



# Data & Network Security

Chapter 5 - Network Security  
~ part 3 ~

# Outline

## 5.1 Introduction to Network Security

## 5.2 Use of Cryptography for Data and Network Security

## 5.3 Architectures for Secure Networks

### 5.3.1 Secure Channels

### 5.3.2 Secure Routing Protocols

### 5.3.3 Secure DNS.

## 5.4 Defence Mechanisms and Countermeasures

### 5.4.1 Network Monitoring

### 5.4.2 Intrusion Detection & Prevention

### 5.4.3 Firewalls

### 5.4.4 Spoofing Protection

### 5.4.5 DoS & DDoS Protection

### 5.4.6 Honeypots

## 5.5 Wireless Security

## 5.6 Mobile and IoT Security

## 5.5 Wireless Security



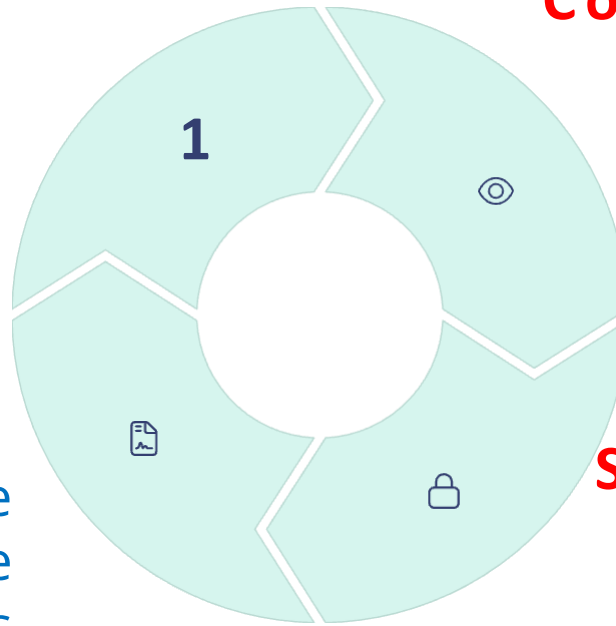
# Key Takeaways for Wireless Security

## Defense in Depth

Implement multiple security layers to protect wireless infrastructure

## Security Policies

Develop comprehensive wireless usage guidelines



## Continuous Monitoring

Actively scan for rogue access points and unauthorized connections

## Strong Authentication

Use WPA3, certificate-based authentication and MFA

Securing wireless networks requires a comprehensive approach that addresses the unique challenges of radio-based communication. Organizations should implement network segmentation to isolate wireless traffic from sensitive systems, employ wireless intrusion detection systems, and regularly conduct security assessments to identify vulnerabilities. Staff training remains critical, as users must understand the risks of connecting to unsecured networks and the importance of following security protocols.

# Preventing Wireless Attacks



## Strong Encryption

Use WPA3 or WPA2 with AES encryption to protect transmitted data.

## Enterprise Authentication

Implement 802.1X with RADIUS for individual user authentication.

## Rogue AP Detection

Monitor for unauthorized access points with wireless scanning tools.

## Network Segmentation

Isolate wireless networks from sensitive internal resources.

# Strong Encryption

Four security approaches:

1. WEP (Wired Equivalent Privacy)
2. WPA (Wi-Fi Protected Access)
3. WPA2 (Wi-Fi Protected Access II)
4. WPA3 (Wi-Fi Protected Access III)

WPA also has two generations named **Enterprise** and **Personal**.

## Cont...

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program

## WEP (Wired Equivalent Privacy)

- The specification of a protocol, along with the chosen key length (if variable) is known as a *cipher suite*. The options for the confidentiality and integrity cipher suite are:
- **ENCRYPTION:** WEP, with either a 40-bit or 104-bit key,
- **PASSPHRASE:** Key 1-4 Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 hex or 5 ASCII characters in length for 40/64-bit encryption and 26 hex or 13 ASCII characters in length for 104/128-bit encryption.



# WPA/WPA2 Personal

- WPA is a **set of security mechanisms** that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- **Encryption:**
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)
- **Pre-Shared Key (PSK):**
  - A key of 8-63 characters

WPA3 will **protect against dictionary attacks** by implementing a new key exchange protocol.

**Smart bulbs, wireless appliances, smart speakers, and other screen-free gadgets** make everyday tasks just a little bit easier, but connecting them to Wi-Fi can be a Sisyphean task. WPA3 streamlines the process.



WPA3 defines a new handshake that “**will deliver robust protections** even when users choose passwords that fall short of typical complexity recommendations”.

In other words, even if you’re using a **weak password**, the WPA3 standard will protect against brute-force attacks

## WPA3 Protocol

Includes optional 192-bit minimum strength security mode, aligned with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems. **This was a request by the US government.**



**Uses 128-bit encryption**

Makes use of a Simultaneous Authentication of Equals (SAE) handshake which protects against brute force attacks

Incorporates Forward Secrecy means that a new set of encryption keys are generated every time a WPA3 connection is made, so if the initial password is compromised, it won't matter

**Bolsters security on public networks**

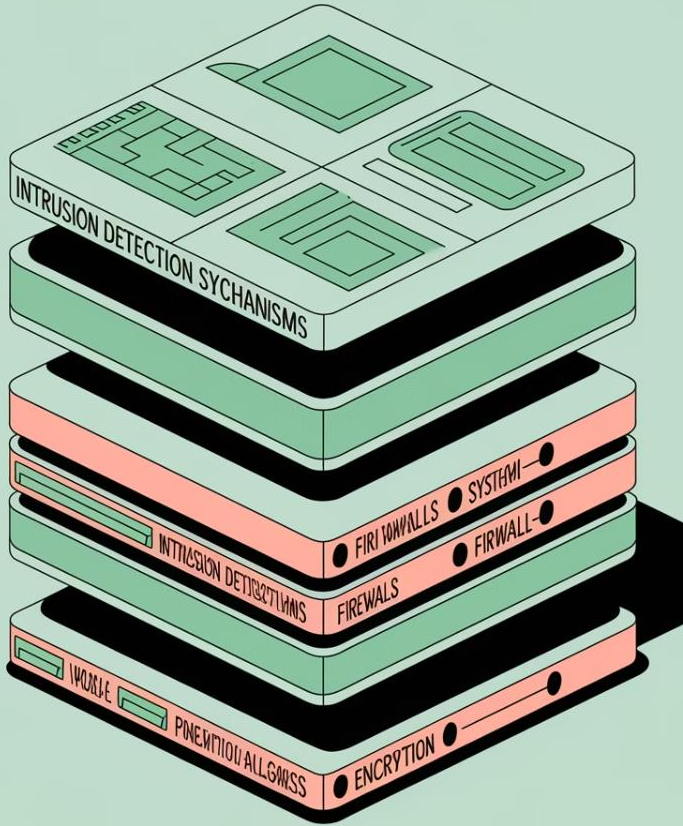
Easily manages connected devices

Allows Natural Password Selection, which the Wi-Fi Alliance claims will make it easier for users to remember passphrases

**WPA3-Personal**

	WEP	WPA	WPA2	WPA3
<b>BRIEF DESCRIPTION</b>	Ensure Wired - like Privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i Features and a new hardware	Announced by wi-fi Alliance
<b>ENCRYPTION</b>	RC4	TKIP +RC4	CCMP/AES	GCMP-256
<b>AUTHENTICATION</b>	WEP - Open WEP - Shared	WPA-PSK WPA- Enterprise	WPA2-Personal WAP2-Enterprise	WPA3- Personal WPA3- Enterprise
<b>Data Integrity</b>	CRC - 32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/ MultiCast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256))
<b>Key Management</b>	None	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) Exchange and Elliptic curve Digital Signature Algorithm (ECDSA)

# Wireless Security Technologies



## Authentication

RADIUS servers provide centralized user verification and access control.



## Endpoint Security

Anti-malware solutions protect individual wireless clients.



## Firewall Protection

Internal and external firewalls filter traffic based on security policies.



## Wireless IPS

Dedicated systems monitor for anomalies and wireless attacks.

# Common Defence Strategies

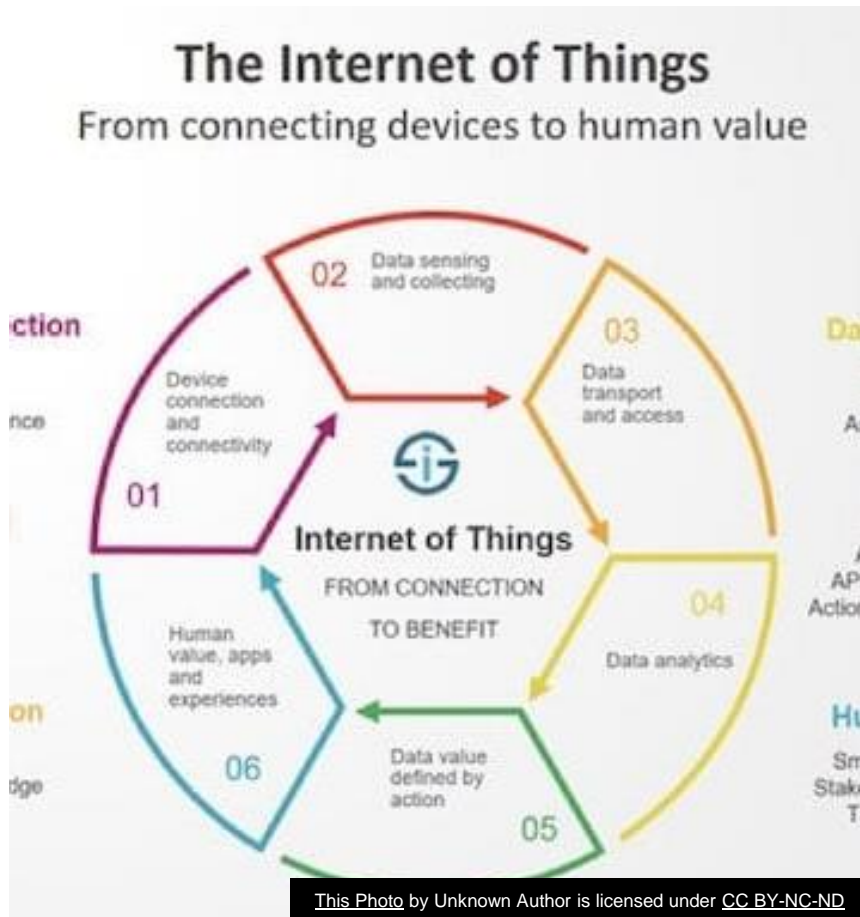
- Change router default username and password.
- Change the internal IP subnet if possible.
- Change the default name and hide broadcasting of the SSID (Service Set Identifier).
- None of the attack methods are faster or more effective when a larger passphrase is used.
- Restrict access to your wireless network by filtering access based on the MAC (Media Access Control) addresses.
- Use encryption.
- Use centralized authentication like the RADIUS server.



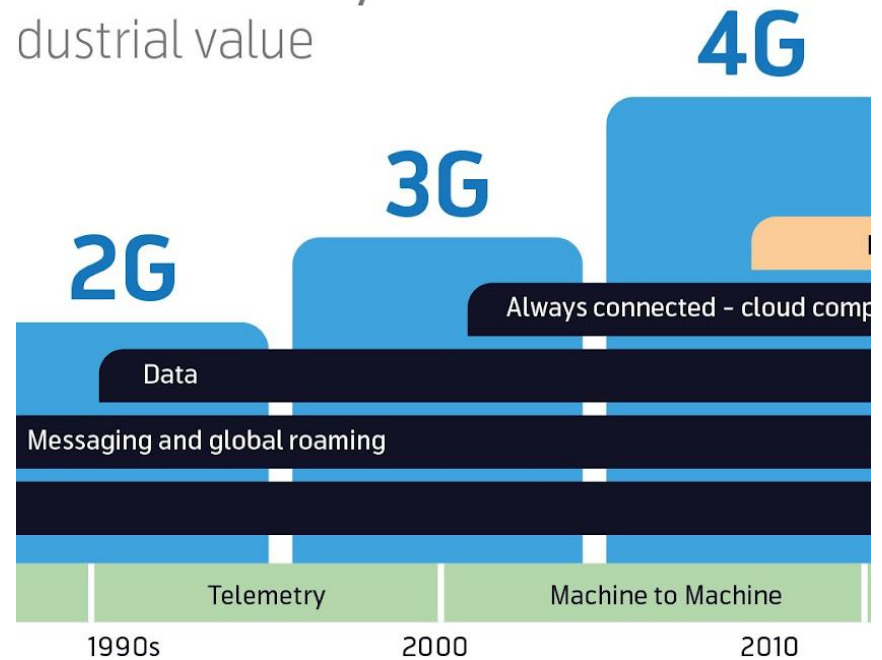
**We do not have WiFi**, talk to each other. Pretend it is 1995.



## 5.6 Mobile and IoT Security



Connectivity  
Industrial value



*This Photo by Unknown Author is licensed under CC BY-SA-NC*



# Device Security Strategy



## Auto-Lock and Authentication

Enable auto-lock and require PIN/password protection to access the device and decrypt data



## Remote Management

Implement remote wipe capabilities and IT access to manage lost or stolen devices



## Software Security

Keep software updated, install antivirus protection, and encrypt sensitive data



## Application Control

Implement whitelisting, digital signatures, or secure sandboxes for applications



# Traffic and Network Security



## Encryption

All traffic should be encrypted via SSL, IPv6, or VPNs



## Authentication

Two-layer authentication for both device and user



## Barrier Security

Firewalls and IDS/IPS with mobile-specific rules

Traffic security relies on strong encryption and authentication mechanisms. Organizations should configure VPNs so all traffic between mobile devices and the network travels through secure channels. A two-layer authentication approach—authenticating both the device and the user—provides stronger security than single-factor authentication.



# BYOD Policy Implementation



## Device Inspection

IT managers should inspect each device before allowing network access



## Configuration Guidelines

Establish clear guidelines for operating systems and applications



## Prohibited Practices


No "rooted" or "jailbroken" devices permitted on the network





## Synchronization Control

Implement restrictions on device synchronization and cloud storage

# IoT Security and Privacy Requirements (ITU-T)

 **Communication Security**  
Secure, trusted, and privacy-protected communication to prevent unauthorized access, ensure data integrity, and protect privacy during transmission

 **Service Provision Security**  
Prevention of unauthorized access to services and fraudulent service provision, protecting IoT user privacy information

 **Data Management Security**  
Protection when storing or processing data to prohibit unauthorized access, guarantee integrity, and protect privacy-related content

 **Integration of Security Policies**  
Ability to integrate different security policies and techniques for consistent security control across diverse devices and networks

# More IoT Security Requirements (ITU-T)

## Mutual Authentication and Authorization

Before a device or user can access the IoT, mutual authentication and authorization must be performed according to predefined security policies.

This ensures that only legitimate devices and users can connect to the network and access resources, preventing unauthorized access and potential attacks.

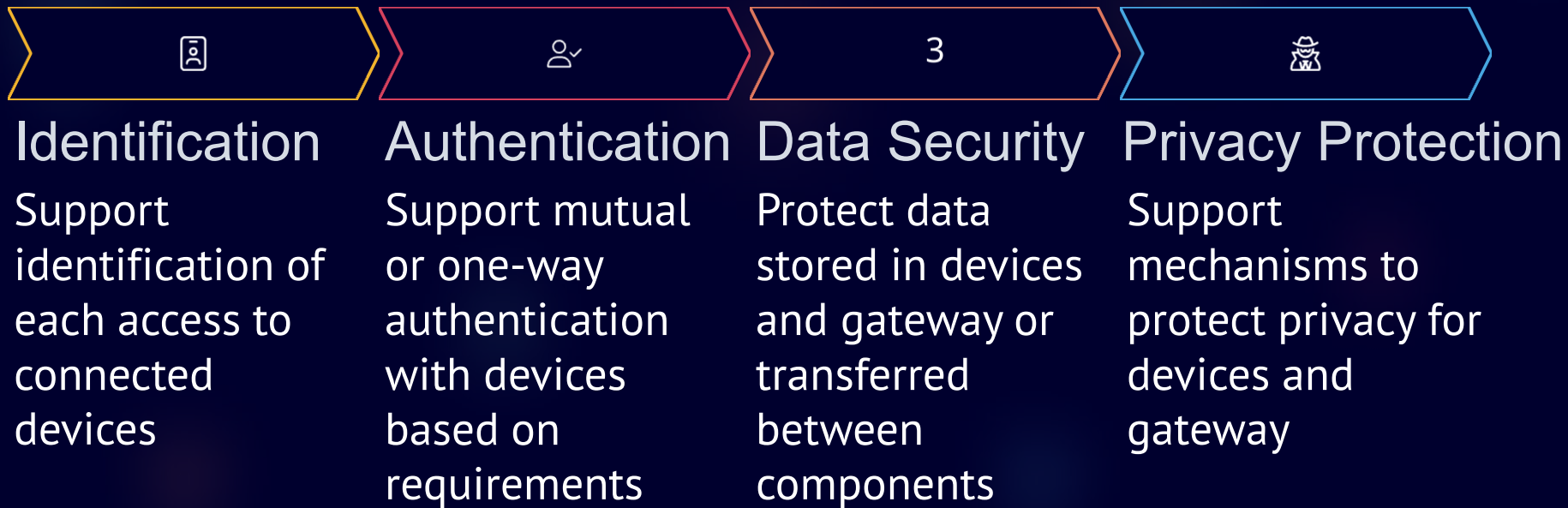
## Security Audit

Security audit must be supported in IoT environments. Any data access or attempt to access IoT applications must be:

- Fully transparent
- Traceable
- Reproducible according to regulations and laws

IoT must support security audit for data transmission, storage, processing, and application access to enable accountability and compliance.





# IoT Gateway Security Functions



Gateways play a crucial role in IoT security by providing security services for constrained devices that may lack their own security capabilities. However, some requirements like securing data stored on constrained devices may be impractical without encryption capabilities on those devices.



# More IoT Gateway Security Functions

-  Self-maintenance  
Support self-diagnosis, self-repair, and remote maintenance capabilities
-  Configuration  
Support multiple configuration modes including remote, local, automatic, manual, and policy-based dynamic configuration
-  Updates  
Support firmware and software updates to address vulnerabilities and add features
-  Application Authentication  
Support mutual authentication with applications to ensure secure communication

These gateway security functions help bridge the security gap between constrained IoT devices and the broader network, providing a security perimeter that protects vulnerable devices while enabling secure communication with applications.

# IoT Security Framework

Cisco has developed a framework for IoT security that serves as a useful guide to security requirements. The framework addresses security across four levels of the IoT architecture:

1

Smart Objects/Embedded Systems

Most vulnerable part of IoT, may not be physically secure and need to function for years

2

Fog/Edge Network

Concerns with variety of network technologies and protocols, requiring uniform security policy

3

Core Network

Traditional network security issues complicated by vast number of endpoints

4

Data Center/Cloud

Application, storage, and management platforms dealing with huge numbers of endpoints



# IoT Security Capabilities

## Role-based Security

RBAC systems assign access rights to roles instead of individual users. Users are assigned to different roles according to their responsibilities.

This well-understood approach can manage access to IoT devices and the data they generate, providing scalable access control across the ecosystem.

## Anti-tamper and Detection

Particularly important at device and fog network levels but extends to core network. These functions protect components that may be physically outside protected enterprise areas.

## Data Protection and Confidentiality

Extends to all levels of the architecture, protecting sensitive information throughout the ecosystem.

## Internet Protocol Protection

Protects data in motion from eavesdropping and snooping between all levels.

# Secure IoT Framework Components

1

## Authentication

Elements that identify IoT devices through non-human means like RFID, certificates, or MAC addresses

---



## Authorization

Controls device access throughout the network fabric, establishing parameters for information exchange

---

3

## Network Enforced Policy

Elements that route and transport endpoint traffic securely over the infrastructure

---



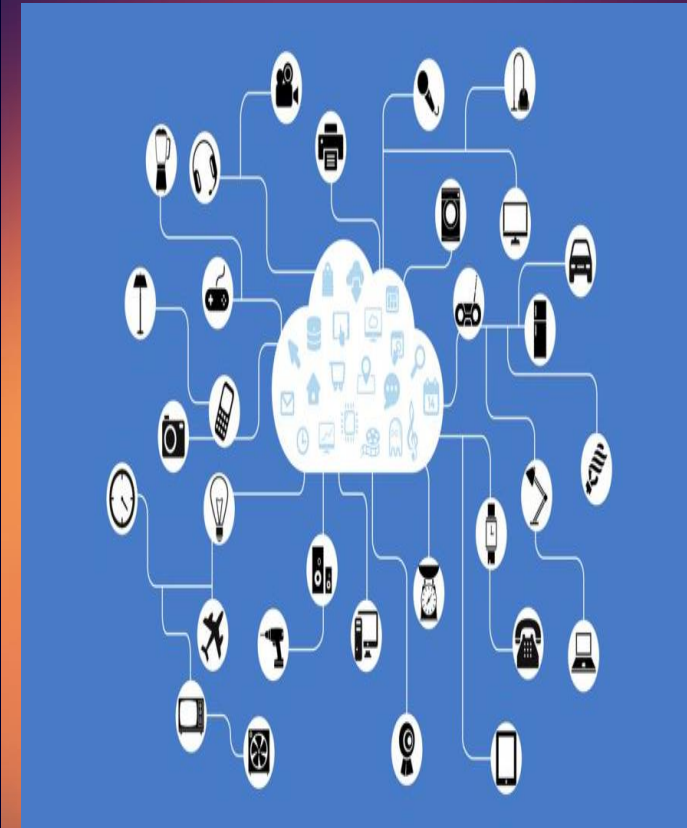
## Secure Analytics

Functions for central management, visibility, and control of IoT devices


# Trust Relationships in IoT

In the IoT security context, trust relationship refers to the ability of two partners to have confidence in the identity and access rights of each other. The authentication component provides a basic level of trust, which is expanded with the authorization component.

For example, a car may establish a trust relationship with another car from the same vendor, allowing them to exchange safety capabilities. When the same car establishes a trusted relationship with its dealer's network, it may share additional information like odometer readings and maintenance records.



This Photo by Unknown Author is licensed under CC BY-SA



# MiniSec: Open-source IoT Security Module

## Overview

MiniSec is part of TinyOS, designed for small embedded systems with tight requirements on memory, processing, real-time response, and power consumption

## Purpose

Link-level security module offering high security while keeping energy consumption low and using minimal memory

## Features

Provides confidentiality, authentication, and replay protection for wireless sensor networks

MiniSec has two operating modes: one for single-source communication and another for multi-source broadcast communication. The latter doesn't require per-sender state for replay protection, making it scalable for large networks.

# MiniSec Requirements

-  **Data Authentication**  
Enables verification that messages originated from legitimate nodes and remained unchanged during transmission
-  **Replay Protection**  
Prevents attackers from recording and replaying packets at a later time
-  **Low Energy Overhead**  
Minimizes communication overhead and uses only symmetric encryption
-  **Confidentiality**  
Ensures that data cannot be read by unauthorized parties
-  **Freshness**  
Guarantees weak freshness where receivers can determine partial ordering of messages without local reference time
-  **Resilience to Lost Messages**  
Tolerates high message loss rates common in wireless sensor networks

# MiniSec Cryptographic Algorithms

## Skipjack

Developed by the NSA in the 1990s, Skipjack is one of the simplest and fastest block cipher algorithms, making it critical for embedded systems with limited resources.

- Uses an 80-bit key
- Most efficient in terms of code memory
- Excellent encryption/decryption efficiency
- Superior key setup efficiency

While 80 bits is generally considered inadequate for modern security, it suffices for the limited application of wireless sensor networks with their short data blocks and slow data links.

## Offset Codebook (OCB) Mode

The block cipher mode of operation chosen for MiniSec offers several advantages:

- Provably secure assuming the underlying block cipher is secure
- Highly efficient one-pass operation
- Only one block cipher call per plaintext block
- Provides both encryption and authentication in a single algorithm
- Well-suited for stringent energy constraints of sensor nodes

## MiniSec-U (Unicast)

Designed for communication between two devices:

- Uses synchronized counters (nonce) with each sender
- Counter ensures semantic confidentiality
- Receiver rejects packets with equal or smaller counter values
- Prevents replay attacks
- Resynchronization protocol handles dropped packets

## MiniSec-B (Broadcast)

Designed for one-to-many communication:

- Avoids counter maintenance for multiple receivers
- Uses time-based epochs as part of the nonce
- Prevents replay of messages from older epochs
- Augments timing approach with bloom-filter
- Bloom-filter prevents replay attacks within current epoch

# Key Security Considerations for Cloud and IoT



As cloud computing and IoT continue to evolve, security measures must adapt to address the unique challenges of each environment while ensuring seamless integration between them. Organizations must implement comprehensive security strategies that protect data and devices across the entire ecosystem, from edge to cloud.



# Summary

- Several combinations of technology and application that suit best based on organization requirement is needed to secure the network.
- Cryptography is best suited to secure data on the fly (Internet access) or in a database.
- For network security, deployment of the defence mechanisms and countermeasures is expected to prevent many attacks related to the network environment.
- If not all, at least network security implementation can reduce attacks or minimize the effect of malicious traffic to an acceptable level while maintaining functionality for users' access.

# Summary

- **Wireless networking** provides numerous opportunities to increase productivity and lower implementation costs. It also **alters** an **organization's overall computer security risk profile**.
- Although it is **impossible** to **eliminate all risks** associated with wireless networking, it is possible and **reasonable** to level the security by **adopting a systematic approach** to assessing and managing risk.
- This chapter discussed **wireless technologies, components and their concepts, wireless threats and vulnerabilities** of wireless networks and described commonly available **countermeasures or security approaches** that could be used to **mitigate those risks**.



## Summary

- 📁 **Cloud Computing**  
Understand service models (SaaS, PaaS, IaaS), deployment models, and security approaches specific to cloud environments
  - 🔒 **Cloud Security**  
Implement comprehensive security measures addressing data protection, access control, and shared responsibility models
  - 🌐 **Internet of Things**  
Recognize the components, architecture, and relationship with cloud computing in IoT deployments
  - 🔒 **IoT Security**  
Address unique challenges including patching vulnerabilities, constrained devices, and gateway security functions
- As these technologies continue to evolve and converge, security professionals must stay informed about emerging threats and countermeasures. Implementing appropriate security frameworks and following best practices will help organizations protect their cloud and IoT assets while enabling innovation and growth.

## References

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). Securing Your Network.

Luciana Obregon. (2016), Infrastructure Security Architecture for Effective Security Monitoring.

William Stallings. (2017). Network Security Essential. Man-in-the-Middle Attack.

<https://www.veracode.com/security/man-middle-attack>

<https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/>

# References

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). Securing Your Network.

Luciana Obregon. (2016), Infrastructure Security Architecture for Effective Security Monitoring

William Stallings. (2017). Network Security Essential.

<https://purplesec.us/wp-content/uploads/2019/11/Intrusion-Detection-IDS-VS-Intrusion-Prevention-IPS-What%E2%80%99s-The-Difference.png>

<https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867>

William Stalling & Lawrie Brown (2018). Computer Security: Principles and Practice (4th Edition)