Security Risk Calculation

In this section, we describe the security metrics and their calculations to assess the security of smart home systems.

Security Model Definition

We define the extended HARM model. The extended HARM has three layers: upper, middle, and lower layers. The upper layer model (an AG) represents the sub-network connectivity of smart home network and the attackers' entry points; the middle layer model (an AG) captures the network reachability information and the attackers' entry points, and the lower layer model (a set of ATs) depicts the vulnerability information of each node (if the node has vulnerabilities) and an attack goal achieved by the attackers by exploiting one or multiple vulnerabilities.

Security Metrics

Security of a smart home system can be assessed by different security parameters that are of prime concern for security executives and decision-makers of an organization. For example, the information regarding likelihood, risk, or impact of exploiting a vulnerability helps the security staff in making appropriate action plan against an attack or security violation. Moreover, smart home systems are following a strict chain of command to execute critical operations at a tactical edge; therefore, the security-related-information should be communicated to a concerned authority. Considering the requirements for securing smart home systems, we have defined pertinent security metrics that provide a holistic picture of the security situation of smart home networks. The security metrics include Attack Success Probability (ASP), Attack Impact (AI), Attack Risk (AR), and Common Vulnerability Scoring System (CVSS) base score. To disseminate the information to a corresponding authority in a chain of command, we have calculated the security metrics for four levels (i.e., vulnerability level, node level, path level, and network level) in a smart home network so that the concerned authority can reciprocate accordingly. Table 1 enlists the security metrics and their definitions in all four levels.

Table 1. Definitions of security metrics at different levels

Security Metrics	Definitions
Vulnerability Level	
-Attack Success Probability	Likelihood of an attack or successful exploitation of a vulnerability (range: [0, 1])
- Attack Impact	Potential loss caused by an attack that successfully exploits a vulnerability (range: [0,10])
- Attack Risk	Potential of a vulnerability to get exploited successfully by an attack (range: [0, 10])
- CVSS Base Score	Severity level of a vulnerability to get exploited by an attack (range: [0, 10])
Node Level	
-Attack Success Probability	Likelihood of an attack or successful exploitation of a node
- Attack Impact	Potential loss caused by an attack that successfully exploits a node
- Attack Risk	Potential of a node to get exploited successfully by an attack
- CVSS Base Score	Severity of a node to get exploited by an attack
Attack Path Level	
-Attack Success Probability	Likelihood of an attack or successful exploitation of a target via an attack path
- Attack Impact	Potential loss caused by an attack that successfully exploits a target via an attack path
- Attack Risk	Potential of a target to get exploited successfully by an attack via an attack path
- CVSS Base Score	Severity of a target to get exploited by an attack via an attack path
Network Level	
- Attack Success Probability	Likelihood of an attack or successful exploitation of a target via all potential attack paths
- Attack Impact	Potential loss caused by an attack that successfully exploits a target via all attack paths
	Potential of a target to get exploited successfully by an attack via all potential attack paths

- Attack Risk **- CVSS Base Score**	Severity of a target to get exploited by an attack via all potential attack paths

The values of some metrics in higher levels are calculated from lower levels. For example, values in the network level are calculated from values in the attack path, node, and vulnerability levels. The value of the attack success probability is in the range of zero to one, while the value of CVSS base score, attack impact and attack risk ranges from zero to ten. Take the attack success probability as an example. The larger the value is within the range, the higher the probability is for an attacker to exploit the vulnerability. By introducing the value range, we use standardized metric values as it is not easy to get the exact values of the security metrics from real-world scenarios. The CVSS uses a similar way to assess the severity of vulnerabilities.

Security Metrics Calculation

Vulnerabilities of a smart home asset are combined using logical *AND* and *OR* gates. If an attacker needs to exploit all the vulnerabilities of a smart home system to overcome the smart home system, all vulnerabilities are connected by *AND* gate. However, if an attacker needs to exploit only one vulnerability, then, the vulnerabilities are linked with each other with *OR* gate. Calculations of security metrices are different for *AND* and *OR* gates. In the following, we describe the calculations for each security metric to assess the security of smart home systems at each level.

Attack Success Probability

Attack success probability is used to measure the probability of an attacker to successfully achieve an attack goal. The attack success probability is equal to exploitability value divided by 10 (Eq. (1)). At the vulnerability level, the exploitability score is retrieved from the NVD database for all vulnerabilities of a smart home system, and then the metric value is calculated by Eq. (1) for each vulnerability. At the node level, the attack success probability depends on the relationship of vulnerabilities among each other, which is calculated by Eq. (2) according to *AND* and *OR* logics. At the path level, Eq. (3) presents the metric value that is the product of all probabilities concerning to the nodes present in an attack path. At the network level, the metric is the probability that is product of all potential attack paths' probabilities.

$$Attack\ Success\ Probability = Exploitability\ Score\ \div 10 \quad (1)$$

$$Attack\ Success\ Probability = \begin{cases} \prod_{v=1}^{n} ASP & (AND\ gate) \\ 1 - \prod_{v=1}^{n} ASP & (OR\ gate) \end{cases} \quad (2)$$

$$Attack\ Success\ Probability = \prod_{node=1}^{n} ASP \quad (3)$$

Attack Impact

Attack impact is used to compute the potential loss caused by an attacker to successfully achieve an attack goal. The potential loss is the loss of confidentiality, integrity, and availability. At the vulnerability level, the impact value is extracted from the NVD database. At the node level, the metric value is a sum of all vulnerabilities

present in a smart home node for *AND* relationship whereas maximum attack impact value is taken in case of *OR* relationship among vulnerabilities, as calculated by Eq. (4). At the path level, the metric value is a sum of the impact values of all smart home nodes present in an attack path (Eq. (5)). In the network level, the metric is the maximum loss caused by an attacker to compromise the target among all potential paths. The network-level value is given by Eq. (6).

$$Attack\ Impact = \begin{cases} \sum_{v=1}^{n} AI & (AND\ gate) \\ \max(AI) & (OR\ gate) \end{cases} \quad (4)$$

$$Attack\ Impact = \sum_{node=1}^{n} AI \quad (5)$$

$$Attack\ Impact = \max(AI) \quad (6)$$

Attack Risk

Attack risk refers to the potential of a vulnerability to get exploited by an attack vector. At the vulnerability level, the risk value is calculated by taking the product of attack success probability metric and attack impact metric (Eq. 7). At the node, attack path and network levels, the risk metric value is calculated in the same manner as attack impact metric, which is given by Eq. (8), Eq. (9), and Eq. (10) respectively.

$$Attack\ Risk = Attack\ Success\ Probability * Attack\ Impact \quad (7)$$

$$Attack\ Risk = \begin{cases} \sum_{v=1}^{n} AR & (AND\ gate) \\ \max(AR) & (OR\ gate) \end{cases} \quad (8)$$

$$Attack\ Risk = \sum_{node=1}^{n} AR \quad (9)$$

$$Attack\ Risk = \max(AR) \quad (10)$$

CVSS Base Score

The Common Vulnerability Scoring System (CVSS) base score reflects the severity of a vulnerability according to its impact on confidentiality, integrity, and availability of a system. Fig. 2 presents the required calculations to evaluate the CVSS base score metric. The corresponding values (e.g., access vector, access complexity) to calculate the CVSS base score are taken from the NVD database for a vulnerability. Similar to the attack risk metric, the CVSS base score metric is also calculated same as attack impact metric for the node, path, and network levels, as presented by Eq. (12), Eq. (13), and Eq. (14), respectively.

CVSS Base Score = round_to_1_decimal(((0.6*Impact) +(0.4*Exploitability)-1.5) *f(Impact))

Impact = 10.41*(1- (1- ConfImpact) *(1- IntegImpact) *(1- AvailImpact))

Exploitability = 20 * Access Vector * Access Complexity * Authentication

f(impact) = 0 if Impact= 0, 1.176 otherwise

Fig. 2. Calculations to evaluate CVSS base score

$$CVSS\ base\ score = \begin{cases} \sum_{v=1}^{n} CVSS\ base\ score & (AND\ gate) \\ \max(CVSS\ base\ score) & (OR\ gate) \end{cases} \quad (12)$$

$$CVSS\ base\ score = \sum_{node=1}^{n} CVSS\ Base\ Score \quad (13)$$

$$CVSS\ Base\ Score = \max(CVSS\ Base\ Score) \quad (14)$$