Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 13: Cloud Security

Identity and Access Management (IAM)

- **Source Disclaimer**: Content for some of the slides is from the course Textbook:
  - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from following book:
  - *Authentication: From Passwords to Public Keys, by Richard E. Smith*

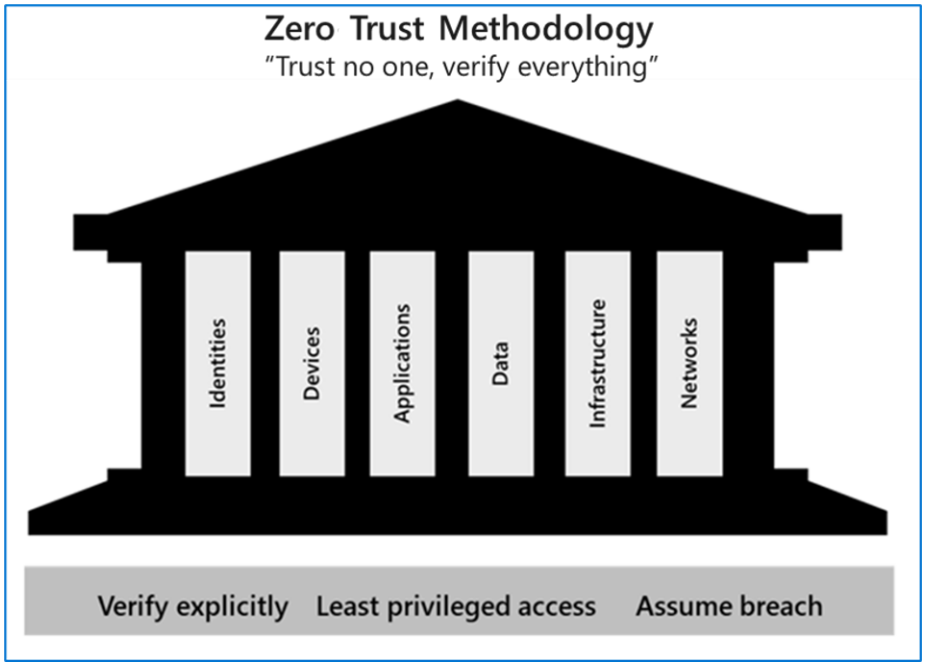
RECAP: AAAA

- *Authentication* is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be.
- *Authorization* refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets.
- Auditing: To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on asset architecture and deployment
  - A *system audit* is a one-time or periodic event to evaluate security.
  - *Monitoring* refers to an ongoing activity that examines either the system or the users, such as intrusion detection
  - An *audit trail or log* is a set of records that collectively provide documentary evidence of different cloud operations
- *Accountability* is the ability to determine the actions and behaviors of a single individual within a cloud system
  - Accountability is related to the concept of *nonrepudiation*, wherein an individual cannot successfully deny the performance of an action
  - Audit trails and logs support accountability

RECAP: The Zero-trust methodology

- Zero Trust guiding principles
- Verify explicitly
- Least privileged access
- Assume breach

- Six foundational pillars
- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Data** should be classified, labeled, and encrypted based on its attributes.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Networks** should be segmented.



IAM: Overview

- What is IAM?
  - IAM = Identity Management (IdM) and Access Management (AcM)
- Identity Management (IdM)
  - User Identities (Unique)
  - Account Management
  - Authentication
- Access Management (AcM)
  - Roles and Privileges
  - Authorization
  - Access Control

IAM: Overview (2)

- Why is ***Identity*** important?
  - Concept of ***Identity*** as a security perimeter
  - Is key behind authentication and authorization

- Why IAM (tools and functions)?
  - Improve Operational Efficiency
    - IAM technology and processes can improve efficiency by automating user on-boarding and other repetitive tasks (e.g., self-service for users requesting password resets
  - Regulatory security compliance management
    - Need to comply with various regulatory, privacy, and data protection requirements

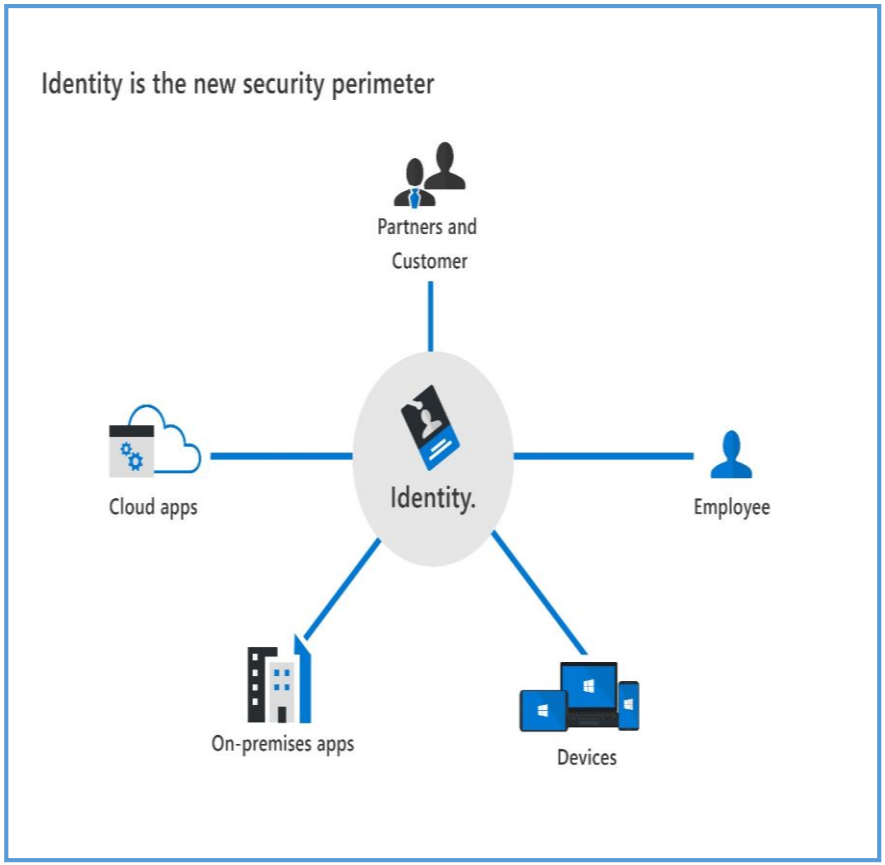
Identity as the primary security perimeter

An identity is how someone or something can be verified and authenticated and may be associated with:

- User
- Application
- Device
- Other

Four pillars of identity:

- Administration
- Authentication
- Authorization
- Auditing

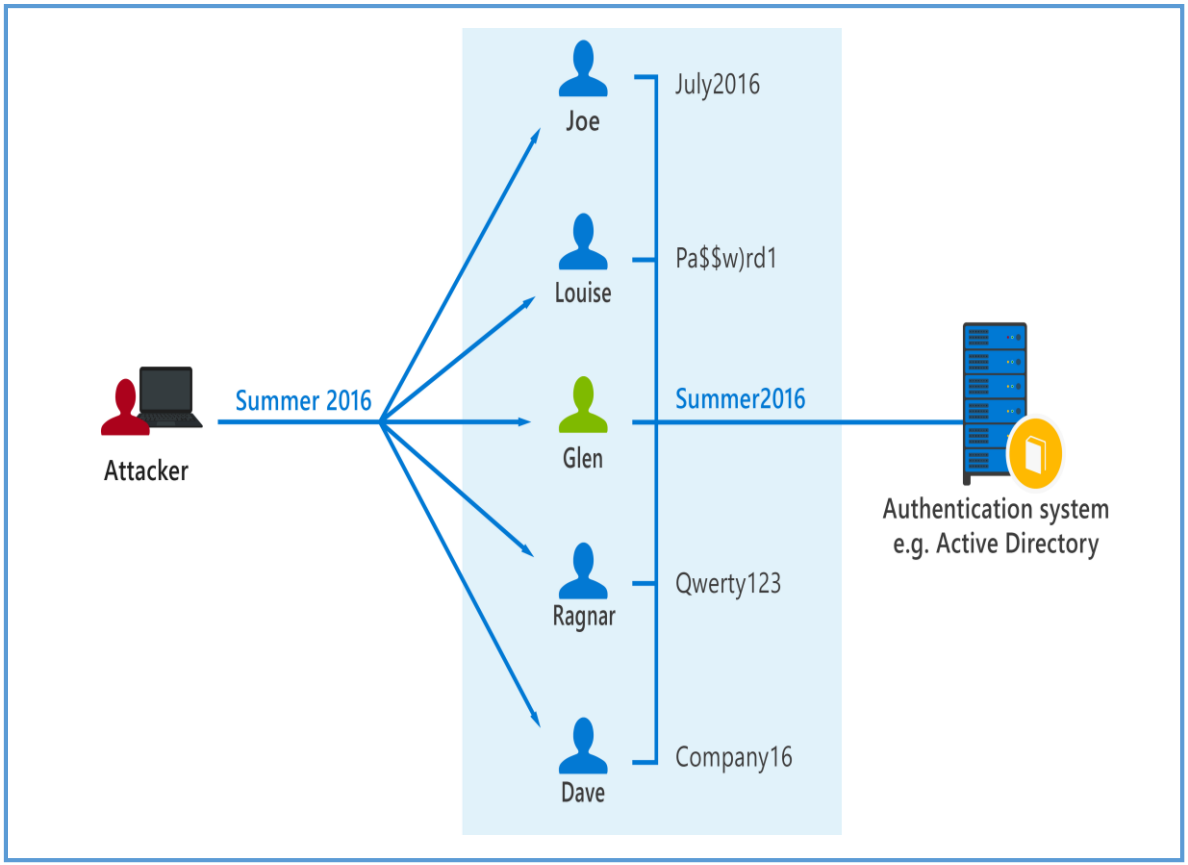


Identity has become the new security perimeter that enables organizations to secure their assets.

Common identity attacks

Types of security threats:

- Password-based attacks
  - Many password-based attacks employ brute force techniques to gain unauthorized access, often using a dictionary
- Phishing
  - hacker sends an email that appears to come from a reputable source, instructing the user to sign in and change their password
- Spear phishing
  - a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails



A password-spray attack – attacker sprays a commonly used password against multiple accounts

Modern authentication and the role of the identity provider

- ***Modern authentication*** is an umbrella term for authentication and authorization methods between a client and a server.

At the center of modern authentication is the role of the ***identity provider (IdP)***.

IdP offers authentication, authorization, and auditing services.

IdP enables organizations to establish authentication and authorization policies, monitor user behavior, and more.

A fundamental capability of an IdP and "modern authentication" is the support for single sign-on (SSO).

Microsoft Azure Active Directory is an example of a cloud-based identity provider.

IAM: Overview (3)

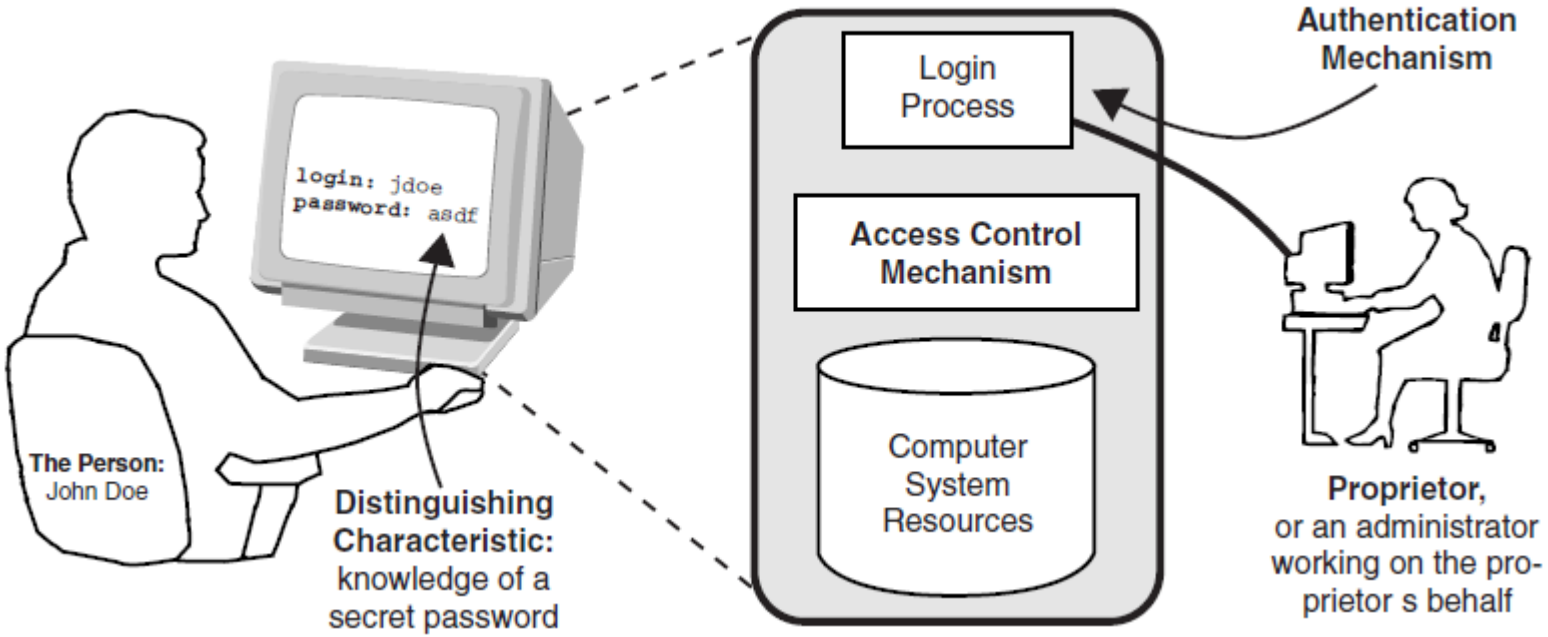
- IAM architecture encompasses several layers of technology, services, and processes.
- At the core of the *deployment architecture is a directory service (such as LDAP or Active Directory) that acts as a repository for the identity, credential, and user attributes of the organization's user poo*l.
- The directory interacts with IAM technology components such as authentication, user management, provisioning, and identity services that support the standard IAM practice and processes within the organization.

Elements of an Authentication System

Authentication Element	Cave of the 40 Thieves	Password Login	Teller Machine	Web Server to Client
Person, principal, entity	Anyone who knew the password	Authorized user	Owner of a bank account	Web site owner
Distinguishing characteristic, token, authenticator	The password "Open, Sesame"	Secret password	ATM card and PIN	Public key within a certificate
Proprietor, system owner, administrator	The forty thieves	Enterprise owning the system	Bank	Certificate authority
Authentication mechanism	Magical device that responds to the words	Password validation software	Card validation software	Certificate validation software
Access control mechanism	Mechanism to roll the stone from in front of the cave	Login process, access controls	Allows banking transactions	Browser marks the page "secure"

Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith

Elements of an Authentication System (2)

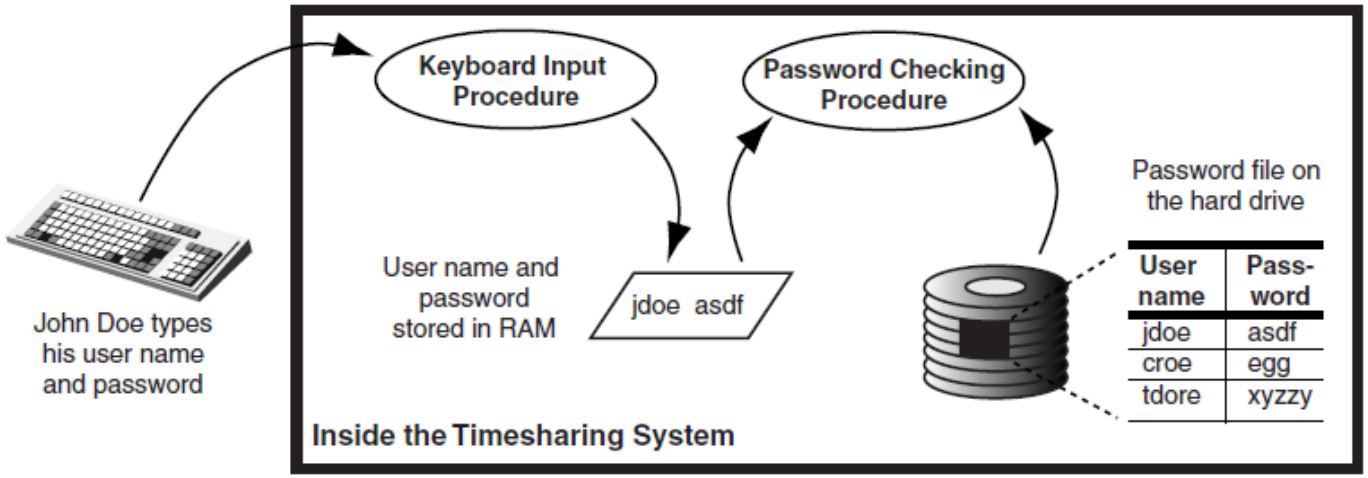


Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith

Authentication Factors

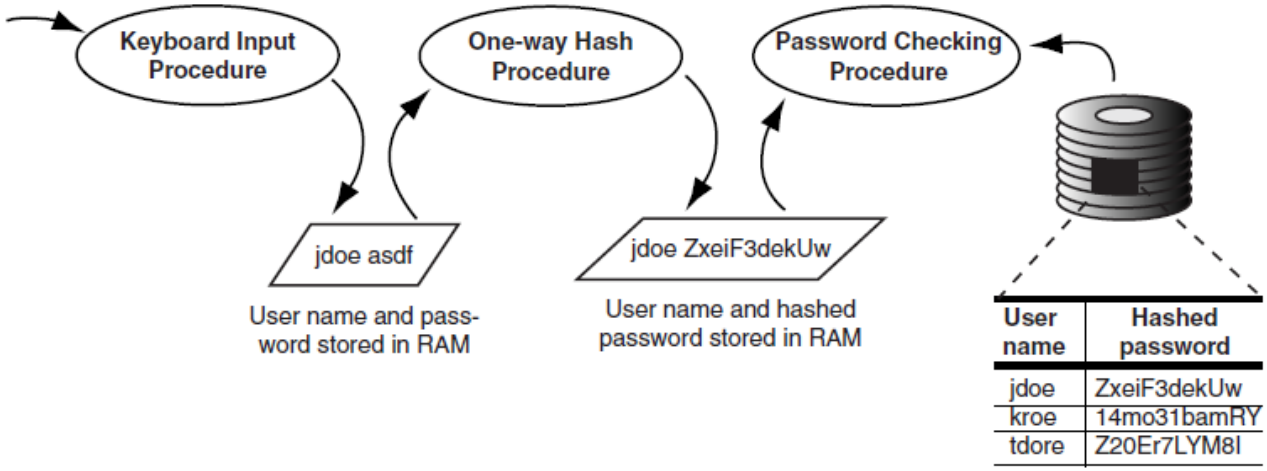
- Authentication can be based on the following three **factor** types:
  - Type 1 — Something you know, such as a personal identification number (PIN) or password
  - Type 2 — Something you have, such as an ATM card or smart card
  - Type 3 — Something you are (physically), such as a fingerprint or retina scan
- 2FA – Two factors are employed
- MFA – More than 2 factors used
  - Factors of the same types are not considered as 2FA or MFA

Authentication via Passwords



- Type 1 Authentication (*Something you know*)
- Passwords can be either:
  - Static: Same password used at each Logon
  - Dynamic: Different password used for each Logon (e.g. OTP)
  - The changing of passwords can also fall between these two extremes (e.g monthly, quarterly etc)

Authentication via Passwords (2)



- Passwords can be stolen from the file-system:
  - Introduction of Hashed Passwords
- Dictionary Attacks
  - Use of multi-word passwords can be more robust against dictionary attacks as against single word passwords (which are relatively simpler to break)
- Guessing attacks, Social engineering attacks, Sniffing attacks…..

Authentication via Tokens

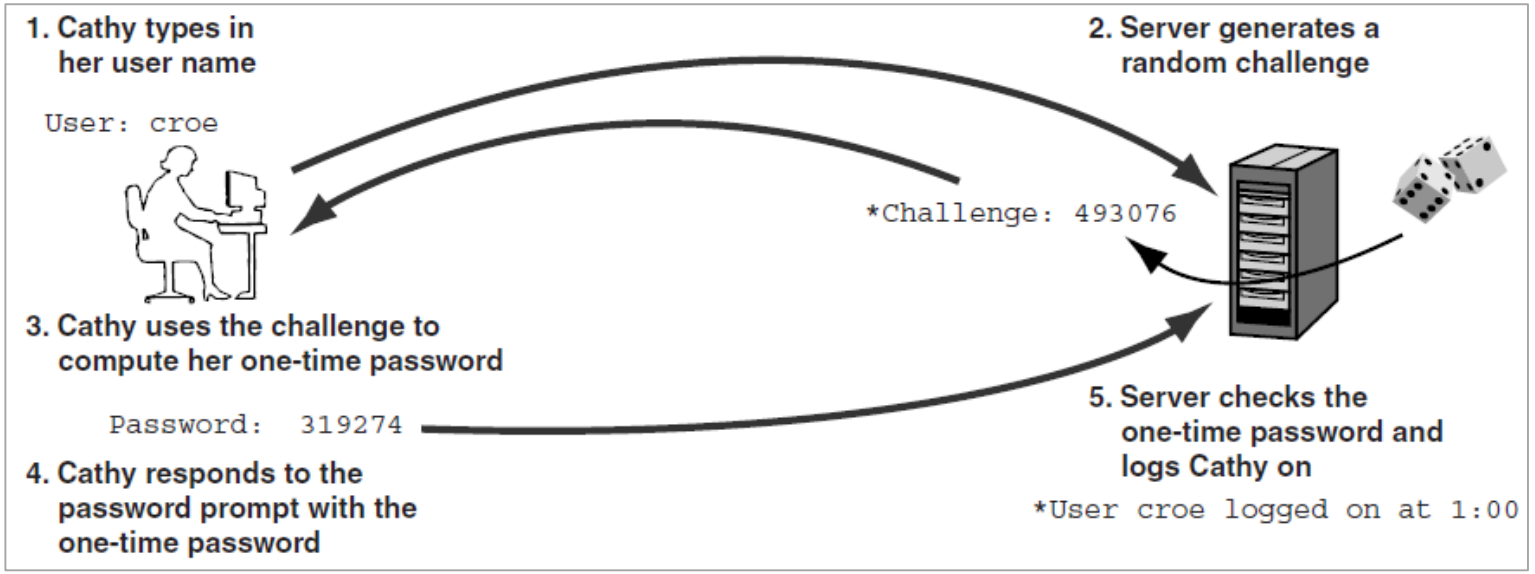
Tokens, in the form of small, hand-held devices, are used to provide passwords. The following are the four basic types of tokens:

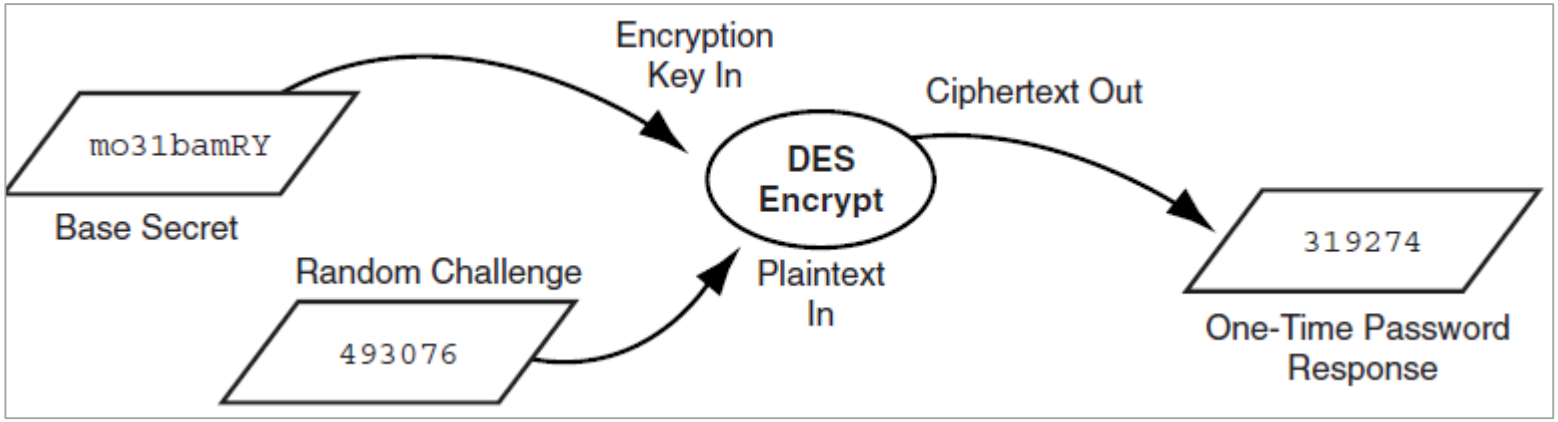
- Static password tokens
  - 1. Owners authenticate themselves to the token by typing in a secret password.
  - 2. If the password is correct, the token authenticates the owner to an information system.
- Synchronous dynamic password tokens, clock-based
  - 1. The token generates a new, unique password value at fixed time intervals that is synchronized with the same password on the authentication server (this password is the time of day encrypted with a secret key).
  - 2. The unique password is entered into a system or workstation along with an owner's PIN.
  - 3. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.

Authentication via Tokens (2)

- Synchronous dynamic password tokens, counter-based
  - 1. The token increments a counter value that is synchronized with a counter in the authentication server.
  - 2. The counter value is encrypted with the user's secret key inside the token and this value is the unique password that is entered into the system authentication server.
  - 3. The authentication entity in the system or workstation knows the user's secret key and the entity verifies that the entered password is valid by performing the same encryption on its identical counter value.
- Asynchronous tokens, challenge-response
  - 1. A workstation or system generates a random challenge string, and the owner enters the string into the token along with the proper PIN.
  - 2. The token performs a calculation on the string using the PIN and generates a response value that is then entered into the workstation or system.
  - 3. The authentication mechanism in the workstation or system performs the same calculation as the token using the owner's PIN and challenge string and compares the result with the value entered by the owner. If the results match, the owner is authenticated.

Challenge-Response





Authentication via Memory Cards and Smart Cards

Type 2 Authentication (*Something you have*)

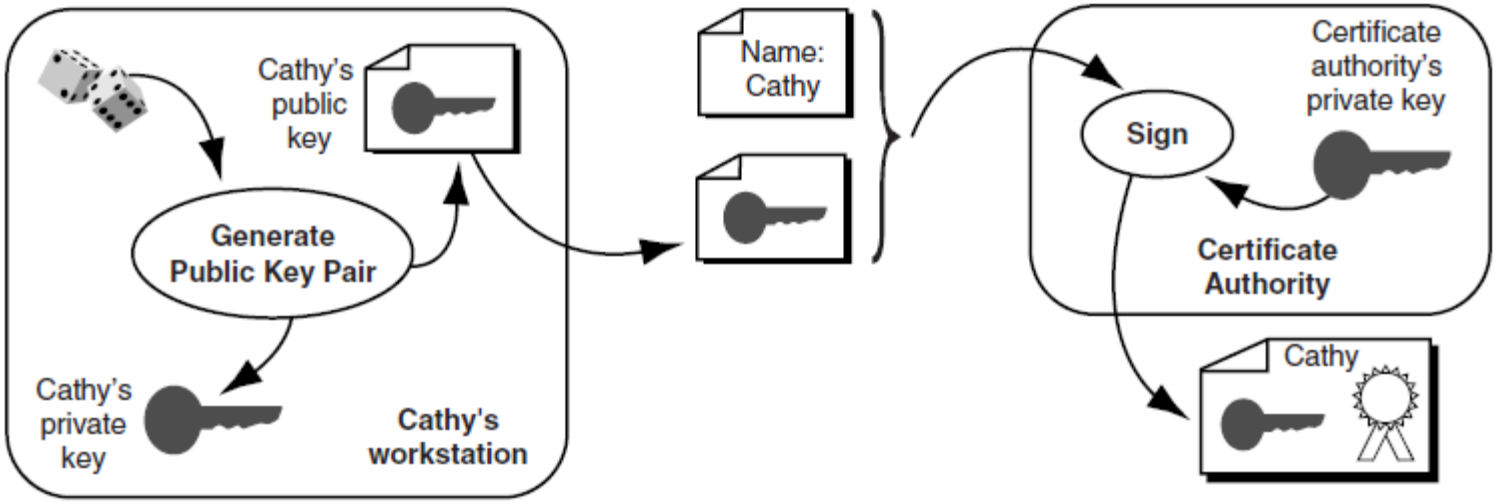
- Memory cards provide nonvolatile storage of information, but they do not have any processing capability
  - A memory card stores encrypted passwords and other related identifying information.
  - An ATM card is an example of memory cards
- Smart cards provide even more capability than memory cards by incorporating additional processing power on the cards
  - These credit-card-size devices comprise microprocessor and memory
  - Are used to store digital signatures, private keys, passwords, and other personal information

Authentication via Biometrics

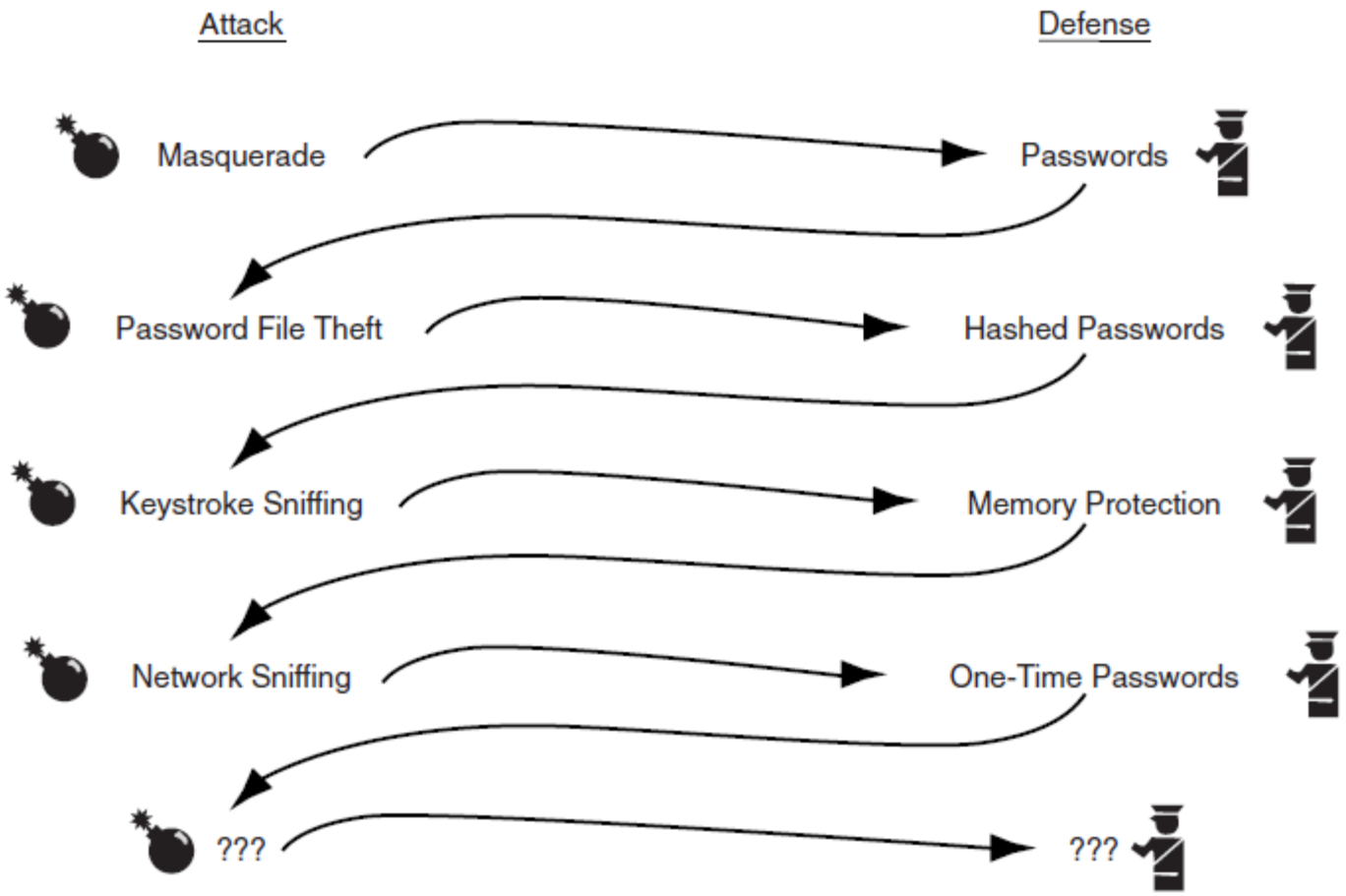
- Type 3 authentication(*something you are*)
- In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images
- There are three main performance measures in biometrics:
  - False rejection rate (FRR) or Type I Error — The percentage of valid subjects that are falsely rejected.
  - False acceptance rate (FAR) or Type II Error — The percentage of invalid subjects that are falsely accepted.
  - Crossover error rate (CER) — The percentage at which the FRR equals the FAR. The smaller the CER, the better the device is performing.
- In addition to the accuracy of the biometric systems, *Enrollment time, Throughput rate and Acceptability* are also other important measures
  - Enrollment Time is the time that it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes
  - The throughput rate is the rate at which the system processes and identifies or authenticates individuals. Acceptable throughput rates are in the range of 10 subjects per minute.
  - Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems might be the exchange of body fluids on the eyepiece.

Authentication using Certificates

- Generating a certificate at Certification Authority



Evolving Attacks and Defense Systems



Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith

Authentication Factors: Pros and Cons

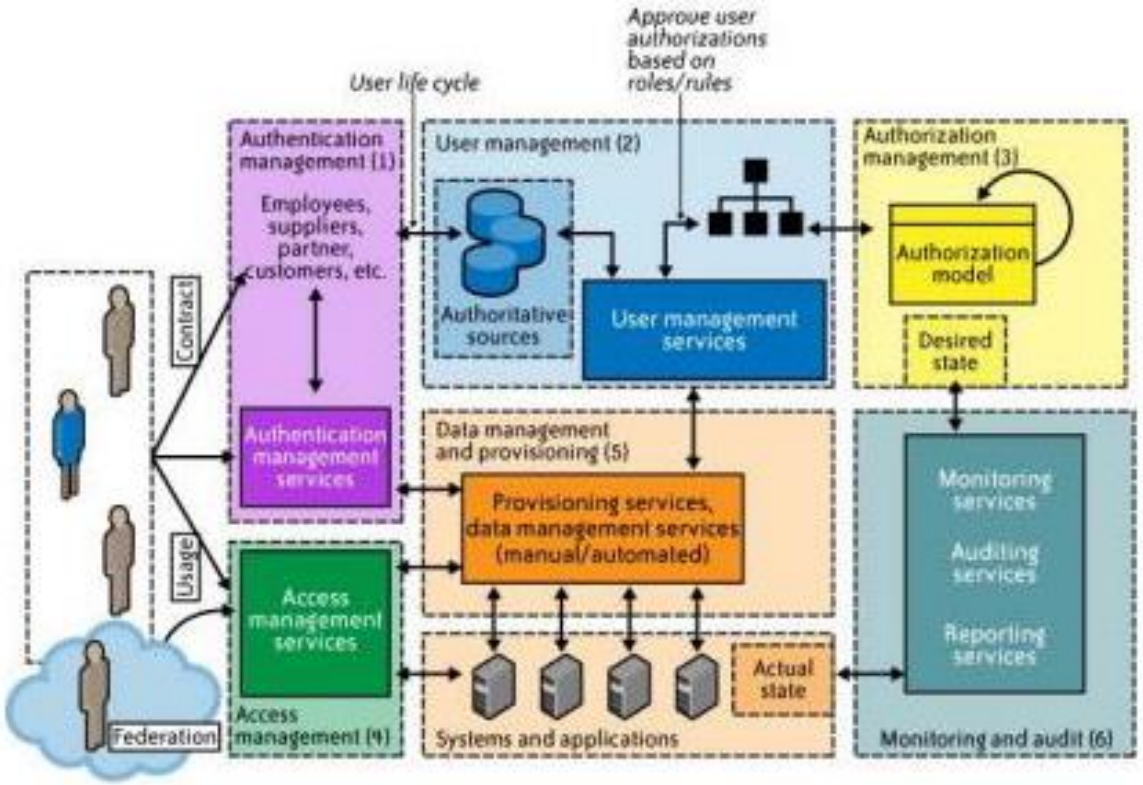
- Summary of strengths and weaknesses of different authentication factors

Factor	Benefits	Weaknesses	Examples
Something you know: password	Cheap to implement, portable	Sniffing attacks, Can't detect sniffing attacks, Passwords are either easy to guess or hard to remember, Cost of handling forgotten pass-words	Password, PIN, Safe combination
Something you have: token	Hardest to abuse	Expensive, Can be lost or stolen, Risk of hardware failure, Not always portable	Token, Smart card, Secret data embed-ded in a file or device, Mechanical key
Something you are: biometric	Easiest to authenticate with, portable	Expensive, Replay threats, Privacy risks, Characteristic can't be changed, False rejection of legitimate users, Characteristic can be injured	Fingerprint, Eye scan, Voice recognition, Photo ID

Implementing IdM

Typical undertakings in putting identity management in place include the following:

- Establishing a database of identities and credentials
- Managing users' access rights
- Enforcing security policy
- Developing the capability tc create and modify accounts
- Setting up monitoring of resource accesses
- Installing a procedure for removing access rights
- Providing training in proper procedures



The concept of directory services and Active Directory

A directory is a hierarchical structure that stores information about objects on the network.

A directory service stores directory data and makes it available to network users, administrators, services, and applications.

The best-known service of this kind is Active Directory Domain Services (AD DS), a central component in organizations with on-premises IT infrastructure.

Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

The concept of Federated Services

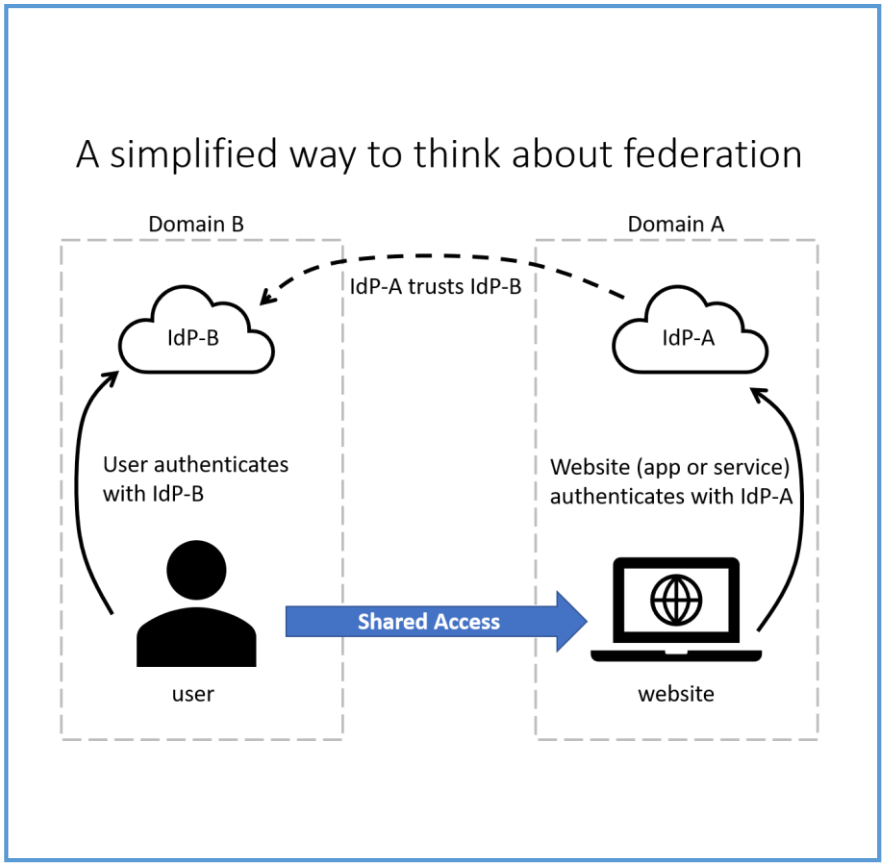
Simplification method of federation scenario:

The website uses the authentication services of IdP-A

The user authenticates with IdP-B

IdP-A has a trust relationship configured with IdP-B

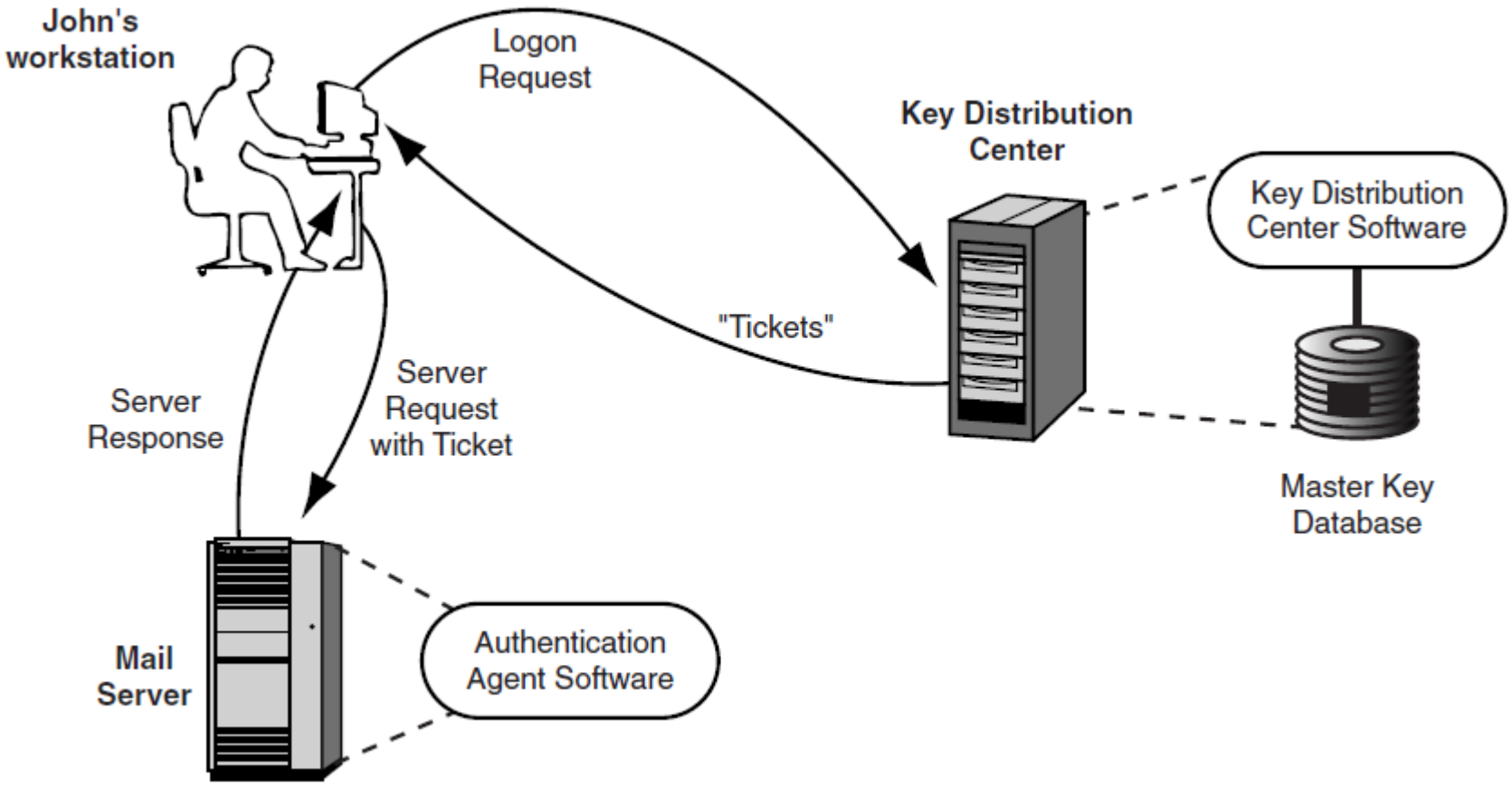
When the user's credentials are passed to the website, the website trusts the user and allows access



Kerberos and Crypto Tokens

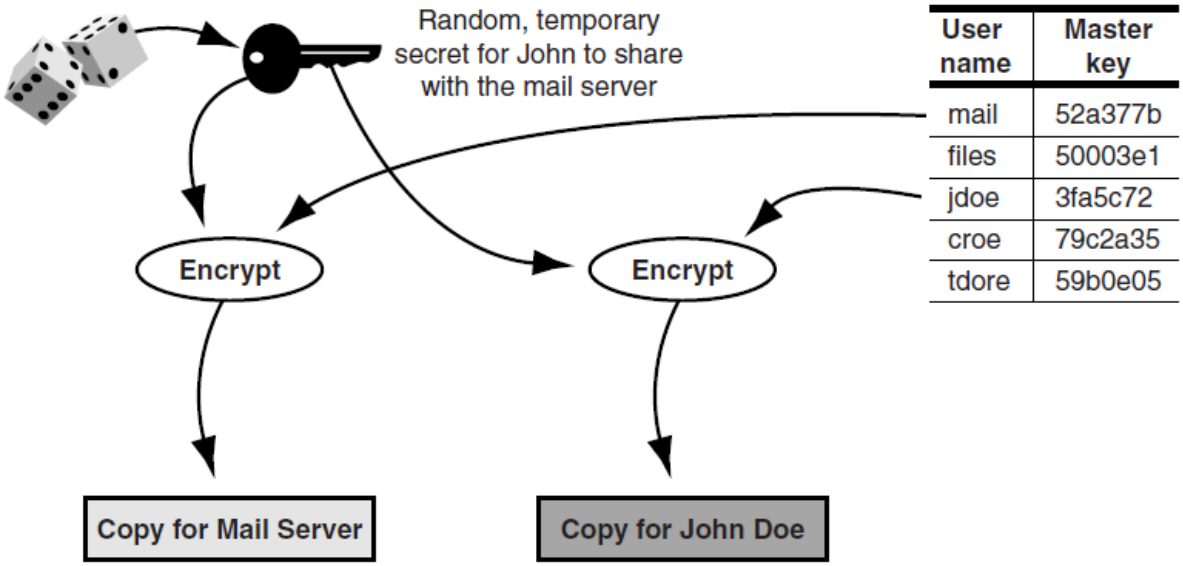
- Kerberos provides a mechanism to authenticate and share temporary secret keys between cooperating processes
- Enables Indirect authentication with a Key Distribution Center (KDC)
- KDC issues tickets for authentication to different services (e.g. a mail server, print server etc)

Kerberos KDC



Tickets

- Each trusted site has a unique *master key* that it shares with the KDC
  - The master key allows each site to talk to the KDC safely
  - In addition, the KDC can cryptographically "package" temporary keys using the master keys so that one site can safely forward the right keys to another site

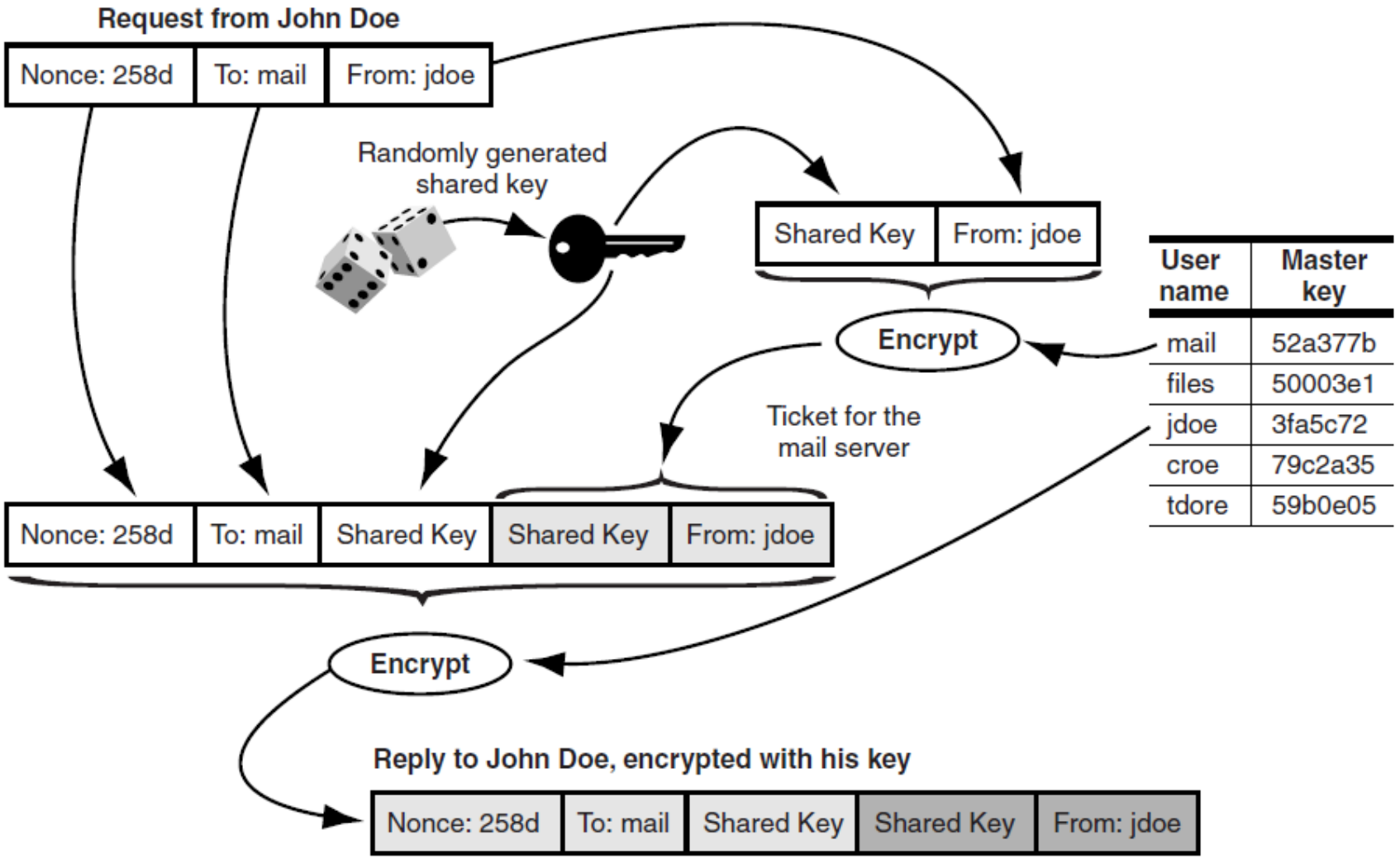


User name	Master key
mail	52a377b
files	50003e1
jdoe	3fa5c72
croe	79c2a35
tdore	59b0e05

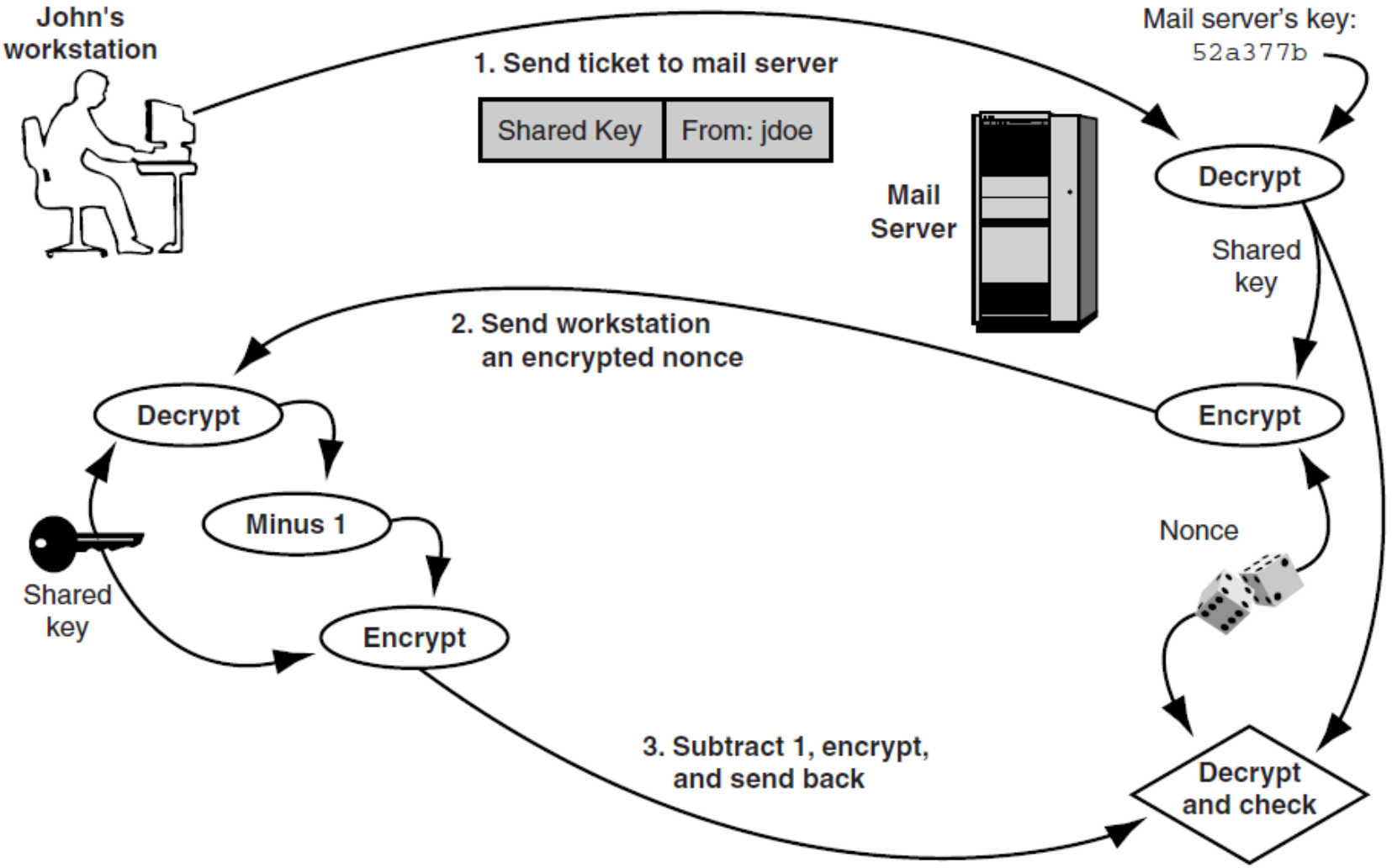
Extensions to Basic KDC

- To combat security problems, the protocol incorporates extra data in key distribution messages, notably message authentication codes, time stamps, and the names of senders and recipients
- In 1978, Needham and Schroeder published a simple protocol to efficiently address forgery problems faced by the KDC
  - This Needham-Schroeder (NS) protocol incorporates nonces and a challenge response to detect forged or replayed messages

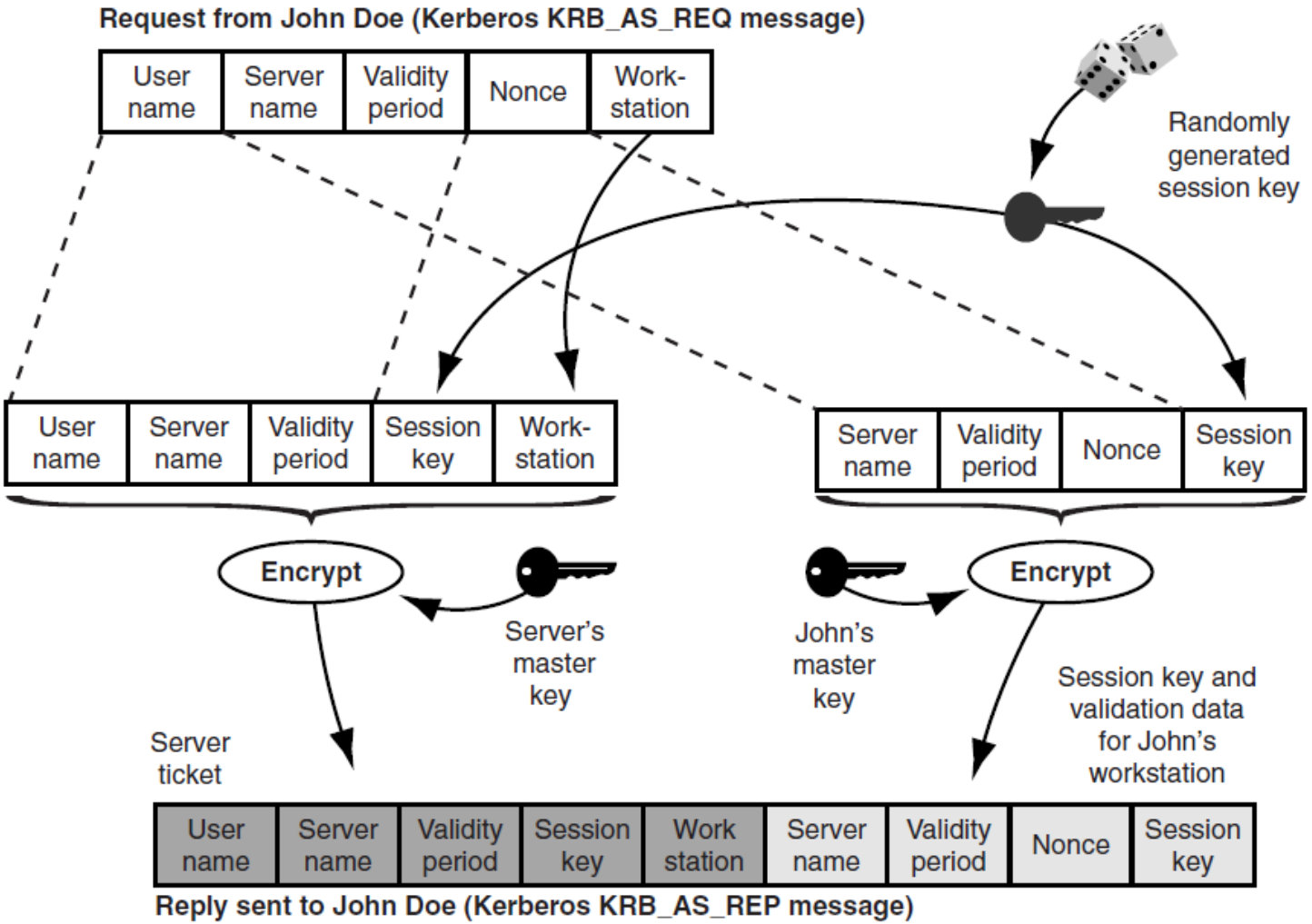
KDC with NS Extensions



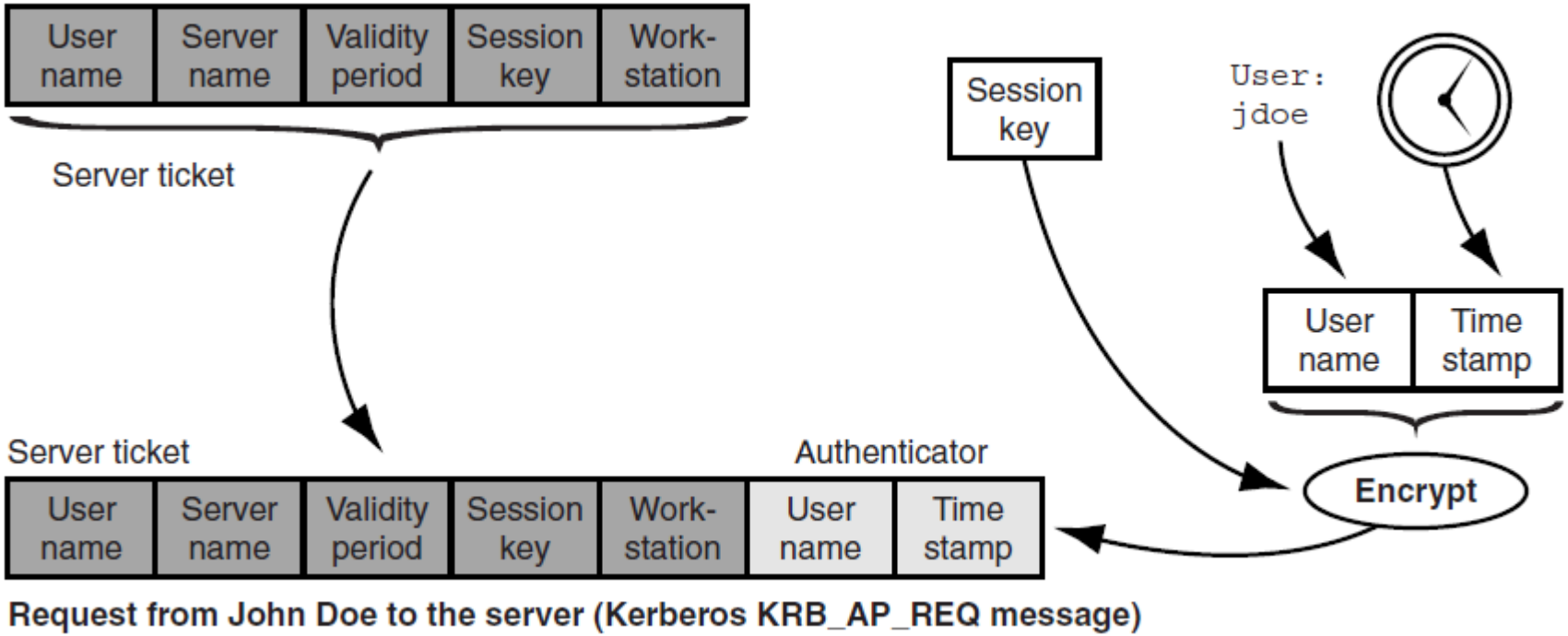
Challenge-Response in NS Protocol



Kerberos Authentication Server



Authenticating to a *Kerberized* Server



Request from John Doe to the server (Kerberos KRB_AP_REQ message)

Ticket Granting Ticket

- Kerberos KDC with 2-step ticket granting process