**CMPE 202 Class Project – Team 4**

**Softcore Inc Monitoring System Security Design and Implementation**



Prepared and Submitted by:

Sushant Dahal

Tyler Lennen

Rajesh Varathraj

Jonathan Lopez

Contents

[1. Overview 3](#_Toc39008190)

[Key Components: 3](#_Toc39008191)

[2. Security Baseline 4](#_Toc39008192)

[*Table 1: Initial Security Baseline* 4](#_Toc39008193)

[3. Threat Model 5](#_Toc39008194)

[*Figure 2: Security Baseline for Softcore Inc Monitoring System Security Design* 5](#_Toc39008195)

[4. Third Party software 5](#_Toc39008196)

[5. Static Analysis and parsing program 6](#_Toc39008197)

[6. Fuzzing Activity 6](#_Toc39008198)

[7. Questions: 7](#_Toc39008199)

# 1. Overview

The purpose of this project is to evaluate security posture of Softcorp inc. which develops and offers a monitoring system that consists of sensors that collect environmental data and appliances that process them. The sensors communicate with 2 services running on an appliance that consists of a Web Server and a Controller. The communication between the sensors and the services is TLS protected managed by services certificates that are bundled in SCF (Signed Certificates File) which are distributed to the sensors using a TFTP server. The sensors root of trust is based on the certificates contained in the SCF.

## Key Components:

The Softcorp Inc. monitoring system consists of the following key components:

* Sensors
  + Sensor External Console
* TFTP server
* Web Server
  + Sensor data collection servlet
  + User configuration servlet
  + Data reporting servlet
* Back end database
* Process Controller
* Web UI for user access

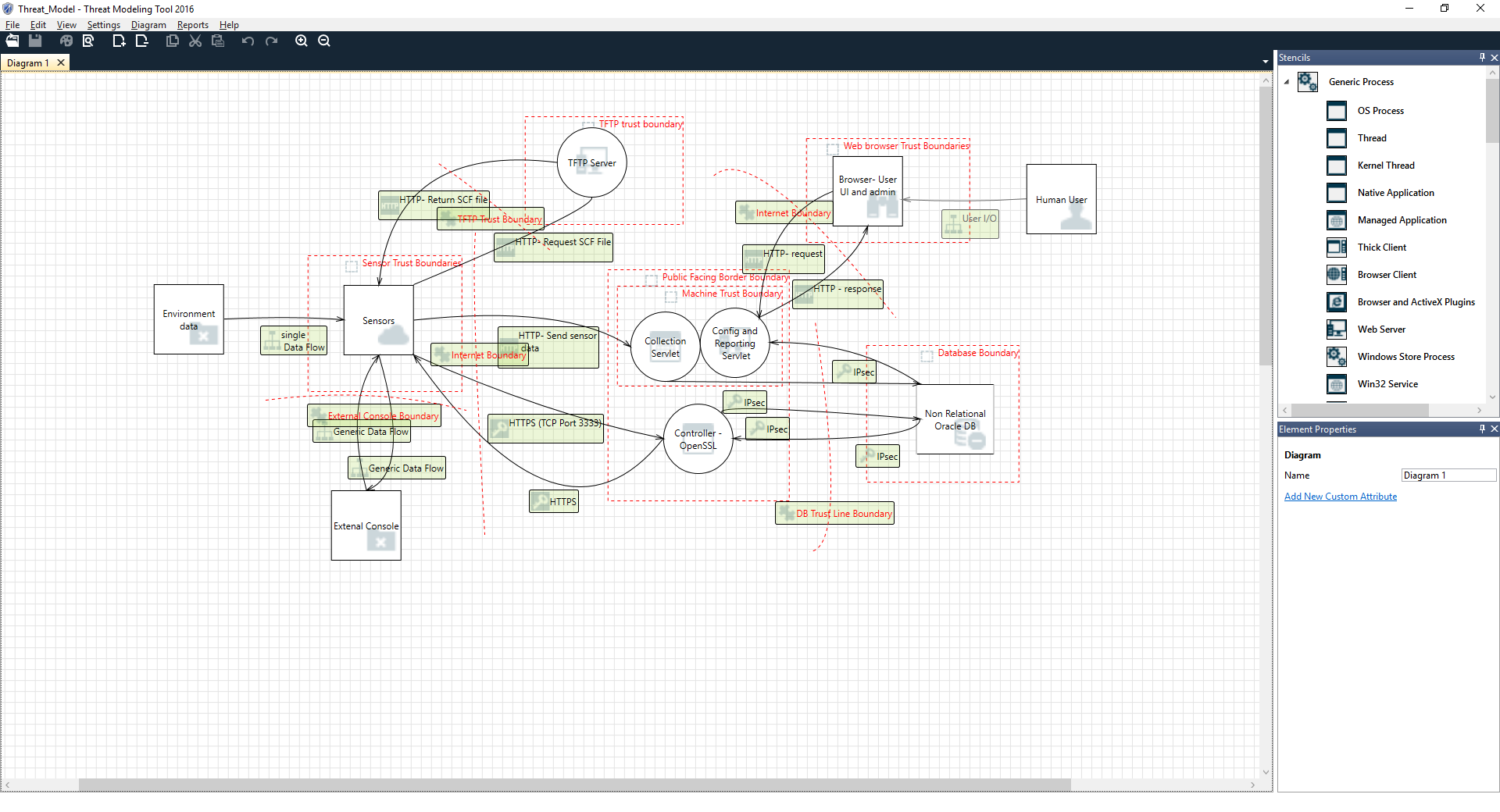
TODO: Add more definition/ content/ diagram if time

2. Security Baseline

### *Table 1: Initial Security Baseline*

# 3. Threat Model

The following threat model depicts the state of our monitoring application and define trust boundries associated with each services associated with collecting the data, storing and transmitting the data and user access and administration. The boundries for each instances where data is entered, transferred, stored and displayed is clearly outlined with necessary protocols in place.



### *Figure 2: Security Baseline for Softcore Inc Monitoring System Security Design*

# 4. Third Party software

The Software Inc. monitoring application uses the following 3rd party software and tools:

TODO: (Provide description of where used in the process/ application)

* Openssl 1.1.0
* Apache Tomcat 9.0.31
* Oracle 12.2.0.1
* BouncyCastle 1.63
* Bandit
* Github repository
* Fuzzing tool\*\*
* IDE used \*\*
* Any other tool we can think of \*\*

# 5. Static Analysis and parsing program

# 6. Fuzzing Activity

# 7. Questions:

1. Custom Sensor/Controller Protocol. You are tasked with designing the custom sensor/controller protocol. Explain in at least a half page the steps you would take to design a secure protocol.

The scope and use case of the monitoring system using sensors and backend interface such as controller is useless without the proper design and enforcement of security of the protocol. The key to the security of this protocol resides in trust between the two parties (sensors sending the data and controller receiving it). The sensor needs to ensure that it is sending/communicating data to a trusted party and the controller on the other side needs to ensure the sender is trusted and authorized entity as well. To resolve this type of issue, we could utilize Public Key Infrastructure (PKI) and utilize asymmetric keys such as RSA to establish secure connection

2. SDL Activities Can you think of any other SDL activities that would be needed for this project beside the ones covered in this project? Explain why you think they are needed.

3. SDL Metrics Meaningful security metrics allow organization to determine the effectiveness of its security controls. List the SDL metrics that you would capture in this project and explain how they would help bring maturity to your SDL process.

4. Changes to the Solution A. Softcorp decides to add more fields in the UI page of the configuration servlet. Which SDL activities would this trigger? B. Softcorp now plans to add a C++ process to its appliance. The process would use the sensors data in the Oracle database and send SNMP traps if some concerning trend is identified in the data set. Which SDL activities would be triggered in this case?