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

Table of Contents

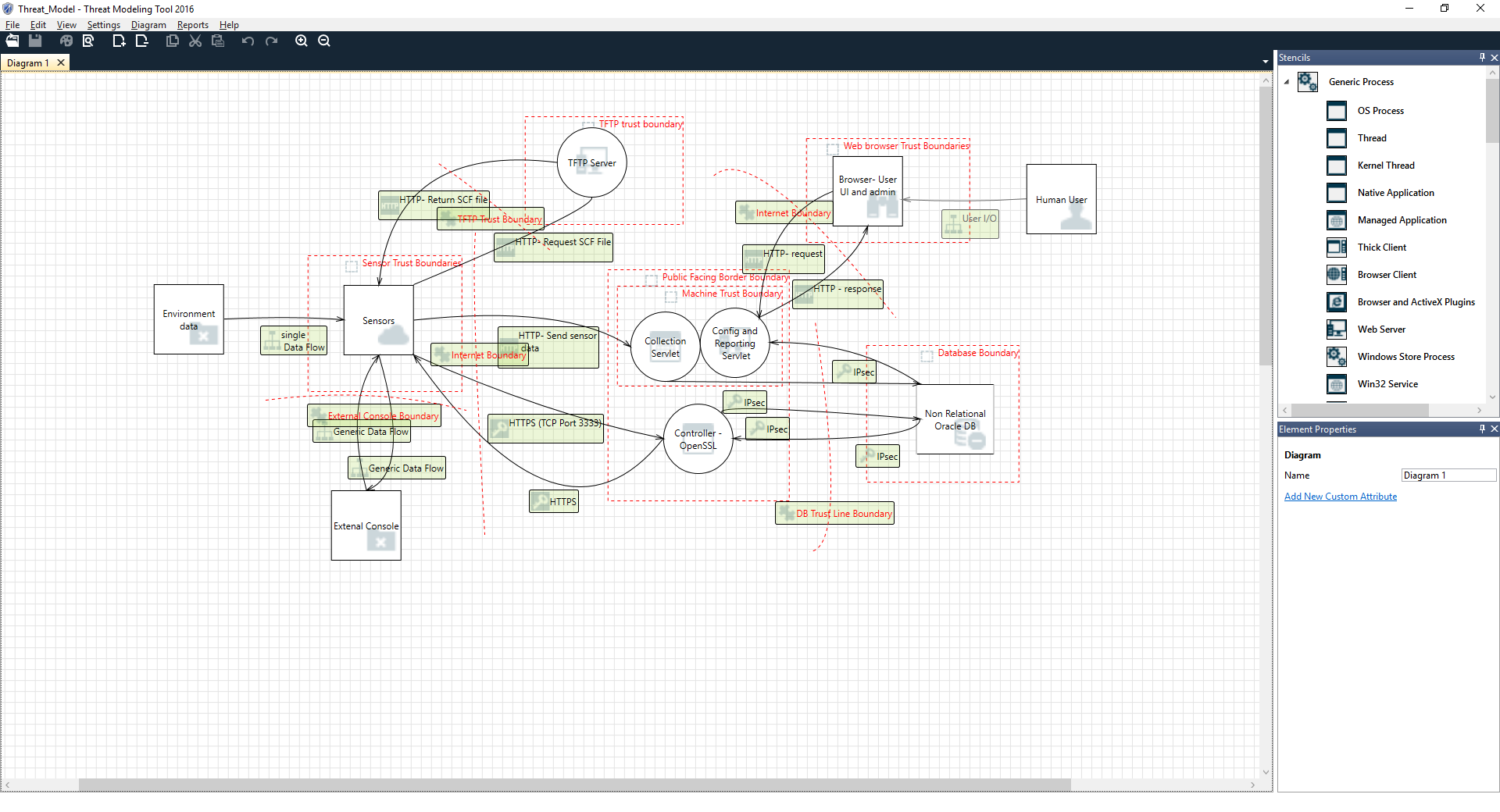
1. Scope

Softcorp inc. 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.

Security Baseline

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.



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.

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?