April 12, 2021
Secure Development

- Secure Development
- Case Study
- Paper Presentations
  - April 12th – Mathews
  - April 12th – Ryan
  - April 19th - Ross
- Assignments
  - Project
    - Presentation: Monday, Apr 26
  - Lab 2
    - Due Monday, Apr 12

Secure Development

- Development
  - Organizational
  - Coding Practices
- DevOps
  - What is it?
  - Why do we care?
- Products
  - Executables
  - Packages
  - Containers
  - Virtual Machines

Case Study

- This is a genericized version of the system I'm designing right now.
- For our purposes we'll call this a financial application:
  - Receives transactions (events) from multiple sources (think other financial institutions, ATMs, etc.)
  - Provides a data model of the transactions allowing AI/ML models to evaluate the state of the accounts and either:
  - Generate recommendations for actions (e.g. move funds around, reject ATM request) or
  - Automatically send events back to the various sources to actually make things happen

Architectural Requirements

- Data-in-motion encryption
- Data-at-rest encryption
- End point (external) encryption
- Role based access control
- 2 factor authentication for all HMI
- Minimize attach surface
- Minimize single points of failure

Architectural Components

- Persistence
  - Ephemeral – Redis
  - Distributed – Apache Cassandra
- Intra-system Communications
  - Asynchronous – MQTT (Mosquitto)
  - Synchronous – gRPC
- Inter-system Communications
  - Restful (JSON over HTTP) API

Platform

- Linux
- Kubernetes
- Containers