IoT Threat Modeling Framework Code Tutorial

This document serves as a tutorial in how to use the C++ code to implement the IoT threat modeling framework, maturity assessment, and sensitivity analysis.

Acquiring, Building, and Running the Code

The details for cloning, building, and running the code from a command line interface are located in the README.md file. To clone the Github repository where the code is located:

```
git clone https://github.com/siddhantjain/IOTRiskAssessmentFramework.git
```

The steps to build the code are:

```
cd IOTRiskAssessmentFramework
mkdir build
cd build
cmake ../Project
make
```

To run the code:

```
./iot_risk_assessment
```

Input Files

All of the files used as inputs to the framework are located in the *Data* directory. These files specify the parameters of the framework, the content of the framework, and the relationships between elements of the framework. Each file must be saved as a .csv file (NOT as a .xlsx file) in order to be read correctly into the framework.

parameters.csv

This file is used to specify the parameters of the framework. For sets of parameters that define a range of values, the left parameter must be smaller than the right parameter for framework calculations to be carried out correctly.

1) “Use Device Prevalency Scores” is a parameter that refers to whether or not device prevalency scores should be used instead of vulnerability prevalency scores. If set to 0, the vulnerability prevalency scores set in *vulnerabilities.csv* will be used. If set to 1, the device prevalency scores set in *devices.csv* along with the mapping *d2vMap.csv* will be used.
2) “Control Sensitivity Delta” is a parameter that refers to how much each control’s implementation score should be increased in the sensitivity analysis. The sensitivity analysis produces data describing how much further the residual risk would decrease if a particular control’s implementation score is increased by the “Control Sensitivity Delta” parameter. For example, a control with an implementation score of 3 would be increased to 3.5 in the sensitivity analysis if the “Control Sensitivity Delta” parameter is set to 0.5.
3) “Asset Likelihood Score Range” refers to two parameters that set the range of possible likelihood score values for each asset listed in *assets.csv*.
4) “Action Likelihood Score Range” refers to two parameters that set the range of possible likelihood score values for each action listed in *actions.csv*.
5) “Vulnerability Prevalency Score Range” refers to two parameters that set the range of possible prevalency score values for each vulnerability listed in *vulnerabilities.csv*.
6) “Impact Score Range” refers to two parameters that set the range of possible impact score values for each property listed in *properties.csv*.
7) “Device Prevalency Score Range” refers to two parameters that set the range of possible prevalency score values for each device listed in *devices.csv*.

8) “Control Implementation Score Range” refers to two parameters that set the range of possible implementation score values for each control listed in *controls.csv*.
9) “Control Effectiveness Score Range” refers to two parameters that set the range of possible effectiveness score values for each control listed in *controls.csv*.
10) “Risk Score Range” refers to two parameters that set the range of possible inherent and residual risk score values for the overall framework and for each risk domain listed in *risks.csv*.

assets.csv
This file specifies the likelihoods of specific threat actors having access to particular assets. Rows of this file can be added and deleted at will. The first column defines the ID number associated with a particular asset. This ID can be any number as long as it is unique from all other asset ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second, third, and fourth columns give the asset name, asset category, and asset subcategory as defined in the IoT attack taxonomy, respectively. To ensure correct framework calculations, assets within the same asset category must have the exact same entries in the asset category column, including capitalization and spacing. Asset likelihood scores are set in columns five and greater, where each column refers to a specific threat actor. Threat actor columns can be added and deleted at will. For a specific threat actor to not be considered in the framework, all asset likelihood scores in that threat actor’s column should be set to the minimum value of “Asset Likelihood Score Range” defined in *parameters.csv*. All asset likelihood scores must lie within this range to ensure correct framework calculations.

actions.csv
This file specifies the likelihoods of specific threat actors carrying out particular actions. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *a2aMap.csv*. The first column defines the ID number associated with a particular action. This ID can be any number as long as it is unique from all other action ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second, third, and fourth columns give the action name, action mechanism, and action category as defined in the IoT attack taxonomy, respectively. Action likelihood scores are set in columns five and greater, where each column refers to a specific threat actor. Threat actor columns can be added and deleted at will. For a specific threat actor to not be considered in the framework, all action likelihood scores in that threat actor’s column should be set to the minimum value of “Action Likelihood Score Range” defined in *parameters.csv*. All action likelihood scores must lie within this range to ensure correct framework calculations.

vulnerabilities.csv
This file specifies the prevalencies of particular vulnerabilities within the IoT environment. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *v2aMap.csv* and *v2pMap.csv*. The first column defines the ID number associated with a particular vulnerability. This ID can be any number as long as it is unique from all other vulnerability ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second, third, and fourth columns give the vulnerability name, attack layer, and vulnerability category as defined in the IoT attack taxonomy, respectively. Vulnerability prevalency scores are set in column five and must lie

within the “Vulnerability Prevalency Score Range” set in *parameters.csv* to ensure correct framework calculations. Vulnerability prevalency scores are only considered in the framework calculations if “Use Device Prevalency Scores” in *parameters.csv* is set to 0.

devices.csv

This file specifies the prevalencies of particular devices within the IoT environment. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *d2vMap.csv*. The first column defines the ID number associated with a particular device. This ID can be any number as long as it is unique from all other device ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second, third, and fourth columns describe the device name, device class, and device subclass, respectively. Device prevalency scores are set in column five and must lie within the “Device Prevalency Score Range” set in *parameters.csv* to ensure correct framework calculations. Device prevalency scores are only considered in the framework calculations if “Use Device Prevalency Scores” in *parameters.csv* is set to 1.

properties.csv

This file specifies the impact of particular properties being compromised within the client’s industry. Rows of this file can be added and deleted at will. The first column defines the ID number associated with a particular property. This ID can be any number as long as it is unique from all other property ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second, third, and fourth columns give the property name, high level classification, and low level classification as defined in the IoT attack taxonomy, respectively. Impact scores are set in column five and must lie within the “Impact Score Range” set in *parameters.csv* to ensure correct framework calculations.

controls.csv

This file specifies how well-implemented and effective particular controls are within the IoT environment. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *c2vMap.csv*. The first column defines the ID number associated with a particular control. This ID can be any number as long as it is unique from all other control ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second column is comprised of the control names. Control implementation scores and control effectiveness scores are set in columns three and four, respectively, and must lie within the “Control Implementation Score Range” and the “Control Effectiveness Score Range” set in *parameters.csv* to ensure correct framework calculations.

risks.csv

This file specifies particular risk domains within an organization. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *r2vMap.csv* and *r2cMap.csv*. The first column defines the ID number associated with a particular risk domain. This ID can be any number as long as it is unique from all other risk domain ID numbers. The uniqueness of each ID number is necessary in order for framework calculations to be carried out properly. The second column is comprised of the risk domain names.

a2aMap.csv
This file specifies the relationship between an attacker's actions and an attacker's assets. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *actions.csv*. The first column defines the ID number associated with a particular action and must match one of the action ID numbers in *actions.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the action name and must match the correct action ID number as defined in *actions.csv* in order for framework calculations to be carried out properly. The asset ID numbers associated with carrying out a particular action are set in columns three and greater. Each asset ID number must match one of the asset ID numbers in *assets.csv* in order for framework calculations to be carried out properly.

v2aMap.csv
This file specifies the relationship between exploited vulnerabilities and an attacker's actions. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *vulnerabilities.csv*. The first column defines the ID number associated with a particular vulnerability and must match one of the vulnerability ID numbers in *vulnerabilities.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the vulnerability name and must match the correct vulnerability ID number as defined in *vulnerabilities.csv* in order for framework calculations to be carried out properly. The action ID numbers associated with exploiting a particular vulnerability are set in columns three and greater. Each action ID number must match one of the action ID numbers in *actions.csv* in order for framework calculations to be carried out properly.

d2vMap.csv
This file specifies the relationship between devices and exploited vulnerabilities. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *devices.csv*. The first column defines the ID number associated with a particular device and must match one of the device ID numbers in *devices.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the device name and must match the correct device ID number as defined in *devices.csv* in order for framework calculations to be carried out properly. The vulnerability ID numbers associated with a particular device are set in columns three and greater. Each vulnerability ID number must match one of the vulnerability ID numbers in *vulnerabilities.csv* in order for framework calculations to be carried out properly. The relationships defined in this file are only considered in the framework calculations if "Use Device Prevalency Scores" in *parameters.csv* is set to 1.

v2pMap.csv
This file specifies the relationship between exploited vulnerabilities and compromised properties. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *vulnerabilities.csv*. The first column defines the ID number associated with a particular vulnerability and must match one of the vulnerability ID numbers in *vulnerabilities.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the vulnerability name and must match the correct vulnerability ID number as defined in *vulnerabilities.csv* in order for framework calculations to be carried out properly. The property ID numbers associated with a particular vulnerability are set in columns three and greater. Each

property ID number must match one of the property ID numbers in *properties.csv* in order for framework calculations to be carried out properly.

c2vMap.csv

This file specifies the relationship between controls and exploited vulnerabilities. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *controls.csv*. The first column defines the ID number associated with a particular control and must match one of the control ID numbers in *controls.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the control name and must match the correct control ID number as defined in *controls.csv* in order for framework calculations to be carried out properly. The vulnerability ID numbers associated with a particular control are set in columns three and greater. Each vulnerability ID number must match one of the vulnerability ID numbers in *vulnerabilities.csv* in order for framework calculations to be carried out properly.

r2vMap.csv

This file specifies the relationship between risk domains and exploited vulnerabilities. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *risks.csv*. The first column defines the ID number associated with a particular risk domain and must match one of the risk domain ID numbers in *risks.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the risk domain name and must match the correct risk domain ID number as defined in *risks.csv* in order for framework calculations to be carried out properly. The vulnerability ID numbers associated with a particular risk domain are set in columns three and greater. Each vulnerability ID number must match one of the vulnerability ID numbers in *vulnerabilities.csv* in order for framework calculations to be carried out properly.

r2cMap.csv

This file specifies the relationship between risk domains and controls. Rows of this file can be added and deleted at will but must be mirrored by adding and deleting rows in *risks.csv*. The first column defines the ID number associated with a particular risk domain and must match one of the risk domain ID numbers in *risks.csv* in order for framework calculations to be carried out properly. Similarly, the second column lists the risk domain name and must match the correct risk domain ID number as defined in *risks.csv* in order for framework calculations to be carried out properly. The control ID numbers associated with a particular risk domain are set in columns three and greater. Each control ID number must match one of the control ID numbers in *controls.csv* in order for framework calculations to be carried out properly.

Output Files

All of the files produced by the framework are located in the *Results* directory. These files contain information about the inherent risk, residual risk, control sensitivities, and vulnerability likelihood and impact of the IoT environment.

CalculatedRisksFullFramework.csv

This file simply lists the overall inherent risk and the overall residual risk for the entire IoT environment. The risk scores provided will lie within the “Risk Score Range” set in *parameters.csv*.

CalculatedRisksPerDomain.csv
This file specifies the inherent risk and the residual risk for each of the risk domains defined in *risks.csv*. The first column lists the name of each risk domain, and the second and third columns list the associated inherent and residual risks, respectively. The risk scores provided will lie within the "Risk Score Range" set in *parameters.csv*.

VulnerabilitiesLikelihoodImpact.csv
This file specifies the likelihood and impact associated with each of the applicable vulnerabilities. The first column lists the name of each vulnerability, and the second and third columns list the likelihood and impact scores associated with the vulnerability, respectively.

ControlSensitivities.csv
This file specifies the overall residual risk reduction, implementation score, and effectiveness score associated with each of the applicable controls. The first column lists the name of each control, and the second column lists how much further the overall residual risk would be reduced if the control implementation score were increased by the "Control Sensitivity Delta" parameter set in *parameters.csv*. The third and fourth columns list the control implementation score and control effectiveness score as defined in *controls.csv*, respectively.

"RISK DOMAIN" Control Sensitivities.csv
This file specifies the overall residual risk reduction, implementation score, and effectiveness score associated with each of the applicable controls in the risk domain specified in the name of this file. The first column lists the name of each control, and the second column lists how much further the overall residual risk would be reduced if the control implementation score were increased by the "Control Sensitivity Delta" parameter set in *parameters.csv*. The third and fourth columns list the control implementation score and control effectiveness score as defined in *controls.csv*, respectively.