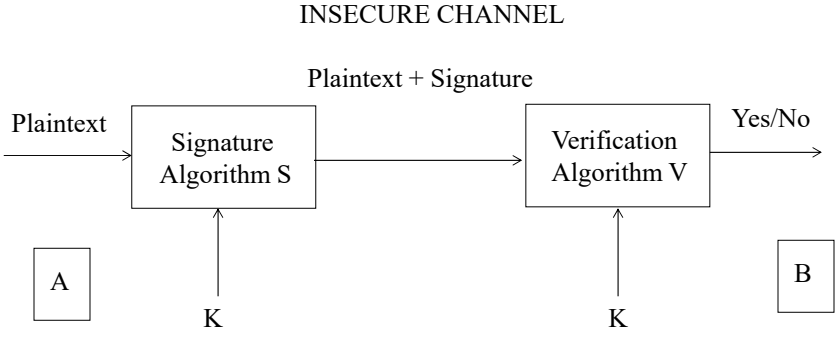
Message Digest

- MD5
  - Proposed by Ron Rivest (of RSA)
  - Improved version of MD4
  - 128 bits digest
  - Simple, compact, and fast
- NIST SHA/SHS (Secure Hash Algorithm or Standard)
  - 160 bits digest
  - Similar to MD5
  - SHA-0, SHA-1, SHA-2, SHA-3

42

Keyed Message Digests – Message Authentication Code (MAC)

- Hash-based Message Authentication Code (HMAC)



Signature = MD of plaintext + K

43

Message Digest

- Pubic-key technology is very slow
- Public-key encryption
  - Use public-key encryption to send a secret key with confidentiality
  - Actual traffic is encrypted using secret key
- Public-key digital signatures
  - Cannot sign big messages
- For performance reasons
  - Sign the message digest
  - Not the message

Message Digest

- Secret-key technique to provide efficient
  - Authentication
  - Integrity
- Does not provide
  - Non-repudiation
- E.g., Program – Secure Hash Algorithm (SHA-1)

45

Non-repudiation Service

- Protect against one party to a transaction or communication activity later falsely denying that the activity occurred
  - Digital signature
- Compared with Public-Key Encryption
- Digital signature and Encryption

46

Digital Signature

- Digital signature
  - A mark that only the sender can make
  - But other people recognize
- Suppose Sandy sends bank a message to transfer money to Tim
  - Bank needs to verify
  - Sandy wants bank not to forge message

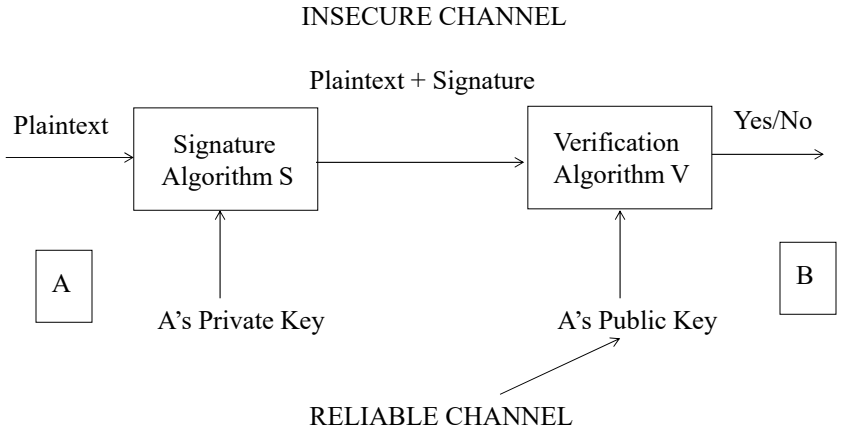
47

Digital Signature

- Person P signs message M with signature S(P, M), and sends [M, S(P, M)] to R
- Two primary properties
  - It must be unforgeable
  - It must be authentic
- Two more properties
  - It is not alterable
  - It is not reusable

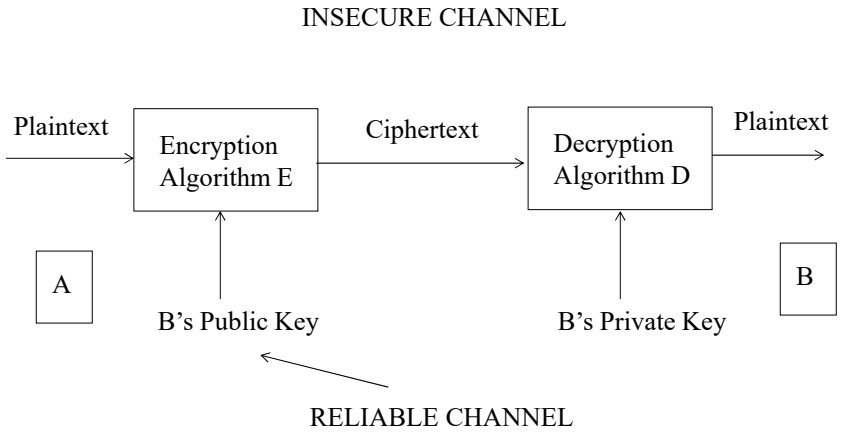
48

Digital Signature



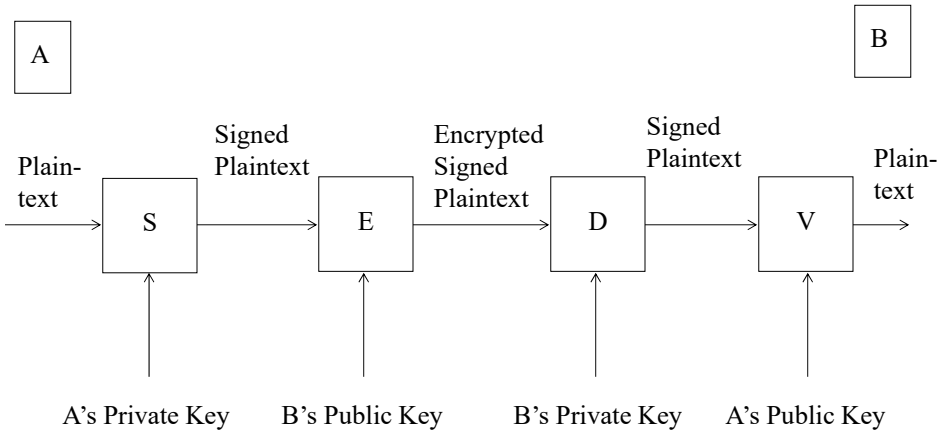
49

Compared with Public Key Encryption



50

Signature and Encryption



51

Digital Signature

- Program – SHA-1 with Digital Signature Algorithm

52

Authentication Service

- Allow an entity (a user or system) to identify itself positively to another entity
- Password, personal identification number (PIN), challenge/response, digital certificate, smart card, or biometrics

53

Authentication Service

- What the user knows
  - Passwords, personal information
- What the user possesses
  - A key, a ticket, a passport, a smartcard
- What the user is (biometrics)
  - Fingerprints, voiceprint, signature

54

Passwords: Inherent Vulnerabilities

- Easy to guess
- Easy to snoop
- Easy to lose
- No control on sharing

55

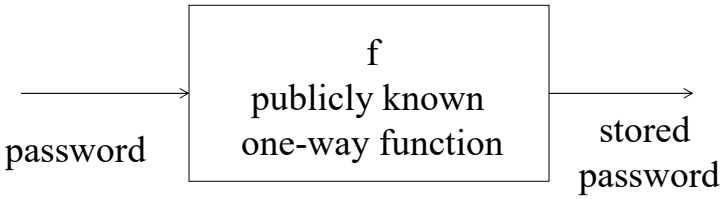
Passwords: Practical Vulnerabilities

- Visible in the clear in distributed and networked systems
- Susceptible to replay attacks if encrypted naively
- Susceptible to dictionary attacks even if encrypted

56

Dictionary Attack

- Infeasible to search all possible passwords to find a match
- Is feasible to search all likely passwords to find a match
- Enter every word in a dictionary as a password
- Users use ordinary words as passwords



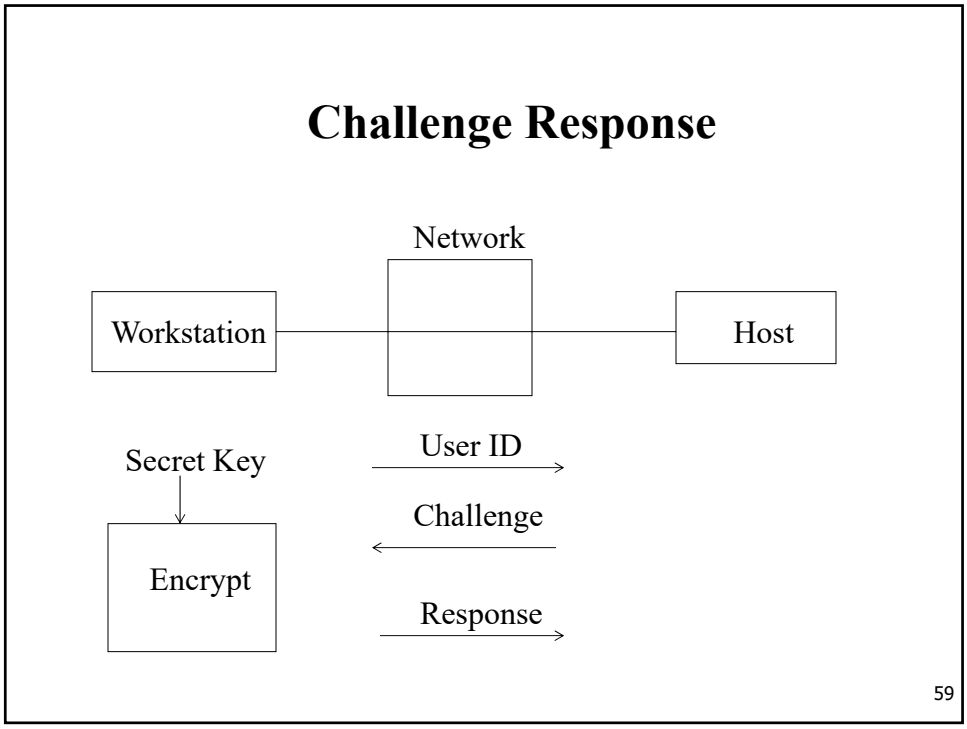
57

57

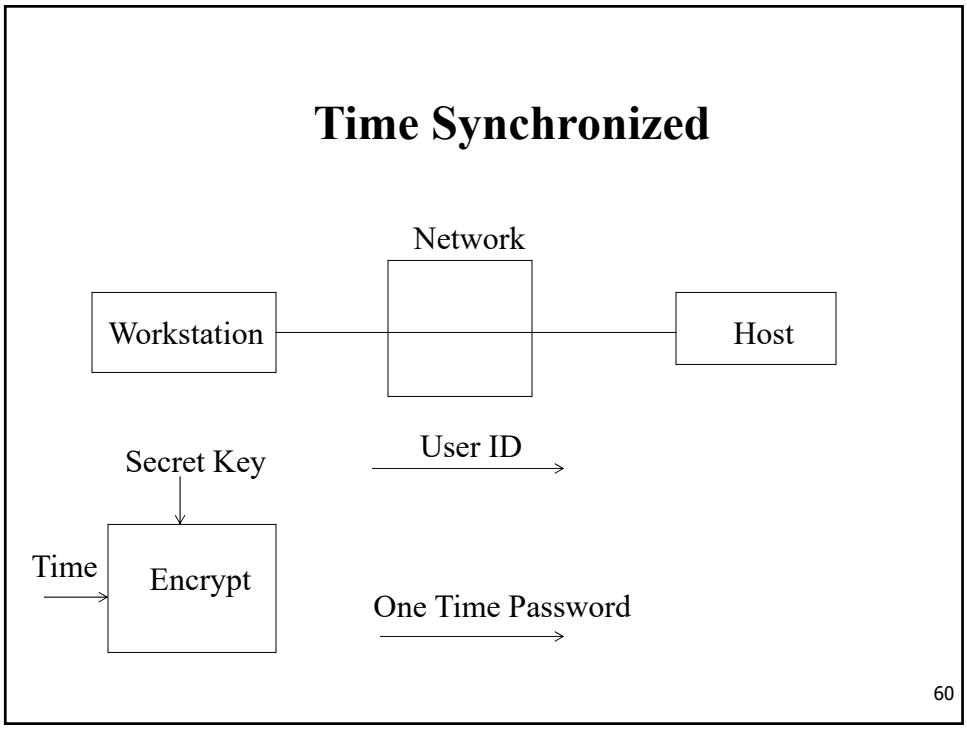
One-Time Passwords

- Random passwords that are used only once
  - User unfriendly
  - Laptop friendly
- F is a one-way function if
  - y=f(x) is easy to compute
  - $x=f^{-1}(y)$ is hard to compute
- Generate f(x), $f^2(x)$, $f^3(x)$, …., $f^{100}(x)$ where $f^k(x)=f(f(f(\ldots f(x)\ldots)))$, k times
- Use passwords in reverse order $f^{100}(x)$, $f^{99}(x)$, $f^{98}(x)$, …, $f^2(x)$, f(x)

58

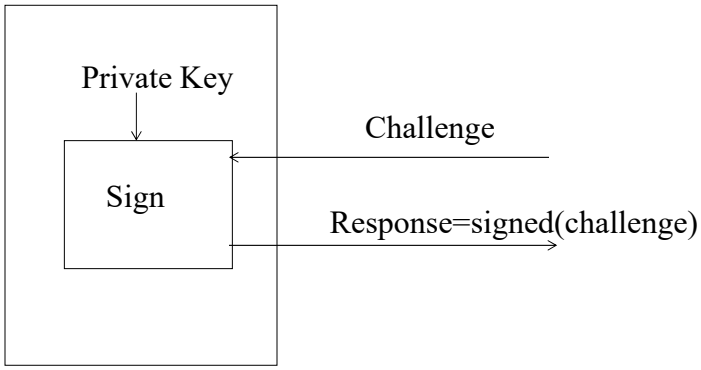

Challenge Response
Network
Workstation
Host
Secret Key
User ID
Challenge
Encrypt
Response
59

59


Time Synchronized
Network
Workstation
Host
Secret Key
User ID
Time
Encrypt
One Time Password
60

60

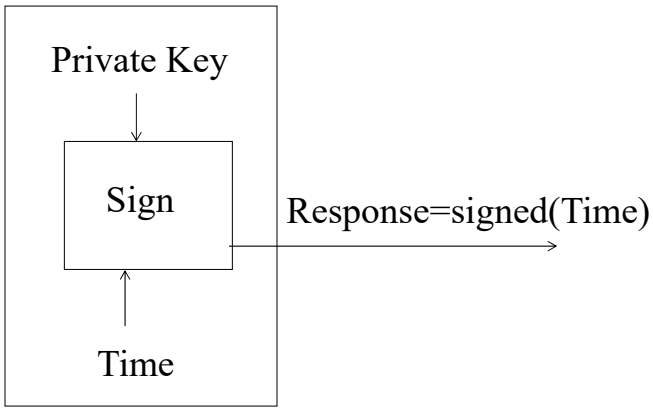
Public Key Based



61

61

Public Key Based



62

62

Access Control Service

- Access Control service
  - Protect against unauthorized access to resources based on security policies, E.g.,
    - Mandatory access control (MAC)
    - Discretionary access control (DAC)
    - Access Control List (ACL)
    - Role-based access control (RBAC)
    - Attribute-based access control (ABAC)

63

Access Control Models

- Mandatory Access Control (MAC)
  - Enforce security policy independently of user actions
  - Access to classified security information or other restricted data at the level of clearance
    - Confidential, Secret, and Top Secret
  - Used for defense arena
  - Bell-LaPadula model
- Discretionary Access Control (DAC)
  - Users can take their own access decisions about files
  - E.g., Unix, allow a team member to access a file

64

Access Control Matrix (List)

- Operating system access control
- Modeled by a matrix of access permissions
  - With columns for files and rows for users

	Operating System	Accounts Program	Account Data	Audit Trail
Sam	rwx	rwx	rw	r
Alice	x	X	rw	-
Bob	rx	R	R	r

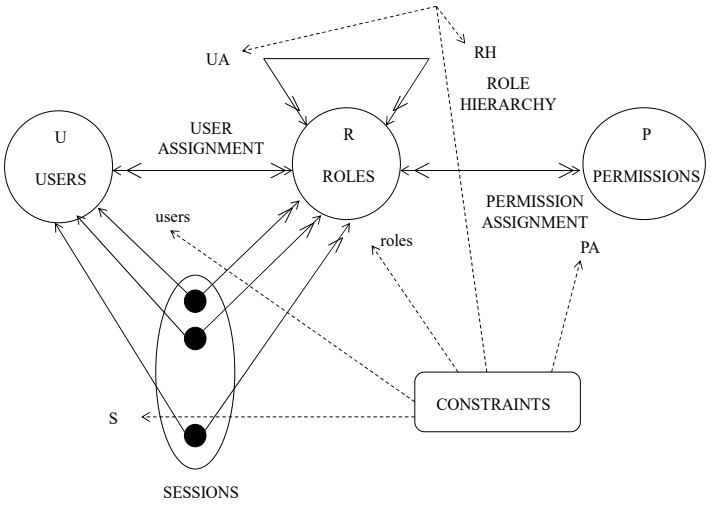
65

Role-Based Access Control (RBAC)

- RBAC
  - Proposed by Sandhu et al [1996]
  - Based on roles of subjects and mapping roles to an organization's structure
- User
  - Human being or autonomous agents
- Role
  - Job function or job title in an organization
  - Role hierarchy
- Permission
  - Some privilege to carry out specific actions
  - $x \geq y$ if role x inherits the permission of role y
- Session
  - A user establishes a session and activates some subset of roles

66

RBAC Model



67

67

RBAC - Separation of duty constraints

- Conflicting permissions cannot be assigned to the same role
  - Two conflicting permission such as *prepare check* and *issue check*
- Conflicting users cannot be assigned to the same role
  - Same family should not prepare the purchase order, and also, not be a user who approves that order
- Conflicting roles cannot be activated in the same session
  - Supervisor roles - inherits permissions from both accounts payable manager role and purchasing manager role

68

Attribute-Based Access Control (ABAC)

- A logical access control methodology
  - where authorization is determined by evaluating attributes associated with
    - the subject, object, requested operations, and,
    - in some cases, environment conditions against policy, rules, or relationships

69

Attribute-Based Access Control (ABAC)

- **Attributes** are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested actions that are predefined and pre-assigned by an authority.
- A **subject** is an active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state. It can be the user, requestor, or mechanism acting on behalf of the user or requestor.
- An **object** is a passive information system-related entity containing or receiving information. It can be the resource or requested entity, as well as anything upon which an operation may be performed by a subject including data, applications, services, devices, and networks.
- **Environmental conditions** are dynamic factors, independent of subject and object, that may be used as attributes at decision time to influence an access decision. Examples of environment attributes include time, location, threat level, temperature, etc.
- An **operation** is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, author, copy, execute, and modify.
- **Policy** is the formal representation of rules or relationships that define the set of allowable operations a subject may perform upon an object in permitted environment conditions.

70

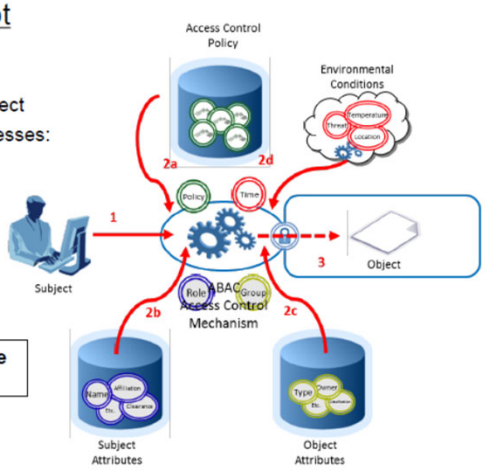
70

NIST Special Publication 800-162
Attribute Based Access Control Definition and Considerations

Basic ABAC Concept

1. Subject Requests Access to Object
2. Access Control Mechanism Assesses:
   a) Rules
   b) Subject Attributes
   c) Object Attributes
   d) Environmental Conditions
3. Subject is Given Access to Object if Authorized and Denied Access if Not Authorized

What happens when we scale this up to an Enterprise?



8

71

71

Why Attribute-Based Access Control?

- RBAC
  - Grant access based on roles
- ABAC
  - Grant access based on attributes,
    - Allows for highly targeted approach to data security.
  - To ensure an extra layer of safety that RBAC can't provide, given that ABAC looks at many variables while establishing access.
- Example
  - https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html

72

Security Services (Security Techniques or Security Measure)

- Security goals
  - CIA(Confidentiality, Integrity, Availability), Privacy, Non-repudiation
- Security services
  - Confidentiality security service
  - Integrity security service
  - Non-repudiation security service
  - Authentication security service
  - Access control security service

73

Backup Slides

- Any volunteer to explore
  - ABAC in detail?
  - Availability Security Services?
  - Privacy Security Services?

74

74