Hacking into a Lightbulb

Presented by Joshua Emo, Rana Mahal & Tyler Crawford

Introduction to IoT Security

- IoT (Internet of Things)
- Easy to hack
- Can affect personal lives up to National Security
- Foothold for further attacks
- Need for security

Summary of Vulnerabilities

- Improper Authentication
- Hard-Coded Short Checksum Shared Secret
- Lack of Randomness in Symmetric Encryption
- Insufficient Message Freshness Checks

Attack Scenarios

- 1: Fake Bulb Discovery Messages Generation
- 2: Password Exfiltration from Tapo User Account
- 3: MITM Attack with a Configured Tapo L530E
- 4: Replay Attack with the Smart Bulb as Victim
- 5: MITM Attack with an Unconfigured Tapo L530E

Attack Scenario 3

- Initial Setup
- Intercepting RSA Key Transmission
- Session Key Manipulation
- Decrypting and Modifying Traffic

Recreating Attack Scenario 3

- Demonstrate how to exploit
- Encountered challenges
- Conducted several steps of troubleshooting
- Unable to capture expected communication
- Further investigation (software patched?)

Experiment Challenges

- Despite obstacles, valuable insight
- Complexities of IoT Security
- Practical challenges of Penetration Testing
- Importance of Up-To-Date Firmware
- Need for robust Authentication
- Still provided basis for further attacks

Review of Experiment / Next Steps

- Learned significant information from Attack 3
- Unable to replicate vulnerability exploitation
- Bulb model and firmware the same (v1.19)
- Research suggests Tapo software updated
- Vulnerabilities Patched Out (or so we thought!)
- Alternative Methods to interact with bulbs?

Rest API

- Open-Source Project enables Remote Control
- Web-Based interface
- Not-Affiliated with TP-Link (Unofficial)
- Official Rest API made for Tapo developers
- Exploits API to send signals to bulbs
- Tricks bulbs into thinking signal from Tapo App
- Can create backdoor and manipulate API

IoT Botnets!

- Encouraging to see improved IoT Security
- IoT devices to reach 18.8 billion by Q4 2024 (13%+)
- Mirai Botnet exploited common devices in 2016
- Largest DDoS attacks in history
- Created botnet using 900,000 IoT devices
- Need for IoT security, regulation
- Successor botnets still in use

Conclusion

- Large contrast in security practices between brands
- Market flooded with unsecured IoT devices
- IoT vulnerability decrease security around the globe
- Need greater security for IoT devices
- Protocols for IoT security across the board
- Create a safer, more secure IoT ecosystem
- Address now before catastrophe in the future!