Unseen Triggers: Exploiting Wireless Channels to Activate Dormant Malware in Air-gapped Critical Infrastructure

Authors: Hosam Alamleh, Ulku Clark, Bilge Karabacak

University of North Carolina Wilmington

Introduction & Background

- Critical infrastructure (power grids, industrial networks) faces cyber threats beyond the internet.
- Air-gapping and segmentation are common security measures, but adversaries exploit non-internet methods.
- Dormant malware can be remotely activated via wireless channels like GPS, AIS, and RF signals.
- Case studies show real-world attacks exploiting these vulnerabilities.

Remote Activation Techniques

Attackers exploit wireless technologies to trigger dormant malware.

TABLE I
WIRELESS TECHNOLOGIES EXPLOITED FOR REMOTE ACTIVATION

Wireless Technology	Sector Used	Frequency	Range
Global Positioning System (GPS)	Navigation, time synchronization, and location-based services in critical infrastructure	L1 (1575.42 MHz), L2 (1227.60 MHz)	Global
Automatic Identification System (AIS)	Maritime navigation, ship tracking, and collision avoidance	161.975 MHz, 162.025 MHz	Up to 74 km (coastal waters)
Radio Frequency (RF) Command Injection	Industrial control systems, military communications, and IoT applications	433 MHz, 868 MHz, 2.4 GHz	Varies from meters to km
Pager Protocols	Emergency and mission critical communications, paging systems	Dedicated paging frequencies	Up to 3 km
Bluetooth and Short-Range Wireless	Industrial IoT, medical devices, and consumer electronics	2.4 GHz ISM band	Up to 100 meters
Wi-Fi Signal Triggers	Industrial automation, enterprise networks, and smart devices	2.4 GHz, 5 GHz	Up to 100 meters
LoRaWAN (Long Range Wide Area Network)	Low power IoT applications, smart cities, and industrial monitoring	433 MHz, 868 MHz, 915 MHz	Up to 15 km (rural), 5 km (urban)
Acoustic Signals	Maritime and underwater systems	10 Hz – 1 MHz	Up to 10 km

System Firmware

System firmware processes wireless inputs, but poor coding practices create vulnerabilities that attackers can exploit. Weaknesses like buffer overflows and improper exception handling can enable malware injection. Attackers may also use insider threats and portable storage devices to compromise firmware security.

The corruption of the system firmware involves two key elements:

- The activation logic
- The payload:

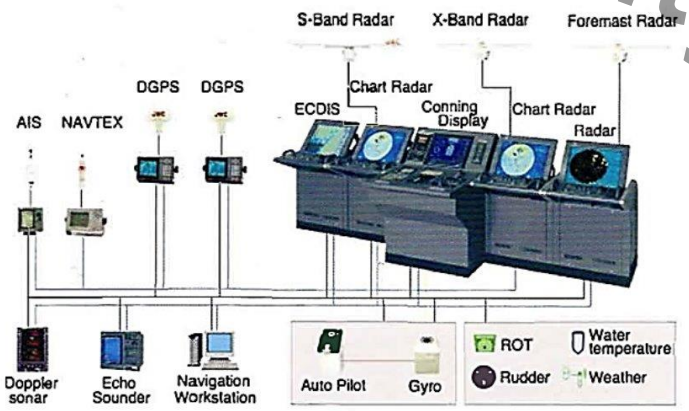
Algorithm 1 Wireless Input Activation Algorithm

```
Function Main():
    Initialize system  while system is running do
        Input ← Read from wireless interface  if Input =
        Activation_Value then
            Payload ()
        end
    end
end
Function Payload():
    Execute predefined payload action
end
```

Case Studies: Real-World Attacks

AIS Spoofing in Maritime Vessels:

- Attackers use AIS signals to trigger malware onboard ships.



GPS-Based Power Grid Attack:

GPS spoofing disrupts time synchronization in power grids.

- Leads to power instability and potential blackouts.