Cyber Attacks on Smart Farming Infrastructure

Authors: Sina Sontowski, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, Ravi Sandhu

Presenter: Sina Sontowski
ssontowsk42@tntech.edu
Outline

• Background
• Network Attacks
• Deauthentication Attack
• Implications of Deauthentication Attack
Background

• Smart-Farming
  • Fulfill global food demand and supply
  • Boost productivity and maintain product quality
• A Smart-Farm, an attack vector
  • Target for foreign competitors
  • Limited investment in cybersecurity
  • Lack of resources
Research Objectives

• Explore different Cyberattacks
• Demonstrate a Cyberattack on a Smart Farming Architecture
• Analyze the attack and why it was possible so that it can be fixed
Network Attacks

• Possible due to use of 802.11 protocol, not limited to Smart-Farm domain:
  • Password Cracking
  • Evil Twin Access Point
  • Key Reinstallation Attack
  • Kr00k - CVE-2019-15126
  • ARP Spoofing Attack
  • DNS Spoofing Attack
Deauthentication Attack
Set-up of the Architecture
Steps of the Attack

a). Scanning for Access Point and Stations
b). Main Menu
c). Select Raspberry Pi
Completion of the Attack
Implications of Deauthentication Attacks

- Sensor Data Obstruction
  - Obstruct real-time communication
  - Disrupt irrigation system’s decision
  - Damage crops, negatively affecting harvest
- Controlling Connected Devices
  - Gains access to entire smart-farm through evil twin access point or password cracking
  - Controlling agricultural drones to spray excessive fertilizers over the plants
Defense against Deauthentication Attacks

- Enabling IEEE 802.11w by encrypting management frames
- Reasonable priced 802.11w routers common in big companies
- Production cost: encryption capability issues
- 802.11w requires vendor to update code/firmware on both Aps and client side
- Raspberry Pi 3 Model B’s network interface card does not support encryption protocol required for protected management frames; however, Model B+ does
Conclusion

- Smart Farming has become popular and widely adopted
- Exposes new attack surfaces
- DoS attack on Smart-Farming Infrastructure
  - Deauthentication Attack
- Weakness of IEEE 802.11 protocol
- Successful attack has serious implications
- Future work, expand on other attacks and use other protocols