HostSecure Intrusion Detection System

Data-intensive security management platform

Sirajuddin Asjad, Bjørn-Ivar Bekkevold, Vetle Bodahl, Ståle Rudin

University of South-Eastern Norway
Campus Kongsberg

September 2021

USN

Agenda

USN

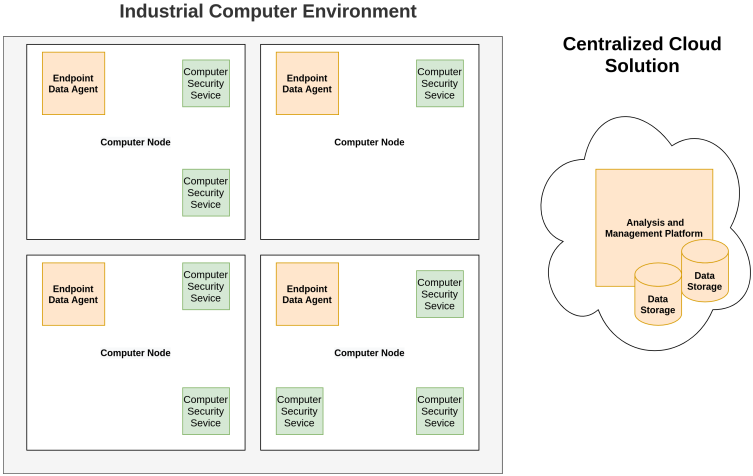
Introduction

- Industrial data-intensive systems require reliability and availability
- Risk of tampering with system operational data
- Critical errors, downtime, undefined behavior and fatal accidents
- Need for a controlled environment, strict access barriers

USN

Objective

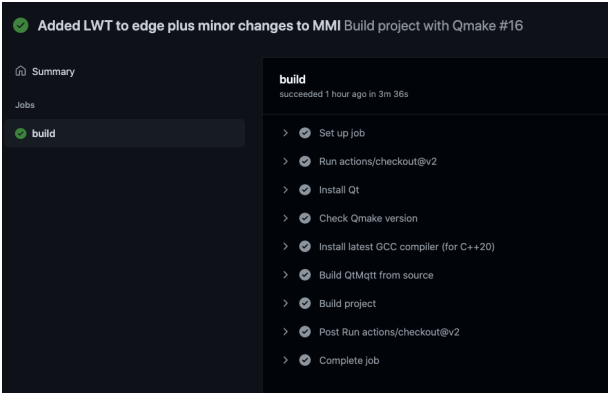
- HostSecure IDS - Data-intensive Security Management Platform
- Intrusion Detection and Prevention for Industrial Systems



Development process

- Week 1: Research and design
- Week 2: Implementation
- Week 3: Integration and documentation

- Continuous Integration, Continuous Deployment (CI/CD)



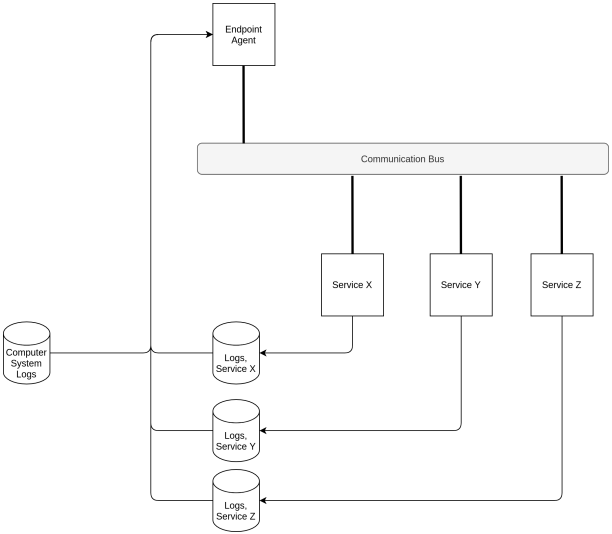
Technologies, tools and standards

- C++ and Qt Framework
- Qmake and QML
- D-Bus
- USBGuard
- MQTT
- SQLite
- Git

USN

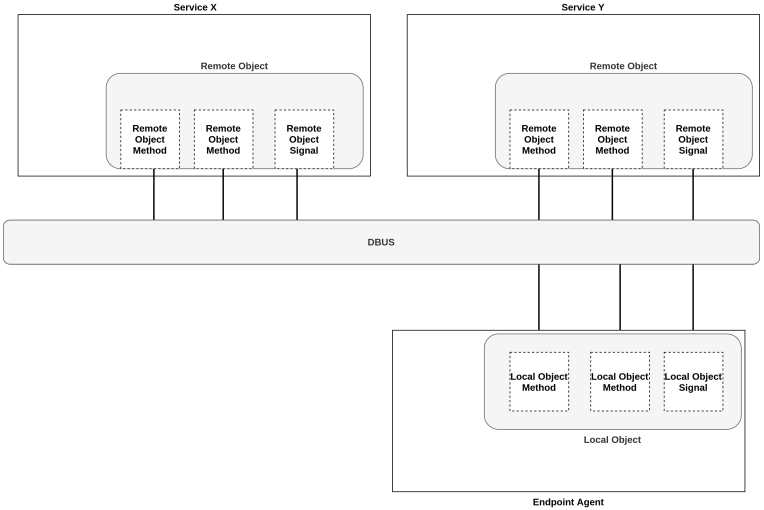
Endpoint Agent

- Data aggregator for security services
- Communicate to cloud or laterally to other endpoint nodes



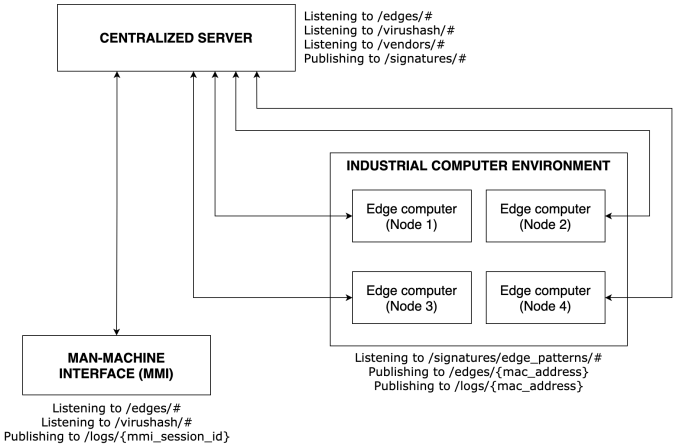
Implementation

- Qt D-BUS Message Bus
- USB Access Security Service



Connectivity and Network Communications

- MQTT messaging protocol
- Machine-to-machine (M2M) communication
- Publish-subscribe messaging architecture



Connectivity and Network Communications

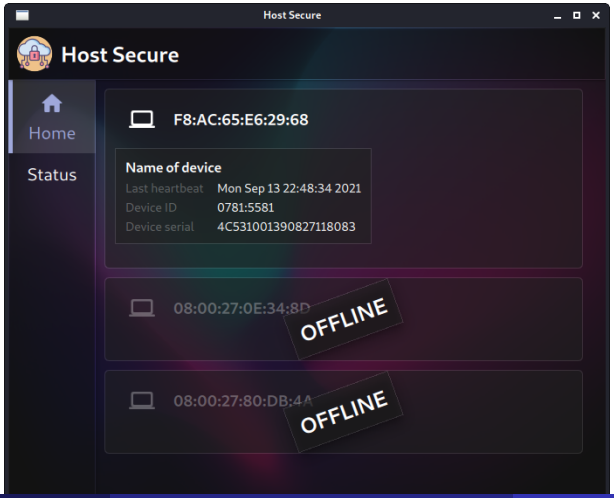
- Publish/subscribe to various topics
- Highly scalable messaging architecture

Type	**Topic**	**Description**
Repository	/virushash/#	Repository for all virus hashes
Repository	/products/#	Repository for all products
Repository	/edges/#	Repository for all edge computers
Action	/edges/{mac-address}/new-edge	Register a new edge computer
Action	/edges/{id}/heartbeat	Send a heartbeat signal to broker
...	...	...

USN

Man-machine Interface (MMI)

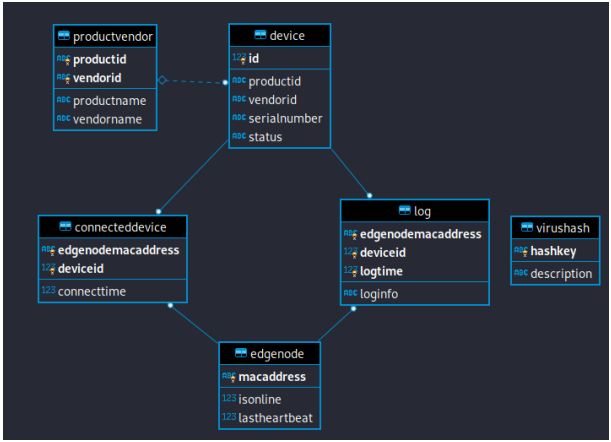
- Qt Framework, C++ and QML
- Security Management Platform
- Create custom rules
- Last Will and Testament



Man-machine Interface (MMI)

Database and Storage

- SQLite
- Qt Framework plugins/drivers
- DatabaseHandler API and DatabaseMqttClient



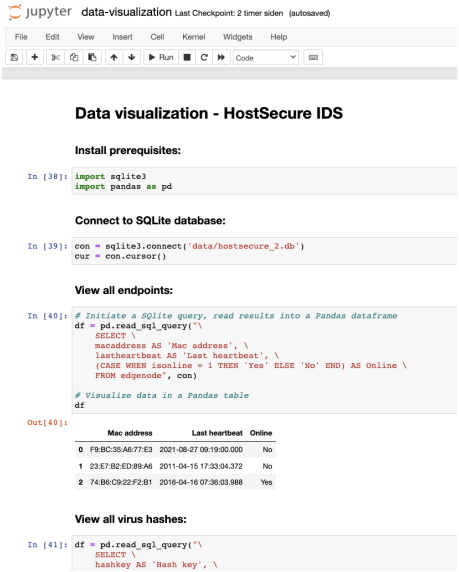
Data Management and Analysis

- Inspect and model the data collected from all endpoints
- Jupyter Notebook and Python

- Future directions and improvements are extensive
  - Machine learning to predict new anomaly patterns and signatures
  - Generate new rules based on human behaviour
  - Improve the intrusion detection model of our system

USN

- Preview:



jupyter data-visualization Last Checkpoint: 2 timer siden (autosaved)

File Edit View Insert Cell Kernel Widgets Help

Run Code

Data visualization - HostSecure IDS

Install prerequisites:

In [38]:
```
import sqlite3
import pandas as pd
```

Connect to SQLite database:

In [39]:
```
con = sqlite3.connect('data/hostsecure_2.db')
cur = con.cursor()
```

View all endpoints:

In [40]:
```
# Initiate a SQlite query, read results into a Pandas dataframe
df = pd.read_sql_query("\
    SELECT \
    macaddress AS 'Mac address', \
    lastheartbeat AS 'Last heartbeat', \
    (CASE WHEN isonline = 1 THEN 'Yes' ELSE 'No' END) AS Online \
    FROM edgenode", con)

# Visualize data in a Pandas table
df
```

Out[40]:

	Mac address	Last heartbeat	Online
0	F9:BC:35:A6:77:E3	2021-08-27 09:19:00.000	No
1	23:E7:B2:ED:89:A6	2011-04-15 17:33:04.372	No
2	74:B6:C9:22:F2:B1	2016-04-16 07:36:03.988	Yes

View all virus hashes:

In [41]:
```
df = pd.read_sql_query("\
    SELECT \
    hashkey AS 'Hash key', \
```

Demonstration

- Example Flow: USB Device :)