



**Tennessee**  
**TECH**

# 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

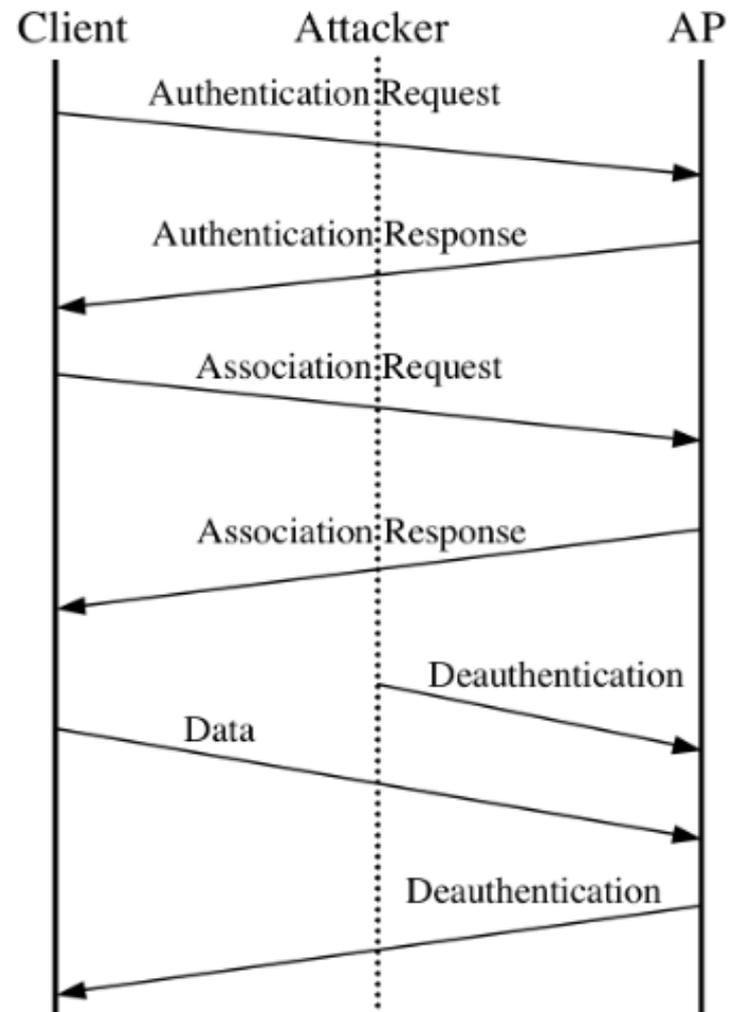


# Network Attacks

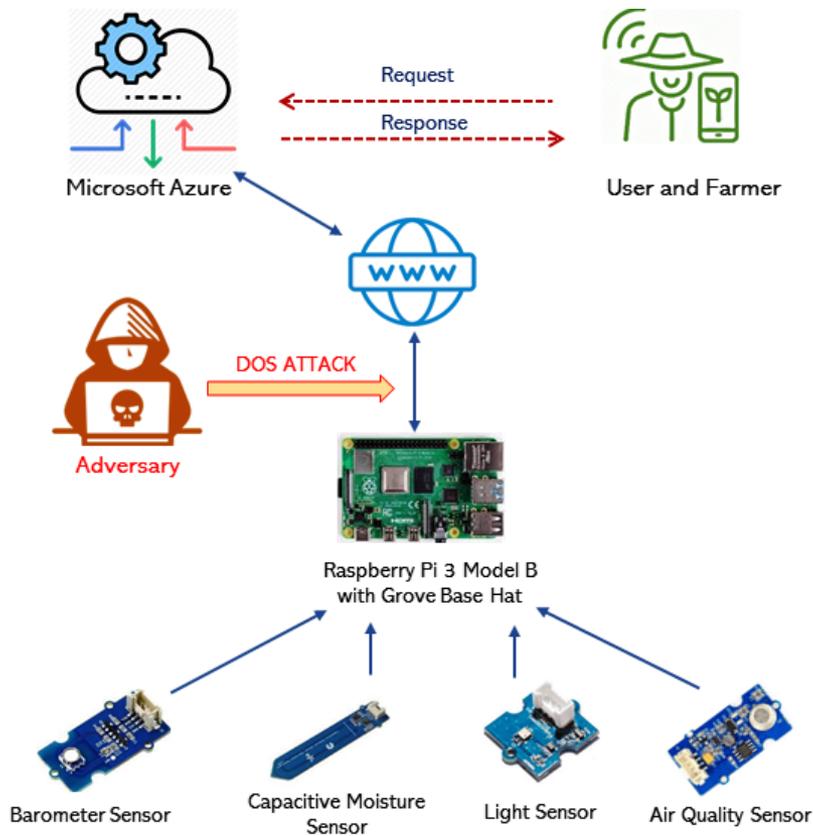
- Possible due to use of 802.11 protocol, not limited to Smart-Farm domain:
  - Password Cracking
  - Evil Twin Access Point
  - Key Reinstallation Attack
  - Kr00k - CVE-2019-15126
  - ARP Spoofing Attack
  - DNS Spoofing Attack



# Deauthentication Attack



# Set-up of the Architecture



Device

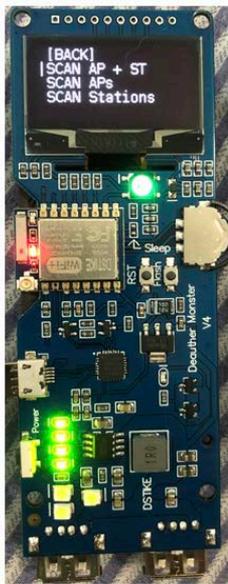
## FarmBeats Labs - IndoorM1 - ...

Measurements Settings Properties **Commands** Rules Dashboard

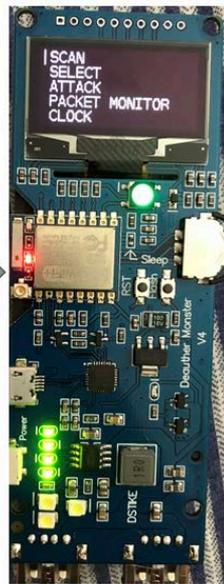
Use the commands to execute actions on your device.

Sensor Update ⓘ ⌛	Image Update ⓘ ⌛	Restart Device ⓘ ⌛
<b>Run</b>	<b>Run</b>	<b>Run</b>
Sent at 19:41 6/18/2020 (UTC)	Sent at 19:41 6/18/2020 (UTC)	Sent at 18:09 5/28/2020 (UTC)

# Steps of the Attack



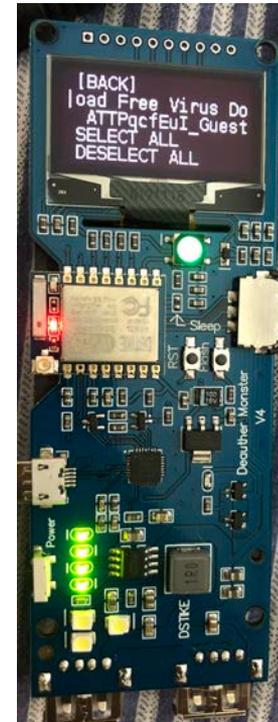
a). Scanning for Access Point and Stations



b). Main Menu



c). Select Raspberry Pi



# Completion of the Attack

FBSK-General-0059 Search

Device **FarmBeats Labs - IndoorM1 - ...**  
Measurements Settings Properties **Commands** Rules Dashboard

Use the commands to execute actions on your device.

Command	Status
Sensor Update	Command Delivery Failed at 18:05 5/28/2020 (UTC)
Image Update	Command Delivery Failed at 18:06 5/28/2020 (UTC)
Restart Device	Command Delivery Failed at 18:05 5/28/2020 (UTC)

Apply a display filter ... <#>

No.	Time	Source	Destination	Protocol	Length	Info
1967	4.893734	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=476, FN=0, Flags=0
2179	5.443789	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=478, FN=0, Flags=0
2190	5.493192	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=490, FN=0, Flags=0
2205	5.543376	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=492, FN=0, Flags=0
2230	5.593361	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=495, FN=0, Flags=0
2252	5.646374	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=497, FN=0, Flags=0
2278	5.693111	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=500, FN=0, Flags=0
2303	5.743159	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=502, FN=0, Flags=0
2321	5.793045	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=505, FN=0, Flags=0
2341	5.843801	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=507, FN=0, Flags=0
2369	5.893045	ARRISGro_01:71:60	Broadcast	802.11	55	Deauthentication, SN=510, FN=0, Flags=0

▶ Frame 1: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)  
▶ Radiotap Header v0, Length 25  
▶ 802.11 radio information  
▶ IEEE 802.11 Request-to-send, Flags: .....C

# 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

