A Framework for Estimating the Mean Time-to-Compromise of a System

Eric Byres, P.Eng.
Byres Research
eric@byressecurity.com

David Leversage, P.Eng.
Dept of Electrical & Computer Engineering Technology, BCIT
david.leversage@gmail.com

Collaborating to Advance Control System Security
The Need for Security Metrics

- Industry can’t afford perfect security.

- Must take some risk – the challenge is figuring out exactly what amount of risk is acceptable at what cost.
Security is About Money

- Security industry says “buy our product or service and it will solve everything”.

- You must answer real-life questions like:
  - Would my company be more secure if I spent $50K on patch management systems or $75K on new firewalls?
  - How do I justify to my boss the need for a $100K security project.
  - Is plant security better or worst than last year?
Common Measurement Techniques

- 3rd Party Security Audits
- Self Assessments
- Penetration Testing
- Counting the Incidents (and guessing at costs)
What Should We Measure?

- The ideal metric for rating a system should:
  - Easy to comprehend by experts & management.
  - Be a single metric.
  - Possible to aggregate separate sub-values.

- Our goal is a comparative metric.
Breaking into Safes

Safes are assigned a burglary ratings based on well defined Underwriters Laboratory (UL) tests.

<table>
<thead>
<tr>
<th>UL Rating</th>
<th>NWT (Min.)</th>
<th>Testing Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TL-15</td>
<td>15</td>
<td>Tool-Resistant (face only)</td>
</tr>
<tr>
<td>TL-30</td>
<td>30</td>
<td>Tool-Resistant (face only)</td>
</tr>
<tr>
<td>TRTL-15X6</td>
<td>15</td>
<td>Torch &amp; Tool-Resistant (6 Sides)</td>
</tr>
<tr>
<td>TRTL-30X6</td>
<td>30</td>
<td>Torch &amp; Tool-Resistant (6 Sides)</td>
</tr>
<tr>
<td>TRTL-60</td>
<td>60</td>
<td>Torch &amp; Tool-Resistant</td>
</tr>
</tbody>
</table>
UL Safe Burglary Ratings

- All ratings based on “Net Working Time” (NWT)

- NWT is the time testers spent trying to break into the safe using tools such as diamond grinding tools, high-speed drills and common hand tools:
  - TL-15: Safe tested for a NWT of 15 minutes.
  - TL30x6: A TL-30 test performed on six sides.
  - TRTL-30: Safe tested for a NWT of 30 minutes with an extended range of tools.
Some Observations

- Rating is based ability to withstand a focused attack by a team of knowledgeable safe crackers following a written set of procedures for testing:
  - Testers are given design level knowledge about the safe which is used in planning the attacks.
  - Although there are maybe dozens of strategies, testers will try only a few.
  - Attacks are arranged by differing surfaces or zones.
  - The rules include using a specific set of common resources for safe cracking. Resources are organized into well-defined levels that represent increasing cost/complexity and decreasing availably to the average attacker.
Attack Time, Resources and Zones

- Two controlled variables – Resources and Zones
- One measured variable – Time to crack safe
The Critical Observation!!

- UL rating does not attempt promise that the safe is secure from all possible attacks strategies.

- Statistically it is reasonable to assume that as a group, TL-30 safes are more secure than TL-15 safes.

- Efficiently estimates a comparative security level for a given system.
Applying Lessons to Control Security

- Given the proper resources and enough time, any control system can be broken into.
- Discovering every possible vulnerability or attack strategy is NOT needed to rate a system.
- Consistent tests, not exhaustive tests!
- Organize attacker resource availability into “levels”.
- Time is the common metric.
Mean Time to Compromise (MTTC)

- The mean time it will take for an attacker within a specific skills level to successfully strike a target PCN or device on it.

**Example of estimated MTTC intervals (in days) for three attacker skill levels.**

- **Expert**: 30 - 60 days
- **Intermediate**: 45 - 165 days
- **Beginner**: 90 - 270 days
Seven Steps to Calculating MTTC Intervals

1. Define Zones
2. Define Predator Model
3. Define Attack Path Model
4. Estimate State Times
5. Build State Time vs. Skill Level Matrix
6. Determine Path Probabilities
7. Calculate MTTC Intervals
Step 1: Define Zones

- Break the system into zones of related devices, procedures and protocols.
Step 2: Define Predator Model

- Decide on a specific set of states that an attacker will go through and create a state-space model (SSM).
Step 3: Define Attack Path Model

- Apply the predator model to the system to map out the attack path model – a SSM of all possible attack paths from the launch node to the target device.
Step 4: Estimate State Times

Calculate state time for each state transition using one of several possible methods:

- A statistical algorithms (such as McQueen et al’s Time to Compromise Model)
- Attack tree-based techniques
- In field sample penetration tests
Step 5: Build State Time vs. Skill Level Matrix

- Build a matrix of state time versus skill levels for each state and skill level.

<table>
<thead>
<tr>
<th>Skill Level</th>
<th>B1</th>
<th>P1</th>
<th>B2</th>
<th>P2</th>
<th>C</th>
<th>I</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert</td>
<td>4.6</td>
<td>2.9</td>
<td>5.2</td>
<td>4.0</td>
<td>1.0</td>
<td>4.8</td>
<td>1.0</td>
</tr>
<tr>
<td>Intermediate</td>
<td>5.2</td>
<td>3.3</td>
<td>5.8</td>
<td>4.5</td>
<td>1.0</td>
<td>5.3</td>
<td>1.0</td>
</tr>
<tr>
<td>Beginner</td>
<td>9.5</td>
<td>7.3</td>
<td>13.9</td>
<td>8.7</td>
<td>1.0</td>
<td>10.3</td>
<td>1.0</td>
</tr>
</tbody>
</table>
Step 6: Determine Path Probabilities

- Determine the probability of all attack paths.

<table>
<thead>
<tr>
<th>Attack Paths</th>
<th>Freq.</th>
<th>Prob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>L, B1, B2, C, S</td>
<td>8</td>
<td>0.3333</td>
</tr>
<tr>
<td>L, B1, P1, B2, A, S</td>
<td>6</td>
<td>0.2500</td>
</tr>
<tr>
<td>L, B1, B2, P2, A, S</td>
<td>4</td>
<td>0.1667</td>
</tr>
<tr>
<td>L, B1, P1, B2, P2, A, S</td>
<td>2</td>
<td>0.0833</td>
</tr>
<tr>
<td>L, B1, B2, I, S</td>
<td>1</td>
<td>0.0417</td>
</tr>
<tr>
<td>L, B1, B2, P2, I, S</td>
<td>1</td>
<td>0.0417</td>
</tr>
<tr>
<td>L, B1, P1, B2, P2, I, S</td>
<td>1</td>
<td>0.0417</td>
</tr>
<tr>
<td>L, B1, P1, B2, I, A, S</td>
<td>1</td>
<td>0.0417</td>
</tr>
<tr>
<td>total</td>
<td>24</td>
<td>1.0001</td>
</tr>
</tbody>
</table>
Step 7: Calculate MTTC Intervals

Calculate the MTTC intervals for each system and skill level.

<table>
<thead>
<tr>
<th>Attack Paths</th>
<th>Path Time (hrs)</th>
<th>Prob.</th>
<th>Product (hrs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L, B1, B2, C, S</td>
<td>41.2</td>
<td>0.3333</td>
<td>13.7</td>
</tr>
<tr>
<td>L, B1, P1, B2, A, S</td>
<td>59.3</td>
<td>0.2500</td>
<td>14.8</td>
</tr>
<tr>
<td>L, B1, B2, P2, A, S</td>
<td>59.3</td>
<td>0.1667</td>
<td>9.9</td>
</tr>
<tr>
<td>L, B1, P1, B2, P2, A, S</td>
<td>77.4</td>
<td>0.0833</td>
<td>6.4</td>
</tr>
<tr>
<td>L, B1, B2, I, S</td>
<td>136.8</td>
<td>0.0417</td>
<td>5.7</td>
</tr>
<tr>
<td>L, B1, B2, P2, I, S</td>
<td>154.9</td>
<td>0.0417</td>
<td>6.5</td>
</tr>
<tr>
<td>L, B1, P1, B2, P2, I, S</td>
<td>173.0</td>
<td>0.0417</td>
<td>7.2</td>
</tr>
<tr>
<td>L, B1, P1, B2, I, A, S</td>
<td>162.3</td>
<td>0.0417</td>
<td>6.8</td>
</tr>
</tbody>
</table>

Mathematical Expectation for MTTC: 71

- 41.2 (Shortest Path)
- 71.0 (MTTC)
- 173.0 (Longest Path)
Example: Using MTTC for Comparing Two Plants with Differing Practices

- **Plant #1**
  - Reviews its firewall rules on a annual basis
  - Average of 2 vulnerabilities per node for EN network
  - Average of 10 vulnerabilities per node on PCN network

- **Plant #2**
  - Reviews its firewall rules on a quarterly basis
  - Average of 4 vulnerabilities per node for EN network
  - Average of 6 vulnerabilities per node on PCN network

- **Which is more secure?**
Example: Using MTTC for Comparing Two Plants with Differing Practices

- Expert
  - 10
  - 18
  - 25

- Intermediate
  - 12
  - 19
  - 20
  - 12
  - 28

- Beginner
  - 22
  - 30
  - 39
  - 28
  - 47
  - 65
  - 72
  - 103
Don’t Take Our Word for It…

- Easy confirmation of MTTC calculations through practical testing:
  - Analysis of MTTC in honeynets
  - Penetration testing times

- Simple correlation to security testing of devices (like MTBF is used for reliability).
What MTTC Gives Us

- MTTC does NOT guarantee a 100% secure system.
- MTTC does allow easy to understand comparisons:
  - Is security solution A better that solution B?
  - How does our security compare to the rest of the industry?
  - How does our security preparedness this year compare to last year?
Questions?