Asset Centric Threat Modeling

ISSA-Utah Fall Seminar 2016

September 22, 2016

Reed Stone
Cyber Threat Intelligence
Reed.Stone@inl.gov
This is for entertainment only. I am just up here vibrating air molecules. If they happen to have any meaning to you it is merely a coincidence. Ok, perhaps I am not that disowning of my ideas; bust seriously folks these are my ideas and not an endorsement of them by the US government or my employer. I reserve the right to change my mind as well.
I recently revisited the Strengths Finder by Tom Rath. I think sharing my results will help you understand the perspective from which I came at the threat modeling problem. Learning excites me. For me it is about the journey not the destination. The entire process is fantastic, when I struggle to understand a new or foreign idea I experience great and rewarding growth. Along with that I love highly technical and precise language of the intellectuals, the more in over my head the better. To facilitate my learning I gather all types of data. Exploring these repositories is like finding a new world with interesting things around every corner. In my mind nearly all things are related. Ideas, concepts, and principles have relationships, understanding these relationships how they work, how they are broken, how compatible or at odds they are with each other facilitates my learning. There are few coincidences in life.

I have a hard time when things are broken or incompatible. I have this drive to fix things, particularly with things of the mind, from intellectual concerns to health, I am one who performs rescue.
Overview

• Context
  – Where Threat Modeling Fits
  – Disparate Models and Ad Hoc Collections
• Examining the Asset/Understanding Data
• Using the Data landscape Model
• Down the Rabbit Hole
• Take away
• Future Work
There is a lot to unpack on this slide. Threat modeling is a high maturity process. If you have an established cyber security program, you are in the continuous improvement phase and you want to take your risk assessments and system security baselines to the next level it is time to consider it.

Cyber Security Program overview:

On the far left and top are the four external feeders to a cyber security program: *Best Practices*, *Laws and Regulations*, *Contractual Obligations*, and Threats with associated mitigations from *Threat Analysis*.

These feed in to a catalog (*Unified Cyber Security Policy Catalog*) of all the things a cyber security program could do.

From this list of all the things a cyber security program could do a subset is selected as those things your cyber security program will do (*Cyber Security Program Description*) items not selected become accepted programmatic risk.

This cyber security program is then executed and monitored with deltas between what you intend to do and reality being identified as risks. During the process of performing risk analysis new previously unidentified threat actions and potential mitigations or other improvements may be identified.

*Risk Collection and Analysis* and *Potential Improvement Prioritization and Scheduling* close the feedback loop by incorporating improvements into the cyber security program.
Threat Modeling is not an essential part of a basic risk assessment but is used to provide an additional level of assurance to the rigor of the assessments. Threat modeling is done in addition to the more essential gap analysis between the evaluated target and applicable components within the Cyber Security Program Description.
Efforts to identify fundamental aspects of information security have been to collect best practices and security principles and to assign them to groups of similar items. While helpful the wide range of separate methods.
Ad Hoc Collections of Security Principles (cont.)

CIS Critical Controls
- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring, and Analysis of Audit Logs
- Email and Web Browser Protections
- Malware Defenses
- Limitation and Control of Network Ports, Protocols, and Services
- Data Recovery Capability
- Secure Configurations for Network Devices such as Firewall Routers, and Switches
- Boundary Defense
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

Other Standards
- CoBiT
- NERC
- ISF Standard of Good Practice
- ITIL Security Management
- IT-Grundschutz-Kataloge
- PCI-DSS
- Katakri
- And many more

Examples of other collections
Many Information security models exist as well. While most are very solid, they are separate, existing on their own, lacking connectedness and relations to other models.
Is there a better way to organize and align both controls and models? In physical security we look at our protected asset, say a building and identify its attributes, behaviors, and all the ways it is interacted with (entry and exit points, etc.). If there is an underlying structure we need to look at the asset we wish to protect (data) and identify its attributes, behaviors, and interactions.

Data can exist as inactive data to maintain a record or can be of an executable type to perform actions.

It can be communicated, interacts with people and exists in some physical form.

It has the attributes of CIA and is protected by AAA.
Viewing the environment of data pictorially looks like this.

There is a dependency like nature that exists between each layer. In information systems, it is seldom that data is interacted without some executable program mediating that action. In order for an executable object to mediate an action, it must be communicated with. These will all to exist physically and be accessible to authorized personnel.

While managers are persons too (and thus are firmly in the Personnel Domain), their actions that set the tone for corporate culture are distinctly different from personnel security concerns. It is this corporate culture that insulates your environment from the rest of the world.
Populating the Landscape

Populating starts on next slide
1. Here we see the same pyramid shaped model looking down from the top.

2. CIA is of course applicable to data.

3. CIA is also applicable to these other domains.

4. After we start talking about execution we are talking about interactions. These interactions are controlled using AAA and while these each have a dependency on the data domain these dependencies only relate to CIA within that domain (i.e. the data domain)

5. AAA also has its analogs in the other domains. This is the computing environment prior to the internet.

6. With the addition of internet connectivity we put in place a way to circumvent our physical and personnel controls while at the same time enabling business transactions like never before.

7. Cloud commuting is much closer to our protected asset (data) circumventing almost all of our own controls. While this further enables business transactions we have to be aware of the risk this presents.

8. Each attribute can be attacked. If we number each attack we find there are 27 basic threats.
## 27 Basic Threats

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Security Objective</th>
<th>Compromise Tactic</th>
<th>Data Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loss or destruction of data</td>
<td>Data</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>2</td>
<td>Data leaked or disclosed</td>
<td>Data</td>
<td>Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>3</td>
<td>Data corruption (including introduction of unauthorized or falsified data)</td>
<td>Data</td>
<td>Manipulation</td>
<td>Integrity</td>
</tr>
<tr>
<td>4</td>
<td>Information system outage or degradation of service</td>
<td>Execution</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>5</td>
<td>Unauthorized access to software or system</td>
<td>Execution</td>
<td>Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>6</td>
<td>Misuse of software functions</td>
<td>Execution</td>
<td>Manipulation</td>
<td>Integrity</td>
</tr>
<tr>
<td>7</td>
<td>Bypass software authentication functions</td>
<td>Execution</td>
<td>Masquerading</td>
<td>Authorization</td>
</tr>
<tr>
<td>8</td>
<td>Bypass software authorization functions</td>
<td>Execution</td>
<td>E0P</td>
<td>Authorization</td>
</tr>
<tr>
<td>9</td>
<td>Bypass software accountability functions</td>
<td>Execution</td>
<td>Reputation</td>
<td>Accountability</td>
</tr>
<tr>
<td>10</td>
<td>Degradation or disruption of communications</td>
<td>Communication</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>11</td>
<td>Interception or monitoring of communications</td>
<td>Communication</td>
<td>Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>12</td>
<td>Corruption or falsification of communications</td>
<td>Communication</td>
<td>Manipulation</td>
<td>Integrity</td>
</tr>
<tr>
<td>13</td>
<td>Bypass communication authentication methods</td>
<td>Communication</td>
<td>Masquerading</td>
<td>Authorization</td>
</tr>
<tr>
<td>14</td>
<td>Bypass communication accountability methods</td>
<td>Communication</td>
<td>Reputation</td>
<td>Accountability</td>
</tr>
<tr>
<td>15</td>
<td>Degradation or disruption of authorized physical access or functions (e.g. facilities, HVAC, power, media, hardware)</td>
<td>Physical</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>16</td>
<td>Unauthorized access to physical assets including information system hardware and media</td>
<td>Physical</td>
<td>Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>17</td>
<td>Unauthorized manipulation of physical assets</td>
<td>Physical</td>
<td>Manipulation</td>
<td>Integrity</td>
</tr>
<tr>
<td>18</td>
<td>Bypass physical authentication methods</td>
<td>Physical</td>
<td>Masquerading</td>
<td>Authorization</td>
</tr>
<tr>
<td>19</td>
<td>Bypass physical authorizations or introduce unauthorized physical assets</td>
<td>Physical</td>
<td>E0P</td>
<td>Authorization</td>
</tr>
<tr>
<td>20</td>
<td>Physical destruction or destroy physical accountability controls and records</td>
<td>Physical</td>
<td>Reputition</td>
<td>Accountability</td>
</tr>
<tr>
<td>21</td>
<td>Physical destruction or destroy physical accountability controls and records</td>
<td>Physical</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>22</td>
<td>Personnel unable to perform job functions</td>
<td>Personnel</td>
<td>DoS</td>
<td>Availability</td>
</tr>
<tr>
<td>23</td>
<td>Personnel are manipulated, coerced, recruited or make unintentional errors</td>
<td>Personnel</td>
<td>Manipulation</td>
<td>Integrity</td>
</tr>
<tr>
<td>24</td>
<td>Bypass or compromise personnel identity proofing, back ground check, ID check etc.</td>
<td>Personnel</td>
<td>Masquerading</td>
<td>Authorization</td>
</tr>
<tr>
<td>25</td>
<td>Bypass personnel authorization controls</td>
<td>Personnel</td>
<td>E0P</td>
<td>Authorization</td>
</tr>
<tr>
<td>26</td>
<td>Claims untrue intentions and/or motives</td>
<td>Personnel</td>
<td>Reputition</td>
<td>Accountability</td>
</tr>
</tbody>
</table>
These core functions have been identified for some time but their relationships have not been well understood.

NIST defines the cyber core functions as Know, prevent, detect, respond, and recover. It does not address demonstrating stewardship to stakeholders nor does it close the feedback loop for continual improvement.

My view differs from NIST by not including response and recovery as core functions. While these are essential they are follow on activities to the core functions of prevention and detection.
Walkthrough of identifying threat actions and posable mitigations involving USB flash media.
Taking the model much further than we have already is not recommended for day to day threat analysis. It is useful to stress the model as it can provide interesting data that will help us learn about how to best use it. Voids, overlaps, duplication and empty cells will teach us both new things about the model and about our current knowledge. Taking it further may also be useful for the development of security standards.
Kill chain developed by Lockheed Martin was taken and adjusted slightly to be more accommodating to the personnel and physical security domains.
Each of the 27 Basic Threats can be broken down further in to Threat Stages. These in turn can be analyzed to identify specific threat actions, related preventative and detective controls along with measures to gauge their efficacy and continued relevance. As a four dimensional model it is a bit more difficult to navigate and thus is not recommended for daily use but it does provide a more fine grained framework that would be beneficial for standards development. Something I am currently working on.
This is something I have slated to do in my free time. I have meet with Sean Barnum, the MITRE architect behind CWE and ATT&CK. He is currently working on merging these two datasets and, I believe, is going to reflect the attack side of each weakness. My work should compliment this quite nicely. Time will tell.
The Take Away

- Don't have an aneurism. Use the data landscape model.
- More natural security domain boundaries facilitate:
  - Threat modeling and risk analysis
  - Communication with Non-cyber experts
  - Defining boundaries and interfaces with other security fields
- Don't be think of the framework as ridged boundaries it is more of a suggestion to aid the mind

[Intentionally left blank, except for me telling you that it is blank which means it is not blank]
Questions?