A Stochastic Modeling of Coordinated Internal and External Attacks

Xiaohu Li and Shouhuai Xu
Department of Computer Science, University of Texas at San Antonio
{xli,shxu}@cs.utsa.edu
September 19, 2007

Abstract

Traditional security analyses are often geared towards cryptographic primitives or protocols. Although such analyses are absolutely necessary, they cannot address a defender’s need for insight into which aspects of a networked system have a significant impact on its security, and how to tune its configurations or parameters so as to improve security, against coordinated internal and external attacks. Such insights may only be offered by appropriate theoretic security models, which have long been sought but not much progress has been made. This paper reports our first step towards modeling coordinated internal and external attacks against networked systems.

Keywords: security in digital systems, analytic security models, internal attacks, external attacks, coordinated attacks.

1 Introduction

Traditional security analyses are typically geared towards cryptographic primitives (e.g., how one should pad a message before encrypting it using the RSA function) or protocols (e.g., how a password-based authentication protocol should operate so that it is immune to the off-line dictionary attack). Although such analyses are absolutely necessary, they do not provide much insight into answering an equally important, if not more important, question: which aspects of a networked system having a significant impact on its security, and how to tune system configurations or parameters so as to improve security, against coordinated internal and external attacks. In such attacks, there is an external attacker that can compromise legitimate system components or participants, which then become internal attackers. The internal attackers can report to the external attacker information such as “which other components have recently been compromised.” In the fully sophisticated scenarios, the internal attackers may receive from the external attacker orders such as “which components should be attacked next.” That is, the external attacker may be fully coordinating the attacks, and the internal attackers may exchange information with each other.

1.1 Our Contributions

This paper makes a first step towards understanding coordinated internal and external attacks, by considering a semi-sophisticated scenario, where the external attacker always gets updated about the system global state information, but the internal attackers do not. This can be fulfilled by, for example, letting the internal attackers report to the external attacker. However, the external attacker does not necessarily send updated global state information back to the internal attackers, and the internal attackers do not necessarily exchange information with each other. While such semi-sophisticated attacks may not be as powerful as fully sophisticated attacks, they are still realistic because communications from the external attacker to the internal attackers may expose the external attacker (in contrast, receiving reports from the internal attackers may not expose the external attacker at all).

The framework of our modeling approach is the following. First, a vulnerability graph is used to abstract a networked system, where a vertex represents a vulnerability, and an arc or edge captures the relation that the exploitation of one vulnerability could lead to the exploitation of the other. Such graphs can be obtained, for example, by combining the output of vulnerability scanners and the systems configurations. (There have been some works on generating vulnerability-like graphs, such as [16, 9, 3, 6].)
Second, given a vulnerability graph, attacks can be modeled as some appropriate stochastic processes. Specifically, we use a discrete non-homogeneous Poisson process to model coordinated internal and external attacks. As we will see, our model offers: (i) A characterization of the attack behavior, which suggests that coordinated internal and external attacks gain power as time goes by. (2) A characterization of the effect of attack strategies, which suggests (from the attacker’s perspective) “which attack strategy is more effective.” (3) A characterization of the effect of immunization strategies, which suggests (from the defender’s perspective) “which immunization strategy is more effective.”

Outline: In Section 2 we explore our model. In Section 3 we conduct some analyses to characterize some aspects of the attack process. In Section 4 we discuss related prior work. We conclude this paper in Section 5.

2 Model

A vulnerability graph is finite graph $G = (V,E)$, where $V$ is the vertex or node set with $|V| > 0$, and $E$ is the edge set with $E \neq \emptyset$. We assume that the edges are undirected and that the graph is connected. (The extension to directed graphs is straightforward.) At system initialization, there is an external attacker, which does not belong to $V$ and is connected to each of the nodes in $V$ via edges that do not belong to $E$. This is to capture that the external attacker may launch attacks against any nodes belonging to $V$. As time goes by, some nodes get compromised, and thus become internal attackers that will not be attacked by the external attacker any further. Each of the internal attackers only knows the identities of its neighbors it has compromised, and only launches attacks against the other neighbors (if any).

We consider a discrete time model with time $t = 0,1,2,\ldots$. We assume that attacks occur in a sequential order. At any point in time, a node is either secure, compromised, or removed. We assume that at time $t = 0$ all nodes are secure. Once a node becomes compromised, it is under complete control of the attacker, and thus may exhibit Byzantine behavior. A compromised node may become removed, which is an absorbing state meaning that such a node will remain removed. As such, our model is in spirit similar to, but actually very different from (see Section 4 for details), the traditional epidemic susceptible-infected-removed (SIR) models.

Denote by $C_t$ the set of nodes that became compromised at or before time $t$. We denote by $N(t)$ the number of nodes that became compromised at or before time $t$, and by $M(t)$ the number of nodes that have become removed by time $t$. Note that $|C_t| = N(t)$, and that $N(t) - M(t)$ is the number of compromised nodes that have not become removed. Given a vulnerability graph $G = (V,E)$, the function $\deg(v) \in V$ returns the degree of node $v$ in $G$, and the function $\text{neighbor}(v) \in V$ returns the set of $v$’s neighboring nodes namely $\{v' : (v, v') \in E\}$. Denote by $T_n$ the time at which the $n$th node changes state from secure to compromised (i.e., the $n$th incident occurs), where $1 \leq n \leq |V|$. The function $\text{node}(T_n)$ returns the identity of the node that became compromised at time $T_n$ (i.e., the $n$th compromised node). For any sequence of compromised nodes $\text{node}(T_1), \ldots, \text{node}(T_{|V|})$, the degree of $\text{node}(T_i)$ follows distribution $D_i$, which is independently and identically distributed as the degree distribution $D$ of $G = (V,E)$, where $1 \leq i \leq |V|$.

For random variables $R_1$ and $R_2$, we say $R_1$ is stochastically larger (or faster) than $R_2$, denoted by $R_1 \succeq_{st} R_2$, if $\Pr[R_1 > k] \geq \Pr[R_2 > k]$ for any $k$ (cf. Shaked [17]). Notice that $\succeq_{st}$ to random variables is what $\geq$ to real numbers.

2.1 Characterizing $T_n$

We aim to characterize $T_n$, the distribution of the time at which the $n$th incident occurs, where $1 \leq n \leq |V|$. For a technical reason, we use a discrete exponential distribution, namely geometric distribution, to substitute the continuous exponential distribution associated with each edge. As illustrated in Figure 1, the discretization makes the $T_n$’s follow a discrete non-homogeneous Poisson process of success probabilities $r_{n-1}$ for $n = 1, \ldots, |V|$. In order to characterize $T_n$, we need to specify $r_0, r_1, \ldots, r_{|V|-1}$.

Note that $\Pr[T_0 = 0] = 1$. At time $t > 0$, the external attacker tries to attack the nodes belonging to $V - C_{t-1}$, while each compromised internal node $u \in C_{t-1}$ tries to attack its neighbors that have not been attacked by $u$ — provided there are still such neighbors. We assume that the delay for an attack launched via an edge to succeed is exponentially distributed with rate $\frac{1}{2|E| + |V|}$. Since at the beginning there is only the external attacker, the success probability should be proportional to $|V|$, namely

$$r_0 = \frac{|V|}{2|E| + |V|}$$
In general, we have

\[ r_i = \frac{|V| + d_1 + d_2 + \cdots + d_i - i}{2|E| + |V|}, \quad i = 1, 2, \ldots, |V| - 1, \quad (2.1) \]

where \( d_j \overset{\text{def}}{=} \deg(\text{node}(T_j)) \) for \( j = 1, \ldots, |V| \).

Consider a sequence \( \text{node}(T_1), \ldots, \text{node}(T_{|V|-1}) \). The probability mass function of \( T_1 \) is geometrically distributed as

\[ q_1(i) \overset{\text{def}}{=} \Pr \left[ T_1 = i \bigg| \bigwedge_{1 \leq l < |V|-1} D_l = d_l \right] = r_0(1 - r_0)^{i-1} = g(i, r_0), \quad i = 1, 2, \ldots. \quad (2.2) \]

Given \( T_{n-1}, S_{n-1} \overset{\text{def}}{=} T_n - T_{n-1} \) is geometrically distributed with probability of success \( r_{n-1} \). Therefore, for \( n = 2, 3, \ldots \), the discrete probability mass function of \( T_n \) is given by

\[ q_n(i) \overset{\text{def}}{=} \Pr \left[ T_n = i \bigg| \bigwedge_{1 \leq l < |V|-1} D_l = d_l \right] = \sum_{j=n-1}^{i-1} q_{n-1}(j) \cdot g(i-j, r_{n-1}), \quad i = n, n+1, \ldots. \]

Now we are ready to characterize the distributions of the \( T_n \)'s by considering all possible \( \text{node}(T_1), \ldots, \text{node}(T_{|V|}) \) with the respective \( r_0, \ldots, r_{|V|-1} \). Note that by definition, we have

\[ T_n = \min\{t : N(t) = n\}, \quad n = 1, 2, \ldots, |V|. \]

Define, for \( n = 1, 2, \ldots, |V| \),

\[ p_n(i) \overset{\text{def}}{=} \Pr[T_n = i], \quad i = n, n+1, \ldots. \]

Then,

\[ p_n(i) = \Pr[T_n = i] = \sum_{(d_1, \ldots, d_{n-1})} \Pr \left[ T_n = i \bigg| \bigwedge_{1 \leq l < n} D_l = d_l \right] \cdot \Pr \left[ \bigwedge_{1 \leq l < n} D_l = d_l \right] \\
= \sum_{(d_1, \ldots, d_{n-1})} \left( \sum_{j=n-1}^{i-1} q_{n-1}(j) \cdot g(i-j, r_{n-1}) \cdot \Pr \left[ \bigwedge_{1 \leq l < n} D_l = d_l \right] \right), \quad (2.3) \]
where
\[
\Pr \left( \bigwedge_{1 \leq l < n} D_l = d_l \right) = \prod_{1 \leq l < n} \Pr[D_l = d_l],
\]
and \(g(i, r)\) and \(q_n(i)\) are given by Equations (2.1), (2.2) and (2.3). As a result, we have
\[
E[T_n] = \sum_{i=n}^{\infty} i \cdot p_n(i), \quad n = 1, 2, \cdots, |V|.
\] (2.4)

### 2.2 Deriving \(N(t)\) and \(M(t)\)

Recall that \(N(t)\) is the random variable indicating the number of nodes that became compromised at or before time \(t\), \(M(t)\) is the random variable indicating the number of compromised nodes that have become removed by time \(t\). Moreover,
\[
E[N(t)] = \sum_{n=1}^{t} n \cdot \Pr[N(t) = n] = \sum_{n=1}^{t} \sum_{i=t+1}^{\infty} n[p_{n+1}(i) - p_n(i)].
\] (2.5)

Figure 2: Illustration of the delay random variable \(X_i\) for the \(i\)th compromised node to become removed.

To capture the nodes’ (i.e., the corresponding computers’) attack-detection-and-recovery mechanisms (e.g., intrusion detection systems), we assume that the length of the time period for a compromised node to get recovered follows the exponential distribution. Let \(I(\cdot)\) be the indicator function. As illustrated in Figure 2, the expected total number of nodes that have become compromised but not yet become removed by time \(t\) is given by
\[
E[N(t)] - E[M(t)] = E \left[ \sum_{i=1}^{N(t)} I(X_i > t - T_i) \right]
\]
\[
= \sum_{n=1}^{t} \Pr[N(t) = n] \sum_{i=1}^{n} \Pr[X_i > t - T_i]
\]
\[
= \sum_{n=1}^{t} \Pr[N(t) = n] \cdot \sum_{i=1}^{n} \left( \sum_{j=i}^{t} \Pr[X_i > t - j] \cdot \Pr[T_i = j] \right)
\]
\[
= \sum_{n=1}^{t} \left\{ \left( \sum_{i=t+1}^{\infty} [p_{n+1}(i) - p_n(i)] \right) \left[ \sum_{i=1}^{n} \left( \sum_{j=i}^{t} p_i(j)(1 - s)^{t-j} \right) \right] \right\}.
\] (2.6)

By Eq. (2.5) and (2.6), we obtain \(E[M(t)]\).

### 3 Analyses

#### 3.1 Characterizing the Sequence of \(T_{i+1} - T_i\)

We are interested in characterizing the sequence of \(S_i = T_{i+1} - T_i\) for \(i = 0, 1, \cdots, |V| - 1\), namely the sequence of the stochastic intervals between two incident occurrences (cf. also Figure 1).
Proposition 1 The sequence $S_0, S_1, \cdots, S_n$ is stochastically decreasing. That is,

$$S_i \succeq_{st} S_{i+1}, \quad i = 0, 1, \cdots, |V| - 1. \tag{3.1}$$

Proof: Given a fixed sequence of nodes $\text{node}(T_1), \ldots, \text{node}(T_{|V|})$, $S_i = T_{i+1} - T_i$ is geometrically distributed with success probability $r_i$, which is given by Eq. (2.1). Thus,

$$\Pr[S_i > k] = \sum_{(d_1, \ldots, d_{i-1})} \Pr[S_i > k] \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right| \cdot \Pr \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right|$$

$$= \sum_{(d_1, \ldots, d_{i-1})} \left( \sum_{j=k+1}^{\infty} r_{i-1}(1 - r_{i-1})^{j-1} \Pr \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right| \right)$$

$$= \sum_{(d_1, \ldots, d_{i-1})} (1 - r_{i-1})^k \Pr \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right| .$$

Since $r_i$ is nondecreasing, it holds that, for all positive integer $k$ and $i = 1, \cdots, |V| - 1$

$$(1 - r_{i-1})^k \geq (1 - r_i)^k .$$

Hence, for any positive integer $k$,

$$\Pr[S_{i+1} > k] = \sum_{(d_1, \ldots, d_{i-1})} \left( (1 - r_i)^k \Pr \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right| \right)$$

$$\leq \sum_{(d_1, \ldots, d_{i-1})} \left( (1 - r_{i-1})^k \Pr \left| \bigwedge_{1 \leq l \leq i} D_l = d_l \right| \right)$$

$$= \sum_{(d_1, \ldots, d_{i-1})} \sum_{r_{i-1}} (1 - r_{i-1})^k \Pr \left| \bigwedge_{1 \leq l \leq i-1} D_l = d_l \right|$$

$$= \sum_{(d_1, \ldots, d_{i-2})} (1 - r_{i-1})^k \Pr \left| \bigwedge_{1 \leq l \leq i-1} D_l = d_l \right|$$

$$= \Pr[S_i > k] .$$

That is, $S_i \succeq_{st} S_{i+1}$ for $i = 0, 1, \cdots, |V| - 2$. \qed

This proposition is useful because it says that the coordinated attack gets more powerful as more internal nodes become compromised. Note that this characterization is valid regardless of the attack strategies explored below, as long as the attacker intends to compromise as many nodes as possible. This is because the two perspectives are orthogonal to each other. Moreover, this characterization is also valid regardless of the immunization strategies explored below. This is because the sequence $S_i = T_{i+1} - T_i$ applies to the attack process against the subgraph obtained by eliminating from $G$ the immunized nodes and their associated edges.

### 3.2 On the Effect of Attack Strategies

Suppose an instance of a given attack strategy imposes a sequence of incidents occurring at time $T_1, T_2, \ldots, T_n$, where $1 \leq n \leq |V|$. We are interested in understanding the effect of attack strategies through the induced node degree sequence
\[ \text{deg}(\text{node}(T_1)), \ldots, \text{deg}(\text{node}(T_n)). \]
In particular, we are interested in comparing the effect of the following three attack strategies:

* **Attack strategy 1**: The degrees of the nodes that became compromised are in a non-decreasing order, namely \( \text{deg}(\text{node}(T_1)) \leq \ldots \leq \text{deg}(\text{node}(T_n)). \)

* **Attack strategy 2**: The nodes became compromised in an arbitrary order.

* **Attack strategy 3**: The degrees of the nodes that became compromised are in a non-increasing order, namely \( \text{deg}(\text{node}(T_1)) \geq \ldots \geq \text{deg}(\text{node}(T_n)). \)

Suppose we are given \( 1 \leq n \leq |V| \), where \( n \) represents the number of nodes that became compromised by the coordinated internal and external attack. Denote by
\[
d_{d_{|V|}} \leq d_{d_{|V|-1}} \leq \cdots \leq d_{d_{1}} \leq d_{d_{|V|}} \]
the ordered sequence of degrees of the nodes. For \( \gamma \in \{1, 2, 3\} \), let \( d_i^{(\gamma)} \) be the degrees of compromised nodes ordered by the times at which they became compromised in attack strategy \( \gamma \). Then, we have \( d_j^{(1)} = d_{j;|V|} \) and \( d_j^{(3)} = d_{|V|−j+1;|V|} \) for \( 1 \leq j \leq n \). Then, for all \( k = 1, 2, \cdots, n \),
\[
\sum_{i=1}^{k} d_i^{(1)} \leq \sum_{i=1}^{k} d_i^{(2)} \leq \sum_{i=1}^{k} d_i^{(3)}.
\]

For \( \gamma \in \{1, 2, 3\} \), let \( r_i^{(\gamma)} \) be the sequence of geometric success probability in attack strategy \( \gamma \). By Eq. (2.1), it is easy to verify that
\[
\sum_{i=0}^{k} r_i^{(1)} \leq \sum_{i=0}^{k} r_i^{(2)} \leq \sum_{i=0}^{k} r_i^{(3)}.
\]

For \( \gamma \in \{1, 2, 3\} \), let \( T_n^{(\gamma)} \) denote the time at which the \( n \)th incident occurs in attack strategy \( \gamma \). Then, we have

**Proposition 2** For any \( n = 1, 2, \cdots, |V| \),
\[
T_n^{(1)} \preceq_{st} T_n^{(2)} \preceq_{st} T_n^{(3)}. \tag{3.2}
\]

This proposition is useful because it says, from the attacker’s perspective, that attack strategy 3 outperforms attack strategy 2, which in turn outperforms attack strategy 1. In other words, a carefully orchestrated adaptive attack strategy is always advantageous to a random attack strategy.

### 3.3 On the Effect of Immunization Strategies

Suppose the administrator of a networked system is given a budget for improving security of the networked system. It is interesting to know how the budget should be spent so that the resulting system can become as secure as possible. When a node \( v \in V \) is immunized (i.e., not subject to attacks orchestrated by the external attacker), this effectively leads to a graph \( G(V(v), E(v)) \) where \( V(v) = V \setminus \{v\} \) and \( E(v) = E - \{(v, v') : (v, v') \in E\} \). We consider three strategies:

* **Immunization strategy 1**: Immunize the node \( z \) at system initialization, where \( \text{deg}(z) = \min\{\text{deg}(v) : v \in V\} \). For the resulting vulnerability graph \( G(z) = (V(z), E(z)) \), we can define \( T_n^{[1]} \) to be the time at which the \( n \)th incident occurs. Similarly, we can define \( r_k^{[1]} \) to be the counterpart of \( r_k \), and \( S_k^{[1]} \) to be the counterpart of \( S_k \).

* **Immunization strategy 2**: Randomly pick a node, say \( u \), and immunize it at system initialization. For the resulting vulnerability graph \( G(u) = (V(u), E(u)) \), we can define \( T_n^{[2]} \) to be the time at which the \( n \)th incident occurs. In a similar fashion, we can define \( r_k^{[2]} \) to be the counterpart of \( r_k \), and \( S_k^{[2]} \) to be the counterpart of \( S_k \).

* **Immunization strategy 3**: Immunize the node \( w \) at system initialization, where \( \text{deg}(w) = \max\{\text{deg}(v) : v \in V\} \). For the resulting vulnerability graph \( G(w) = (V(w), E(w)) \), we can define \( T_n^{[3]} \) to be the time at which the \( n \)th incident occurs. In a similar fashion, we can define \( r_k^{[3]} \) to be the counterpart of \( r_k \), and \( S_k^{[3]} \) to be the counterpart of \( S_k \).
Now we explore the effect of different immunization strategies.

**Proposition 3** For all $1 \leq n \leq |V|$, we have

$$T_n^{[3]} \geq_{st} T_n^{[2]} \geq_{st} T_n^{[1]}.$$

*Proof:* Note that for any sequence of compromised nodes belonging to $V(u)$,

$$v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_{|V|-1},$$

in immunization strategy 2 with $u$ being immunized, there is a corresponding sequence of compromised nodes belonging to $V(w)$,

$$v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_{|V|-1},$$

in immunization strategy 3 with $w$ being immunized. Since

$$r_k^{[2]} = r_k^{[3]},$$

and $\deg(w) \geq \deg(u)$, Eq. (2.1) implies

$$r_k^{[2]} > r_k^{[3]},$$

for $k = i, \ldots, |V| - 2$.

Thus, for any $k = 0, 1, \ldots, |V| - 2$, “$S_k^{[3]}$” corresponding to the sequence $v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_{|V|-1}$” is stochastically larger than “$S_k^{[2]}$” corresponding to the sequence $v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_{|V|-1}$.” Hence $\sum_{k=1}^{n} S_k^{[3]}$ corresponding to the sequence $v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_{|V|-1}$ is stochastically larger than $\sum_{k=1}^{n} S_k^{[2]}$ corresponding to the sequence $v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_{|V|-1}$.

Since $T_n^{[2]}$ is the mixture of $\sum_{k=1}^{n} S_k^{[2]}$ corresponding to the sequence $v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_{|V|-1}$, and $T_n^{[3]}$ is the mixture of $\sum_{k=1}^{n} S_k^{[3]}$ corresponding to the sequence $v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_{|V|-1}$, we conclude that $T_n^{[3]} \geq_{st} T_n^{[2]}$ for any $n = 1, 2, \ldots, |V| - 1$.

In a similar fashion, one can show $T_n^{[2]} \geq_{st} T_n^{[1]}$ for any $n = 1, 2, \ldots, |V| - 1$.

This proposition is useful because it suggests that for a given budget that imposes a bound $m$ on the number of nodes that can be immunized, it is wise to immunize the nodes that have large degrees. Note that there have been some results (e.g., [2]), which are spiritually similar to this proposition. However, both the settings of, and the attacks modeled by, these results are different from their counterparts in this paper; see Section 4 for details.

### 4 Related Work

There have been some works at understanding security by considering a networked system as a whole. Nevertheless, our approach is seemingly the first at understanding and modeling (rather than detecting) coordinated internal and external attacks. In what follows we elaborate on the differences between existing modeling efforts and ours.

**Epidemic-like modeling vs. ours.** The main differences between traditional epidemic models (cf. [11, 4]) and their adaptations to model computer networked systems (cf. [10, 5, 12, 15, 14, 18]) are the following. First, traditional epidemic models capture the spreading of infections among the legitimate internal nodes. Whereas our model captures coordinated internal and external attacks, where the external attacker may always launch attacks against the legitimate internal nodes.

Therefore, our model is strictly more general and powerful. Second, in real-life attacks, an adversary will not try to compromise an already compromised node, because the adversary knows which nodes have been compromised. This fact cannot be captured by traditional epidemic models, whereas our model can. Third, traditional epidemic models often make the homogeneous assumption that all the nodes have the equal power to infect other nodes. This is not necessarily true in real-life because compromise of some node may lead to more catastrophic consequences than compromise of another. That is, the homogeneous assumption is violated. Our model captures the heterogeneity of the nodes in terms of their degrees.

**Privilege graph and attack graph based approaches vs. our approach.** In a privilege graph [7, 13], a vertex represents a set of privileges on some objects and an arc represents a vulnerability. An arc exists from one vertex to another if there is a method allowing a user owning the former vertex’s privileges to obtain those of the latter. In an attack graph, a vertex represents the state of a network (i.e., the values assigned to relevant system attributes such as specific vulnerabilities on various hosts and connectivity between hosts), and an edge represents a step in an attack (cf. [16, 9, 3] and the references.
A designated vertex (or set of vertices) represents the initial state(s), and each transition represents a specific exploit that an attack can carry out.

The main difference between privilege and attack graphs and ours lies in the model purpose and scalability. From a purpose perspective, privilege graphs can be used to estimate the effort an attacker, in order to defeat the system security objectives, might expend to exploit the vulnerabilities. Attack graphs can be used to identify end-to-end attack paths by chaining together the vulnerabilities uncovered by the vulnerability scanners. In contrast, our model focuses on investigating the impact of system attributes on system security. Moreover, our approach suggests methods to “tune” configurations or parameters to lead to more secure systems. From a scalability perspective, privilege and attack graph based approaches suffer from limited scalability, because of their inherent exponential state explosion [3, 6]. In contrast, our approach is scalable because there is no issue of state explosion.

Key challenge graph based approach vs. our approach. In a key challenge graph [6], a vertex represents a host, and an arc represents a key challenge — an abstraction to capture access control. A key challenge is, for instance, a password authentication prior to accessing to a resource. The starting point of an attack could be one or more vertices, which are assumed to be initially in the control of the attacker. The target of an attack could be one or more vertices, for which the attacker knows the location and the paths to reach them. A successful attack is a sequence of zero or more vertices not in the initial set but eventually containing all the target vertices. The cost of an attack is measured as the sum of the effort required to compromise individual vertices by attempting to counter the key challenges on the edges. Since there are multiple paths from the starting point to the target, a problem of particular interest is to find an attack path of minimum cost.

Connectivity-oriented analysis vs. our security-oriented analysis. Connectivity-oriented analysis of networked systems can be traced back to the early days of random graph theory [8]. A central problem in this context is to investigate the network reliability subject to edge removals, namely the probability that graph remains connected after removing some edges. Recently, such analysis has been extended to explore the impact of topologies of complex communication networks, including the impact of removing vertices, which is more damaging because removal of a vertex implies the removal of all its edges as well. It turns out that there is a strong correlation between connectivity and network topology [1]. For example, consider networks that have the same number of vertices and edges, and differ only in their degree distributions. Then, power-law networks are more robust than random networks against random vertex failures, but are more vulnerable when the most connected vertices are targeted [2].

Connectivity-oriented analysis does not necessarily bring much insight for security analysis. This is because a malicious attacker would be more likely to use the compromised vertices as “stepping stones” to attack some more vertices, rather than simply undermining the network connectivity. Therefore, the connectivity of a system may never be jeopardized, but the security has been undermined. Our model focuses on the security aspect by taking into consideration the perspective of topologies as well as vertex properties.

5 Conclusion and Future Work

We presented a first towards modeling coordinated internal and external attacks against networked systems. For a class of semi-sophisticated coordinated attacks, our model offers a characterization of (1) the attack behavior, (2) the effect of attack strategies, and (3) the effect of immunization strategies. An important next step is to model fully coordinated internal and external attacks.
References


