



Asset Centric Threat Modeling

ISSA-Utah Fall Seminar 2016

September 22, 2016

Reed Stone
Cyber Threat Intelligence
Reed.Stone@inl.gov

www.inl.gov



INL
Idaho National
Laboratory



Disclaimer

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

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; but 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.



About Me

- Reed Stone, Idaho National Laboratory
 - Cyber Threat Intelligence Program
 - Over a decade in InfoSec
 - CISSP, GWAPT
 - Learner, Intellection, Input, Connectedness, Restorative



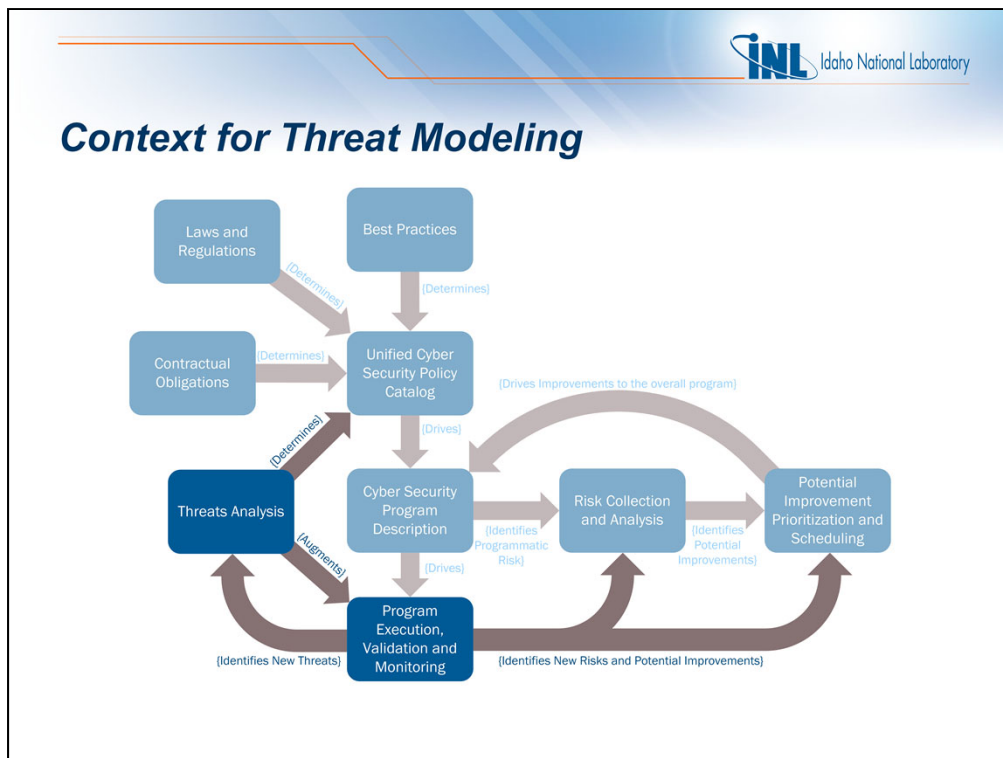
I recently revisited the Strengths Finder by Tom Rath. I think sharing my results will help you understand the perspective from which I came at the threat modeling problem. Learning excites me. For me it is about the journey not the destination. The entire process is fantastic, when I struggle to understand 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*.



Ad Hoc Collections of Security Principles

<p>(ISC)^2</p> <ul style="list-style-type: none"> • Security and Risk Management • Asset Security • Security Engineering • Communication and Network Security • Identity and Access Management • Security Assessment and Testing • Security Operations • Software Development Security 	<p>NIST SP 800-53</p> <ul style="list-style-type: none"> • Access Control • Awareness and Training • Audit and Accountability • Certification, Accreditation and Security Assessments • Configuration Management • Contingency Planning • Identification and Authentication • Incident Response • System Maintenance • Media Protection • Security Planning • Risk Assessment • System and Services Acquisition • System and Communications • System and Information Integrity 	<p>ISO 27001</p> <ul style="list-style-type: none"> • Information Security Policies • Organization of information security • Human resources security • Asset management • Access control • Cryptography • Physical and environmental security • Operations security • Communications security • System acquisition, development and maintenance • Supplier relationships • Information security incident management • Information security aspects of business continuity management • Compliance
---	--	---

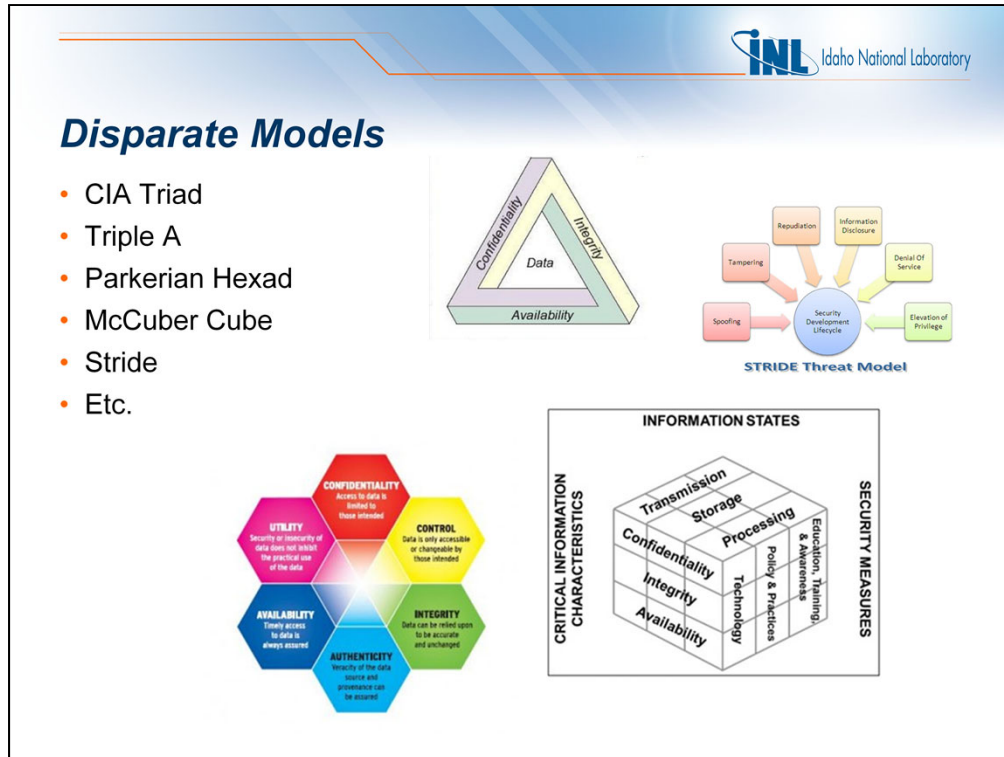
Efforts to identify fundamental aspects of information security have been to collect best practices and security principles and to assign them to groups of similar items. While helpful the wide range of separate methods.




Ad Hoc Collections of Security Principles (cont.)

CIS Critical Controls	Other Standards
<ul style="list-style-type: none">• Inventory of Authorized and Unauthorized Devices• Inventory of Authorized and Unauthorized Software• Secure Configurations for Hardware and Software on Mobile Device Laptops, 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	<ul style="list-style-type: none">• 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.



Examining the Asset

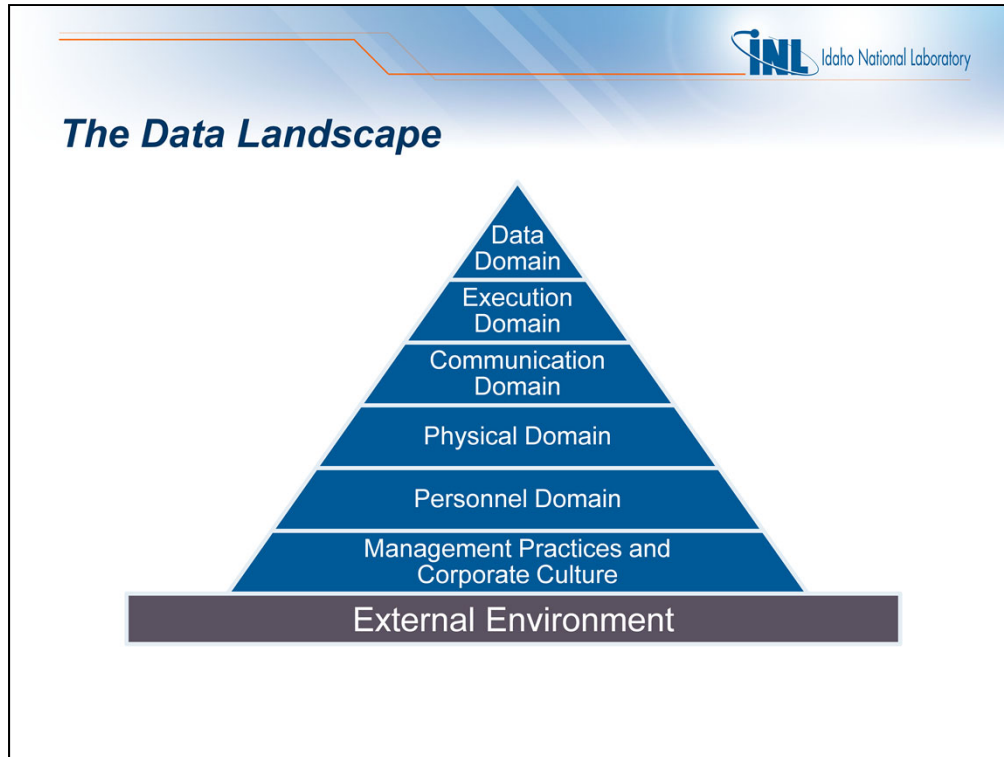
- What is data?
- What behaviors surround data?
- What other attributes are important to data?
- Data Related Actions
 - Create (write)
 - Read
 - Copy
 - Modify
 - Execute
 - Delete
- Environment of Data
 - Physical
 - People
 - Communicated
- Attributes of Data
 - Availability
 - Integrity
 - Confidentiality
- Protective Measures
 - Authorization
 - Authentication
 - Accountability

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.



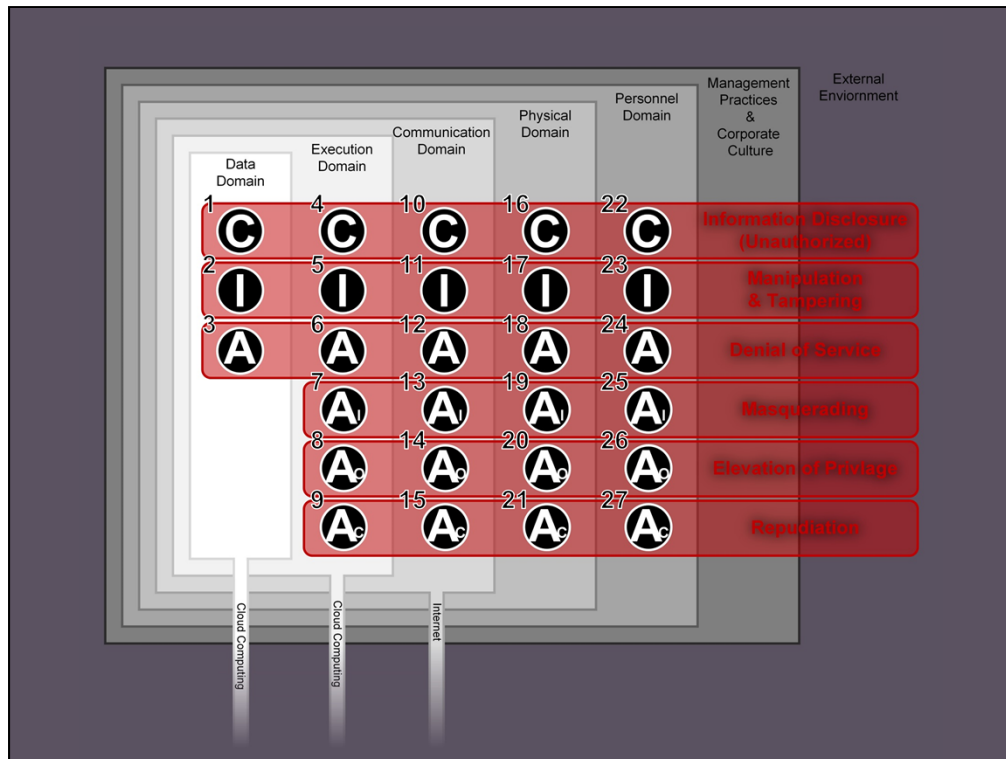
Viewing the environment of data pictorially looks like this.

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 exist physically and be accessible to authorized personnel.

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



Populating starts on next slide

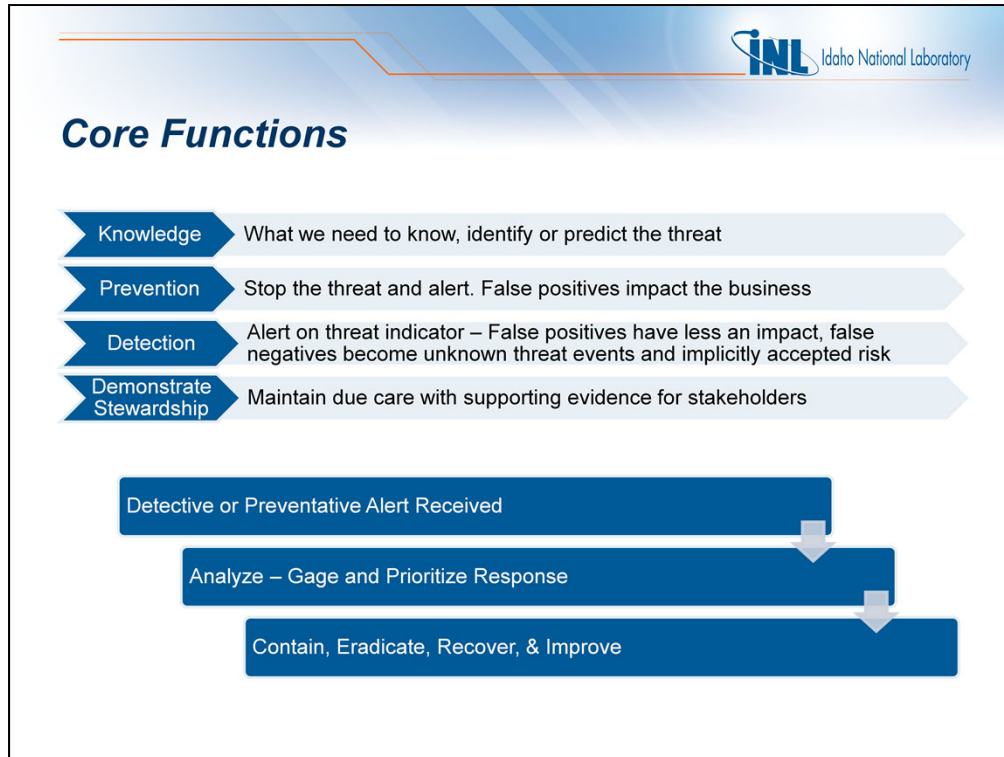


1. Here we see the same pyramid shaped model looking down from the top.
2. CIA is of course applicable to data.
3. CIA is also applicable to these other domains.
4. After we start talking about execution we are talking about interactions. These interactions are controlled using AAA and while ,yes, these 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

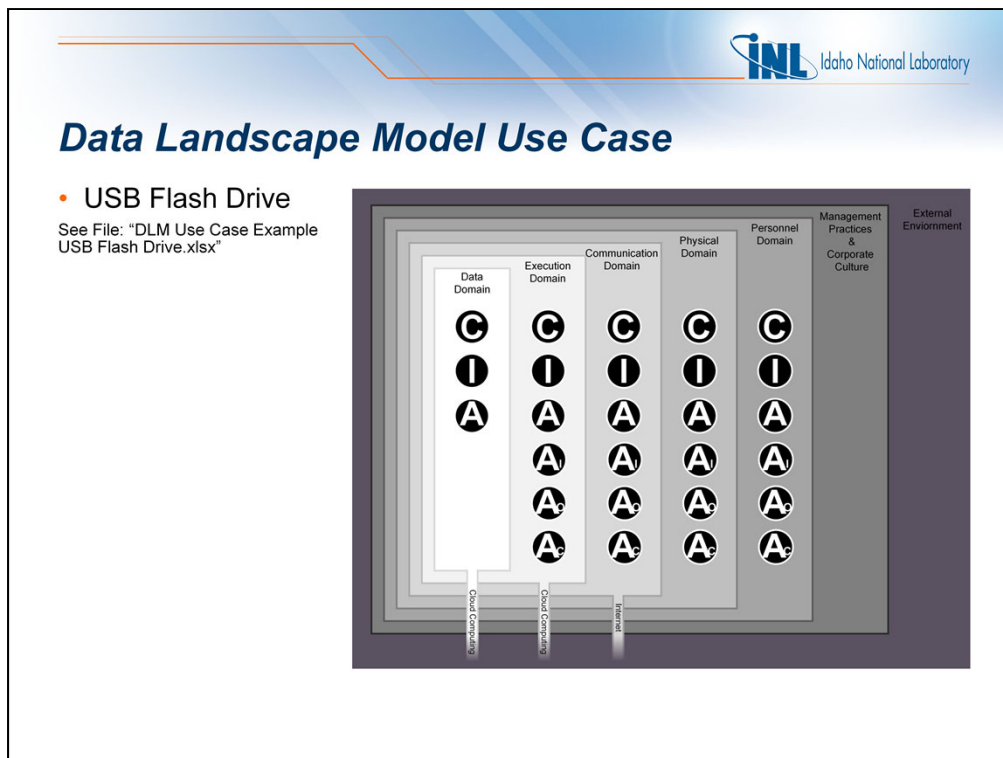
Index #	Description	Security Domain	Compromise Type	Data Attribute
1	Loss or destruction of data	Data	DoS	Availability
2	Data leaked or disclosed	Data	Disclosure	Confidentiality
3	Data corruption (including introduction of unauthorized or falsified data)	Data	Manipulation	Integrity
4	Information system outage or degradation of service	Execution	DoS	Availability
5	Unauthorized access to software or system	Execution	Disclosure	Confidentiality
6	Misuse of software functions	Execution	Manipulation	Integrity
7	Bypass software authentication functions	Execution	Masquerading	Authentication
8	Bypass software authorization functions	Execution	EoP	Authorization
9	Bypass software accountability functions	Execution	Repudiation	Accountability
10	Degradation or disruption of communications	Communication	DoS	Availability
11	Interception or monitoring of communications	Communication	Disclosure	Confidentiality
12	Corruption or falsification of communications	Communication	Manipulation	Integrity
13	Bypass communication authentication methods	Communication	Masquerading	Authentication
14	Bypass communication authorization methods	Communication	EoP	Authorization
15	Bypass communication accountability methods	Communication	Repudiation	Accountability
16	Degradation or disruption of authorized physical access or functions (e.g. facilities, HVAC, power, media, hardware)	Physical	DoS	Availability
17	Unauthorized access to physical assets including information system hardware and media	Physical	Disclosure	Confidentiality
18	Corruption or manipulation of physical assets	Physical	Manipulation	Integrity
19	Bypass physical authentication methods	Physical	Masquerading	Authentication
20	Bypass physical authorizations or introduce unauthorized physical assets	Physical	EoP	Authorization
21	Dispute, avoid or destroy physical accountability controls and records	Physical	Repudiation	Accountability
22	Personnel unable to perform job functions	Personnel	DoS	Availability
23	Insider personnel are known, monitored, and targeted	Personnel	Disclosure	Confidentiality
24	Personnel are manipulated, coerced, recruited or make unintentional errors	Personnel	Manipulation	Integrity
25	Bypass or compromise personnel identity proofing, back ground check, ID check etc.	Personnel	Masquerading	Authentication
26	Bypass personnel authorization controls	Personnel	EoP	Authorization
27	Claim untrue intentions and/or motives	Personnel	Repudiation	Accountability




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.



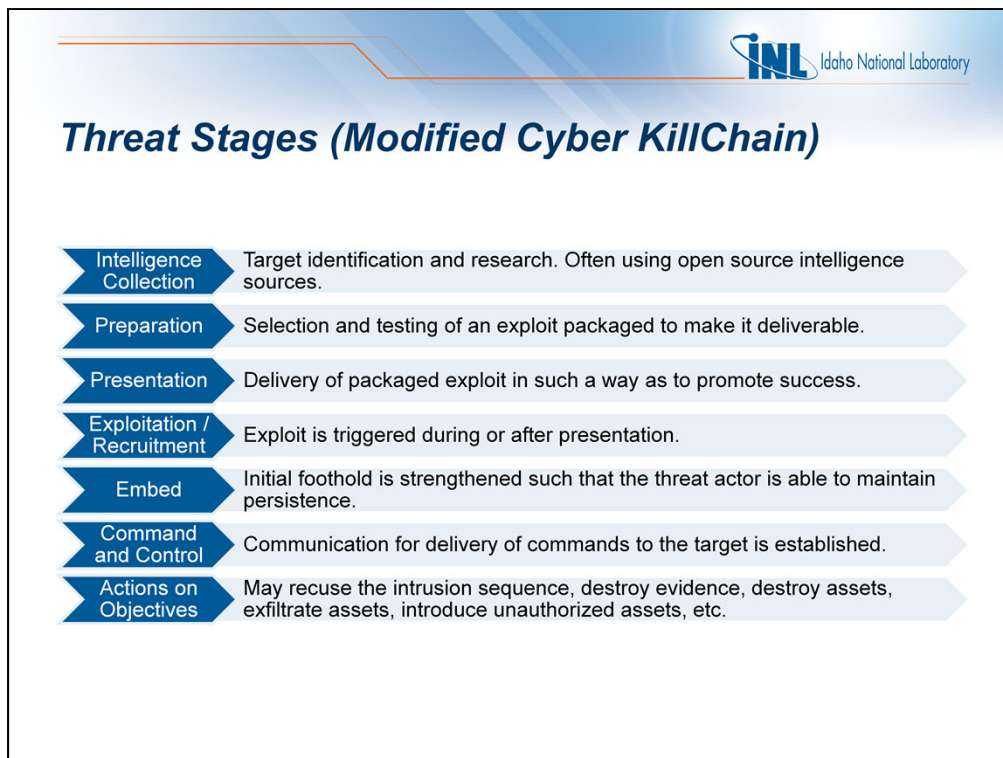
Walkthrough of identifying threat actions and posable mitigations involving USB flash media.



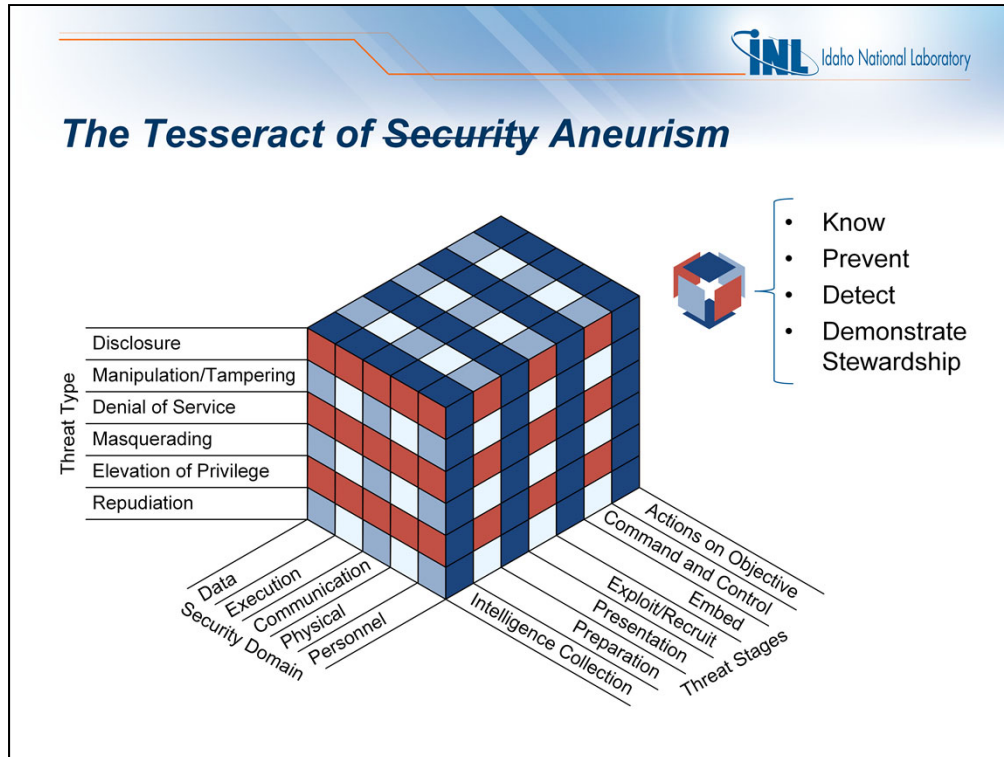
Down the Rabbit Hole – Current & Future Work

- Adding a Fourth Dimension
- Adding Data Sets


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.



Populating Datasets

- Data from MITRE
 - Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
 - 121 techniques organized according to threat stages
 - Common Weakness Enumeration (CWE)
 - Approximately 1000 types of technology weaknesses

This is something I have slated to do in my free time. I have met 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?