OPEN THREAT TAXONOMY (VERSION 1.1)

Edited By: James Tarala and Kelli K. Tarala

“

Why should every organization have to identify threats on their own? We all face the same threats, possibly to differing degrees. If we can agree on a common set of threats, we are free to focus on defending ourselves against them.

JAMES TARALA
Principal Consultant, Enclave Security

OCTOBER 2015

Enclave Security
1435 East Venice Ave, Suite 133
Venice, FL 34292

What follows is Version 1.1 of the Open Threat Taxonomy. It is the result of numerous conversations between information security professionals over dinners, in the hallways of security conferences, and over countless email exchanges. It is the first official and formal release of a catalog of threats that organization can use as an input to their risk assessment and control selection processes.

Scott Adams, of Dilbert fame, warns – never be the creator, always be the criticizer. Creators open themselves up to attack and criticism. It is better, he says, to show your moral and intellectual superiority through criticizing someone else's work than to create something yourself. With this project, we are violating that principle by organizing those conversations, cocktail napkins diagrams, and email exchanges into a repository for the community.

This effort is a work in progress. We hope that Version 1.1 will be soon replaced with another better version, and this update and improvement cycle will continue. The community needs to start somewhere and we hope that this version is a start in the right direction.

If you have suggestions or want to help, please let us know. This will continue to be a community effort. Taxonomies are designed to evolve over time and we hope this document will for years to come.

Your Humble Zookeepers,

James Tarala
Kelli K. Tarala
Principal Consultants, Enclave Security
james.tarala@enclavesecurity.com
kelli.tarala@enclavesecurity.com

TABLE OF CONTENTS

INTRODUCTION

Since 2008, we have had the privilege of working with organizations such as the SANS Institute and the Center for Internet Security on the Critical Security Controls project. This project began as an effort to parse information about threats to information systems and develop a prioritized defense model that the community could share as they attempted to defend their information systems. These controls are based on the knowledge of threats to information systems.

As we sought to formalize the data regarding these threats, we hoped to map to existing cyber security threat models to help explain the effort. However, as we researched available models we found examples of threat models with no attempts to create a full catalog of threats to information systems. We found a number of organizations who published threat reports of the most critical threats of the day, but few groups were attempting to document a full list of threats to information systems.

This project is our attempt to do just that.

The goal of this project is simple; to maintain a free, community driven, open source taxonomy of potential threats to information systems. Our hope is that this taxonomy will serve as a resource for organizations attempting to prioritize their defenses and choose controls most appropriate for defending their information systems. We believe that the nature of a common internet and homogeneous systems leads to common threats to information systems. This taxonomy has been created to identify those threats in order to help organizations choose defenses most appropriate to defend such systems.

Mission:

“To maintain a free, community driven, open source taxonomy of potential threats to information systems.”

CONTRIBUTORS

No project of this size is ever the work of just one person. Thankfully at the time of publishing this version of the Open Threat Taxonomy, we have had over 150 different international organizations contributing to the effort.

The early work for the Open Threat Taxonomy was performed by many of the same people who contributed to the Center for Internet Security's Critical Security Controls. In fact, one of the early needs that led to the creation of this project was a need to have a formal way of determining how to prioritize control selection based on threat priorities. As such, many of the contributors to that original project have been instrumental in the development of this threat taxonomy.

Work on the taxonomy has been an international effort. Representatives from numerous countries and international groups have contributed their time and resources to the development of this effort. In the future, we hope to continue to receive such broad support to help ensure that the information produced can be useful to any member of the global internet community.

People have often asked whether this taxonomy is specific to a particular industry. The answer is no, it has been correlated by a diverse group of organizations seeking to develop a broad understanding of threat. However, whether an organization works in the energy sector, financial services, or healthcare, if they are utilizing a Linux server or network router, then the threats to each system often overlap, regardless of the industry. Having said that, contributors to the project represent organizations such as:

- The US Department of Defense & other US Federal Agencies
- NATO & International Governments
- US State & Municipal Governments
- Banks, Monetary Funds and others in Financial Services
- Energy Sector & others utilizing Industrial Control Systems
- Clinical Healthcare & Insurance Providers
- Universities and other Educational Institutions
- The Center for Internet Security
- The SANS Institute
- Multiple Information Sharing and Analysis Centers (ISACs)

We sincerely thank all of the people who spent their time to make this project a reality and hope to continue to see more organizations engage the project in order to make this an even more useful resource in the future.

DEFINITIONS & SCOPE

One of the first things that needed to be defined by this project was a working definition of threat. There are a number of groups such as the United States' National Institute of Standards in Technology and others who have their own definitions. For the sake of this effort, the consensus definition is that:

Threat is the potential for a threat agent to cause loss or damage to an information system.

It also seems that there is a large degree of confusion regarding what threats actually are. When reading industry threat reports it seems that there is not a clear definition of what a threat would be. It is our understanding that one of the biggest reasons for this is that when considering threats, there are actually a number of different components to consider, including:

- Threat sources or agents
- Threat actions
- Threat targets
- Threat consequences

A threat source will most often perform a threat action against a threat target, which leads to threat consequences. Threat reports often leave out the distinction between these elements and therefore classify things such as the Syrian Electronic Army, SQL Injection Attacks, and Point of Sale Systems all in the same definition. While each of them could be classified as a part of the threat equation, they are not all representative of the same element of threat. They need to be classified according to where they fit into this chain. For the sake of this taxonomy, we will attempt to define threat actions.

Incident handlers or hunters will likely want more discussion of threat actors in this discussion. There are good resources, such as those provided by the Information Assurance Analysis Centers that will be useful in this regard. Nevertheless, for the sake of this discussion, only threat actions will be considered to limit the scope of the discussion and focus on defending against such actions. While the motivation for an attack matters, for the sake of this discussion, we will not differentiate between the groups who may be motivated to perform a particular attack.

In an effort to rank each of the threats identified as a part of this project we have also assigned priority weighting to each of the identified threat actions. The purpose of these rankings is to quantify the relative importance of choosing controls to defend against this particular threat. All threats are worthy of consideration when designing a defense model. However, when organizations have limited resources they should consider where to focus their resources and efforts. These scores are provided in order to give organizations a general ranking system they can use when prioritizing defenses.

The ranking provided are the result of information gathered by the contributors to this effort, the results of industry threat models, and observations of attacks in the wild and should be viewed as consensus guidance. While admittedly the scores listed are qualitative in nature, they do reflect the generally held beliefs of the groups participating in this effort.

All threat rankings have been listed on a one to five scale. The higher the threat weighting, the more likely that a particular threat should be considered when prioritizing an organization’s defensive capabilities. The score listed is based on the likelihood of a threat being realized and does not represent the potential consequences of the attack. Full scoring that considers the consequences and other factors should be included in the full risk management model adopted and is not the focus of this research.

OVERVIEW OF THREAT CATEGORIES

Knowing that the goal of this project is to catalog any threats to information systems, four categories or families of threats have been identified. Those categories are as follows.

PHYSICAL THREATS

Includes:

Threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.

RESOURCE THREATS

Includes:

Threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.

PERSONNEL THREATS

Includes:

Threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization’s personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.

TECHNICAL THREATS

Includes:

Threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.

THREAT ACTIONS & RATINGS

PHYSICAL THREATS

The following represent physical or environmental threats to information systems and often result in physical harm to the information system being defended.

Threat ID	Threat Action Name	Threat Rating
PHY-001	Loss of Property	5.0
PHY-002	Theft of Property	5.0
PHY-003	Accidental Destruction of Property	3.0
PHY-004	Natural Destruction of Property	3.0
PHY-005	Intentional Destruction of Property	2.0
PHY-006	Intentional Sabotage of Property	2.0
PHY-007	Intentional Vandalism of Property	2.0
PHY-008	Electrical System Failure	4.0
PHY-009	Heating, Ventilation, Air Conditioning (HVAC) Failure	3.0
PHY-010	Structural Facility Failure	2.0
PHY-011	Water Distribution System Failure	2.0
PHY-012	Sanitation System Failure	1.0
PHY-013	Natural Gas Distribution Failure	1.0
PHY-014	Electronic Media Failure	3.0

RESOURCE THREATS

The following threats represent resource threats to information systems. Resources of various types are needed for the successful operation of information systems. Disruption of these resources can lead to loss or harm on those systems.

Threat ID	Threat Action Name	Threat Rating
RES-001	Disruption of Water Resources	2.0
RES-002	Disruption of Fuel Resources	2.0
RES-003	Disruption of Materials Resources	2.0
RES-004	Disruption of Electrical Resources	4.0
RES-005	Disruption of Transportation Services	1.0
RES-006	Disruption of Communications Services	4.0
RES-007	Disruption of Emergency Services	1.0
RES-008	Disruption of Governmental Services	1.0
RES-009	Supplier Viability	2.0
RES-010	Supplier Supply Chain Failure	2.0
RES-011	Logistics Provider Failures	1.0
RES-012	Logistics Route Disruptions	1.0
RES-013	Technology Services Manipulation	3.0

PERSONNEL THREATS

Organizations rely on knowledgeable and ethical personnel to operating information systems. However when those personnel experience disruptions, knowledge gaps, or make mistakes the result can be loss or harm to the information systems being protected.

Threat ID	Threat Action Name	Threat Rating
PER-001	Personnel Labor / Skills Shortage	5.0
PER-002	Loss of Personnel Resources	3.0
PER-003	Disruption of Personnel Resources	3.0
PER-004	Social Engineering of Personnel Resources	4.0
PER-005	Negligent Personnel Resources	4.0
PER-006	Personnel Mistakes / Errors	4.0
PER-007	Personnel Inaction	3.0

TECHNICAL THREATS

Most commonly discussed in terms of threats to information systems are technical threats to these systems. Threat actors are able to engage in technical activities that can cause loss or harm to a system. The following are categories of such threats.

Threat ID	Threat Action Name	Threat Rating
TEC-001	Organizational Fingerprinting via Open Sources	2.0
TEC-002	System Fingerprinting via Open Sources	2.0
TEC-003	System Fingerprinting via Scanning	2.0
TEC-004	System Fingerprinting via Sniffing	2.0
TEC-005	Credential Discovery via Open Sources	4.0
TEC-006	Credential Discovery via Scanning	3.0

TECHNICAL THREATS (CONTINUED)

Threat ID	Threat Action Name	Threat Rating
TEC-007	Credential Discovery via Sniffing	4.0
TEC-008	Credential Discovery via Brute Force	4.0
TEC-009	Credential Discovery via Cracking	4.0
TEC-010	Credential Discovery via Guessing	2.0
TEC-011	Credential Discovery via Pre-Computational Attacks	3.0
TEC-012	Misuse of System Credentials	3.0
TEC-013	Escalation of Privilege	5.0
TEC-014	Abuse of System Privileges	4.0
TEC-015	Memory Manipulation	4.0
TEC-016	Cache Poisoning	3.0
TEC-017	Physical Manipulation of Technical Device	2.0
TEC-018	Manipulation of Trusted System	4.0
TEC-019	Cryptanalysis	1.0
TEC-020	Data Leakage / Theft	3.0
TEC-021	Denial of Service	2.0
TEC-022	Maintaining System Persistence	5.0
TEC-023	Manipulation of Data in Transit / Use	2.0

TECHNICAL THREATS (CONTINUED)

Threat ID	Threat Action Name	Threat Rating
TEC-024	Capture of Data in Transit / Use via Sniffing	3.0
TEC-025	Capture of Data in Transit / Use via Debugging	2.0
TEC-026	Capture of Data in Transit / Use via Keystroke Logging	3.0
TEC-027	Replay of Data in Transit / Use	2.0
TEC-028	Misdelivery of Data	2.0
TEC-029	Capture of Stored Data	3.0
TEC-030	Manipulation of Stored Data	3.0
TEC-031	Application Exploitation via Input Manipulation	5.0
TEC-032	Application Exploitation via Parameter Injection	4.0
TEC-033	Application Exploitation via Code Injection	4.0
TEC-034	Application Exploitation via Command Injection	4.0
TEC-035	Application Exploitation via Path Traversal	3.0
TEC-036	Application Exploitation via API Abuse	3.0
TEC-037	Application Exploitation via Fuzzing	3.0
TEC-038	Application Exploitation via Reverse Engineering	3.0
TEC-039	Application Exploitation via Resource Location Guessing	2.0
TEC-040	Application Exploitation via Source Code Manipulation	3.0
TEC-041	Application Exploitation via Authentication Bypass	2.0

RELEVANT RESEARCH

The contributors to this project did not gather this threat information in a vacuum. Many other groups and research projects have worked on this issue as well. It would be naïve to assume that this project would be as far along as it is without being able to learn from the research performed by these other groups. Our hope is that many others will take up the mantle of brainstorming potential threats and this taxonomy will grow as a community effort. In order to give credit to the good work done by these other groups and to encourage others to learn more about threat, we wanted to list other valuable sources of information on the topic that influenced this process.

Some of the most noteworthy resources that helped influence the development of this taxonomy include:

- Numerous Vendor Industry Threat Reports
- MITRE Corporation's CAPECs
- OWASP's WASCs
- NIST's SP 800-30
- CMUSEI's Taxonomy of Operational Risk
- Cambridge Centre for Risk Studies' Resources
- General Motor's Concentric Vulnerability Map
- Treasury Board of Canada's Guide to Risk Taxonomies

These are simply a few of the many solid resources available in the open source that discuss the creation of threat taxonomies. If the reader identifies other resources that they believe can contribute to this effort, please let us know so we can all benefit from the research.

CONCLUDING THOUGHTS

An accurate understanding of threat can lead to better information security controls. Better information security controls can lead to better assurance of the continued confidentiality, integrity, and availability of information assets entrusted to our organizations. This project was created to fill a gap in the security community and provide a better understanding of threat. If organizations misunderstand or misinterpret threats, this will lead to inappropriate defenses and potentially a waste of valuable resources that could be used to better defend these assets. We hope this threat taxonomy is a step in the right direction towards understanding and cataloging threat.

For this information to be useful, it must be accurate and it must be current. As a community we can work together to make this more accurate. If we share our ideas and collaborate on the threats we are seeing then we can use this information to prioritize how we respond to the threats we collectively observe. We hope that as someone benefiting from this project, you will consider contributing to the effort as well. Please reach out to us if you believe you have information you can contribute that will help make this resource even more useful to others.

Please remember that this is a continuously evolving document. We hope to release many more versions in the future and on a regular basis. Expect the taxonomy to change and to grow. Eventually the need for quick updates will slow, but especially in these early phases, we expect there to be a number of regular updates that are released.

We look forward to your feedback and even more releases ahead.

Enclave Security
1435 East Venice Ave, Suite 133
Venice, FL 34292

Enclavesecurity.com
Auditscripts.com