emergent security techniques

Semester 5 – January 2025

[Industrial Security 2](#_Toc187569068)

[Introduction to ICS 2](#_Toc187569069)

[Overview 2](#_Toc187569070)

[What is ICS? 2](#_Toc187569071)

[ICS Architecture 2](#_Toc187569072)

[Key Components of ICS 2](#_Toc187569073)

[Safety and Redundancy in ICS 3](#_Toc187569074)

[Communication in ICS 3](#_Toc187569075)

[Control and Automation in ICS 3](#_Toc187569076)

[Industrial Security Challenges 3](#_Toc187569077)

[Historical Evolution of ICS 3](#_Toc187569078)

[Conclusion 4](#_Toc187569079)

[PLC Programming 4](#_Toc187569080)

[Overview 4](#_Toc187569081)

[What is a PLC? 4](#_Toc187569082)

[Features and Architecture of PLCs 4](#_Toc187569083)

[Advanced Features and Modern Developments 5](#_Toc187569084)

[Programming PLCs 5](#_Toc187569085)

[Practical Tools 5](#_Toc187569086)

[Key Takeaways 5](#_Toc187569087)

[Industrial Protocols 5](#_Toc187569088)

[Overview 5](#_Toc187569089)

["Industrial Ethernet" vs. "Traditional Ethernet" 5](#_Toc187569090)

[Evolution of Industrial Communication 6](#_Toc187569091)

[Overview of Ethernet-Based ICS Protocols 6](#_Toc187569092)

[Detailed Protocol Analysis 7](#_Toc187569093)

[Key Security Considerations 7](#_Toc187569094)

[Software Defined Radio 8](#_Toc187569095)

[Analog Radio Transmission 8](#_Toc187569096)

[Overview 8](#_Toc187569097)

[What is Software Defined Radio (SDR)? 8](#_Toc187569098)

[Frequency Spectrum and Radio Bands 8](#_Toc187569099)

[Basic Signal Theory 8](#_Toc187569100)

[Analog Modulation Techniques 9](#_Toc187569101)

[Signal Processing in SDR 9](#_Toc187569102)

[SDR Systems and Tools 9](#_Toc187569103)

[Applications of SDR 9](#_Toc187569104)

[Digital Radio Transmission 10](#_Toc187569105)

[Overview 10](#_Toc187569106)

[Recap – Analog Modulation 10](#_Toc187569107)

[Digital Modulation 10](#_Toc187569108)

[Encoding Techniques 11](#_Toc187569109)

[Digital Signal Processing (DSP) in SDR 11](#_Toc187569110)

[Demonstrations and Applications 11](#_Toc187569111)

[RFID and NFC 12](#_Toc187569112)

[Overview 12](#_Toc187569113)

[RFID and NFC Basics 12](#_Toc187569114)

[How RFID Works 12](#_Toc187569115)

[RFID Tag Types 12](#_Toc187569116)

[RFID Spectrum and Frequencies 13](#_Toc187569117)

[RFID Security Challenges 13](#_Toc187569118)

[Applications of RFID and NFC 13](#_Toc187569119)

[Advanced Implementations 14](#_Toc187569120)

[High-Frequency RFID and NFC 14](#_Toc187569121)

[HF RFID Standards and Implementations 14](#_Toc187569122)

[MIFARE Classic Card Details 15](#_Toc187569123)

[MIFARE Plus and DESFire 15](#_Toc187569124)

[Security Challenges for HF RFID 16](#_Toc187569125)

[AI 17](#_Toc187569126)

# Industrial Security

## Introduction to ICS

### Overview

* The presentation introduces **Industrial Control Systems (ICS)** and their importance in securing critical infrastructure and industrial assets.
* **Key Challenge**: Cyberattacks on critical infrastructure are one of the top five global risks, as reported by the World Economic Forum (2018).

### What is ICS?

ICS refers to command and control networks used to support industrial processes, e.g.:

* SCADA (Supervisory Control and Data Acquisition) systems.
* DCS (Distributed Control Systems).
* PCS (Process Control Systems).
* SIS (Safety Instrumented Systems).
* PLCs (Programmable Logic Controllers).

### ICS Architecture

**Hierarchical Layers**:

* **Corporate IT**: ERP servers and production management systems.
* **Supervision Network**: SCADA servers, engineering stations, and supervision consoles.
* **Production Network**: PLCs, HMIs (Human-Machine Interfaces), sensors, robots, and historians.

### Key Components of ICS

#### SCADA (Supervisory Control and Data Acquisition)

* Manages and controls systems over long distances.
* Handles unique communication challenges (e.g., delays, data integrity).

#### DCS (Supervisory Control and Data Acquisition)

Distributes intelligence for controlling processes individually.

#### PLC (Programmable Logic Controllers)

* Solid-state control system with programmable memory for various industrial tasks.
* Features include reliability, modularity, ease of programming, and compatibility with other devices.

#### RTU (Remote Terminal Unit)

Combines remote communication capabilities with programmable logic for remote process control.

#### IED (Intelligent Electronic Device)

Intelligent electronic devices equipped with microprocessors for digital communication.

#### HMI (Human Machine Interface)

User interface to manage and monitor processes in ICS.

#### Historian

Centralized database for time-stamped data, supporting process analysis and reporting.

### Safety and Redundancy in ICS

#### Safety Instrumented Systems (SIS)

* Prevents or mitigates hazardous conditions.
* Examples: Fail-safe mechanisms for gas pressure, reactor temperature, and column pressure.

#### Redundancy Protocols

* **STP/RSTP**: Prevents network loops.
* **MRP**: Enables rapid recovery in Ethernet rings.
* **PRP**: Uses dual independent networks for zero recovery time.
* **HSR**: Ensures availability via duplicated paths in a ring topology.

### Communication in ICS

#### Historical Context

Transitioned from proprietary protocols and limited interconnectivity to Ethernet-based systems with open protocols.

#### Common Protocols

Examples: Modbus TCP, OPC UA, PROFINET, BACnet/IP, and energy-specific protocols like DNP3.

### Control and Automation in ICS

#### Control Loops

Closed-loop systems where control variables are compared with setpoints.

#### PID (Proportional-Integral-Derivative) Controllers

Feedback mechanisms for continuously modulated control in industrial applications.

#### P&ID (Piping and Instrumentation) Diagrams

Detailed representation of piping, instrumentation, and control devices.

### Industrial Security Challenges

#### Remote Access Risks

* Remote access to ICS over the internet can expose systems to vulnerabilities.
* Examples include unsecured protocols and default passwords.

#### Key Takeaways

* Protocols are complex but often lack robust security.
* Web servers add functionality but can introduce risks if misconfigured.

### Historical Evolution of ICS

* **First Industrial Revolution (1700-1900)**: Focus on mechanical production powered by steam.
* **Second Industrial Revolution (1900-1970)**: Mass production powered by electricity.
* **Third Industrial Revolution (1970-2000)**: Automation using electronics and early computing.
* **Present**: Integration of advanced networking, IoT, and cloud-based management systems.

### Conclusion

The presentation emphasizes:

* The complexity of securing ICS.
* The need to understand factory operations and gain trust with engineering teams.
* An innovative, creative, and entrepreneurial mindset to address evolving cybersecurity challenges.

## PLC Programming

### Overview

* **Focus**: Introduction to PLC (Programmable Logic Controller) programming within industrial control systems.
* **Objective**: Understand PLC functionality, architecture, programming languages, and practical applications.

### What is a PLC?

A **Programmable Logic Controller** is a solid-state control system with user-programmable memory, enabling automation in industrial processes.

#### Key Functions

* Input/Output (I/O) control.
* Logic processing.
* Timing, counting, and PID control.
* Communication, arithmetic, and file processing.

#### Historical Context:

* Originally, logic control relied on electromechanical relays.
* The first PLC was designed by Modicon as a relay replacer, reducing cabinet space and rewiring needs.

### Features and Architecture of PLCs

#### Core Characteristics

* Reliable and robust.
* Long lifecycle.
* Modular construction for easy replacement or expansion.
* Simple programming and debugging.

#### Basic Building Blocks

* **Input/Output Modules**: Interface with external devices.
* **Central Processing Unit (CPU)**: Executes control logic.
* **Memory**:
  + **Work Memory**: Volatile, for runtime elements.
  + **Load Memory**: Non-volatile, for program storage.
  + **Retentive Memory**: Stores critical values across power cycles.
* **Communication Modules (CM)**: Enable connectivity with other systems.
* **Programming Terminal**: Interface for developing and deploying programs.

### Advanced Features and Modern Developments

#### New Technologies

* Beckhoff PLCs with Intel Atom x64 CPUs.
* Sysmac NX7 controllers with AI engines for predictive maintenance and multitasking.
* Infineon microcontrollers offering real-time performance and safety compliance.

#### Memory and Storage

SIMATIC Memory Cards for program storage and updates.

### Programming PLCs

**IEC 61131-3 Standard**: Defines five programming languages for PLCs:

1. **Instruction List (IL)**: Low-level, assembly-like.
2. **Structured Text (ST)**: High-level, based on Pascal, suitable for complex logic.
3. **Function Block Diagram (FBD)**: Graphical, using interconnected blocks.
4. **Ladder Diagram (LD)**: Derived from relay logic, intuitive for electricians.
5. **Sequential Function Chart (SFC)**: Graphical representation of sequential tasks.

### Practical Tools

**LogixPro 500 ProSim II**: A simulator for Allen-Bradley PLCs, enabling hands-on practice in a virtual environment.

### Key Takeaways

* PLCs form the backbone of industrial automation.
* Programming flexibility and modularity are critical for effective industrial control.
* Understanding different programming languages and their use cases is essential for practical application.
* New technologies integrate AI and advanced communication for enhanced performance.

## Industrial Protocols

### Overview

* **Focus**: Understanding industrial communication protocols used in Industrial Control Systems (ICS), with emphasis on security considerations and practical applications.
* **Objectives**:
  + Highlight differences between "Industrial Ethernet" and "Traditional Ethernet."
  + Provide an overview of Ethernet-based ICS protocols.
  + Explore security concerns in common protocols.
  + Conduct hands-on analysis with Wireshark captures.

### "Industrial Ethernet" vs. "Traditional Ethernet"

#### Environmental Requirements

Industrial Ethernet hardware is designed to endure harsh conditions:

* High temperatures, vibrations, electromagnetic noise, and chemicals.
* Features rugged construction, no moving parts, and low power consumption (≤ 24V).

#### Installation Requirements

* **Office Networks**:
  + Tree/star topologies.
  + Flexible cabling for variable workplace setups.
* **Industrial Networks**:
  + Bus (linear) or ring (redundant) topologies.
  + System-specific connections with rare modifications.

#### Performance

* **Office Networks**:
  + Medium availability.
  + Acyclic transmissions with timing in seconds.
* **Industrial Networks**:
  + High availability with isochronous, cyclic transmissions.
  + Timing in microseconds for real-time operations.

### Evolution of Industrial Communication

#### Historical Context

Early systems used proprietary serial protocols with limited interconnectivity.

#### Modern Systems

* Transition to Ethernet-based communications with open protocols.
* Integration with business systems and internet for remote access.

### Overview of Ethernet-Based ICS Protocols

#### Universal ICS Protocols

* Modbus TCP: TCP/502.
* OPC UA: TCP/4840.
* OP UA XML: TCP/80, TCP/443.

#### Process Automation Protocols

* EtherCat: UDP/34980.
* PROFINET: TCP/34962-34964.

#### Building Automation Protocols

* BACnet/IP: UDP/47808.
* LonTalk: UDP/1628, UDP/1629.

#### Energy Sector Protocols

* DNP3: TCP/20000, UDP/20000.
* IEC 104: TCP/102.

### Detailed Protocol Analysis

#### Modbus

* Originated in 1979 by Modicon (Schneider Electric).
* Variants include Modbus TCP/IP, RTU, and ASCII.
* **Security Concerns**: Lacks authentication, encryption, and broadcast suppression.
* **Recommendations**: Use industrial firewalls and intrusion protection systems.

#### PROFINET

* Developed by Siemens and PROFIBUS User Organization in 2003.
* Supports real-time and isochronous communication.
* **Security Concerns**: Lacks authentication and encryption.
* **Recommendations**: Implement network zones, packet inspection, and passive monitoring.

#### S7Comm

* Siemens proprietary protocol for ICS communication.
* Operates via ISO TCP with command-response structure.

### Key Security Considerations

ICS protocols often lack robust security features such as encryption and authentication.

#### Best Practices

* Define network zones and restrict access via conduits.
* Employ deep-packet inspection and intrusion detection systems.
* Continuously monitor network behavior for anomalies.

# Software Defined Radio

## Analog Radio Transmission

### Overview

* **Focus**: Introduction to Software Defined Radio (SDR) and its application in analyzing and transmitting analog radio signals.
* **Objectives**:
  + Understand the frequency spectrum, radio waves, and basic signal theory.
  + Explore analog modulation and demodulation techniques.
  + Practical implementation using GNU Radio and SDR tools.

### What is Software Defined Radio (SDR)?

SDR replaces traditional hardware components with software implementations, enabling:

* Versatility in analyzing and processing radio signals.
* Simplified evaluation of radio communication security.

### Frequency Spectrum and Radio Bands

#### Electromagnetic Spectrum

* Radio waves are a form of electromagnetic radiation with wavelengths longer than infrared light.
* Energy is transported via **electromagnetic waves** (does not require a medium).

#### Radio Spectrum Segments for Amateur Use

* **Medium Frequency (MF)**: 300 kHz–3 MHz (AM broadcasting, some HAM bands).
* **High Frequency (HF)**: 3–30 MHz (shortwave broadcasting, HAM bands, maritime communication).
* **Very High Frequency (VHF)**: 30–300 MHz (TV, FM, public safety).
* **Ultra High Frequency (UHF)**: 300 MHz–1 GHz (cellular, satellite TV, Wi-Fi).
* **Microwave**: Above 1 GHz (GPS, wireless networks, satellite communication).

### Basic Signal Theory

#### Wave Parameters

* **Period (T)**: Time for one cycle.
* **Frequency (f)**: Cycles per second (in Hz).
* **Amplitude (A)**: Height from midline to crest.
* **Phase (φ)**: Position relative to a reference wave.

#### Fourier Theorem

* Any periodic function can be represented as a sum of sines or cosines with specific amplitude and phase (Fourier coefficients).
* Utilized in signal analysis to separate frequency components.

### Analog Modulation Techniques

#### Modulation

Combines a message signal with a higher-frequency carrier wave for transmission.

Types:

* **Amplitude Modulation (AM)**: Amplitude of the carrier varies with the message signal.
* **Frequency Modulation (FM)**: Carrier frequency changes in proportion to the message signal.
* **Phase Modulation (PM)**: Carrier phase changes in relation to the message signal.

#### Demodulation

Process of extracting the original message signal from the modulated carrier.

### Signal Processing in SDR

#### Sampling and Quantization

* **Sampling**: Converts continuous-time signals to discrete-time.
* **Quantization**: Maps continuous amplitude values to discrete ones.

#### Fast Fourier Transform (FFT)

Converts signals from the time domain to the frequency domain, enabling analysis of frequency components.

#### Digital Signal Representation

Use of **in-phase (I)** and **quadrature (Q)** components for more accurate signal representation and analysis.

### SDR Systems and Tools

#### Popular SDR Hardware

* RTL2832u, HackRF One, Yard Stick, PandwaRF.
* Devices vary in frequency range, cost, and functionality.

#### Software

* **SDR#**: Simple and accessible SDR software.
* **GNU Radio**: Open-source toolkit for designing and implementing SDR applications.

### Applications of SDR

SDR allows flexibility in exploring radio technologies, including:

* Amateur radio.
* Security evaluations.
* Wireless network analysis.

## Digital Radio Transmission

### Overview

* **Focus**: Introduction to digital signal processing in SDR, covering digital modulation, encoding techniques, and practical applications.
* **Objectives**:
  + Recap analog modulation principles.
  + Explore digital modulation methods and encoding schemes.
  + Implement practical SDR applications through demonstrations.

### Recap – Analog Modulation

Converts data into a higher-frequency signal for transmission.

#### Three types of analog modulation

1. **Amplitude Modulation (AM)**:
   * Varies amplitude of the carrier signal based on the message signal.
   * **Advantages**: Simple design.
   * **Disadvantages**: Susceptible to noise.
   * **Applications**: AM radio.
2. **Frequency Modulation (FM)**:
   * Varies frequency of the carrier signal.
   * **Advantages**: Less noise interference.
   * **Disadvantages**: Complex circuitry.
   * **Applications**: FM radio.
3. **Phase Modulation (PM)**:
   * Varies phase of the carrier signal.
   * **Advantages**: Resistant to noise.
   * **Disadvantages**: Most complex of the three.
   * **Applications**: Satellite communication.

### Digital Modulation

Converts digital data into higher-frequency signals suitable for transmission.

#### Types

1. **Amplitude Shift Keying (ASK)**:
   * Varies amplitude of the carrier to represent binary data (on-off keying).
   * **Applications**: Infrared remotes, optical transmitters.
2. **Frequency Shift Keying (FSK)**:
   * Varies frequency of the carrier.
   * **Applications**: Telemetry systems, modems.
3. **Phase Shift Keying (PSK)**:
   * Shifts the phase of the carrier signal.
   * Special case: **QPSK (Quadrature PSK)** transmits 2 bits per phase shift.
   * **Applications**: Broadband modems, satellite communication, mobile phones.
4. **Quadrature Amplitude Modulation (QAM)**:
   * Combines ASK and PSK to increase bit rate.
   * Higher-order QAM (e.g., QAM16, QAM64) supports more data per symbol.

### Encoding Techniques

#### Line Encoding

Translates binary data into signals suitable for transmission.

Types:

* **Unipolar**:
  + Uses pulses for "1" and absence for "0."
  + Variants: Non-Return to Zero (NRZ), Return to Zero (RZ).
* **Polar**:
  + Positive pulse for "1" and negative for "0."
  + Variants: NRZ, RZ.
* **Bipolar**:
  + Alternates polarity for "1" and uses zero voltage for "0."
  + Example: Alternate Mark Inversion (AMI).

#### Manchester Encoding

* Splits each bit period into two, ensuring transitions for synchronization.
* "1": 0 in the first half, 1 in the second half.
* "0": 1 in the first half, 0 in the second half.

### Digital Signal Processing (DSP) in SDR

#### Key Concepts

* **Sampling**: Converts continuous signals into discrete ones.
* **Quantization**: Maps amplitude to discrete values.
* **FFT (Fast Fourier Transform)**: Converts signals to frequency domain for analysis.
* **IQ Data**: Combines in-phase and quadrature components for accurate representation.
* **Constellation/Scatter Plots**: Visualizes signal phase and amplitude in modulation schemes like QPSK and QAM.

#### Baud Rate vs. Bit Rate

* **Baud Rate**: Number of symbol changes per second.
* **Bit Rate**: Number of bits transmitted per second.

### Demonstrations and Applications

#### Automatic Dependent Surveillance-Broadcast (ADS-B)

Tracks aircraft positions and information (e.g., identity, altitude).

#### Wireless Clock Synchronization

Demonstrates RF signal usage in timing devices.

#### Weather Services and Wireless Fax

Displays practical implementations of RF data transmission.

#### 433 MHz Wireless Remotes

Analyzes signals from common remotes using tools like:

* **rtl\_433**: Decodes ISM band signals (e.g., 433 MHz, 868 MHz).
* **Universal Radio Hacker (URH)**: Investigates wireless protocols.

# RFID and NFC

### Overview

* **Focus**:
  + Understanding Radio-Frequency Identification (RFID) and Near-Field Communication (NFC) technologies, their components, and applications.
  + Understanding high-frequency RFID implementations, NFC technologies, and MIFARE card systems.
* **Objectives**:
  + Introduce RFID and NFC concepts.
  + Explain how RFID systems operate.
  + Explore RFID tag types, frequencies, and security considerations.
  + Explore NFC and high-frequency RFID (13.56 MHz).
  + Examine common HF card implementations, including MIFARE types.
  + Discuss security considerations for HF RFID systems.

### RFID and NFC Basics

#### RFID

Uses electromagnetic fields to identify and track tags remotely.

**Components**:

* **Tag**: Stores data.
* **Reader**: Queries tags.
* **Antenna**: Facilitates communication.

#### NFC

* A subset of high-frequency RFID (13.56 MHz).
* Enables peer-to-peer communication where devices act as both readers and tags.
* Popular for secure data exchange, payments, and smart devices.

### How RFID Works

#### Operational Steps

* Reader generates an electromagnetic field via its antenna.
* The tag's antenna receives energy from this field.
* Induced current powers the tag's chip.
* The tag sends data back to the reader.
* The reader demodulates and processes the tag's data.

### RFID Tag Types

#### Passive Tags

* No internal power source.
* Powered by electromagnetic energy from the reader.

#### Battery-Assisted Passive (BAP) Tags

Use a small battery to extend functionality.

#### Active Tags

Include internal batteries for longer ranges and additional features.

### RFID Spectrum and Frequencies

#### Low Frequency (LF)

* Range: 125–134 kHz.
* Short read range (up to 10 cm).
* Applications: Animal tracking, access control.
* Limitations: Low data rates, limited security.

#### High Frequency (HF)

* Range: 3–30 MHz (NFC operates at 13.56 MHz).
* Read range: 10 cm to 1 meter.
* Applications: Ticketing, data transfer, payments.
* Features: High data rate, encryption support.

#### Ultra-High Frequency (UHF)

* Range: 860–960 MHz.
* Read range: Up to 30 meters for passive tags and over 100 meters for active tags.
* Applications: Inventory management, vehicle tracking.
* Limitations: Less effective near metals or liquids.

### RFID Security Challenges

#### Security Issues

* Data printed on tags is often visible, creating a risk of cloning.
* Tags can be read, skimmed, or emulated from a distance.
* Small keyspaces (e.g., 26-bit UIDs) make brute-force attacks feasible.

#### Research Tools

* **Proxmark 3**: Supports sniffing, cloning, and emulation of RFID tags.
* Open-source and widely used in security research.

### Applications of RFID and NFC

#### LF RFID

Animal tracking, basic access control.

#### HF RFID/NFC

Payments, smart marketing, public transport ticketing.

#### UHF RFID

Logistics, inventory tracking, vehicle and cargo monitoring.

### Advanced Implementations

#### Common Low-Frequency Implementations

* **HID Cards**: Branded proximity cards used in access control.
* **EM4x Cards**: Carry 64 bits of read-only memory.
* **T55xx Cards**:
  + Read/write capability.
  + Supports multiple data rates and encoding schemes (e.g., Manchester, FSK).
  + Can be password-protected.

#### Security Tools and Exploits

* Devices like handheld RFID writers and specialized PCBs enable cloning and emulation.
* Security research highlights risks in poorly secured systems.

### High-Frequency RFID and NFC

#### High-Frequency RFID (HF)

* Operates at 13.56 MHz, widely used in contactless applications.
* Applications include payment systems, public transport cards, and identification.

#### Near-Field Communication (NFC)

* A branch of HF RFID designed for secure peer-to-peer communication.
* **Key Features**:
  + Allows devices to act as both readers and tags.
  + Popular in smartphones, payment systems, and marketing tools.

#### NFC Data Exchange Format (NDEF)

* Lightweight format for exchanging information.
* Messages are structured with records containing metadata and payloads.

### HF RFID Standards and Implementations

#### ISO/IEC 14443

* Defines proximity cards and transmission protocols.
* Used in more than 80% of contactless smart cards.
* Applications:
  + NFC technology.
  + MIFARE cards.
  + EMV payment systems (e.g., Visa payWave, PayPass).

#### MIFARE Card Families

Manufactured by NXP Semiconductors; over 10 billion sold.

**Types**:

* **MIFARE Classic**:
  + Stores 1–4 KB of data.
  + Security: Uses proprietary Crypto-1 encryption, now considered insecure.
* **MIFARE Plus**:
  + Backward-compatible with Classic.
  + Offers AES-128 encryption for higher security.
* **MIFARE DESFire**:
  + Advanced security features and AES encryption.
  + Supports multiple storage sizes (2–8 KB).
* **MIFARE Ultralight**:
  + Low-cost, limited memory (512 bits).
  + Includes minimal security features like one-time programmable bits.

### MIFARE Classic Card Details

#### Key Features

* Anti-collision loop for distinguishing multiple cards.
* Sectors protected with two keys (A and B) for authentication.

#### Security Challenges

* UID (Unique Identifier) is always readable, even without keys.
* Many implementations reuse default or empty keys.
* Crypto-1 encryption is broken, making cloning and attacks feasible.

#### Common Attacks

* Exploiting default keys.
* Recovering non-default keys using known attacks.

### MIFARE Plus and DESFire

#### MIFARE Plus

* Adds AES encryption for secure communication.
* Supports proximity checks to prevent relay attacks.
* Four security levels:
  + Level 0: Factory configuration.
  + Level 1: Emulates MIFARE Classic.
  + Level 2: AES authentication with CRYPTO1.
  + Level 3: AES-only secure communication.

#### MIFARE DESFire

* Based on SmartMX core with improved security.
* Supports AES or Triple DES encryption.
* Configured with a directory structure for multiple applications.

#### MIFARE Ultralight

* **Variants**:
  + **Ultralight EV1**: Adds OTP bits and configurable counters.
  + **Ultralight C**: Incorporates Triple DES for cloning prevention.
* **Challenges**:
  + Attacks demonstrated on data pages, lock bits, and counter systems.
  + Reliance on OTP areas for security can be circumvented if misconfigured.

### Security Challenges for HF RFID

#### Common Issues

* UID reliance: UIDs are readable without authentication.
* Weak or broken encryption: Many cards use outdated crypto protocols.
* Misconfigured security features: Real-world systems often fail to utilize provided protections effectively.

#### Default Keys

* Default production keys are often reused, making attacks feasible.
* Wordlist attacks can guess keys efficiently.

#### Tools for Security Research

* **Flipper Zero**: Versatile tool for cloning and analyzing RFID tags.
* **Proxmark3**: Gold standard for RFID security research.
* **Chameleon Mini/Tiny**: Investigates RFID protocols.
* Mobile apps like NFC Tools and NFC TagInfo.

# AI