CSE 543
Information Assurance and Security

Introduction

Professor Stephen S. Yau

Fall 2022

Other Course Information (cont.)

- **Instructor:** Professor Stephen S. Yau (Sik-Sang Yau)
  - Email: ***yau@asu.edu***
  - Office hours: Tue, Thurs 3:30 p.m. to 4:00 p.m.

  Additional Appointment through email
  - Office: BYENG 488

Other Course Information (cont.)

- **Teaching Assistant**: Siddharth Gianchandani
  - Email: sgiancha@asu.edu
  - Office hours: Tue, Thurs 4:00 p.m. to 5.00 p.m.

  Additional Appointment through email
  - Office: BYENG 490BB

CSE 543
Information Assurance and Security

Security Principles

Professor Stephen S. Yau

Fall 2022

Information Forms and States

- ***Information Forms***
  - Hard copy
  - Softcopy
  - Records of formal and informal meetings
  - Telephone conversations
  - Video teleconferences
  - ………
- ***Information States***

Transmitted, processed, and stored

Threats and Vulnerabilities

- A ***threat*** is a ***potential occurrence*** that can have an undesirable effect on the system assets or resources
- A ***vulnerability*** is a ***weakness*** that makes a threat to possibly occur

Four Categories of Threats

- ***Disclosure*: Unauthorized access to information**
  - Snooping
- ***Deception*: Acceptance of false data**
  - Alteration
  - Spoofing
  - Denial of receipt

Four Categories of Threats (cont.)

- ***Disruption*: Interruption or prevention of correct operations**
- ***Usurpation*: Unauthorized control of part of a system**
  - Alteration
  - Spoofing
  - Delay
  - Denial of Service

Possible Protection

- Protect ***working areas***
- ***Keep equipment*** in ***secure environment*** and ensure it ***works properly.***
- Review ***software*** carefully to detect potential ***malicious logic.***

Possible Protection (cont.)

- Keep ***track*** of all ***sensitive files, documents, conference records, experiment results***, on printed papers or in any types of storage media.
  - ***Protect*** them from ***unauthorized access.***
  - ***Backup*** this information periodically

Possible Protection (cont.)

- ***Encrypt sensitive information*** during storage or transmission
- Obfuscate ***sensitive data*** during processing
- Choose good ***passwords*** and change them periodically
- Report ***abnormal action***s immediately

Security Principles

1. Auditability and *Accountability*

- ***Auditability*** is the ability to ***verify*** the activities of a ***control***
- ***Accountability*** is to hold ***individuals answerable, responsible or liable f***or specific activities
- ***Security control*** must produce ***reliable, indisputable evidence***
  - Evidence can take forms of **audit trails**, **system logs**, **alarms**, other overt or covert notifications

Security Principles (cont.)

2. Access Control

- ***Prevent reading modification disclosure or use*** of ***unauthorized information***

Security Principles (cont.)

2. Access Control (cont.)

- **Access control principles:**

  a) ***Separation of functions***:

  - No one owns all the processes, controls all security features, or possesses ***unrestricted access to all information***

Security Principles (cont.)

2. Access Control (cont.)

- **Access control principles** (cont.):

b) ***Independence of control and subjects***

c) ***Least privilege***

d) ***Control***

  - All access to the system must be regulated

Security Principles (cont.)

- **Access control types**

a) *Discretionary Access Control (DAC)*

b) *Mandatory Access Control (MAC)*

c) *Role-Based Access Control (RBAC)*

d) *Situation-Aware Control (SAC)*

Security Principles (cont.)

3. Confidentiality

- ***Protect*** information from ***unauthorized disclosure*** to persons, processes, or devices
- ***Confidentiality principles*** include*:*
  1. ***Need to know:*** Possess combination of clearance, privilege of access, and need-to-know before being authorized access
  2. ***Data separation***
  3. ***Compartmentalization***

Security Principles (cont.)

3. Confidentiality (cont.)

4) Classification

- Assign labels to information to identify the appropriate level of protection, handling and control of *the information*.

Corporation

- Public Use
- Internal Use Only
- Confidential
- Confidential-Restricted
- Registered-Confidential

US Government

- Unclassified
- Official Use Only
- Confidential
- Secret
- Top Secret

Security Principles (cont.)

3. Confidentiality (cont.)

5) Encryption

- A reversible process of transforming plain text into enciphered text using an encryption algorithm.

4. Integrity:

- Protection against ***unauthorized modification or destruction*** of information

Security Principles (cont.)

5. Asset Availability

- Possible mechanisms
  - Backup procedures
  - Data recovery procedures
  - Preventive maintenance plan
  - Continuity of operations plan
  - Emergency action plan

Security Principles (cont.)

6. Cost Effectiveness
7. Risk Management

- Risk is an expected loss of accountability, access control, confidentiality, integrity, or availability due to an attack or incident

Security Principles (cont.)

8. Comprehensive and Integrated Approach

- Measures, practices and procedures should address ***all relevant security considerations and security interdependencies***.

9. Life-cycle Management

Security Principles (cont.)

10. Training and Awareness

- Everyone in organization should understand his/her ***security responsibility***

11. Continuous Reassessment

12. Respect of Ethical and Democratic Rights

13. Legal Issues

Additional Definitions

- ***Choke point***
  - ***Funneling activities through a narrow channel*** improves ability to control and monitor activities
- ***Consistency***
- ***Defense in depth***
  - Multiple, overlapping layers of control provides better protection

Additional Definitions (cont.)

- ***Deny upon failure***
  - Failed control default to denial of access or service
- ***Diversity of defense***

Additional Definitions (cont.)

- ***Interdependency***
  - Security depends on other services to achieve IA
- ***Override***
  - Permit proper authorities to stop operation of control only in special circumstances

Additional Definitions (cont.)

Authentication:

Security measure designed to establish validity of transmission, message, or originator, or means of verifying an individual's authorization to receive specific categories of information

Additional Definitions (cont.)

Nonrepudiation:

Assurance that sender of data is provided with proof of delivery to recipient, and recipient is provided with proof of sender's identification.

Additional Definitions (cont.)

Secrecy:

Refers to the effect of mechanisms used to limit the principals who can access information, such as cryptography or computer access control

Additional Definitions (cont.)

Privacy:

Ability and/or right to protect certain ***personal data***; extends ability and/or right to prevent invasion of ***personal information or space***. Extends to ***families***, but not to legal persons, such as corporations and organizations.

Additional Definitions (cont.)

- Information system consists of
  - Computer systems and networks
  - Information
  - Operating environments

Additional Definitions (cont.)

- ***INFOSEC***: Information Systems Security
  - Protection of information systems against ***unauthorized access* to**, or ***modification of*, *information***, whether in storage, processing or transit, and against ***denial of service to authorized users*** or ***provision of service to unauthorized users***, including those measures necessary to detect, document, and counter such threats.

Additional Definitions (cont.)

- ***OPSEC*****: Operations Security**
  - A *process* that determines ***what information*** adversaries can obtain or piece together from observation and to provide ***measures*** for ***reducing such vulnerabilities*** to acceptable levels

Additional Definitions (cont.)

- ***Indicators:***
  - ***Profile*** indicator – normal activities
  - ***Deviation*** indicator – different from normal activities
  - ***Tip-off*** indicator – drawing attention to information that otherwise might pass unnotices.

References

- M. E. Whitman and H. J. Mattord , *Principles of Information Security*, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431

- "DoD Instruction 8580.1, Information Assurance (IA) Implementation, 9/7/2004". Department of Defense. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858001p.pdf

CSE 543
Information Assurance and Security

Security Strategies

Professor Stephen S. Yau

Fall 2022

Security Strategies

- Obscurity Strategy
- Perimeter Defense Strategy
- Defense in Depth Strategy

Security by Obscurity Strategy (Stealth)

- If the existence of an organization’s IA baseline and critical objects are ***unknown***, the organization might avoid or reduce threats
- Intent to secure the system by ***hiding*** the details of security mechanisms
- IA involves use of obscurity strategy to a variety of extent

Perimeter Defense Strategy

- Focus on threats from ***outsiders***
- Intent to ***control flow of information*** between organization’s internal trusted network and untrusted external networks
- Not much IA capabilities is allocated to secure ***internal*** system
- Examples: Firewalls, security access keys, access codes
- Major weaknesses?

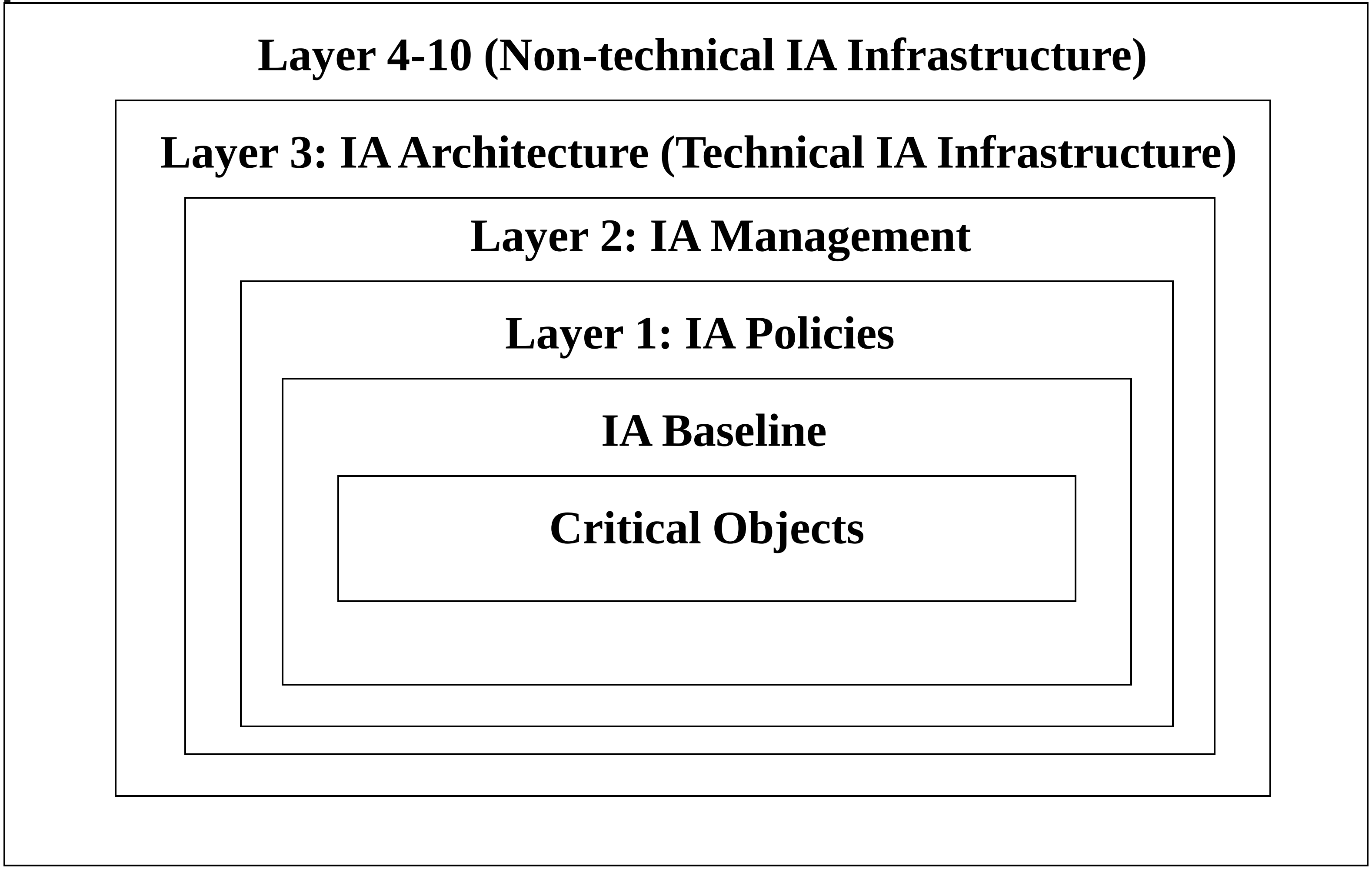
Defense in Depth Strategy

- Define a number of ***inter-operable and complementary technical and non-technical IA layers of defense***
- Separate organization’s network into ***enclaves***
  - An ***enclave*** is an environment under control of a single authority with personnel and physical security measures.

Defense in Depth Strategy (cont.)

- ***Perimeter defense*** for each enclave
- ***Complicated and multiple connections*** among enclaves and between an enclave and outside
- Need ***multiple layers*** and ***different solutions for each connection***

Defense in Depth Strategy
--- Layered Architecture Model



Layer 4-10 (Non-technical IA Infrastructure)

Layer 3: IA Architecture (Technical IA Infrastructure)

Layer 2: IA Management

Layer 1: IA Policies

IA Baseline

Critical Objects

Defense in Depth Strategy (cont.)
--- Layered Architecture Model

-***Core*** consists of ***critical objects*** and ***IA baseline*** that collect, input, process, store, output, and communicate with any element in core.

Defense in Depth Strategy (cont.) *--- Layered Architecture Model*

-IA Policies (Layer 1) define the actions and behavior required to accomplish the organization's IA needs.

Defense in Depth Strategy (cont.)
--- Layered Architecture Model

-***IA Management*** (Layer 2) monitors and controls implementation of the IA policies.

Defense in Depth Strategy (cont.)
--- Layered Architecture Model

-IA Architecture (Layer 3) provides a means to allocate and integrate technical and non-technical controls

Defense in Depth Strategy (cont.)
--- Layered Architecture Model

- ***Layers 4 - 10***: non-technical implementations of IA policies, and provide ***infrastructure*** for IA Architecture
  - Layer 4 Operational security administration
  - Layer 5 Configuration management
  - Layer 6 Life-cycle security
  - Layer 7 Contingency planning
  - Layer 8 IA education, training, awareness
  - Layer 9 IA policy Compliance Oversight
  - Layer 10 IA incident response and reporting

Layer 3: IA Architecture

- Ensures that at least the minimum level of interoperability and services is available to authorized users to perform their tasks, to coordinate with other users, and to exchange information ***securely***
- Integrates three levels of security:
  - Physical security
  - Procedure security
  - Logical security

Layer 4: Operational Security Administration

- People:
  - Users: general and privileged
  - Separation of roles
  - Prevention
  - Limitation
  - Accountability
  - Detection
  - Deterrence
  - Outsourcing
- Security operations

Layer 5: Configuration Management

- Provide a mechanism to ensure ***documentation of all changes***

- Identify anticipated ***effects of changes*** on ***cost/schedule*** as a basis for approving or disapproving proposed changes

Layer 5: Configuration Management (cont.)

- Maintain ***integrity of schedule***
- Maintain updated documentation on ***status of each proposed change***
- Ensure all changes ***communicated to appropriate personnel***

Layer 6: Life-Cycle Security

- Security is involved in each state of the system's life cycle:
  - Initiation
  - Definition
  - Design
  - Acquisition
  - Development and Implementation
  - Operation and Maintenance
  - Destruction and Disposal

Layer 7: Contingency Plan

- Planning for the worst
  - Backups
  - Power outage
  - Emergency action plan/disaster recovery plan
  - Continuity of operations plan

Layer 8: IA Education, Training, and Awareness

- IA support services
- IA awareness programs
- IA curriculum development, certification and accreditation
- IA compliance inspection and validation
- Workshop, conference and symposia support

Layer 9:
IA Policy Compliance Oversight

- Provide a means of ***detecting, reporting, and correcting noncompliance*** with the ***IA policies***
  - Intrusion detection systems
  - Scanners
    - Probing vulnerabilities of network
    - Specifying IP addresses to check origins of communication (OS, servers, routers, firewalls,…)
  - Automated auditing
  - Virus detectors
  - Periodic assessments of IA management and vulnerabilities

Layer 10: IA Incident Response & Reporting

- No perfect prevention systems, and incidents are expected
- General incident handling procedures:
  1. Determine appropriate response
  2. Collect and safeguard relevant information
  3. Contain the situation
  4. Assemble the incident management team

Layer 10: IA Incident Response & Reporting (cont.)

- General Incidence handling procedures (cont.)
  5. Create evidence disks and printouts
  6. Eradicate/clean up/recover
  7. Prepare preliminary status report for management and other authorities
  8. Document and report all activities
  9. Lesson learned: make improvements

References

- J. G. Boyce, D. W. Jennings, *Information Assurance*: *Managing Organizational IT Security Risks*. Butterworth Heineman, 2002, ISBN 0-7506-7327-3
- M. E. Whitman and H. J. Mattord , Principles of Information Security, 6th edition, Thomson Course Technology, November 2018
- Rahul Gupta, "The Need for Mission Assurance". *PRTM Magazine*, 2006.

CSE 543

Information Assurance and Security

Blockchain and IA Applications

Professor Stephen S. Yau

Fall 2022

Important Features of Blockchain

- Decentralization
- Immutability
- High Fault Tolerance
- High Availability
- Transparency
- Auditability

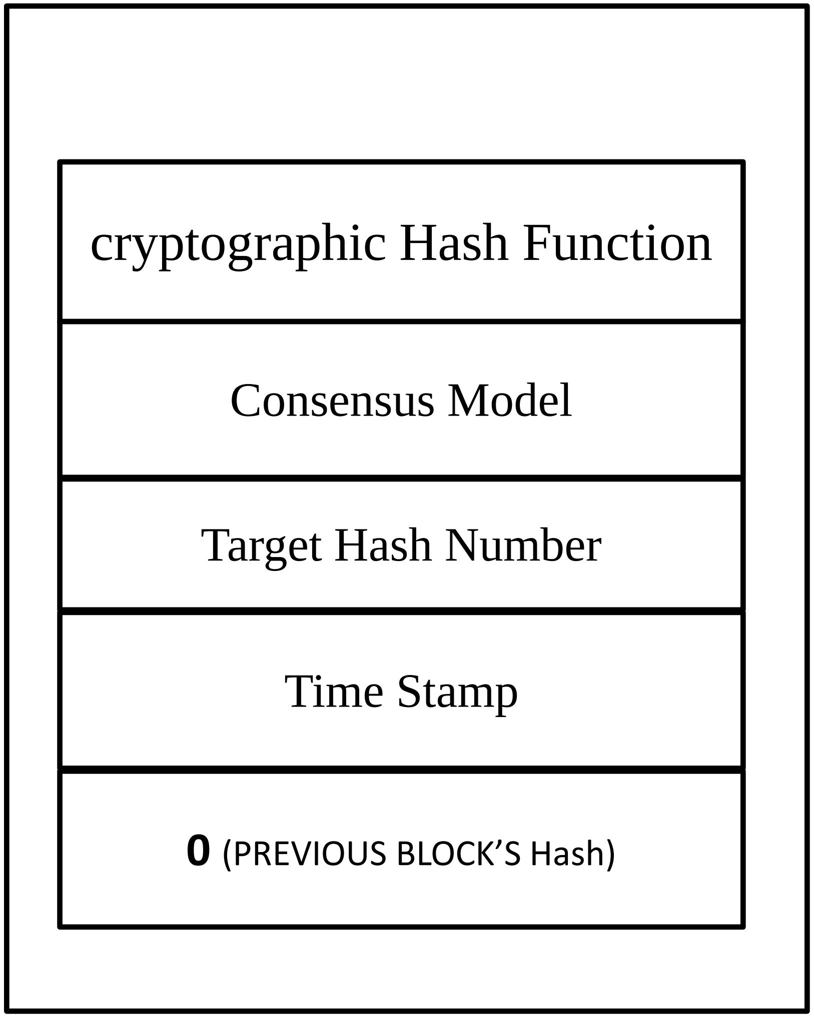
Major Applications of Blockchain

- Software development
- Supply chain
- Electronic voting
- Cloud, edge and/or IoT computing
- Finances
- Healthcare
- Smart city and/or smart world
- …

What Is a Blockchain?

- A sequence of blocks, in which *each block consists of a header and body*, and the *blocks are linked by storing the previous block's hash in the current block header*
- The first block in blockchain is called ***genesis block***

Genesis Block



cryptographic Hash Function

Consensus Model

Target Hash Number

Time Stamp

0 (PREVIOUS BLOCK’S Hash)

Cryptography

Cryptography:

- Study of mathematical techniques related to certain aspects of information security, such as confidentiality, data integrity, entity authentication, and data origin authentication.
- The basic component of cryptography is a ***cryptosystem***

Cryptosystem

A ***cryptosystem*** is a 5-tuple (E, D, M, K, C), where M is the set of plaintexts,

K is the set of keys,

C is the set of ciphertexts,

E: $M \times K \rightarrow C$ is the set of encipher functions,

D: $C \times K \rightarrow M$ is the set of deciphering functions.

Types of Cryptosystems

Symmetric cryptosystems are ***classical cryptosystems***:

$$M = D(K, E(K, M))$$

K, is used as both encryption and decryption

Types of Cryptosystems (cont.)

Asymmetric cryptosystems:

$$M = D(K_d, E(K_e, M))$$

K_d is the decryption key and K_e is the encryption key

$K_\mathrm{d} \neq K_\mathrm{e}$

Cryptography in Blockchain

- A ***one-way hash function***, also known as ***a message digest***, is a mathematical function that takes a variable-length input string and converts it into a fixed-length binary sequence that is computationally difficult to invert - that is, generate the original string from the hash.

Cryptography in Blockchain (cont.)

- ***Hashing*** is a process using a ***one-way cryptographic function*** to generate a digest of fixed size from a string of input text, such as SHA256 and Scrypt.
- **Digital Signatures** for source verification

Cryptography in Blockchain

- In blockchain, private keys are used to digitally sign the records in block body, and public keys are used to verify signatures

Consensus in Blockchain

- A means for majority of the nodes to reach an agreement before adding validated blocks to the blockchain.
  - Two consensus models used in blockchain: Proof of Work, and Proof of Stake.

Blockchain Network

- **Blockchain Network is a peer-to-peer network**
  - Each node (peer) has the following functions:
    - ***Store a part of the blockchain***
    - ***Store the entire copy of blockchain***
    - ***Generate and validate blocks being added to the blockchain***

Blockchain Network

- For nodes to actively participate in a blockchain network, they must be ***always connected*** to the network
- The nodes that generate new blocks are called ***miners***

Target Hash In Genesis Block

- ***Difficulty level*** (from 0 to 2^256) set in genesis block
- When a new block is added to a blockchain, the hash number Hn of the new block is computed with the input as block header of the new block:

```
if Hn < Target Hash:
        add new block to blockchain
else:
        reject new block
```

Consensus in Blockchain

- **Proof of Work:**
  - A block generated by a miner is accepted, when it shows proof of spending a pre-determined amount of computational resources in generating the block.
  - For example, in bitcoin, the nodes are required to solve the cryptographic problem of finding a hash of the block which is less than the target hash of the blockchain.

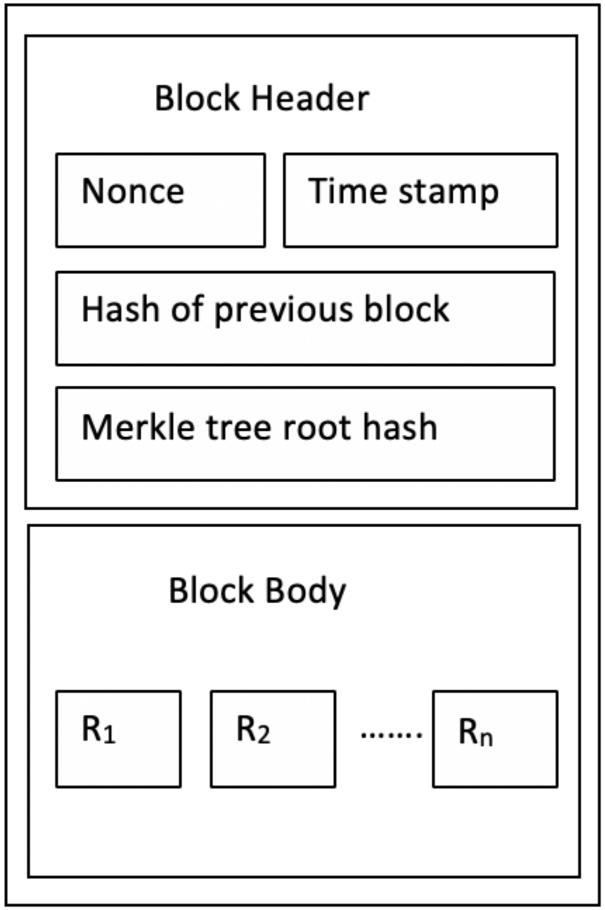
Consensus in Blockchain (Cont.)

- **Proof of Stake**
  - The ***miner*** which creates a block is chosen randomly based on what is at stake by the miner
  - For example, the wealth of the miner could be at stake

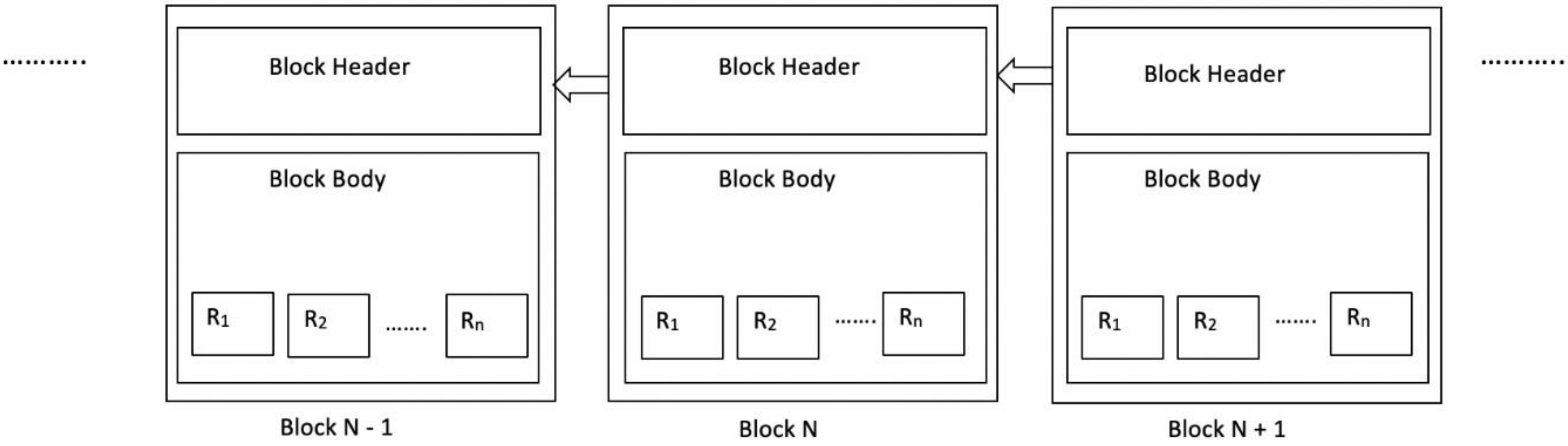
Timestamp

- **Timestamp**
  - The current time (in seconds) in universal time since January 1, 1970 when the block is created.

Block structure



Blockchain Structure



Block Structure in Blockchain

- **Header**
  - Previous block's hash
  - Merkle tree root hash
  - Timestamp
  - Nonce

- **Body**
  - Records. For examples,
    - Validated healthcare records
    - Financial records (e.g. Bitcoin Transactions)

Header

- **Previous block's hash**
  - Calculated as Hash (Merkle root hash | Previous block hash | Timestamp | Nonce)
- **Merkle tree root hash**
  - Created by repeatedly hashing pairs of records in block body until there is only one hash left, which is called Merkle root tree hash
  - Each leaf node stores transaction record from block body
- **Nonce (Number Only used Once)**
  - A random number that meets the requirements of a target hash.

Smart Contracts

- An interactive computer program that ***defines transaction protocol, including*** the ***<u>high level</u> terms*** of a contract of an agreement
- ***Automatically executed*** in blockchain

Smart Contracts Creation

Two Phases:

1. Initialization

   Initialize agreement with ***actionable*** ***clauses and properties***

2. Execution methods

   Implement methods to handle actionable clauses

A Smart Contracts Example

1. Client and Tasker agree on blockchain platform
2. Client creates and deploys smart contract on blockchain platform with agreement clause(s)
3. Tasker performs task and provides the result to smart contract
4. Smart contract automatically verifies the result against agreement clauses
5. Smart contract automatically triggers execution action in the agreement on blockchain platform.

Reference: https://rubygarage.org/blog/ethereum-smart-contract-tutorial

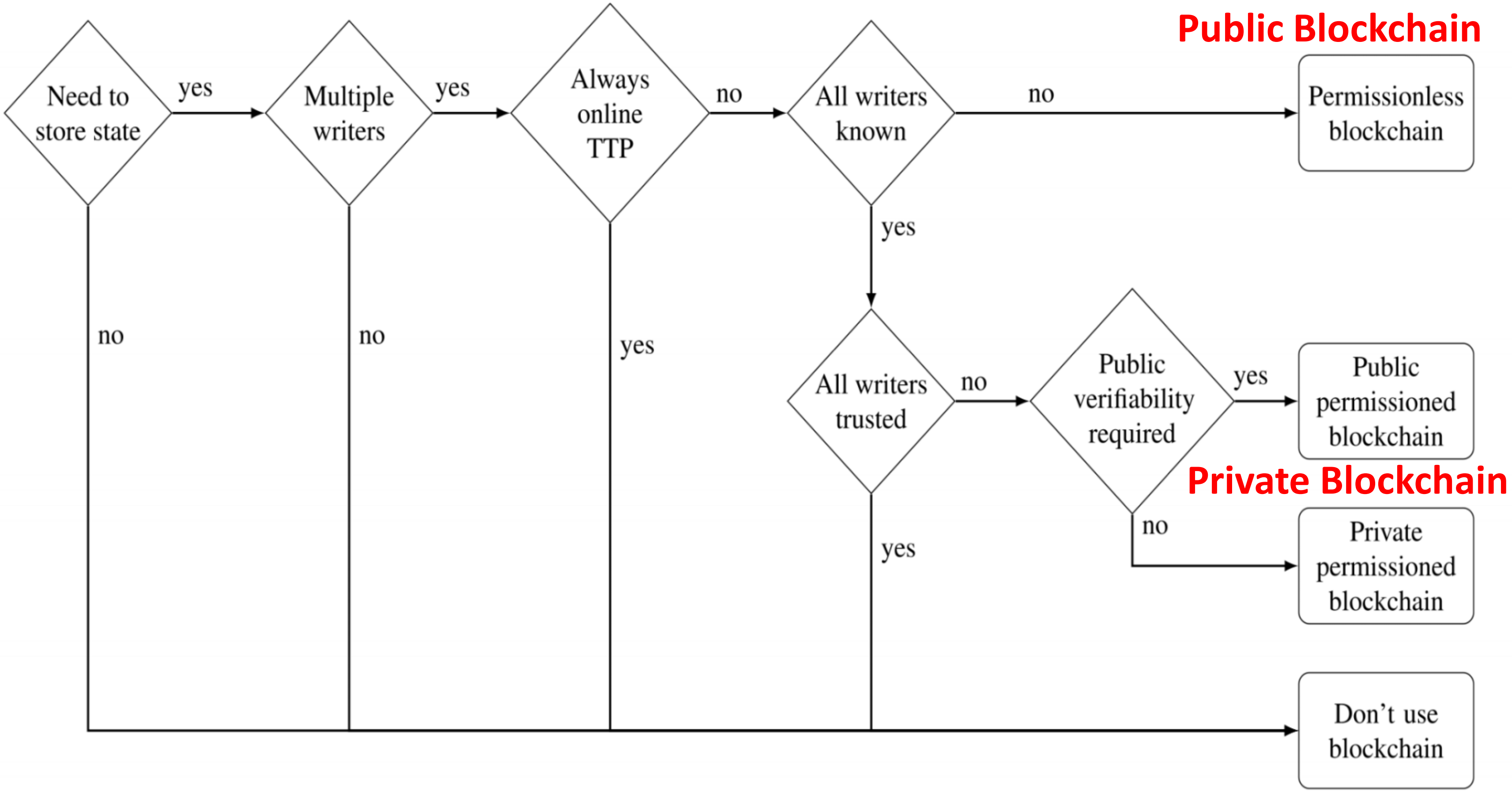
Types of Blockchains

- **Public (Permissionless)**
  - Participation/access not restricted to any nodes
  - Anyone with an Internet connection can be part of this blockchain
  - Example - Bitcoin
- **Public (Permissioned)**
  - Anyone can join after passing a suitable identity verification process.
  - Mixture of public permissionless and private blockchains and support many options for customization.
  - Example - Ethereum

Types of Blockchains

- **Private (Permissioned)**
  - Under administrative control of an entity/organization, or a closed group
  - Does not require expensive mining process
  - Example – Corda
- **Consortium**
  - Combination of several blockchains
  - Example - Hyperledger

Is blockchain suitable for your application?



Reference: Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When intrusion detection meets blockchain technology: a review. Ieee Access, 6, pp.10179-10188.

Popular Blockchain Platforms

- Hyperledger (https://www.hyperledger.org/)
- Ethereum (https://www.ethereum.org/)

Challenges

- **Scalability**
  - All the active nodes must have entire copy of blockchain which is a huge storage requirement
- **High computational resource requirements**
  - Proof of Work consensus algorithms require significant amount of computation power to calculate hash of block
- **51% attack**
  - If a group of miners can control more than half of blockchain network’s computational resources, this will undermine the major features of blockchain

References for Blockchain and IA Applications

1. Zheng, Zibin, et al. "An overview of blockchain technology: architecture, consensus, and future trends." *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017.
2. M. E. Whitman and H. J. Mattord , Principles of Information Security, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431
3. Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When intrusion detection meets blockchain technology: a review. 10.1109/ACCESS.2018.2799854 https://ieeexplore.ieee.org/document/8274922.

References for Blockchain and IA Applications

4. M. Conti et. al, “A Survey on Security and Privacy Issues of Bitcoin”, ArXiv: DOI:10.1109/COMST.2018.2842460
5. P. Zhang et al, “FHIRChain: Applying Blockchain to Securely and Scalable Share Clinical Data”, in J. Comp. & Struct. Biotechnology, 2018.
6. H. Zhu and Y. Zhang, "Collaborative Testing of Web Services," in IEEE Transactions on Services Computing, vol. 5, no. 1, pp. 116-130, Jan.-March 2012, doi: 10.1109/TSC.2010.54.

References for Blockchain and IA Applications

7. B. Anderson and S. S. Yau, “A Blockchain-based Scalable Approach to Protecting Electronic Voting from Central Authority Attacks,” Proceedings of 6th IEEE Cyber Science and Technology Congress, (virtual). October 2021, 8 pages.
8. Stephen S. Yau and Jinal S. Patel School of Computing, Informatics, and Decision Systems Engineering Arizona State University “A Blockchain-based Testing Approach for Collaborative Software Development”
9. Stephen S. Yau and Jinal S. Patel School of Computing, Informatics, and Decision Systems Engineering Arizona State University “Application of Blockchain for Trusted Coordination in Collaborative Software Development”

CSE 543
Information Assurance and Security

Cryptography

Professor Stephen S. Yau

Fall 2022

Cryptography

- In Greek means “secret writing”
- An interceptor, intruder or adversary can make following threats:
  - Block message
  - Intercept message
  - Modify message
  - Fabricate message

Cryptography (cont.)

- ***Cryptography:* *Study*** of ***mathematical techniques*** related to **certain aspects of information security**, such as confidentiality, data integrity, entity authentication, and data origin authentication

Cryptography (cont.)

- The basic component of cryptography is a ***cryptosystem***

- ***Cryptology: Study*** of ***encryption and decryption***, including cryptography and cryptanalysis.

Cryptosystem

- A ***cryptosystem*** is a 5-tuple (E, D, M, K, C), where M is the set of plaintexts,

  K is the set of keys,

  C is the set of ciphertexts,

  E: $M \times K \rightarrow C$ is the set of encipher functions, D: $C \times K \rightarrow M$ is the set of deciphering functions.

Types of Cryptosystems

- ***Symmetric*** cryptosystems are ***classical cryptosystems***:

  $M = D(K, E(K, M))$

  - K, is the encryption/decryption key

Types of Cryptosystems (cont.)

- ***Asymmetric*** cryptosystems:

  $M = D(K_d, E(K_e, M))$

  - K_d is the decryption key and K_e is the encryption key
  - $K_\mathrm{d} \neq K_\mathrm{e}$

Classical Cryptography

- Basic techniques for classical ciphers
  - ***Substitution:*** One letter is exchanged for another
  - ***Transposition:*** The order of the letters is rearranged
- Classical ciphers
  - ***Mono-alphabetic:*** Letters of the plaintext alphabet are mapped to ***other unique*** letters
  - ***Poly-alphabetic:*** Letters of the plaintext alphabet are mapped to letters of the ciphertext space depending on their ***positions*** in the text

Substitution

- Substitute each letter in the plaintext for another one.
- *Example* (Caesar Cipher)
  - a b c d e f g h i j k l m n o p q r s t u v w x y z
  - q e r y u i o p a s d f g w h j k l z x c v b n m t

Plaintext: under attack we need help

Ciphertext: cwyul qxxqrd bu wuuy pufj

Transposition

- Change the positions of the characters in the plaintext
- ***Example:***
  - message: meet me after the toga party
    - m e m a t r h t g p r y
    - e t e f e t e o a a t
  - Ciphertext: MEMATRHTGPRYETEFETEOAAT

Symmetric Cryptosystems

Four Secure Key Distribution Strategies

1. A key K can be selected by A to be shared with B, and K needs to be ***physically delivered*** to B

2. A third party can select the same key K and ***physically deliver*** K to A and B

Symmetric Cryptosystems

Four Secure Key Distribution Strategies (cont.)

3. If A and B have ***previously used*** a key K’, one party can ***transmit*** the new key K to the other, ***encrypted*** using the old key K’
4. If A and B each has an ***encrypted connection*** to a third-party C, C can ***transmit*** the new key K on the ***encrypted links*** to both A and B

Asymmetric Key Cryptosystem (Public Key Cryptosystem)

- Uses public and private keys
  - Public key can be used for encryption (or decryption)
  - Private key can be used for decryption (or encryption)
- Examples:
  - RSA, Trapdoor one-way function
  - Elliptical curve cryptography

Public Key Distribution and Authentication

- Using the “right” Public Key:
    - Must be **authentic**, not necessarily secret
- Obtaining the “right” Public Key:
    - *Directly* from its owner
    - *Indirectly*, in a signed message from a *Certification Authority* (CA):
        - A ***Certificate*** is a digitally signed message from a CA binding a public key to a name
        - Certificates can be passed around, or managed in directories
        - Protocols for certificate generation: e.g., X.509 (RFC 2459), SPKI/SDSI

Encryption in Android Devices

- Android has two methods for device encryption:
  - file-based encryption
  - full-disk encryption.

Encryption in Android Devices (cont.)

- ***File-based encryption:***
  - Android 7.0 and later supports file-based encryption. File-based encryption allows different files to be encrypted with different keys that can be unlocked independently. Devices that support file-based encryption can also support Direct Boot, which allows encrypted devices to boot straight to the lock screen, thus enabling quick access to important device features like accessibility services and alarms.

Encryption in Android devices (cont.)

- ***Full-disk encryption:***
  - Full-disk encryption is the process of encoding all user data on an Android device using an encrypted key. Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk and all reads automatically decrypt data before returning it to the calling process.

Homomorphic Encryption

- Perform computations on homomorphically encrypted data without decryption, and the result is in the form of plain text.
  - Obscurification?
  - Provide privacy-preserving storage. (why?)

Steganography

- In Greek, steganography means "***covered writing***"
- ***Prevent detection of hidden messages***
- Goals of cryptography and steganography:
  - Cryptography: conceal the ***content*** of the messages
  - Steganography: conceal the ***existence*** of the messages

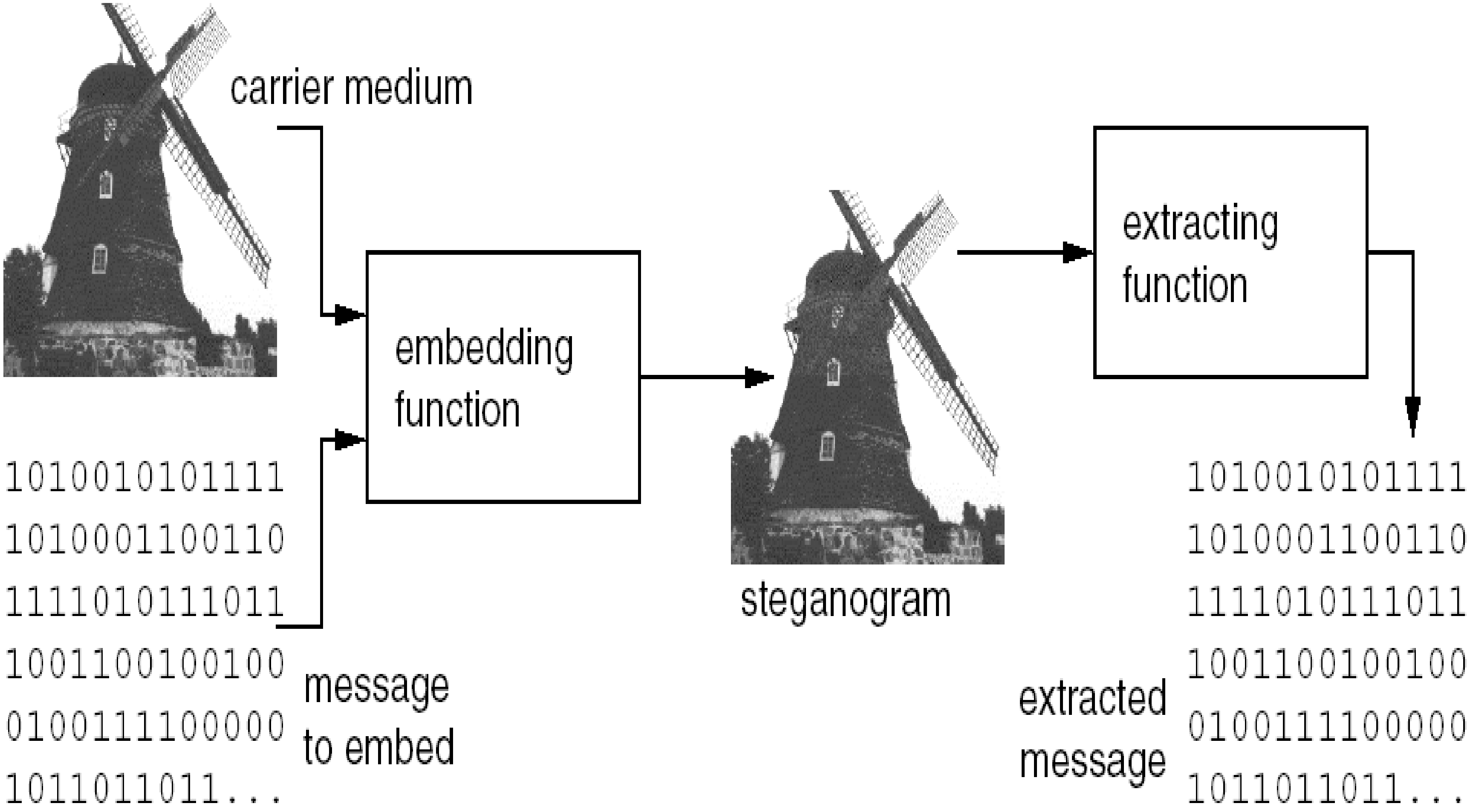
Steganography (cont.)

- What to hide
  - Texts
  - Images
  - Sound
  - ……
- How to hide
  - – embed text in text/images/audio/video files
  - – embed image in text/images/audio/video files
  - – embed sound in text/images/audio/video files

A Real Steganographic Example

- During WWI, the following cipher message was sent by a German spy
    - "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils"
- Hidden Message
    - "Pershing sails from NY June 1"
    - How to extract the hidden message from the sent message?

A Steganographic System



carrier medium

embedding function

steganogram

extracting function

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

message to embed

extracted message

1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

Digital Watermarking

- Used primarily for identification and embedding a unique piece of information within a medium without noticeably altering the medium

Digital Watermarking

- ***Publishing and broadcasting industries*** are interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

Applications of Digital Watermarking

- ***Copyright protection***
- ***Identification of financial instruments***, such as bills, coins, treasury bonds, cashier's checks, traveler's checks, notes, food stamps

Applications of Digital Watermarking

- ***Broadcast monitoring*** (television news often contains watermarked video from international agencies)
- Others

Digital Signature

- A mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity).

Digital Signature (cont.)

- Standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.
- Example - biased blind multisignature

Digital Signature (cont.)

- A digital signature scheme typically consists of three algorithms:
  - A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
  - A signing algorithm that, given a message and a private key, produces a signature.
  - A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Advantages of Digital Signature

- **Authentication**
  - Can be used to authenticate the identity of the source messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
- **Non-repudiation**
  - An entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Advantages of Digital Signature (cont.)

- **Integrity**
  - If a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions

References

- M. E. Whitman and H. J. Mattord , Principles of Information Security, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431
- Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2nd edition, November 2007.
- A. B. Levina, V. Y. Kadykov and D. I. Kaplun, "New direction in Cryptography: Homomorphic Encryption," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 234-237, doi: 10.1109/ICAI52893.2021.9639809.
- Encyprion and Data Protection, https://source.android.com/docs/security/encryption

CSE 543
Information Assurance and Security

Machine Learning in IA Applications

Professor Stephen S. Yau

Fall 2022

Areas Enabling AI Applications

- Computing paradigms and systems
  - Architecture, hardware, software, ...
- Algorithms
- Smart and big data
- Internet and mobile networks
- Sensing devices
- Semiconductor technologies
- …

IEEE World Congress On Services

September 5-11, 2021 (virtual).
https://conferences.computer.org/services/2021/

July 11-15, 2022 (hybrid) Barcelona, Spain
https://conferences.computer.org/services/2022/

Major Applications of Machine Learning

- **Cybersecurity**
- **Speech recognition**
- **Customer service**
- **Pattern recognition**
- **Finances**
- **Healthcare**
- **Transportation**
- **Smart city**
- **…**

Applications of Machine Learning Algorithms to Cybersecurity

- Cloud Systems
- IoT Networks
- Social Networks
- Smart Cities
- Cyber Threat Identification
- Attacks Prediction
- Trusted Coordination of Collaborative Services for Effective Space-Air-Ground-Water Computing and Communications
- …

What Is Machine Learning?

Machine learning focuses on the use of ***relevant data and powerful algorithms*** to imitate ***humans*** to learn and improve the accuracy of the ***recognition process*** of applications.

Machine Learning Methods

- Supervised
- Unsupervised (clustering)
- Reinforcement
- Data mining
- Deep Learning
- Statistical machine learning
- …

Neural Networks

- Neural Network is inspired by and resembles the human nervous system and the structure of the human brain.
- It consists of processing units (nodes) organized in input and output layers. The nodes in each layer are connected to nodes in adjacent layers.

References for Machine Learning and IA Applications

1. S. Durga, R. Nag and E. Daniel, "Survey on Machine Learning and Deep Learning Algorithms used in Internet of Things (IoT) Healthcare," Proc. 3rd Int'l Conf. on Computing Methodologies and Communication (ICCMC), 2019, pp. 1018-1022.
2. U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu and M. Stanley, "A brief survey of machine learning methods and their sensor and IoT applications," Proc. 8th Int'l Conf. on Information, Intelligence, Systems & Applications (IISA), 2017, pp. 1-8.
3. A. Arpteg, B. Brinne, L. Crnkovic-Friis and J. Bosch, "Software Engineering Challenges of Deep Learning," Proc. 44th Euromicro Conf. on Software Engineering and Advanced Applications (SEAA), 2018, pp. 50-59.

References for Machine Learning and IA Applications

4. P. Podder, S. Bharati, M. R. H. Mondal, P. K. Paul, and U. Kose, “Artificial Neural Network for Cybersecurity: A Comprehensive Review,” Jour. Information Assurance and Security, 2021, oo. 10-26.
5. S. S. Yau, A. B. Buduru and V. Nagaraja, “Protecting Critical Gloud Infrastructures with Predictive Capability”, Proc. IEEE 8th Int’l Conf. on Cloud Computing, New York, NY, June 2015, pp. 1119-1124
6. S. Guha, S. S. Yau and A. B. Buduru, "Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection", Proc. IEEE Int’l Conf. on Dependable, Autonomic and Secure Computing (DASC), Auckland, New Zealand, August 2016, pp. 414-419

CSE 543
Information Assurance and Security

IA Applications of Formal Methods

Professor Stephen S. Yau

Fall 2022

IA Applications of Formal Methods

- ***Objective:***

More precisely determine the requirements, and analyze the information system so that ***security incidents can be prevented or at least identified.***

IA Applications of Formal Methods

Step 1*: System Specification:** ***Abstraction and modeling with a well-defined syntactic and semantic structure for system to operate.

IA Applications of Formal Methods

Step 2*: Requirement Specification:** Security modeling (e.g., BLP model) to represent the security requirements ***unambiguously.

IA Applications of Formal Methods

Step 3*: *Validation: Formally validate the system with respect to its requirements.

- ***Model checkin***g (by searching the satisfiability of the given characteristics of the system in the possible models)
- ***Theorem proving*** (by inference of given system characteristics using syntactical inference rules in theory proving)

Formal Methods – Modeling

- Abstract representations of a system using mathematical entities and concepts
- **Modeling: C*apture essential system characteristics and ignore irrelevant details***
- Model can be used for mathematical reasoning to prove system properties or predict new behavior
- Two types of models: continuous and discrete

Formal Methods – Modeling

- ***Advantages of using formal specification***:
    - Clarify ***requirements and design***
    - Articulate ***implicit assumptions***
    - Identify ***undocumented or unexpected assumptions***
    - Expose ***defects***
    - Identify ***exceptions***
    - Evaluate ***test coverage***

Formal Methods – Generating Formal Specifications

- Need ***to translate non-mathematical description*** (diagrams, table, natural language) ***to a formal specification language***
- The specification is a ***concise and precise description of high-level behavior and properties of a system***
- Well-defined language ***semantics*** are needed to support formal deduction of specification

Formal Methods – Generating Formal Specifications (cont.)

- Types of formal specifications,
  - ***Model oriented*:** Based on a model of the system behavior in terms of mathematical objects, like sets, sequences, etc.
    - Statecharts, SCR (Software Cost Reduction), VDM (Vienna Development Method)
    - Petri nets, automata theoretic models

Formal Methods – Generating Formal Specifications (cont.)

- Types of formal specifications (cont.)
  - ***Property oriented***: Based on a set of properties sufficient to describe system behavior in terms of axioms, rules, etc.
    - Algebraic semantics
    - Temporal logic

Formal Method – Role in System Design and Engineering

- Motivated by the expectation that performing appropriate mathematical analysis can contribute to the reliability and robustness of an information system design

* ***https://en.wikipedia.org/wiki/Formal_methods***

Formal Method – Role in System Design and Engineering (cont.)

- Formal specification of an information system may be used as a guide while the system is being developed.
  - If the formal specification is in ***operational semantics*** (executable), the observed behavior of the system can be compared with the behavior of the specification.
  - If the formal specification is in ***axiomatic semantics***, the pre-conditions and post-conditions of the specification may become assertions in the executable code.*

* ***https://en.wikipedia.org/wiki/Formal_methods***

Formal Methods –
Bell-LaPadula (BLP) Model

- For ***enforcing*** ***access control*** in information systems and built on the concept of a ***state machine with allowable states in a computer system***.

[***http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model***](http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model)

Formal Methods – Bell-LaPadula (BLP) Model (cont.)

- The model defines ***two MAC rules and one DAC rule with three security properties:***
    - Simple Security Property - a subject at a given security level ***may not read*** an object at a higher security level (**no read-up**)

Formal Methods – Bell-LaPadula (BLP) Model (cont.)

- ★-property ("star"-property) - a subject at a given security level ***must not write*** to any object at a lower security level (**no write-down**)
- Discretionary Security Property - use of an access matrix to specify the discretionary access control. ***http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model***

Limitations of Formal Methods

- Requires sound mathematical knowledge of the developer
- Different aspects of a design may be represented by different formal specification methods
- Useful for ***consistency checks***, but cannot guarantee the ***completeness*** of a specifications

CSE 543
Information Assurance and Security

Mission Assurance

Professor Stephen S. Yau

Fall 2022

Mission Assurance

- ***Mission Assurance***
  - A ***life-cycle engineering process*** to ***<u>identify and mitigate</u>*** <u>the</u> ***<u>deficiencies</u> of mission requirements, design, production, test, and field support for <u>mission success</u>***

Mission Assurance

- ***Goal*** of Mission Assurance
  - To create a ***state of resilience*** that supports the ***continuation*** of an entity's ***critical business processes and protects its employees, assets, services, and functions.***

Mission Assurance (cont.)

- Includes ***disciplined application*** of ***system engineering, risk management, quality and management principles*** to achieve ***success*** of the following,
  - ***Requirement analysis***
  - ***Design***
  - ***Development***
  - ***Testing***
  - ***Deployment***
  - ***Operations process***

Mission Assurance *(cont.)*

- Also covers the ***enterprise, supply base, business partners, and customer base*** to enable ***mission success***.

Mission Assurance (cont.)

- In practice, information assurance (IA) focuses on protection of data and systems, often conflicts with the “get the job done” attitude of mission assurance.

Mission Assurance (cont.)

- This conflict is largely eliminated when the focus of information assurance is bifurcated into
  - ***protecting** the infrastructure and data*, and
  - ***securely sharing** information with authorized recipients.*

Mission Assurance Use Cases

- The US DoD 8500-series of policies has defined three ***mission assurance categories (MACs)*** that form the basis for ***availability and integrity requirements***

Mission Assurance Use Cases

- ***MAC I*** systems handle information ***vital*** to the ***operational readiness or effectiveness of deployed or contingency forces***.
  - Loss of MAC I data would cause ***severe damage*** to the successful completion of a DoD mission.
  - MAC I systems must maintain the ***highest*** *levels* of both ***integrity and availability*** and ***use the most rigorous measure of protection.***

Mission Assurance Use Cases (cont.)

- ***MAC II*** systems handle information ***important*** to ***the support*** of ***deployed and contingency forces***.
  - Loss of MAC II systems could have a ***significant negative impact on the success of the mission or operational readiness***.
  - MAC II systems must maintain the ***highest*** level of ***Integrity***.
  - The loss of availability of MAC II data can be ***tolerated only for a short period of time***, so MAC II systems must maintain a ***medium level of availability***.
  - MAC II systems require ***protective measures above industry best practices*** to ensure ***adequate integrity and availability of data.***

Mission Assurance Use Cases ***(cont.)***

- ***MAC III*** systems handle information that is ***necessary*** for ***day-to-day operations***, but not directly related to the support of deployed or contingency forces.
  - Loss of MAC III data would ***not have a significant immediate impact*** on mission effectiveness or operational readiness in short term
  - MAC III systems are required to maintain ***basic levels of integrity and availability.*** MAC III systems must be protected by measures considered as ***industry best practices***.

References

- J. G. Boyce, D. W. Jennings, *Information Assurance*: *Managing Organizational IT Security Risks*. Butterworth Heineman, 2002, ISBN 0-7506-7327-3
- M. E. Whitman and H. J. Mattord , Principles of Information Security, 6th edition, Thomson Course Technology, November 2018
- Rahul Gupta, "The Need for Mission Assurance". *PRTM Magazine*, 2006.

CSE 543

Information Assurance and Security

Physical and Personnel Security for Information Systems

Professor Stephen S. Yau

Fall 2022

Importance of Physical Security

- ***Physical security*** deals with who have access to buildings, computer rooms, and the devices within them
- Protect ***sites*** from natural and man-made physical threats

Physical Security Threats

- **Weather**
  - Tornadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity
- **Earth movement**
  - Earthquakes, mudslides, tsunami
- **Fire/chemical**
  - Explosions, toxic waste/gases, smoke, fire
- **Biological**
  - Virus, bacteria

Physical Security Threats (Cont.)

- **Structural failure**
  - Building collapse due to snow/ice/load weight, or moving objects (cars, trucks, airplanes, etc.)
- **Energy**
  - Loss of power, radiation, magnetic wave interference,
- **Human**
  - Strikes, theft, sabotage, terrorism and war

Physical Security Areas

- Administrative controls
- Physical security controls
- Technical controls
- Environmental/life-safety controls
- Educating personnel

Administrative Controls

- **Restricting Work Areas**
  - Identify access rights to the ***site in general***
  - Decide various access rights ***required by each location*** (rooms, elevators, buildings) within the site
- **Escort Requirements and Visitor Control**
  - Visitor information?
  - Foreign nationals?
  - Escorted access?
  - On-site identity check?
  - Temporary badge?

Administrative Controls *(cont.)*

- <u>**Site Selection**</u>
  - **Visibility**
  - **Locale considerations**
    - Neighborhood
    - Local ordinances
    - Crime rate
    - Hazardous sites nearby, such as landfills, waste dumps, and nuclear reactors.
  - **High Probability for Natural disasters**
  - **Transportation**

Physical Security Controls

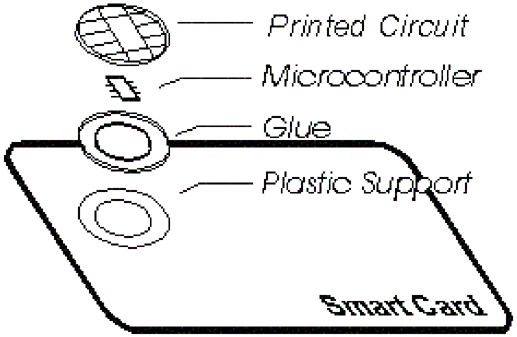
- **Perimeter Security Controls**
  - Gates, fences, turnstiles, mantraps
- **Badging**
  - Photo identification that not only authenticates an individual, but also continues to identify the individual while inside the facility

Physical Security Controls (Cont.)

- **Locks**
  - Mechanical locks
  - Password locks
  - Electronic locks
- **Security Dogs**
  - Detecting intruders
  - Sniffing out explosives
- **Lighting**

Technical Controls

- **Smart card**
  - Semiconductor chip with logic and nonvolatile memory
  - Software that detects unauthorized tampering and intrusions to the chip and if detected, can lock or destroy the contents of the chip
  - Three major types: contact, contact-less and combinations of the two.



Technical Controls (Cont.)

- **Audit Trails/Access Logs**
- **Physical Intrusion Detection**
  - Metallic foil tape, infrared light beams, motion sensors
- **Alarm Systems**
  - Systems like ADT, monitoring and responding to intrusion alert
- **Biometrics**

Environmental/Life-safety Controls

- **Power**
  - ***Power-outage***: Emergency lights and continuing functioning of those electronic gates are needed
  - ***Uninterrupted power***: Uninterrupted Power Service (UPS) and emergency power-off switch
  - ***Constant voltage and current: Regulator***

Environmental/Life-safety Controls (Cont.)

- **Fire/Chemical Detection and Suppression**
  - *Targets*: Explosions, toxic waste/gases, smoke, fire
  - ***Detectors:*** Heat sensor, flame detector, smoke detector
  - ***Extinguishing systems***: Water-sprinkler or gas-discharge system
- **Heating, Ventilation and Air Conditioning**

Educating Personnel

- **Security staff** should be prepared for ***potential of unforeseen acts***
- **Other employees** should be reminded ***periodically*** of ***importance of helping their surroundings secure***
  - Mindful of ***physical and environmental considerations*** required to protect information systems
  - Adhering to ***emergency and disaster plans***
  - ***Monitoring unauthorized use*** of equipment and services, and ***reporting*** those activities to security personnel
  - ***Recognizing security objectives*** of organization
  - ***Accepting individual responsibilities*** associated with their jobs and that of their coworkers

What Is Personnel Security?

- Security mechanisms ***reducing risks of human errors, thefts, frauds or misuse of facilities*** within an organization
- Not just an IT issue
  - ***Human Resource (HR)*** is the main player
  - Cross reference (refer to other organizations' IA in HR) and provide input to HR policies

Types of Implementation

- *Background checks*
- *Security clearances*
- *Employment agreements*
- *Hiring and termination practices*
- *Job descriptions*
- *Job rotation*
- *Separation of duties and responsibilities*

Background Checks

- Personnel controlling IT resources
  - Security Personnel
  - Network Administrators
  - Managers
  - Auditors
- Support hiring decisions
- Provide some protection and assurance

Background Checks ***(Cont.)***

- What can be checked on an applicant?
  - Credit (financial) report
  - SSN searches
  - Workers compensation reports
  - Criminal record
  - Motor vehicle report
  - Education verification
  - Reference checks
  - Prior employment verification

Security Clearances

- Applicable to
  - Uniformed members of the military
  - Civilian employees working for government agencies
  - Employees of government contractors

Employment Agreements

- ***Non-competitive:***
  - Will not compete with your employer by engaging in any business of similar nature as an employee, independent contractor, owner, partner, significant investor, etc.
  - May broadly limit from working in same field, even if employee does not work for a direct competitor. May restrict in both time and locations

Employment Agreements *(Cont.)*

- ***Non-disclosure:***
  - Used when employer with unpatented ideas wants employees to maintain the idea confidential
  - Restricts dissemination of corporate information to unauthorized entities, especially competitors, press, analysts, and foreign agents

Hiring and Termination Practices

- Hiring manager responsible for review of background checks
- Managers must take ***timely and appropriate disciplinary actions***
- Applicable to contractors/sub-contractors.

Hiring and Termination Practices (Cont.)

- From IT perspective
  - Starting/closing accounts
  - Notifying employee of account information
  - Forwarding e-mail and voice-mail
  - Changing locks and number-combinations
  - Changing system passwords
  - Notifying all personnel

Job Descriptions

- Designated position title, classification and sensitivity
- Sensitivity of information handled
- Security responsibilities of the position
- Considerations in periodic performance evaluation

Job Rotation

- Implemented where feasible
  - Discourages ***fraud, waste, and abuse***
  - Discourages ***collusion*** (secret agreements or cooperation. especially for illegal or deceitful purposes)
  - Promotes ***cross-training***
  - Often not possible in highly specialized jobs or small organizations

Separation of Duties

- Ensure people *checking* for ***inappropriate use of IT resources***
- No one individual should be responsible for completing a task involving sensitive, valuable, or critical information from beginning to end
- A person must not be responsible for approving his/her own work
- What to separate?
  - Security from audit
  - Accounts payable from accounts receivable
  - Development from production

Summary

- Make sure to hire ***"good employees"*** as much as possible, i.e. ***competent, honest, and dependable***
- Make sure employees know their ***responsibilities***
- Encourage being ***good employees***
- Know how to handle ***if good employees are discovered to turn bad***

Classification Schemes

- Early 1980s: Confidentiality of classified information on computers with multiple users (time sharing systems)
- Mid 80s to mid 90s:
  - **Orange Book** : standard reference for computer security for DoD
  - **Red Book:** covering Trusted Network Interpretation (TNI) of the Orange Book
  - **Rainbow Series*** is outdated and superseded by Common Criteria Evaluation and Validation Scheme (CCEVS)*

http://www.iwar.org.uk/comsec/resources/standards/rainbow/rainbow.html

Classification Scheme (Cont.)

- Data classification based on ***need for confidentiality***
- US Classification Scheme
  - ***Top secret***: Publicly disclosed would ***compromise national security***
  - **Secret**: …would ***cause serious damage*** to ***national security***
  - ***Confidential***: …would ***damage national security***
  - ***Unclassified***

Classification Scheme *(Cont.)*

- Unclassified includes
  - ***Sensitive But Unclassified (SBU)***
  - ***Unclassified – Law Enforcement Sensitive (U//LES)***
  - ***For Official Use Only (FOUO).*** Not subject to release under the Freedom of Information Act (FOIA). May include company proprietary information
  - …..
- Other Countries and Organizations

http://en.wikipedia.org/wiki/Security_classification

Classified Information Management

- ***Accountability*** for classified data
- **Declassification/Downgrade**
- ***Sanitization/Purging***
- ***Destruction***

References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, Course Technology, 2018
- M. Merkow, J. Breithaupt, *Information Security: Principles and Practices*, Prentice Hall, August 2005, ISBN 0131547291
- Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, 2004, ISBN: 0321247442
- Matt Bishop, *Computer Security: Art and Science*, Addison- Wesley, 2002, ISBN: 0201440997