Georgia Tech School of Electrical and Computer Engineering
College of Engineering

Azure Zero Trust IoT Data Collection System

Team #8, Azure Zero Trust IoT

Project Faculty Advisor: Professor Brendan D. Saltaformaggio

External Partner: Dr. John D. Williams (Boeing), Michael F. Mitchell (Boeing)

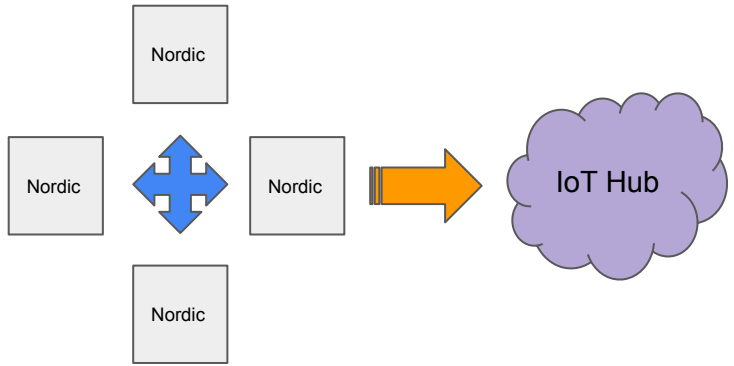
James Thomas Computer Engineering jthomas8@gatech.edu
Aaron J Wasserman Computer Engineering wasserman@gatech.edu
Jayla Williams Computer Engineering jwilliams664@gatech.edu
Noah G Dorfman Computer Engineering n.dorfman00@gatech.edu
Zixuan Kang Computer Engineering zkang35@gatech.edu

Overview/Agenda

- Introduction
  - Objectives
  - Motivation
  - Background
- Project Description and Goals
- Technical Specification
- Design Approach and Details
  - MQTT vs AMQP
  - RP4 vs LTE
- Project Demonstration Plan
- Schedule, Tasks and Milestones (Planned)
  - Schedule Changes (Modified and purchasing problems)
- Marketing and Cost Analysis
- Leadership Roles
- Next Steps

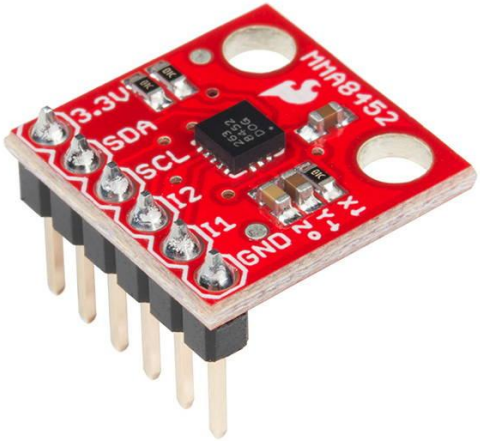
Objectives

- Design and prototype a secure IoT system for data collection and remote storage
  - Nordic microcontroller devices to form bluetooth, data-collection mesh
  - Transmit data via cellular connection to Azure IoT Hub cloud platform
  - Employ Azure Zero Trust framework throughout
- Demonstrate security of the system
  - Hardware attacks
  - Network attacks
  - Software attacks



Motivation

- CPS/IoT improves our daily lives
- 5G initiative
- Provide information protection and monetization



Background

- Past: Castle-and-Moat Approach
  - IPv4/IPv6
  - Verify IP addresses
  - Geographical Location
- Nowadays: Cloud Services/Outsourcing Server
  - Once the system is conquered, nothing in there is safe.
  - Lateral attack
- Solution: Always verify, never trust -- Zero Trust Architecture (ZTA)
  - Microsoft Authenticator
  - Duo Mobile

Project Description and Goals

Relatively inexpensive, secure, IoT data collection system

- Use Nordic devices that can support:
  - BLE mesh
  - LTE data transmission
- Follow Azure Zero Trust framework
  - Network traffic security
  - Software development practices

Technical Specifications

General System

Item	Specification
Supported Number of Devices in Network	> 2 nodes
Cost	< $500
Data Collection Frequency	100 Hz
Battery Life (minimum)	4 hours

Security

Item	Specification
Zero Trust Protocol	1 handshake/transmission
Hardware Access to Sensor Data	0 known vulnerable side-channel vectors
Software Access to Sensor Data	0 leaks to non-authorized accesses
Resistance to “Fuzzing”	0 device crashes

Design Approach and Details -- MQTT vs AMQP

AMQP	MQTT
● Can be more secure. ● More configurable ● For Azure, AMQP is needed for using their service endpoints ● For Azure, Microsoft offers various security features with AMQP	● Low overhead ● Simple to implement and send data from embedded systems. ● Best for many small messages on low-bandwidth networks ● For Azure, MQTT works well with Azure Data Lake Storage ● For Azure, IoT Protocol Gateway offers a way to bridge to AMQP if a service offering from MS is required

Design Approach and Details -- RP4 vs LTE

LTE	Separate Gateway (RP4)
● Lightweight system (eliminate the need for extra devices) ● useful everywhere with a cellular connection ● Security less complicated	● Initialization is easier. ● More existing community support ● More versatile ● Allows for more complicated tasks to be completed. ● Useful for future applications (doing work on the network edge, rather than going to the server for everything)

Project Demonstration Plan

- Functional Demo
  - Present a functional mesh network of Nordic devices actively measuring and transmitting environmental data to a database
  - Have laptop showing the data updating in real time w/ minimum sampling rate spec shown
- Dummy System Demo
  - Poster detailing attacks tested on the system showing robustness against common attack vectors
  - Show a dummy system implemented on a Raspberry Pi or similar where the attacks are successful side by side with the attacks failing on our system

Schedule, Tasks, and Milestones (Planned)

- Intent was to complete the following tasks over the summer
  - Order nordic devices
  - Test program reading data
  - Setup BLE mesh network
  - Setup cloud services
  - Setup comms with server
  - Test basic functionality
- Would’ve left only the vulnerability assessment, patching, and presentation/documentation preparation for the fall
- A delay on purchasing has caused us to have to adjust this schedule

Schedule Changes (Modified after purchasing problems)

- Original plan was to get mesh network functionality completed over summer
  - Intended to leave more time for vulnerability screening and patching in the fall
- Attempted to purchase the nordic devices however our requests were pushed back while they were setting up the purchasing/reimbursement system
- As of last week purchasing still isn’t live so we still have had no development time with hardware
- Will expedite system development at the front of the semester to leave as much time for security assessment and patching as possible
  - May have to focus on a smaller portion of the attack surface for the system

Marketing and Cost Analysis

- Please review the proposal document for detailed breakdown of costs and for market research

Item	Unit Cost	Quantity	Cost
NRF6943 (Thingy:91)	126.25	4 devices	505.00
USB A to Micro 5 pack	21.99	1	21.99
USB A to wall 5 pack	10.75	1	10.75
		Total	536.74 + s/h

Development Hours Per Engineer

Task	Hours
Weekly Meetings	32
Reports	3
Research	7.5
Presentation	2
Assembly and Coding	15.1
Vulnerability Testing	23.7
Total Hours	83.3
Labor Cost per Engineer	2707.25
Labor Cost for Team	13536.25

Table 6. Engineering Labor Cost Breakdown

Total Development Costs

Development Components	Cost
Parts	1325.75
Labor	13536.25
Fringe Benefits. % of Labor	4060.875
Subtotal	18922.875
Overhead, % of Material, labor, and fringe benefits	22707.45
Total Cost	41630.325

Table 7. Cost Summary

Leadership Roles

Jayla Williams - Webmaster, Networking Lead

Aaron Wasserman - Expo Coordinator, Hardware Security Testing Lead

James Thomas - Azure IoT Software Lead

Noah Dorfman - Documentation, Embedded Hardware Lead

Harry Kang - Implementation Testing, Embedded Software Lead

Attack Plan

- Hardware:
  - Wiretapping
  - Power Analysis Attack
  - VFI Glitching Attacks
  - Check for Radiation, Single Event Upset
- Software:
  - Wireless Attack (Wireshark)
  - Wired Attack
  - Fuzzing

Next Steps

- Deliver Proposal Presentation (Right now!)
- Revise project proposal and summary with feedback
- Continue escalating our purchasing requests
  - Need hardware in hand to keep moving forward
  - Already behind on our original schedule since purchasing wasn’t supported during the summer
- Finalize weekly group meeting time

Questions?