SCREAM: Sensory Channel Remote Execution Attack Methods

N.Brown, N. Patel, P. Plenefisch, A. Moghimi, T. Eisenbarth, C. Shue, K.Venkatasubramanian
Worcester Polytechnic Institute, Worcester, MA
POC Email: kven@wpi.edu

Internet of Things

Internet of Things

- 50 billion devices and $7 triilion market by 2020.
- New security challenges, internet-connected embedded devices
- In recent news: car exploitation, security camera attacks

Example IoT devices, Nest Thermostat (left) and Apple Watch (right)

Current embedded devices **implicitly trust** sensor data.

We explore ways to exploit this possibly misplaced trust.

Background & Problem Statement

Sources of threat[1]

- Communication Channel
- Preloaded Malware or Firmware update
- Sensory Channel Threats[1][2]

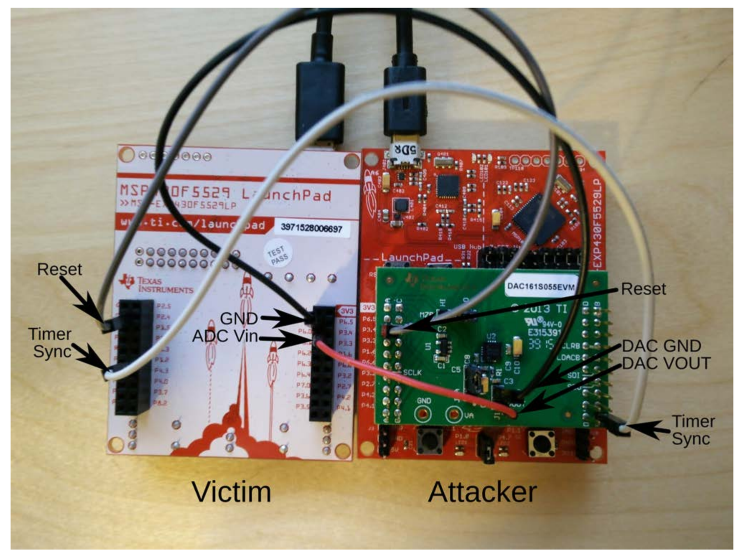
Traditional solution classes:

- Cryptographic and secure protocol design
- Program attestation[3]

Problem Statement

Demonstrate an attack on IoT systems that gains arbitrary code execution via the analog sensory channel, **bypassing traditional security solutions**

Target System



Victim H/W Assumptions

- MSP430F5529
  - 16-bit microcontroller
  - **von Neumann architecture**
  - 12-bit on-chip ADC
  - No NX support

Attacker Assumptions

- Access to high fidelity 12-bit external DAC
- Has access to victim IoT device, particularly its ADC pins

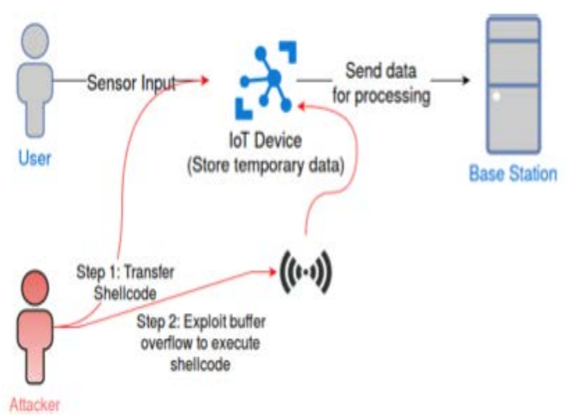
S/W Assumptions

- Vulnerable firmware application
- No stack protection (e.g., canary, non-executable stack etc.)
- Firmware attestation (e.g., SWATT) executing on the device

Code Execution via Sensory Channel

The basic mechanism of the attack is:

- The attacker physically interfaces with analog-sensor channel of the IoT device.
- The attacker identifies vulnerable digital software processing performed by the IoT application and induce appropriate voltage to the sensor interface to exploit the vulnerabilities.



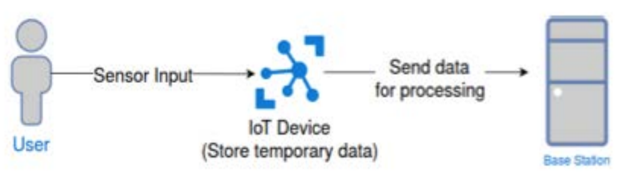
Attack Method

- We use a Digital- to-Analog converter (DAC) to modulate platform-specific shell code bytes into appropriate voltages
- The shell code is written to the memory of the IoT device.
- That code can then be executed either directly or by exploiting additional vulnerabilities (e.g., buffer overflow)

Vulnerable Application 1

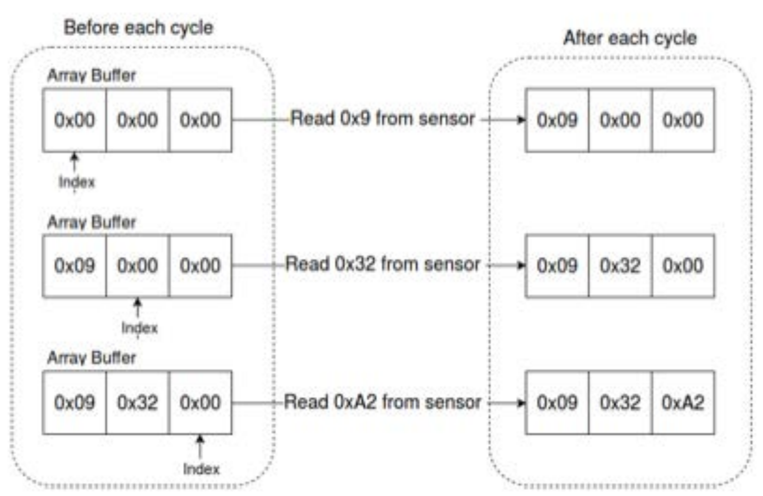
Store and Send

- Stores raw data into buffer **without any processing**
- Emulates a system that buffers and sends sensor data to another device like a base station



Application Operational Overview

Attack Overview



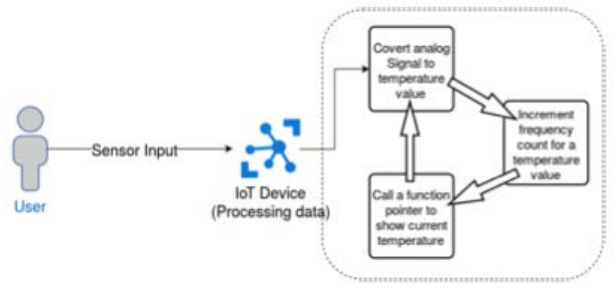
Memory Layout

- Only allows malware transfer – requires another exploit to trigger

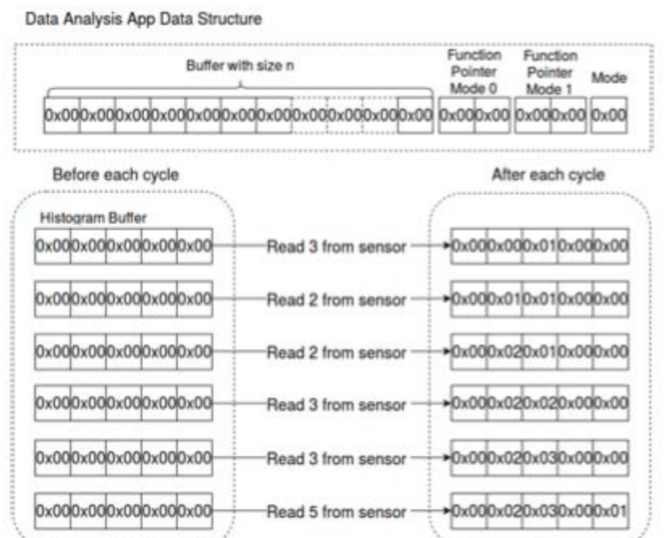
Vulnerable Application 2

Data Analysis

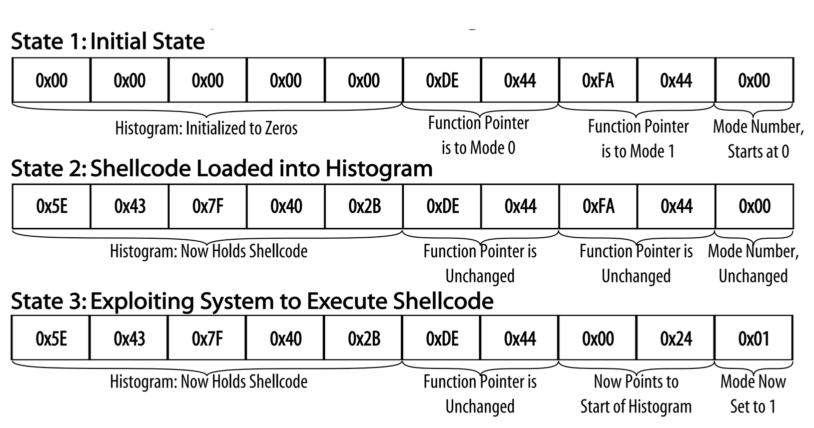
- Stores **histogram** of sensor readings
- Periodically calls one of two function pointers stored in RAM, depending on mode bit



Application Operational Overview

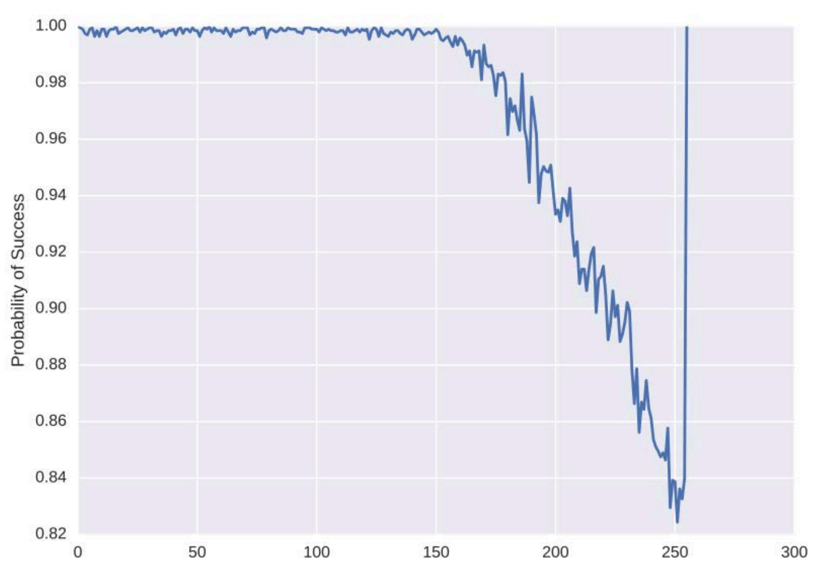


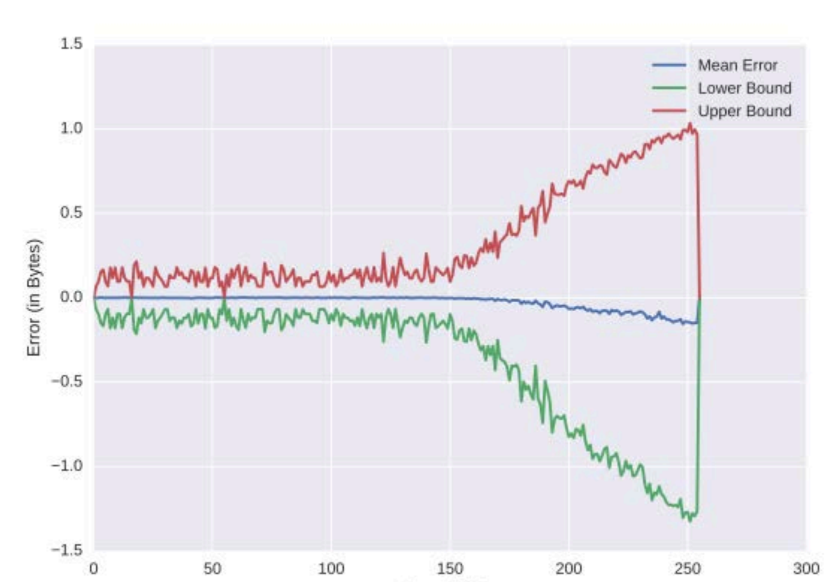
Memory Layout



Memory Layout During Attack

Performance Analysis of SCREAM





Success Rates for All Methods

Method	Success Rate (%)
Store & Send	83.3%
Analysis, bin width = 1	45.7%
Analysis, bin width = 2	92.8%
Analysis, bin width = 3	100.0 %

Our attack was very successful, **bypassing current defenses**.

We have exposed a gap in current defense mechanisms that **needs to be addressed**, given the impending Internet of Things.

Future Work

- Improve accuracy with better hardware
- Wireless sensory channel manipulation – removing need for physical access
- Volatile memory attestation
- Propose solutions to defend against the attack

1. D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu. GhostTalk: Mitigating emi signal injection attacks against analog sensors. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP '13, pages 145–159, Washington, DC, USA, 2013. IEEE Computer Society.
2. A. S. Uluagac, V. Subramanian, and R. Beyah. Sensory channel threats to cyber physical systems: A wake-up call. In Communications and Network Security (CNS), 2014 IEEE Conference on, pages 301–309, Oct 2014.
3. A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. SWATT: software-based attestation for embedded devices. In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pages 272–282, May 2004.