Security Risk Analysis using Markov-chain Model

Dr. Ferenc Leitold  
College of Dunaújváros, Veszprog Ltd.  
kleitold@veszprog.hu
Agenda

Traditional attacks
Attacks nowadays
Theory of Markov-chains
Using Markov-chain in the security risk analysis
Traditional attacks
Traditional attacks
Traditional attacks
Traditional attacks

![Diagram of traditional attacks]

- Plaintext, $P$ → Encryption method, $E$ → Ciphertext, $C = E_K(P)$ → Decryption method, $D$ → Plaintext, $P$
- Intruder
- Passive intruder just listens
Attacks thru communication channel

Based on message (packet) sending

SOURCE: user or application

TARGET: user or application
Attacks thru communication channel

The target is (mainly) the user:
(email, skype, msn, ICQ, IRC, phone, …)

• Code is sent within the message (e.g. attachment)
  – Abuse the user AND / OR
  – Execute the code automatically

• Code is not sent
  – The user executes the required activity
    • The user sends the message toward (e.g. HOAX)
    • The user executes manually the malicious activity
  – Link of malicious code or URL in the message
    (e.g. phishing)
The target is an application:

Vulnerability problem
It can be related:
- operating systems
- applications
- protocols
- “file formats”
  (applications handling particular files)
Attacks thru communication channel

Two problems:

- the user
- vulnerabilities

Both of them are related to the human factor.

“The biggest problem with computers is the bit between the keyboard and the chair.”
Theory of Markov-chain

Example:

Homer and Marge repeatedly play a gambling game. Each time they play, the probability that Homer wins is 0.4, and the probability that Homer loses is 0.6.

Homer and Marge both start with $2.
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Theory of Markov-chain
Homer and Marge repeatedly play a gambling game. Each time they play, the probability that Homer wins is 0.4, and the probability that Homer loses is 0.6.

Example:

Homer and Marge both start with $2.
Theory of Markov-chain

\[
P = \begin{bmatrix}
1 & 0.6 & 0 & 0 & 0 & 0 \\
0 & 0 & 0.6 & 0 & 0 & 0 \\
0 & 0.4 & 0 & 0.6 & 0 & 0 \\
0 & 0 & 0.4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0.4 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

\[P(\text{Homer wins}) = 0.4 \quad P(\text{Homer loses}) = 0.6\]
A Markov-chain is a mathematical model for a process which moves step by step through various states.

In a Markov-chain, the probability that the process moves from any given state to any other particular state is always the same, regardless of the history of the process.
A Markov-chain consists of states and transition probabilities.

Each transition probability is the probability of moving from one state to another in one step. The transition probabilities are independent of the past, and depend only on the two states involved. The matrix of transition probabilities is called the transition matrix.
Theory of Markov-chain

\[ P = \begin{bmatrix}
1 & .6 & 0 & 0 & 0 \\
0 & 0 & .6 & 0 & 0 \\
0 & .4 & 0 & .6 & 0 \\
0 & 0 & .4 & 0 & 0 \\
0 & 0 & 0 & .4 & 1 \\
\end{bmatrix} \]
If $P$ is the transition matrix for a Markov Chain, then the $n$th power of $P$ gives the probabilities of going from state to state in exactly $n$ steps.

<table>
<thead>
<tr>
<th></th>
<th>$v$</th>
<th>$Pv$</th>
<th>$P^2v$</th>
<th>$P^3v$</th>
<th>$P^4v$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.53</td>
<td>0.62</td>
<td>0.62</td>
<td>0.66</td>
<td>0.66</td>
</tr>
<tr>
<td>0.13</td>
<td>0</td>
<td>0.07</td>
<td>0</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0.11</td>
<td>0</td>
<td>0.05</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0.09</td>
<td>0</td>
<td>0.04</td>
<td>0</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>0.24</td>
<td>0.27</td>
<td>0.27</td>
<td>0.29</td>
<td>0.29</td>
<td></td>
</tr>
</tbody>
</table>
Purpose of modelling

Calculating or estimating a metric which typifies how immunized is an infrastructure (in a particular environment and in a certain time) against attacks arriving from different communication channels.
Problems

Everything is changing
  – Attack possibilities
  – Malware (used attack vectors, prevalence, geolocation)
  – Known and/or published vulnerabilities
  – Update of elements in an IT system
  – User knowledge about security
  – …
Graph representation
Graph representation
Matrix representation

$A[i,j]$: 

The “risk of attack” on the $E_j \Rightarrow E_i$ communication channel

If $\sum_j A[i,j] = 1$

Markov-chain model
Matrix representation

\[ A[i,j] = 0 \]

- \( E_i \) is not attackable thru the \( E_j \Rightarrow E_i \) communication channel

\[ A[i,j] > 0 \]

- Reliability, attack possibility of the communication channel.
- Reliability, vulnerabilities, security updates of entity \( i \).
Risk analysis

Input
- Elements of IT infrastructure: topology, protocols, versions, …
- Security tools: types, versions, settings, …
- Contacts of users (with each other and with IT elements): results of questionnaires, tests of their security level
- Properties, prevalence and geolocations of possible attacks (malware)
Risk analysis

Output
- Security risks of the elements of IT infrastructure
- The weakest point of the IT infrastructure