SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade Approved by AICTE,
New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19EC402- WIRELESS ADHOC AND SENSOR NETWORKS

IV ECE / VII SEMESTER

UNIT 5 – SECURITY ISSUES IN AD HOC / SENSOR NETWORKS

AUTHENTICATION AND ITS TYPES

Authentication

- Authentication is a process used to verify the identity of a user, system, or entity attempting to access a particular resource or service.
- It is a crucial aspect of information security and is employed in various contexts, including computer systems, networks, websites, applications, and physical facilities.
- The primary goal of authentication is to ensure that only authorized individuals or systems are granted access to specific resources, while unauthorized entities are denied.
- Common challenges in authentication include the risk of password theft, the need for a balance between security and user convenience, and adapting to evolving security threats.

Need for Authentication

- **Protecting Confidential Information:**

  - Authentication helps safeguard sensitive and confidential information from unauthorized access. It ensures that only individuals with the proper credentials or permissions can access certain resources, such as personal data, financial information, or proprietary business data.

- **Preventing Unauthorized Access:**

  - Unauthorized access to systems, networks, or applications can lead to various security threats, including data breaches, theft, or manipulation of information.

- **Preventing Identity Theft:**

  - Authentication is a critical tool in preventing identity theft. Verifying the identity of users helps ensure that the person accessing sensitive information or services is indeed who they claim to be..

- **Adapting to Remote Access:**

  - With the increasing trend of remote work, authentication becomes even more critical. Remote access authentication ensures that only authorized users can connect to corporate networks and systems from outside the traditional office environment.

Authentication Types

- **Password-Based Authentication:**

  - Users provide a secret passphrase or password to access a system or resource.

- **Token-Based Authentication:**

  - Users use physical or digital tokens, such as key fobs, smart cards, or mobile apps, to generate temporary codes for authentication.

- **Certificate-Based Authentication:**

  - Digital certificates, often issued by a trusted third party, are used to verify the authenticity of a user or system.

- **Risk-Based Authentication:**

  - Authentication decisions are based on risk factors, considering user behavior, location, and other contextual information to determine the level of risk associated with a particular login attempt.

Digital Signatures

- **Definition**

  - A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital messages or documents.

- **Key Components**

  - **Private Key :** The signer uses their private key to create the digital signature.

  - **Public Key :** The recipient uses the sender's public key to verify the signature.

Process:

- The sender creates a unique digital signature by applying a mathematical algorithm to the message using their private key.
- The recipient receives the message along with the digital signature.
- The recipient uses the sender's public key to verify the signature, ensuring the message hasn't been tampered with and confirming the sender's identity.

Digital Signatures

Advantages:

- **Security:** Provides a higher level of security compared to traditional signatures.
- **Efficiency:** Streamlines document workflows by eliminating the need for physical signatures.
- **Cost Savings:** Reduces costs associated with paper, ink, and manual processes.
- **Non-Repudiation:** Offers legal evidence of the origin and integrity of the document

Applications:

- **E-Signatures:** Used in electronic documents, contracts, and agreements.
- **Email Security:** Ensures the authenticity of emails and prevents tampering.
- **Financial Transactions:** Secures online transactions and authorizations.
- **Legal Documents:** Authenticates digital contracts and legal paperwork.

Digital Certificates

- **Definition**

- A digital certificate is a digital form of identification that includes information about the identity of an entity, such as an individual, a website, or an organization.

- It is issued by a trusted third party, known as a Certificate Authority (CA).

Key Components

1. **Public Key:** The digital certificate contains a public key associated with the entity.
2. **Identity Information:** Details about the entity, including name, public key, issuer, and expiration date.
3. **Digital Signature:** The certificate is signed by the CA to verify its authenticity.

Purpose:

- Digital certificates are used to establish secure communication channels, verify the identity of parties involved, and ensure the integrity of transmitted data.

Digital Certificates

Types of Certificate:

- **SSL/TLS Certificates:** Secure websites and encrypt data in transit.
- **Code Signing Certificates:** Ensure the authenticity of software and applications.
- **Email Certificates:** Secure email communication and verify sender identity.

Certificates LifeCycle:

- **Issuance:** The CA issues a certificate after verifying the identity of the entity.
- **Renewal:** Certificates have a limited validity period and need renewal.
- **Revocation:** Certificates can be revoked if compromised or no longer valid.

Applications:

- **Digital Signatures:** Supports the creation of verifiable digital signatures.
- **VPN Authentication:** Authenticates users in virtual private network connections.
- **Wi-Fi Security:** Ensures secure Wi-Fi connections using certificates.

User Authentication

- **Definition**

- User authentication is the process of verifying the identity of an individual seeking access to a system, application, or network.

- It ensures that only authorized users can gain entry.

Common Authentication Protocols:

1. **OAuth:** Used for delegated authorization, common in web and mobile applications.
2. **OpenID Connect:** Built on OAuth, focuses on user authentication.
3. **SAML (Security Assertion Markup Language):** Used for single sign-on (SSO) in enterprise environments.

Single vs Multi-Factor Authentication:

- **Single-Factor Authentication (SFA)**: Relies on one authentication factor.
- **Multi-Factor Authentication (MFA):** Involves two or more factors, enhancing security.

User Authentication

Importance of User Authentication:

1. **Data Protection:** Safeguards sensitive information from unauthorized access.
2. **Network Security:** Prevents unauthorized entry into systems and networks.
3. **Compliance:** Meets regulatory requirements for securing user data.
4. **User Trust:** Enhances user confidence in the security of the system.

Adaptive Authentication:

- **Contextual Authentication:**
  - Considers user behavior, location, and device information.
- **Risk-Based Authentication:**
  - Adjusts security measures based on perceived risk.

Elliptic Curve Cryptosystems (ECC)

- **Definition**

- Elliptic Curve Cryptosystems (ECC) is a form of public-key cryptography that uses the mathematics of elliptic curves to provide strong security with shorter key lengths compared to traditional methods.

Key Components:

1. **Elliptic Curve Equation:** The mathematical equation defining the curve over a finite field.
2. **Base Point (Generator Point):** A specific point on the curve used as the starting point for cryptographic operations.
3. **Scalar Multiplication:** The core operation involving repeated addition of the base point to generate public and private keys.

ECC Key Pair:

- **Public Key:** A point on the elliptic curve derived from the scalar multiplication of the base point.
- **Private Key:** A randomly chosen scalar used in the scalar multiplication process.

Elliptic Curve Cryptosystems (ECC)

Comparison with Other Cryptosystems:

1. **RSA vs. ECC:** ECC offers similar security with shorter key lengths, reducing computational overhead.
2. **Key Exchange Protocols:** ECC is often preferred for key exchange in protocols like Diffie-Hellman.

Applications:

- **Secure Communication:** Used in protocols like TLS and HTTPS to secure internet communication.
- **Digital Signatures:** Provides efficient and secure signing of messages.
- **Mobile and IoT Security:** Suited for devices with limited resources.
- **Blockchain and Cryptocurrencies:** Used in the creation of digital signatures and key pairs.

Challenges:

- **Implementation Complexity:** Proper implementation is crucial for security.
- **Standards and Patents:** Variability in ECC standards and potential patent issues.
- **Quantum Threat:** Quantum computers could potentially break ECC, leading to the exploration of ECC-resistant algorithms.

Thank You