Estimating Security Risk Using Adversary Capability

David J. Weller-Fahy

2020 MIT STAMP Workshop

2020-08-03

LINCOLN LABORATORY
Massachusetts Institute of Technology

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
This material is based upon work supported by the Federal Aviation Administration under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Federal Aviation Administration.

© 2020 Massachusetts Institute of Technology.

Delivered to the U.S. Government with Unlimited Rights, as defined in DFARS Part 252.227-7013 or 7014 (Feb 2014). Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed above. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.
Outline

- Problem overview
- Capability-based risk
- Comparison with control effectiveness
- Questions and acknowledgements
Outline

• Problem overview
  • Capability-based risk
  • Comparison with control effectiveness
  • Questions and acknowledgements
Assessing Safety Risk of Cyber Attack on Aircraft

• Requested to develop risk assessment methodology for FAA
  – Focus: cyber security impact on safety
  – Flexible enough to assess a range of subjects including components, systems, systems of systems, and processes
  – Can integrate testing as well as analysis
  – Risk matrix preferred as overview of risks

• STPA/STPA-Sec selected as core
Traditional Risk Matrix

- Useful summary when used properly

- Has problems:
  - Not very accurate
  - Hides useful details

- Likelihood has problems
  - Historical rates may not be predictive/available
  - Adversary intent is not measurable
  - Can change rapidly with technology changes/popularity of attack
  - Many others [1]

## Proxies for Likelihood Considered by the Team

<table>
<thead>
<tr>
<th>Proxy</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood of accidents (failure of systems that are cyber-linked)</td>
<td>Some data available, but accidents are not attacks, historical is not predictive</td>
</tr>
<tr>
<td>SME estimations</td>
<td>Bias problems, expertise scarce</td>
</tr>
<tr>
<td>Scalability</td>
<td>Cyber attacks tend to be scalable</td>
</tr>
<tr>
<td>Required adversary capability level</td>
<td>Detailed data not available, requires modeling each scenario</td>
</tr>
</tbody>
</table>
### Considered Proxies for Likelihood

<table>
<thead>
<tr>
<th>Proxy</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Likelihood of accidents (failure of systems that are cyber-linked)</td>
<td>• Some data available, but accidents are not attacks, historical is not predictive</td>
</tr>
<tr>
<td>• SME estimations</td>
<td>• Bias problems, expertise scarce</td>
</tr>
<tr>
<td>• Scalability</td>
<td>• Cyber attacks tend to be scalable</td>
</tr>
<tr>
<td>• Required adversary capability level</td>
<td>• Detailed data not available, requires modeling each scenario</td>
</tr>
</tbody>
</table>
Outline

• Problem overview
• Capability-based risk
• Comparison with control effectiveness
• Questions and acknowledgements
Setting Capability Levels

• Defense Science Board report “Resilient Military Systems and the Advance Cyber Threat”
  – Resource pyramid
  – Six tiers of adversary

• We derived the following categories
  – 1: Novice/Intermediate
  – 2: Proficient
  – 3: Organized Group
  – 4: Lesser Nation State
  – 5: Greater Nation State
Adversary Cyber Capability Levels

- Levels are defined by two characteristics
  - Resources – rough estimates, can be used to acquire competency (external or internal)
  - Competencies – skills necessary to accomplish attacks

- In practice, adversaries will have a mix of both

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Description</th>
<th>Resources and Competencies</th>
</tr>
</thead>
</table>
| 1     | Novice to intermediate | Generally employs capabilities developed by others, with little to no variation. | Resources: <$100K  
Novice: Download and run preexisting vulnerability discovery and remote administration tools; e.g., Metasploit, Nessus, Wireshark.  
Intermediate: Limited ability to modify existing tools to desired application. Limited ability to craft tools to employ known vulnerabilities. |
| 2     | Proficient actors   | Actors that have advanced understanding of a particular area and can generally develop their own solutions using Commercial Off-The-Shelf (COTS) tools and equipment. | Resources: <$1M  
Trained and in possession of well-developed skills. Expanded platform expertise and time resources. Ability to discover and exploit vulnerabilities. Buying moderately priced commercial equipment. |
| 3     | Organized group    | A group of proficient adversaries to leverage individual knowledge of different technical areas. An example would be a terrorist group. | Resources: <$50M  
Large and heterogeneous capability set, both technical and non-technical such as any of the following:  
- Can coerce insiders to cooperate  
- Capable of buying or building custom tools (e.g., aircraft; transmitters) |
| 4     | Lesser Nation State| An adversary that can bring national level resources to multiple groups under its direction. They may not have access to the most advanced national-level assets. | Resources: <$1B  
Create vulnerabilities through influencing design, development, manufacturing or supply chain |
| 5     | Greater Nation State| Adversaries at the bleeding edge of development, national resources, and organizational integration. | Resources: $1B+  
Boundary pushing technical development in conjunction with effective espionage and military operations. |

- Adversary cyber capability levels provide tiers, but not specific capabilities
Capability Level != Capability

• Questions to answer:
  – Where does one find a list of capabilities?
  – How does one determine *which* capabilities matter for a given scenario or set of scenarios?
  – How does one determine the necessary capability level if multiple capabilities are required for a scenario?

• Answers to questions:
  – There was no central list, so we created one that is intended to be a constant work in progress
  – Model the scenario in some way – attack trees are a reasonable way to model each individual scenario
  – Use the highest capability level required to complete the scenario (the maximum value of all the *required* capabilities)
Cyber Capabilities

- Collaborators from the penetration testing and reverse engineering communities provided the initial list

- Added to the list as assessments were completed

- Contact FAA ANG-E2 for the current list (sample shown below)

<table>
<thead>
<tr>
<th>Capability Type</th>
<th>Title</th>
<th>Description</th>
<th>Required Adversary Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expertise</td>
<td>Avionics testbed development</td>
<td>Development of components and diagnostic tools. High-level assets needed.</td>
<td>3</td>
</tr>
<tr>
<td>Expertise</td>
<td>Network attack</td>
<td>Unsecured network</td>
<td>1</td>
</tr>
<tr>
<td>Expertise</td>
<td>Network attack</td>
<td>Network deployed with industry standard user authentication and intrusion detection</td>
<td>2</td>
</tr>
<tr>
<td>Expertise</td>
<td>Network attack</td>
<td>Network configured to enforce least privilege, service isolation, data isolation, and incidence response</td>
<td>3</td>
</tr>
<tr>
<td>Expertise</td>
<td>Cryptanalysis</td>
<td>Deploy commercially available decryption tools</td>
<td>2</td>
</tr>
</tbody>
</table>
• Attack trees
  – Successful attack at the root
  – Capabilities required to execute the attack at the leaves

• Capability levels
  – Assigned to each capability
Adversary level required for this scenario

- Develop malicious software requires an organized group (3)
- Defeat software verification requires a proficient actor (2)
- Network attack requires a proficient actor (2)
- AND = max of the inputs
Outline

• Problem overview
• Capability-based risk
• **Comparison with control effectiveness**
• Questions and acknowledgements
Adversary Level vs. Control Effectiveness

- **Adversary Level**
  - Corresponds to ease with which an adversary can realize hazard
  - Based on capabilities required to accomplish attack
  - Can lead to better understanding of adversarial loss scenarios
  - Only applicable to analyses that address adversarial causal factors

- **Control Effectiveness**
  - Corresponds to the strength of the control used to prevent a loss
  - Based on the level by which the causal factor is affected by the control
  - Can lead to better understanding of loss scenarios
  - Applicable to any analyses that address causal factors using controls
Or Adversary Level with Control Effectiveness?

- Control effectiveness is based on how well the hazard can be controlled

- Adversary level is based on how capable an adversary must be to bypass controls

- Perhaps use both when dealing with analyses accounting for adversarial action?
  
  - “Control X reduces causal factor B (level 2 control effectiveness), and requires an adversary level 3 (organized group) to be bypassed”
Outline

• Problem overview
• Capability-based risk
• Comparison with control effectiveness
• Questions and acknowledgements
Questions?

Team Members:

• MIT Lincoln Laboratory
  – Rodolfo Cuevas
  – Gabriel Elkin
  – Tom Jagatic
  – Dr. Melva James
  – Dr. Michael McPartland
  – Dr. Eric Quintero
  – David Weller-Fahy

• Astronautics Corporation of America
  – Beau Branback
  – Kathleen Finke
  – Christopher Kerr
  – Elijah Liu
  – Joe Reisinger

• Diakon Solutions
  – Bill Trussell

• FAA
  – John Peace
  – Isidore Venetos

For any questions not answered within this presentation, feel free to contact me at djwf@ll.mit.edu