Purpose

This document serves as a high-level description regarding the calculations involved in the IoT threat modeling framework, maturity assessment, and sensitivity analysis.

IoT Attack Taxonomy Overview

The IoT attack taxonomy is comprised of a comprehensive list of atomic attacks where any IoT incident is composed of a series of atomic attacks. Any atomic attack can be broken down into four parts, each of which is associated with a particular dimension of the IoT attack taxonomy: an attacker with a specific set of 1) assets carries out a particular 2) action to exploit a specific 3) vulnerability, compromising a particular set of 4) properties. Because the threat modeling framework calculations are built around this IoT attack taxonomy, the taxonomy's structure must be understood before the calculation methodology. Of interest is the fact that the first dimension (attacker assets) is composed of six sub-dimensions. Consequently, a particular attacker asset is a vector composed of six elements, one element from each sub-dimension. Each of the other dimensions (attacker action, exploited vulnerability, and compromised property) do not have any sub-dimensions.

IoT Threat Modeling Framework Overview

The threat modeling framework is concerned with calculating the inherent and residual risks associated with particular risk domains. The inherent risk is calculated first, and based on the results of the maturity assessment, that inherent risk is reduced by a certain amount to yield the residual risk. Each risk domain is associated with a specific set of vulnerabilities. The inherent risk associated with each individual vulnerability is calculated first by multiplying together the likelihood and impact of that vulnerability being exploited. The inherent risk for a particular risk domain is then calculated by carrying out a weighted addition of the inherent risks associated with each individual vulnerability within that domain. Each weight corresponds to the prevalency of the vulnerability within the IoT environment being assessed. If desired, the prevalencies of each vulnerability can be determined by the prevalencies of the associated devices within the IoT environment.

Inherent Risk Calculation

As described in the previous section, the inherent risk associated with any particular vulnerability is equal to the likelihood of that vulnerability being exploited times the impact associated with exploiting that vulnerability.

Likelihood

To calculate the likelihood of exploiting a particular vulnerability, we consider the threat actor and all the possible combinations of attacker assets and actions that may be used to exploit that particular vulnerability. A likelihood is assigned to each asset and each action given a specific threat actor. For example, the likelihood of an attacker possessing an IoT botnet (asset) given that the attacker is a nation state (threat actor) would be assigned to the element in the asset dimension of the IoT taxonomy corresponding to IoT botnets. Continuing the example, the likelihood of an attacker carrying out a replay attack (action) given that the attacker is a nation state (threat actor) would be assigned to the element in the action dimension of the IoT taxonomy corresponding to replay attacks.

Assumptions

In order to calculate the likelihood of exploiting a particular vulnerability given a specific set of threat actors, the joint probability of an attacker possessing a particular asset vector and carrying out a specific action must be calculated. In addition, the probability of an attacker using any asset vector/action pair to exploit a particular vulnerability must be calculated. In order to carry out these calculations, a few simplifying assumptions have to be made:

1) It is assumed that the sub-dimensions of dimension one (attacker assets) are independent from one another. That is, information about the likelihood of one sub-dimension does not have any effect on the likelihood of other sub-dimensions. For example, it is assumed that information about the likelihood of the attacker's location does not have any effect on the likelihood of the attacker's equipment.

2) It is assumed that given a particular asset vector/action pair, the asset vector is independent from the action. That is, given a particular asset vector/action pair, information about the likelihood of the asset vector does not have any effect on the likelihood of the action. For example, it is assumed that information about the likelihood of an attacker with [publicly available information, remote Internet access, a commercial PC, specific niche skills, a short time requirement, and no attack persistence requirements] does not have any effect on the likelihood of the attacker carrying out a replay attack given the knowledge that this asset vector can be used to carry out a replay attack.

3) It is assumed that the set of asset vector/action pairs that compromise a particular vulnerability are independent from one another. That is, information about the likelihood of one asset vector/action pair that exploits a particular vulnerability does not have any effect on the likelihood of another asset vector/action pair that exploits the same vulnerability.

4) It is assumed that the threat actors are independent from one another. That is, information about the likelihood of one threat actor does not have any effect on the likelihood of other threat actors. For example, it is assumed that information about the likelihood of an attacker being financially motivated does not have any effect on the likelihood of an attacker being a hacktivist.

Calculation

By making the assumptions listed above, we can use principles for joint probabilities of independent events and the inclusion-exclusion principle to calculate the probability of an attacker exploiting a particular vulnerability using any possible asset vector/action pair given that the attacker is one of a specific set of threat actors. This calculation yields the likelihood of a particular vulnerability being exploited.

Impact

To calculate the impact associated with exploiting a particular vulnerability, we consider all the properties that are compromised when that particular vulnerability is exploited. Each property has an impact score assigned to it representing the impact of compromising that particular property. For example, the impact of causing human harm or injury (property) would be assigned to the element in the property dimension of the IoT taxonomy corresponding to human injury. The impact associated with exploiting a particular vulnerability is calculated by adding together the impact scores for each property that would be compromised if that vulnerability were exploited.

Maturity Assessment Overview

The maturity assessment is concerned with gathering information about how well a client has implemented specific controls to mitigate risk. By interacting with the client, an implementation percentage for each control is obtained that represents how well the client has implemented that particular control. In addition, a measure of effectiveness for each control is obtained that represents how effective that particular control is in mitigating risk. A control mitigation percentage is calculated for each control by multiplying the implementation percentage by the effectiveness percentage. Each risk domain is associated with a particular set of controls, implying that high mitigation percentages for the controls in a particular domain will lower the inherent risk in that domain. Similarly, each vulnerability is associated with a particular set of controls, implying that high mitigation percentages for the controls associated with a particular vulnerability will lower the inherent risk associated with that vulnerability. A mitigation percentage for a particular vulnerability is obtained by calculating the union of the control mitigation percentages associated with that vulnerability.

Residual Risk Calculation

Once the inherent risk associated with each vulnerability has been calculated and the maturity assessment has obtained mitigation percentages for each vulnerability, the residual risk can be calculated. The residual risk associated with a particular vulnerability is obtained by multiplying the inherent risk associated with the vulnerability by (100% - the mitigation percentage associated with the vulnerability). This value in parentheses reduces the inherent risk by a factor proportional to how well the client has implemented effective controls. The residual risk for a particular risk domain is then calculated by carrying out a weighted addition of the residual risks associated with each individual vulnerability within that domain. Each weight corresponds to the prevalency of the vulnerability within the IoT environment being assessed. If desired, the prevalencies of each vulnerability can be determined by the prevalencies of the associated devices within the IoT environment.

Sensitivity Analysis

To understand which controls are the most important in reducing inherent risk, a one-at-a-time sensitivity analysis is conducted. This sensitivity analysis increases the control implementation percentage for a control by a small amount, calculates the residual risk, records the reduction in residual risk, returns the control implementation percentage back to its normal value, and repeats this process for each control. Once this process is complete, the controls are rank-ordered according to which controls reduce inherent risk the most. This rank-ordered list is provided for controls in the framework as a whole as well as controls in individual risk domains.

Summary of Process

1) Assign likelihood values to each asset representing the probability of an attacker possessing the asset given that the attacker is a specific threat actor. Repeat this process for each type of threat actor.
2) Assign likelihood values to each action representing the probability of an attacker carrying out the action given that the attacker is a specific threat actor. Repeat this process for each type of threat actor.

3) Assign prevalency scores to each vulnerability corresponding to how prevalent the vulnerability is in the IoT environment being assessed. If desired, prevalency scores can be assigned to each device within the IoT environment instead.
4) Assign impact scores to each property proportional to the impact that would occur if the property were compromised.
5) Assign control implementation scores to each control proportional to how well the client has implemented the control. In addition, assign control effectiveness scores to each control proportional to how effective that control is in mitigating risk.
6) Run the C++ code which:
- calculates the overall inherent and residual risk for the IoT environment
- calculates the inherent and residual risk for each risk domain
- provides a rank-ordered list of the individual controls that are most important in reducing overall inherent risk
- for each risk domain provides a rank-ordered list of the individual controls in that risk domain that are most important in reducing overall inherent risk
- provides a list of each applicable vulnerability along with its likelihood and impact score