

IT Infrastructure Architecture

Infrastructure Building Blocks
and Concepts

Security Concepts

Security Patterns

Identity and Access Management (IAM)

- The process of managing the identity of people and systems, and their permissions
- The IAM process follows three steps:
 - Users or systems claim who they are: **identification**
 - The claimed identity is checked: **authentication**
 - Permissions are granted related to the identity and the groups it belongs to: **authorization**

Identity and Access Management (IAM)

- Single Sign-On (SSO):
 - A user logs in once and is passed seamlessly, without an authentication prompt, to SSO enabled applications
 - Can be implemented using identity providing systems
 - LDAP
 - Kerberos
 - Microsoft Active Directory
 - Users authenticate to these identity providers
 - Applications trust the identity provider, so they allow access when a user is authenticated

Identity and Access Management (IAM)

- Federated identity management:
 - Extends SSO above the enterprise level
 - Creates a trusted identity provider across organizations
 - Participating organizations share identity attributes based on agreed-upon standards

Authentication

- Using one of three ways:
 - Something you *know*, like a password or PIN
 - Something you *have*, like a bank card, a token or a smartphone
 - Something you *are*, like a fingerprint or an iris scan
- Multi-factor authentication:
 - At least two types of authentication are required

Role Based Access Control (RBAC)

- In RBAC, instead of granting permissions to individual identities, groups are granted permissions
- Identities are members of one or more groups
- Groups are related to their roles in the organization
- Groups can be nested (a group is member of another group)
- RBAC is used in almost all organizations

Segregation of duties and least privilege

- Segregation of duties (also known as separation of duties):
 - Assigns related sensitive tasks to different people or departments
 - No single person has total control of the system's security mechanisms
- Least privilege:
 - Users of a system should have the lowest level of privileges necessary to perform their work
 - Users should only have privileges for the shortest length of time

Segregation of duties and least privilege

- In secure systems, multiple distinct administrative roles should be configured:
 - Security manager
 - Systems manager
 - Super user
- A two-man control policy can be applied
 - Two systems managers must review and approve each other's work
 - Two systems managers are needed to complete every security sensitive task

Layered security

- Layered security (also known as a Defense-In-Depth strategy) implements various security measures in various parts of the IT infrastructure
 - Instead of having one big firewall and have all your security depend on it, it is better to implement several layers of security
- Preferably security layers make use of different technologies
 - This makes it harder for hackers to break through all barriers, as they will need specific knowledge for each step
- Disadvantage: increases the complexity of the system

Cryptography

- The practice of **hiding information** using encryption and decryption techniques
- **Encryption** is the conversion of information from a readable state to apparent random data
- Only the receiver has the ability to **decrypt** this data, transforming it back to the original information
- A **cipher** is a pair of algorithms that implements the encryption and decryption process
- The operation of a cipher is controlled by a **key**

Cryptography

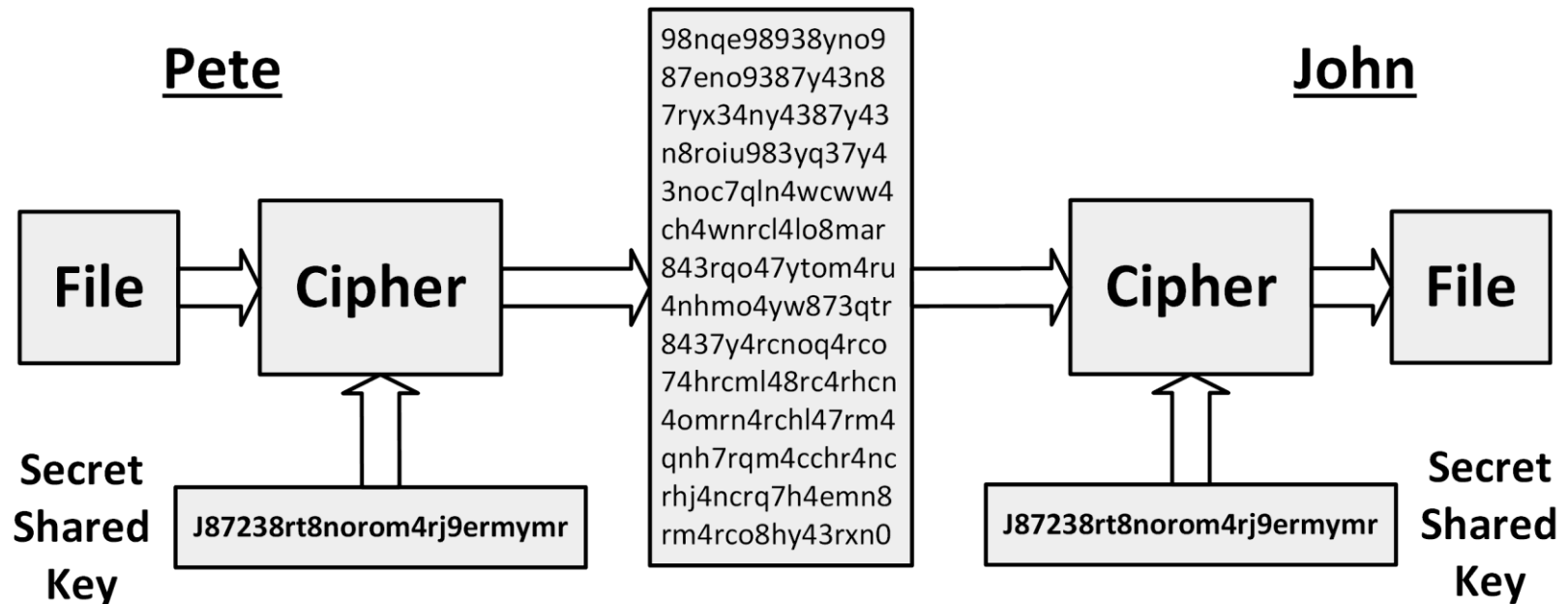
- Block ciphers
 - Input:
 - A block of plaintext
 - A key
 - Output:
 - A block of cipher text
 - Used across a wide range of applications, from ATM machine data encryption to e-mail privacy and secure remote access
 - Standards:
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)

Cryptography

- Stream ciphers
 - Create an arbitrarily long stream of key material
 - Combines key stream with the plaintext bit-by-bit or character-by-character
 - Used when data is in transit over the network
 - RC4 is a widely-used stream cipher

Symmetric key encryption

- Both the sender and receiver share the same key

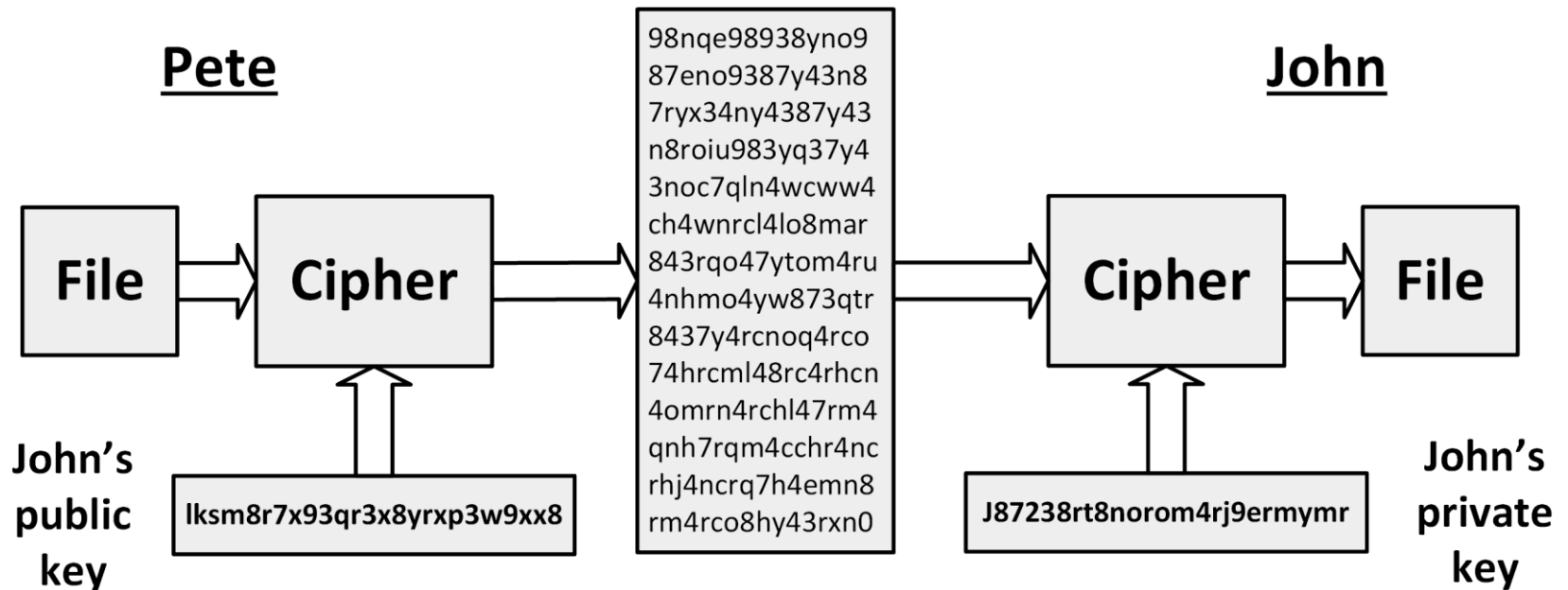


Symmetric key encryption

- Disadvantage: key management
- *Each pair* of communicating parties must share a *different key*
- The number of keys required for a group of N systems is $N \times \frac{N-1}{2}$
- Chicken-and-egg problem:
 - The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them

Asymmetric key encryption

- Two different but mathematically related keys are used: a public key and a private key



Asymmetric key encryption

- Two different but mathematically related keys are used:
 - a public key - may be freely distributed
 - a private key - must remain secret by the organization
- Diffie–Hellman and RSA algorithms are the most widely used algorithms
- Disadvantage: slow
 - About 1000 to 10,000 times slower than symmetric key encryption

Asymmetric key encryption

- Mostly used to setup a channel between two parties, to safely exchange a new, temporary symmetric key
 - Pete creates a random secret key and encrypts it using the public key from John
 - The encrypted secret key is sent to John using an open channel (like the internet)
 - John is the only party that can decrypt the message, because he has the private key that is related to the public key. John decrypts the message and now knows the secret key
 - Pete and John start communicating using symmetric key encryption, using the exchanged secret key
 - When the communication is finished, the shared key is no longer valid and is deleted

Hash functions

- Hash functions take some piece of data, and output a short, fixed length text string (the hash)
- The hash is unique for that piece of data
 - The input string “hello world” produces the following MD5 hash:
5eb63bbbe01eeed093cb22bb8f5acdc3
 - The input string “hallo world” produces the following MD5 hash:
5fd591a948dc76dd731f8998e19c773a
 - While only one letter was changed, the hash is completely different

Hash functions

- Hash functions can be used to validate the integrity of the data
- It is practically impossible to find two pieces of data that produce the same hash
- Hash functions:
 - MD5
 - SHA1
 - SHA512

Digital signatures

- To create a digital signature of some text (like an e-mail), a hash is created and encrypted with the private key of the sender
- The receiver decrypts the hash key using the sender's public key
- The receiver also calculates the hash of the text and compares it with the decrypted hash to ensure the text wasn't tampered with
- Since the hash was encrypted using a private key, it is guaranteed that the hash was created by the owner of the private key – the only person that could have created the encrypted hash

Cryptographic attacks

- Every encryption method can be broken using a brute force attack
 - Except a one-time pad cipher with the key of equal or greater length than the message
- A brute force attack consists of systematically checking all possible keys until the correct key is found
- The amount of effort needed is exponentially dependent on the size of the key
- Effective security could be achieved if it is proven that no efficient method (as opposed to the time consuming brute force method) can be found to break the cipher
- Most successful attacks are based on flaws in the implementation of an encryption cipher
- To ensure a cipher is flawless, the source code is usually open source and thus open to inspection to everyone