

Creating Practical Security Metrics

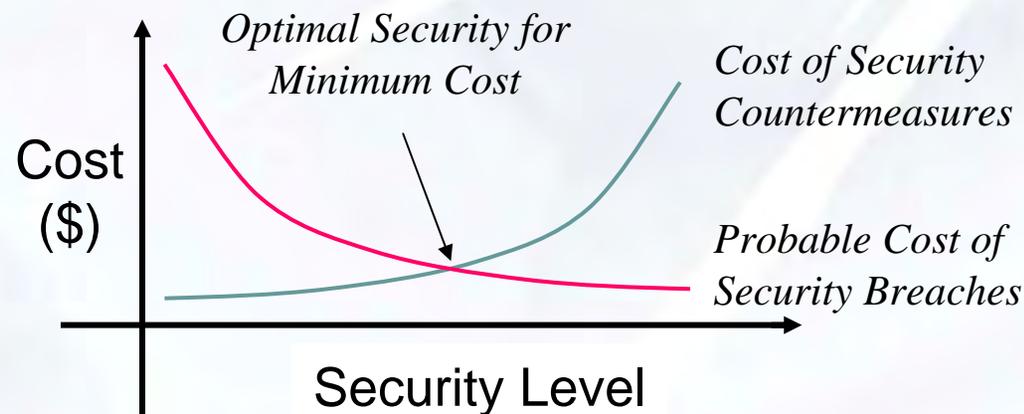
Eric Byres, P.Eng.
Director – Industrial Security
Wurldtech Analytics Inc.
ebyres@wurldtech.com

David Leversage
Dept of Electrical & Computer Engineering Technology
British Columbia Institute of Technology
david.leversage@gmail.com



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

- The security industry just tells you to buy their product or service and it will solve everything.
- In real life you must answer 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

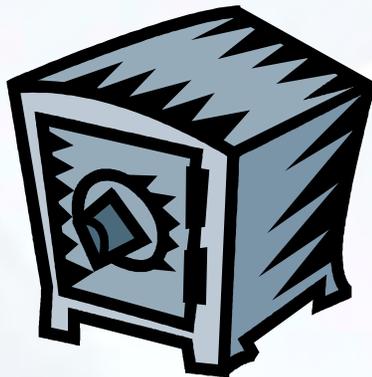
- 3rd Party Security Audits
- Self Assessments
- Penetration Testing
- Counting the Incidents (and guessing at costs)

What Should We Measure?

- What Should We Measure?
 - Number of Security “Holes” or Vulnerabilities?
 - Money (potential cost of incidents)?
 - Incident Rates?
- The ideal metric for rating a system should:
 - Easy to comprehend by experts & management.
 - Be a single metric.
 - Possible to aggregate separate sub-values.

Breaking into Safes

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



UL Ratings	Description
B1	Theft Resistant (minimal security)
B2	UL Residential Security Container Label
B3	Non-rated Anti-theft
B4	UL TL-15 Label
B5	UL TL-30 Label
B6	UL TL-30x6 or TRTL-30 Label

UL Safe Burglary Ratings

- 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.
- Examples of ratings:
 - **TL-15:** Safe tested for a NWT of 15 minutes.
 - **TL30x6:** A TL-30 test has been performed on all six sides.
 - **TRTL-30:** Safe tested for a NWT of 30 minutes with an extended range of tools.

Some Observations

- Implied assumption that given the proper resources and enough time, any safe can be broken into.
- Rating is based ability to withstand a focused attack by a team of knowledgeable safe crackers following a written set of rules and 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 (classified as attack types), testers will try only a few.
 - The rules include using a specific set of common resources for safe cracking.

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, matter.
- Time is the common metric.

Mean Time to Compromise (MTTC)

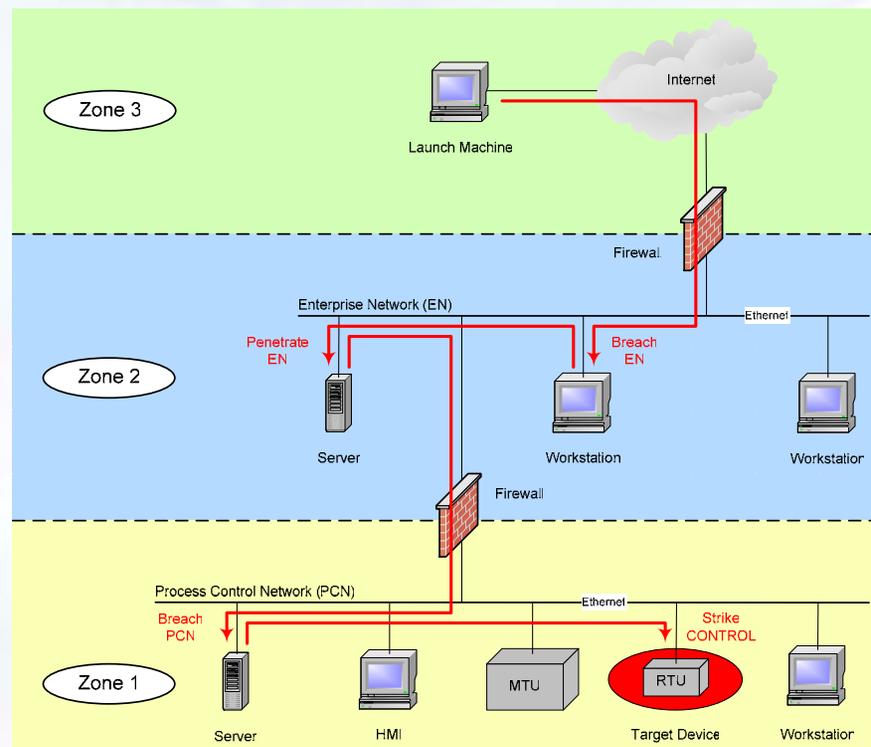
- The mean time it will take for an attacker within a specific skills level to successfully strike a target PCN or device on it.



Fig. 1. Example of estimated MTTC intervals (in days) for three attacker skill levels.

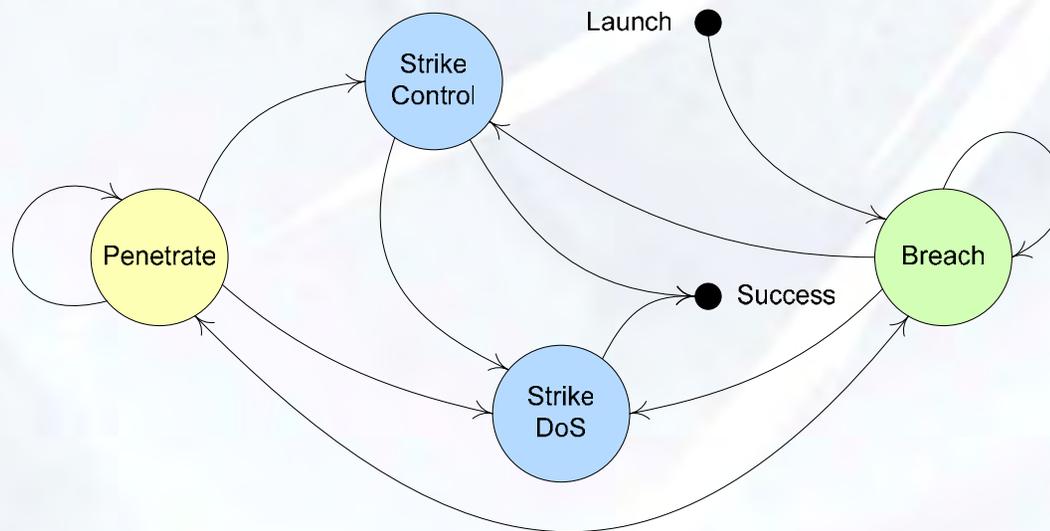
Calculating MTTC – Zone Definition

1. Break the system into zones of related devices, procedures and protocols.



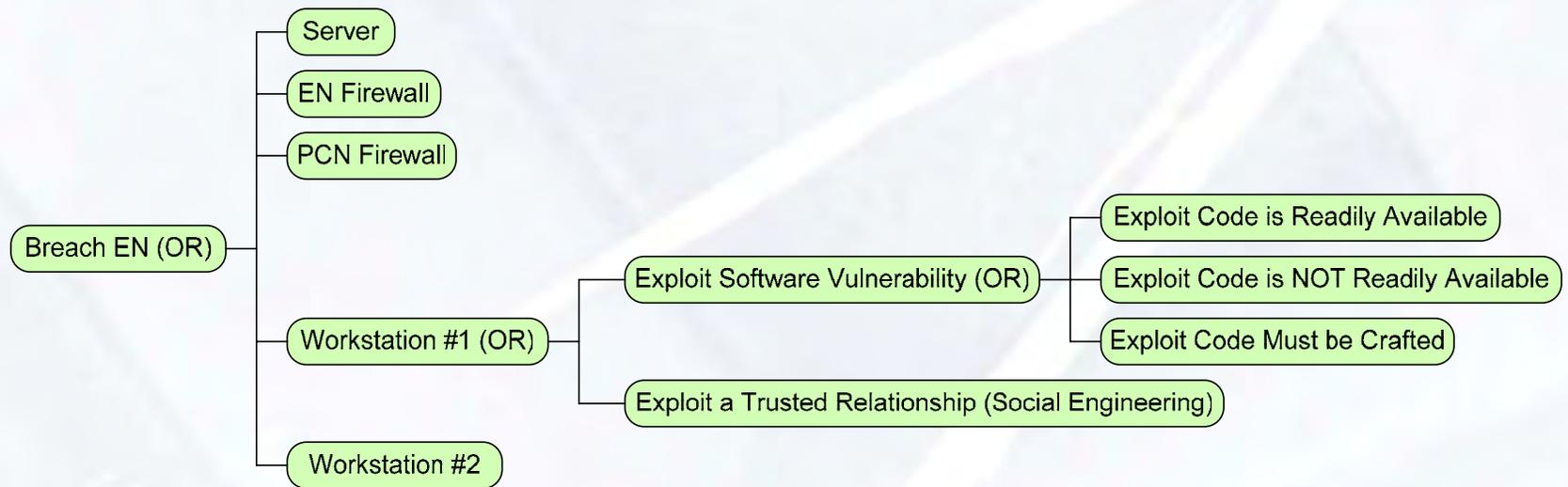
Calculating MTTC – State Space Model

- Decide on a specific set of states that an attacker will go through and create state-space model (SSM):



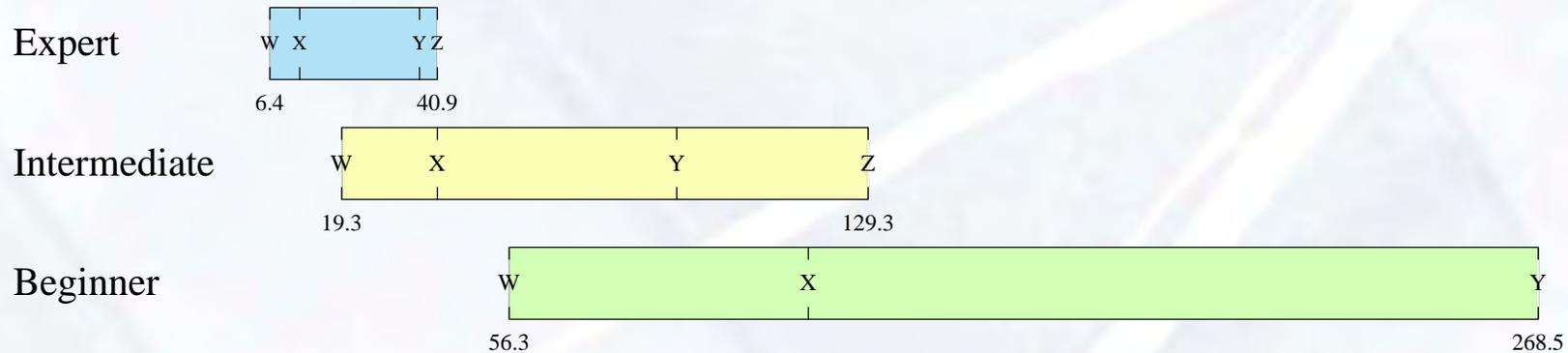
Calculating MTTC – State MTTC

3. Calculate MTTC for each state transition



Calculating MTTC – System MTTC

4. Calculate MTTC for complete system



Legend

- W = Breach to PCN facing firewall and Strike DoS
- X = Breach EN, Breach PCN and Strike DoS
- Y = Breach EN, Breach PCN, Penetrate PCN until saturation and Strike DDoS
- Z = Breach EN, Breach PCN and Strike Control

Confirming and Using MTTC

- 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 than 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?



© 2006 Wurdtech Analytics Inc. – All Rights Reserved

