Using Open Tools to Convert Threat Intelligence into Practical Defenses

A Practical Approach

Presented by James Tarala (@isaudit)

© 2016

Principal Consultant Enclave Security
Historic Threat Hunting – German U-boats
Historic Threat Hunting – German U-boats (cont)

Ships Attacked by German U-boats (1939-1945)
Historic Threat Hunting – German U-boats (cont)

- Submarine threat hunters had access to defenses:
  - Naval escorts / air cover
  - Improved detection equipment
  - Improved offensive weapons
  - Improved training for hunters

- Submarine threat hunters had access to intelligence:
  - RF traffic analysis
  - Decrypted offensive communication

Historic vs. Modern Threat Hunting

• Successful organizations, regardless of the time period, combine the following for effective defense:
  – An understanding of threat
  – Layered preventive defenses
  – Layered detective defenses
  – Threat intelligence
  – Intelligent hunters / operators
Problem Statements

• 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?
• 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?
Problem Statements (cont)

• Threat intelligence is great, but many, many organizations don’t have the tools to utilize it effectively

• How can you block malicious hashes without a whitelisting tool?
• How can you detect IDS signatures without an IDS?
• How can you analyze network malware without packet captures?

• Knowledge of threat should lead to control selection
• Control selection provides an architecture for utilizing threat intelligence
Case Study: Mandiant APT1 Report

• In 2013 Mandiant released their APT1 report outlining the activities of a Chinese hacking team

• The report’s appendix describes:
  – 3,000 specific indicators of compromise
  – Certificates (13) used during compromises
  – Detailed descriptions of 40 malware families

• At the time of the report’s release, the report was extremely popular in infosec circles

• But who used this information for defense? How?
A Model for Threat Intelligence

Detecting Evil

Threat Intelligence

Implementing Controls

Selecting Controls
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

• Threat: TROJ_POSHCODER.A (Powershell Ransomware)
• Control: Microsoft AppLocker (Whitelisting)
• Consequence: Data Encryption / Loss

• Scenario:
  – An organization is fearful that PowerShell ransomware will execute on their workstations and encrypt data on 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:
  - Does a taxonomy of threat agents influence control selection?
  - Do we need to know specific threat agents?
  - Does threat intelligence change control selection?
  - 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-Invalidated Redirects and Forwards
Case Study: Web Server Attacks (cont)

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)

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

ACME Corp 2014 Observed Attacks
ACME Corp 2015 Observed Attacks
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
What’s Really Our Goal?

http://threatbutt.com/map
A Proposed Solution

1. Organizations who understand threat should share what they know
2. The community should work together to classify threats to information systems
3. A comprehensive threat taxonomy should be agreed upon
4. The threat taxonomy should be used to define & prioritize defensive controls
5. Organizations should implement those prioritized controls
6. Implemented controls paired with threat intelligence can be used to detect specific attacks

• But what if most organizations could simply skip to step five?
• What if organizations aren’t special snowflakes?
But What is a Threat?

• In 2015-2016, security vendors listed each of the following as a threat:
  
  – Iranian Hackers Linked to the Islamic Revolutionary Guard Corps
  – Chinese Hackers Linked to the People’s Liberation Army
  – Crimeware Exploit Toolkits
  – Ransomware
  – Point of Sale Systems
  – The Internet of Things
  – Encrypted Data Communications
  – Lost or Stolen Laptops
The Behavior of Threat

“Threat agents perform threat actions against threat targets in order to cause threat consequences.”
Components of Threats

- Agents
- Actions
- Targets
- Consequences
Proposed Solutions

• An Open Source Threat Taxonomy & Control Definition

• 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
The Open Threat Taxonomy (OTT)

- Maintained by a community group of volunteers, 150+ organizations have contributed so far

- One of the latest efforts is the release of a community threat model, the Open Threat Taxonomy (v1.2), which will be used to document and prioritize threats

- OTT will be used to define threats to define controls
- Will help standardize risk assessments, make one less paperwork step for organizations to complete
Goals of the Project

- To maintain an open-source taxonomy of threats to information systems.

- 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
Relevant Industry Research

- Numerous Industry Threat Reports
  (Verizon, Microsoft, Symantec, Sophos, etc.)
- MITRE CAPECs
- OWASP WASCs
- ENISA Threat Taxonomy
- 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
Threat Agent Catalog

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

- Physical
- Resource
- Personnel
- Technical
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 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 release is in development)
• The Critical Security Controls (vNext) we hope will be based upon a common 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
Freely Available Tools

- Free, open tools are available to help any organization defend itself:
  - Threat models / taxonomies
  - Preventive defenses
  - Detective defenses
  - Threat intelligence

- The research is done, it’s time for us to act

- “Quit whining, act like a man, defend yourself.”
  - Ret. Gen. Michael Hayden, Blackhat 2010
Next Steps - How Can You Help?

- We are still looking for people willing to contribute to these projects
- Although the skeleton has been created, this will be an ongoing effort

- We are currently updating the OTT:
  - Finalizing categories of threat agents
  - Finalizing categories of threat consequences
  - Reviewing weights / likelihoods for each threat
  - Continuing 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/

• Resources for further study:
  – AuditScripts.com Audit Resources
  – SANS SEC 566: Implementing and Auditing the Critical Security Controls
  – Center for Internet Security (CIS) Resources