RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-R04

Using an Open Source Threat Model for Prioritized Defense

James Tarala

Principal Consultant
Enclave Security
@isaudit

Problem Statements

- In information assurance today, there are no clear taxonomies for threat
- If we cannot understand threats, how can we possibly decide how best to defend ourselves?
- Unclear definitions of threat lead to unclear architectures for defense
- If we cannot agree what threats face our systems, how can we possibly agree on how best to defend ourselves?

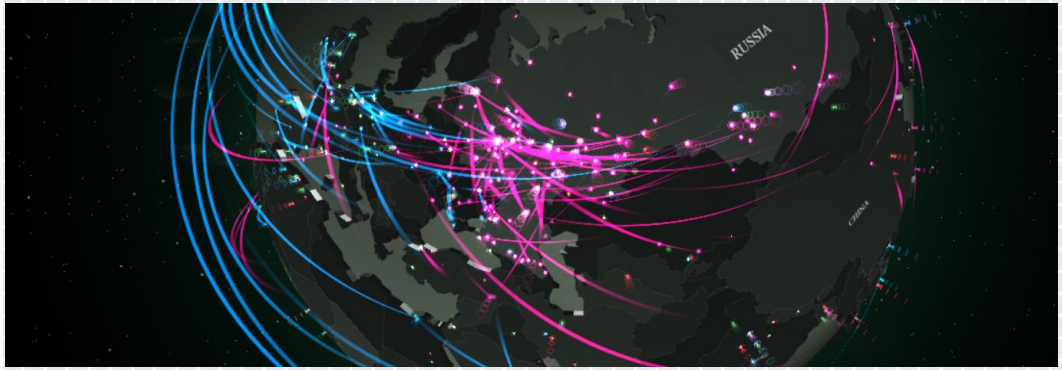
Threat Defined (NIST)

- NIST 800-30 (rev1):
  - "A *threat* is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."

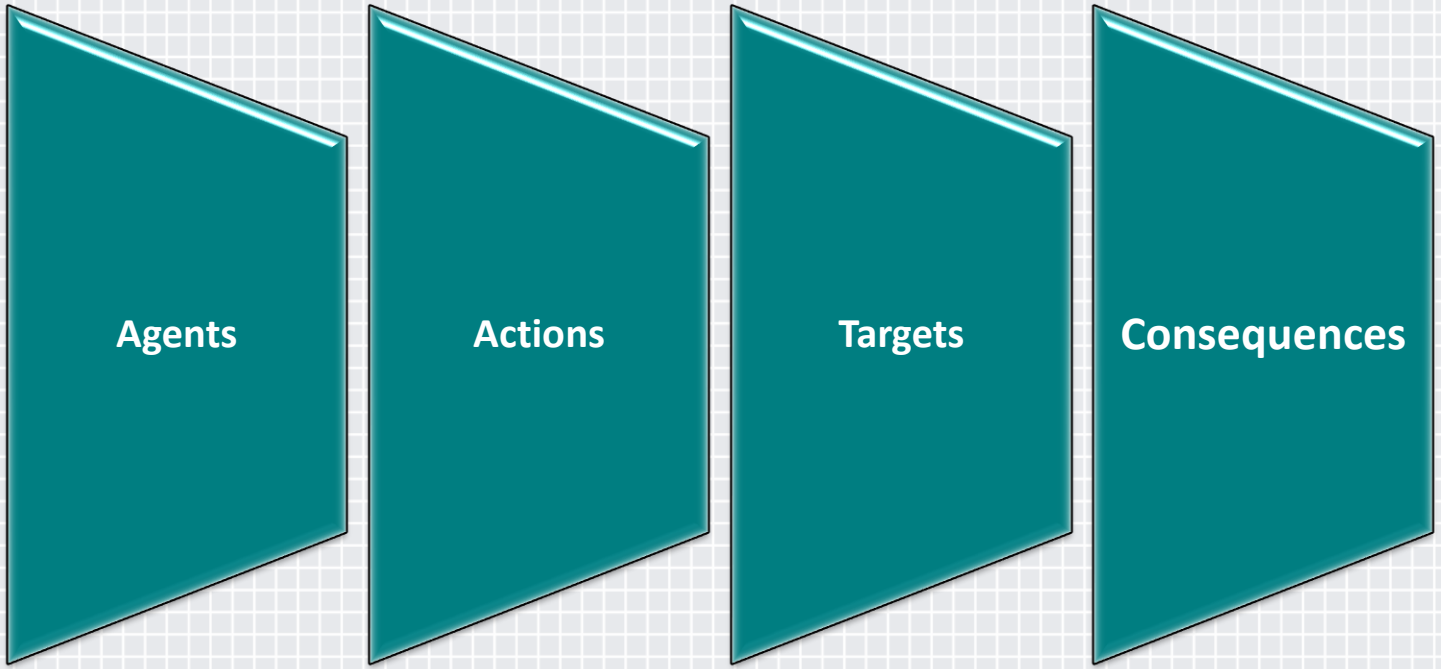
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

The Behavior of Threat

"Threat ***agents*** perform threat ***actions*** against threat ***targets*** in order to cause threat ***consequences***."



Components of Threats



Threat Agent Catalog

- Nation States
- Criminal Groups
- Corporate Competitors
- Hacktivists
- Mischievous Individuals
- Malicious Insiders
- Unintentional Humans
- Well-intentioned Insiders
- Mother Nature

Threat Definition Leads to Control Definition

- By defining threats we can understand those agents with the potential to cause harm to an organization
- By necessity, threat definition leads to control (countermeasure) definition
- If we can understand those things that can harm an organization (threats), we can identify controls to protect the organization from those threats becoming reality
- Therefore a better understanding of threat leads to the selection of better defenses for our organizations

Control Selection Example: Whitelisting

- Sample threat: Malicious Code
- Sample control: Application Whitelisting
- Sample consequence: Data Theft

- Scenario:
  - An organization is fearful that malware will execute on their workstations and steal data from their systems
  - The threat (malware) must be allowed to execute in order for the consequence to become reality
  - Therefore the organization deploys application whitelisting to block the execution of unknown software code

Questions to Consider About Threat

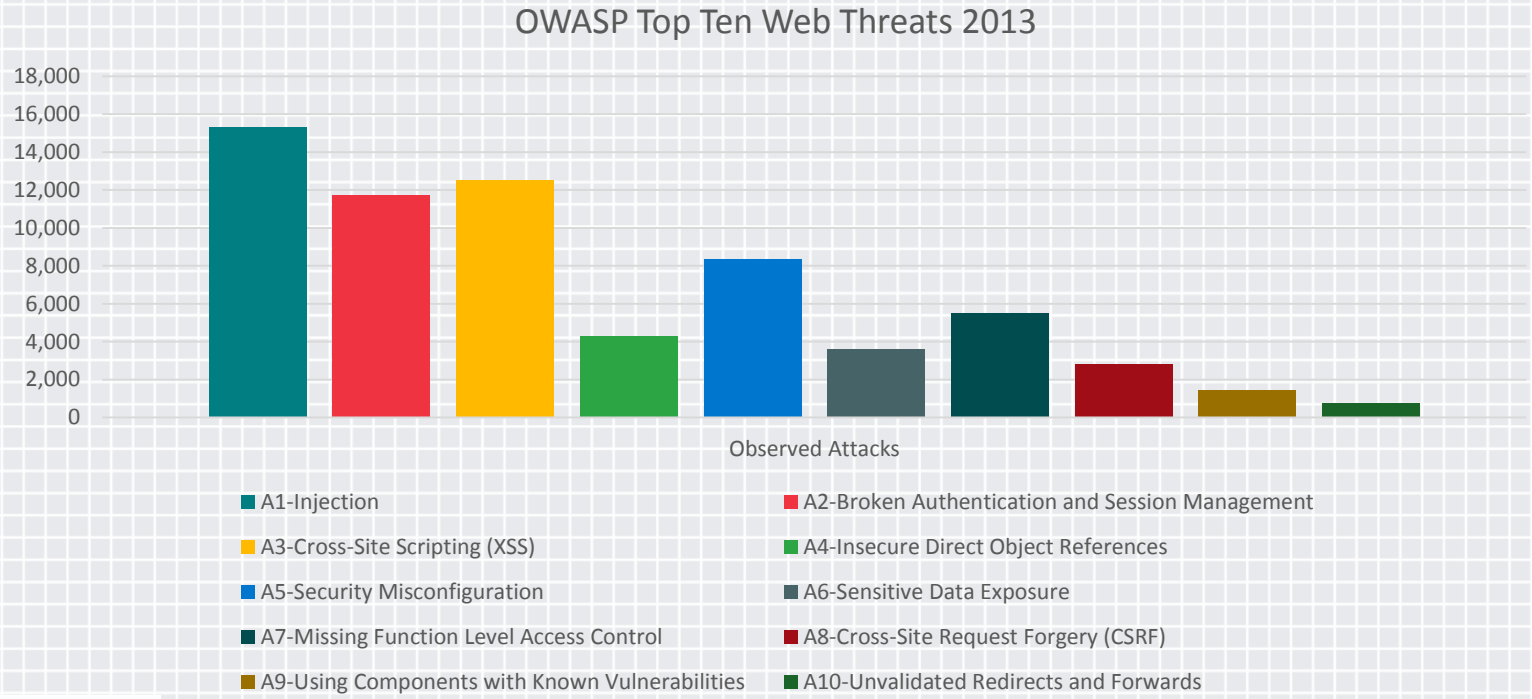
- However, is there a point of diminishing returns when it comes to the knowledge of specific threats?
- Is more information truly useful when defending ourselves?

- Organizations should consider therefore:
  - Do up to date threat agents modify control selection?
  - Do we need to know specific threat agents?
  - Does threat intelligence change behavior?
  - Is a relatively comprehensive list of threats sufficient for control selection?

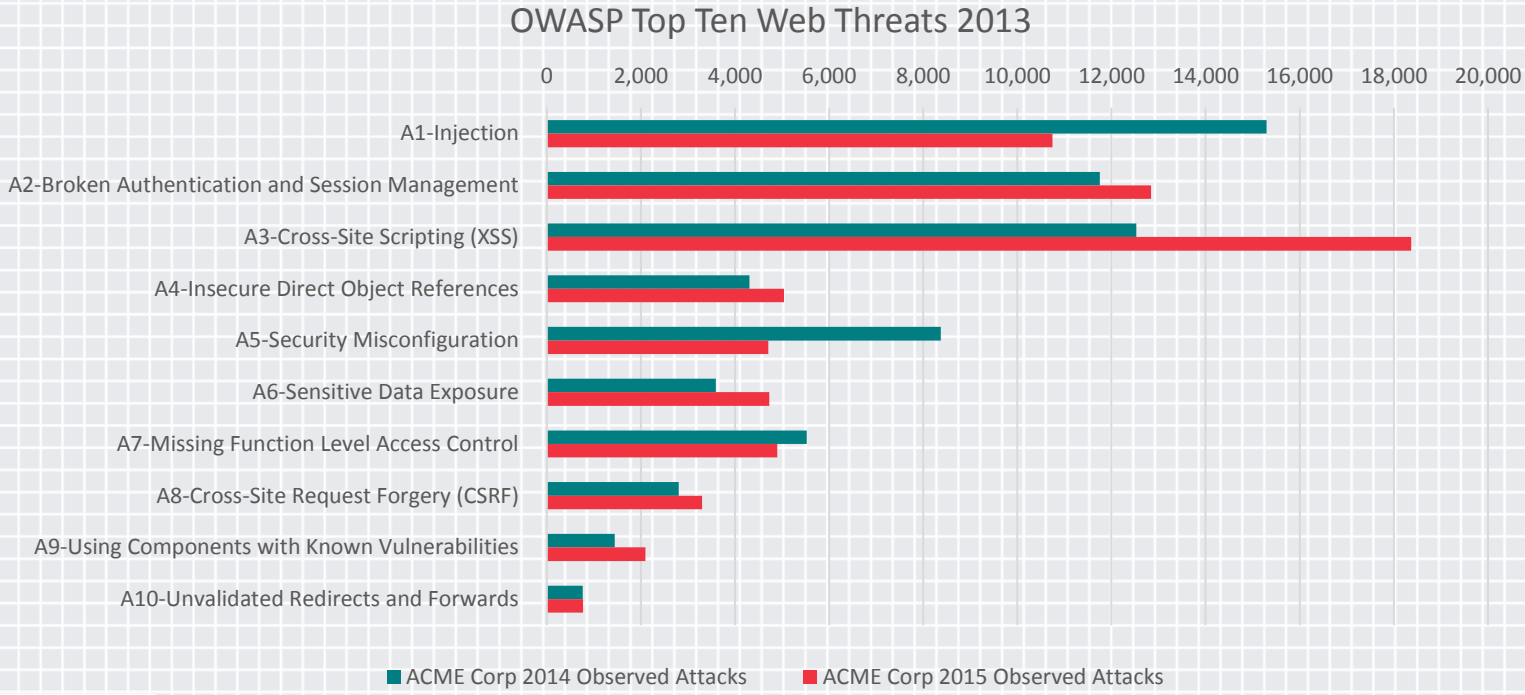
Case Study: Web Server Attacks

- OWASP Top Ten Web Threats 2013
  - A1-Injection
  - A2-Broken Authentication and Session Management
  - A3-Cross-Site Scripting (XSS)
  - A4-Insecure Direct Object References
  - A5-Security Misconfiguration
  - A6-Sensitive Data Exposure
  - A7-Missing Function Level Access Control
  - A8-Cross-Site Request Forgery (CSRF)
  - A9-Using Components with Known Vulnerabilities
  - A10-Unvalidated Redirects and Forwards

Case Study: Web Server Attacks (cont)



Case Study: Web Server Attacks (cont)



Case Study: Web Server Attacks (cont)

- In light of the data observed, let's answer the following questions:
  - Should this organization implement a web application firewall?
  - Should this organization scan their applications for vulnerabilities?
  - Do you believe the organization's defenses should change in light of what has been observed?
  - Is the threat data useful when determining which controls to implement?
  - How heavily should an organization value likelihood scores when measuring risk?

Case Study: Web Server Attacks (cont)

- So what can we learn in light of this discussion?
  - Although attack frequencies may vary, if an attack exists controls need to be considered to defend against the attack
  - Not implementing controls for known threats represent risk
  - Just because a risk is lower, it does not mean an organization is safe if they choose not to implement sufficient controls
  - Documented prioritizations are not a valid defense

Proposed Solution

- An Open Source Threat Taxonomy

- Organizations need to benefit of community knowledge of threats to help them determine how best to defend themselves
- The community should be able to create:
  - A common list of identified threats
  - Rankings of identified threats based on industry wide research
  - This should naturally lead to a common control model for defense

- Organizations are not that special, threats are more common than we think

Goals of the Project

- To create an open source, community driven threat taxonomy

- Specifically we will define:
  - Categories of Threats
  - A Hierarchy of Threats
  - Specific Threat Inventory / Taxonomy
- Provide documentation to promote a common language
- The project will focus on threat only – not vulnerability or risk
- Practicality, not academics, is driving the effort

Taxonomy Defined

tax·on·o·my

/takˈsänəmē/

noun BIOLOGY

noun: **taxonomy**

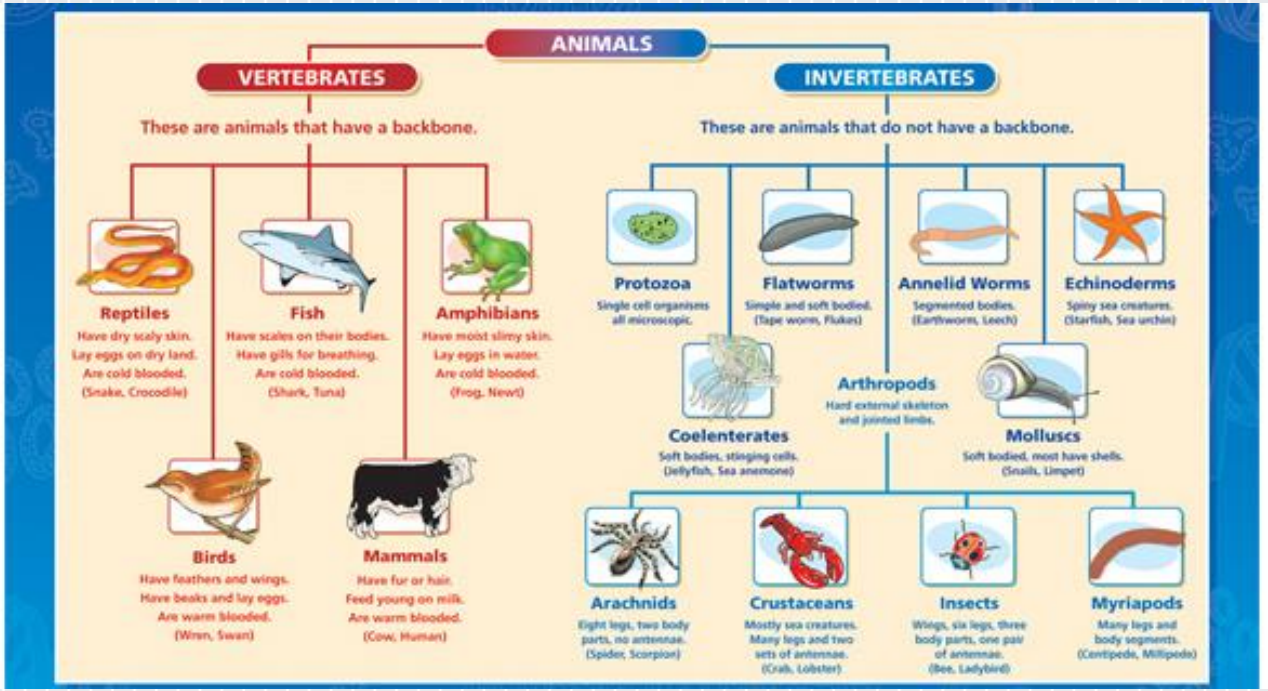
the branch of science concerned with classification, especially of organisms; systematics.

- the classification of something, especially organisms.
  "the taxonomy of these fossils"
- a scheme of classification.
  plural noun: taxonomies
  "a taxonomy of smells"

Origin

GREEK taxis — arrangement
GREEK -nomia — distribution
→ FRENCH → taxonomy
early 19th century

Taxonomy Example from Science



Who This Project Impacts

- Threat Modelers
  - Provide a common taxonomy to map threat models against
- Control Definers
  - Define threats in order to define appropriate controls
- Risk Managers
  - Define threats so each organization can tweak priorities (not have to create it from scratch themselves)
  - Everyone is only a ***little*** unique

Relevant Industry Research

- Numerous Industry Threat Reports
  (Verizon, Microsoft, Symantec, Sophos, etc.)
- MITRE CAPECs
- OWASP WASCs
- NIST 800-30 (rev1)
- CMUSEI Taxonomy of Operational Risk
- Cambridge Centre for Risk Studies
- General Motors Concentric Vulnerability Map
- Treasury Board of Canada - Guide to Risk Taxonomies

High Level Threats Defined

- At a high level the committee has identified five high level threat categories:
  - Physical (PHI)
  - Natural (NAT)
  - Supplier (SUP)
  - Personnel (PER)
  - Technical (TEC)

Sub-Categories Defined (cont)

- **Physical (PHI)**
  - Theft of Property
  - Loss of Property
  - Destruction of Property
  - Social Instability
  - Physical Plant Failures
  - External Service Failures
  - Media failure
- **Natural (NAT)**
  - Dangerous Weather
  - Natural Environmental
  - Manmade Environmental
  - Biological

Sub-Categories Defined (cont)

- **Supplier (SUP)**
  - Supplier Disruption
  - Resource Disruption
  - Service Disruption
  - Logistics Provider Failures
  - Logistics Route / Mode Disruptions
  - Technology Manipulation
- **Personnel (PER)**
  - Labor / Skills Shortage
  - Loss of Key Staff
  - Negligent/Uninformed Workforce Member
  - Mistakes / Errors
  - Workforce Member Inaction
  - Process Failure
  - Fraud / System Abuse
  - Eavesdropping / Shoulder Surfing
  - Social Engineering

Sub-Categories Defined (cont)

- **Technical (TEC)**
  - Organizational Fingerprinting
  - System / Device Fingerprinting
  - Account Fingerprinting
  - Authentication Bypass
  - Software Exploits
  - Escalation of Privilege
  - Privilege Abuse
  - Malicious Code In Email
  - Malicious Code on Websites
  - Malicious Code on Systems
  - Application Exploitation
  - System / Device Memory Manipulation
- **Technical (TEC) cont.**
  - Cache Poisoning
  - Physical Device Manipulation
  - Cryptanalysis
  - Data Leakage / Theft
  - Denial of Service
  - Maintaining System Persistence
  - Manipulation of Data in Transit / Use
  - Capture of Data in Transit / Use
  - Replay of Data in Transit / Use
  - Mis-delivery of Data
  - Capture Stored Data
  - Manipulate Stored Data

Mappings to Threat Reports

- With the definition of a common model / taxonomy, we can create mappings to both control models and threat reports that are released

- Threat reports can fuel the threat taxonomy and map to the taxonomy
- Most reports are not all that different, and are poor at defining terms
- By mapping threat reports to a taxonomy we can bring create clarity

- By mapping the taxonomy to control models, we can identify gaps in control models and places where additional controls make sense

Community Based Risk Assessment

- Community based threat taxonomies lead to community based risk assessment methodologies
- The creation of a practical threat taxonomy is the first step in the creation of a practical risk assessment methodology

- There is no reason every organization should have to develop a methodology on their own
- Let's collaborate on the entire process and begin to build consensus
- This will leave us free to focus on what is important – actually trying to stop the threat from becoming a reality

Future of the Critical Security Controls

- The next version of the Critical Security Controls is being collaborated on as we speak (an upcoming 2015 release is planned)
- The Critical Security Controls (vNext) we hope will be based upon [illegible]n threat model such as this

- By agreeing on threats we can ensure:
  - We have consensus on the problem
  - We have a common language for discussion
  - We don't have glaring gaps in the control model

Next Steps - How Can You Help?

- We are still looking for people willing to contribute to the project
- Although the skeleton has been created, this will be an ongoing effort
- The next steps for the project are to:
  - Finalize categories of threat agents
  - Finalize categories of threat consequences
  - Create weights / likelihoods for each threat
  - Continue to refine the lists of threat actions
- Interested in helping? Drop me a note.

Further Questions

- James Tarala
  - Principal Consultant & Founder, Enclave Security
  - E-mail: james.tarala@enclavesecurity.com
  - Twitter: @isaudit
  - Website: http://www.auditscripts.com/

- Kelli Tarala
  - Principal Consultant & Founder, Enclave Security
  - E-mail: kelli.tarala@enclavesecurity.com
  - Twitter: @kellitarala
  - Website: http://www.auditscripts.com/