A Taxonomy of Cyber Events Affecting Communities

Keith Harrison, Gregory White
The University of Texas at San Antonio
kharriso@cs.utsa.edu, greg.white@utsa.edu

Abstract

Communities, whose reliance on critical cyber infrastructures is growing, are threatened by a wide range of cyber events that can adversely affect these systems and networks. The development of computer security taxonomies to classify computer and network vulnerabilities and attacks has led to a greater insight into the causes, effects, mitigation, and remediation of cyber attacks. In developing these taxonomies researchers are better able to understand and address the many different attacks that can occur. No current taxonomy, however, has been developed that takes into account the community aspects of cyber attacks or other cyber events affecting communities. We present a new taxonomy that considers the motivation, methodology, and effects of cyber events that can affect communities. We include a discussion on how our taxonomy is useful to e-government, industry, and security researchers.

1. Introduction

Communities are growing ever more dependent on cyberspace for the operation of critical services. This is true for both industry and government services which can increasingly be found online. This movement toward e-commerce and e-government (electronic-government) makes communities even more reliant on cyberspace. As this dependency grows communities become even more vulnerable to attacks or other cyber events. Much research has been done on classifying computer and network vulnerabilities and attacks. These taxonomies, however, have focused classifying the methods used to attack individual systems or the vulnerabilities that make attacking individual systems possible.

We propose a new taxonomy focusing on cyber events affecting communities. No cyber attack taxonomy has taken into account either the motivation for attacking a community, or the impact on a community of such an attack. Another important contribution of our work is the consideration of all cyber events that affect communities including cyber attacks, human error, and natural disasters.

Our taxonomy provides several benefits to e-government, industry, and security researchers. First, our taxonomy is useful to e-government and industry for classifying cyber events and their effects on communities and critical infrastructure. Secondly, our work is a key step in providing security researchers insights into what constitutes an attack on a community and eventually what metrics should be gathered in order to facilitate real-time detection of attacks on communities by the community government.

2. Background

A taxonomy is a system used for the classification of specimens. Traditionally, a taxonomy is represented using a tree structure such as the taxonomy developed by Carolus Linnaeus [1] which has eventually led to the commonly known biological taxonomic ranks of kingdom, phylum, class, order, family, genus, and species.

Scientifically classifying specimens within computer science and other sciences requires different types of classification schemes depending on the system being studied. A simple taxonomy may be a single category, while a more complex taxonomy may be made of multiple categories. Usually, when classifying using multiple categories, each category is used to classify a different attribute of a single specimen. There are two common types of categories used for classification:

- **List** – A list is a single category classification system composed of terms, classes, or rankings. A well known example is the Color-coded Threat Level system used by the Homeland Security Advisory System [2]. Another example is Bloom’s taxonomy which is used to classify levels of intellectual behavior [3].

- **Multi-level/Tree** – Multi-level taxonomies can also be represented as a tree. Each level represents a different level of abstraction. The most well known example of a multi-level taxonomy is the previously discussed Linnaean taxonomy [1].
Although there exists some overlap, computer security taxonomies can be divided into three general categories: attack taxonomies, vulnerability taxonomies, and intrusion detection signature taxonomies [4]. Several specialized attack and vulnerability security taxonomies have been developed for classifying a particular threat such as Distributed Denial of Service (DDoS) attacks [5,6].

Attack taxonomies focus on the attack vector used to attack a system and may include information such as the different methods used to compromise a system, the types of tools used, the vulnerabilities exploited, the potential effects on a system, and possible defenses. Vulnerability taxonomies seek to classify vulnerabilities by analyzing characteristics such as their associated faults, methods of introduction, effects of exploitation, and defenses. Intrusion Detection signature taxonomies classify threats by the intrusion detection metrics and signatures required for detection.

2.1. Characteristics

Previous works [7,8,9] have identified several important characteristics of successful taxonomies.

- **Accepted** – Well structured, with logical and intuitive categories, to facilitate general approval. Additionally, the taxonomy should be based on generally approved previous work.
- **Comprehensible** – Easily understandable to both specialists in the field and those with a casual interest.
- **Exhaustive** – Classification categories include all possibilities. Each specimen corresponds to at least one category.
- **Mutually exclusive** – Classification categories do not overlap. Each specimen corresponds to at most one category.
- **Repeatable** – Classification of a specimen should be the same regardless of who is classifying.
- **Terms well defined** – Category definitions should use terminology that is clear and in compliance with previously accepted work.
- **Unambiguous** – Classification should be done without ambiguity. If a specimen belongs to a category, it should be clear.
- **Useful** – The taxonomy should be usable by industry, and allow specialists greater insight into the field.

3. Previous work

Bishop [10] developed a taxonomy of vulnerabilities with six axes: nature, time of introduction, exploitation domain, effect domain, minimum number, and source. The vulnerability nature is also referred to as the vulnerability class and taken from the Protection Analysis Study [11]. The time of introduction is refined from the work of Landwehr [12] and may be during development, during maintenance, or during operation. The exploitation domain describes in which domain the vulnerability occurs, and the effect domain describes what domains are affected. Minimum number is the minimum number of components needed to exploit the vulnerability and indicates the difficulty of discovering the exploitation of a vulnerability. Source is where the vulnerability was originally disclosed.

Lindqvist and Jonsson [8] presented the idea of a taxonomy with dimensions for classifying the different attributes of a specimen. They proposed that the two most important dimensions of an intrusion are intrusion techniques and intrusion results. Each of their dimensions can be viewed as a tree. The first level categories of their intrusion techniques are bypassing intended controls, active misuse of resources, and passive misuse of resources. These three categories were based on earlier work by Neumann and Parker [13]. The first level categories of the intrusion results dimension are exposure, denial of service, and erroneous output. Lindqvist and Jonsson’s taxonomy is notable due to their identification and adherence to important taxonomic characteristics, especially completeness and usefulness.

Howard and Longstaff [14] created a common language, consisting of terms and taxonomies, for computer security incidents. In their taxonomy, an event as the combination of an action and a target. An attack consists of a tool, vulnerability, event, and unauthorized result. An incident is composed of attackers, an attack, and objectives. Howard’s taxonomy is notable because he considers the more abstract objectives of an attacker, the process by which an attack happens, and the unauthorized result of an attack on a system. However, as pointed out by Lough [15], Howard’s taxonomy is not mutually exclusive.

Lough’s [15] taxonomy, VERDICT, stands for Validation, Exposure, Randomness, and Deallocation Improper Conditions Taxonomy. Lough’s taxonomy is meant to be applicable to both wired and wireless networks. VERDICT classifies attacks by what are proposed to be the four main characteristics of error in computer systems: improper validation, improper exposure, improper randomness, and improper deallocation. An attack or attack type may be comprised of one or more of these characteristics.

Hansman and Hunt [9] developed a taxonomy of network and computer attacks based on four dimensions: attack class, attack target, vulnerabilities and exploits, and payloads or effects beyond
themselves. The attack class and attack target dimensions have multiple levels each with a different level of abstraction. For example, the attack class may be a worm, and a worm may either be a mass-mailing worm or a network aware worm. At a high level of abstraction the target may be either hardware or software, at the lowest level of abstraction the target may be a specific version of an application or operating system. Vulnerabilities may be a specific Common Vulnerabilities and Exposure (CVE) entry or a general type of vulnerability such as implementation, design, or configuration.

Simmons et al. [16] proposed a cyber attack taxonomy called AVOIDIT. Their taxonomy classifies cyber attacks using 6 categories: attack vector, operational impact, defense, informational impact, and attack target. The attack vector is a vulnerability or path used to compromise a system such as a buffer overflow or social engineering. The operational impact is the effect on the operation of the system. An example of operational impact may be denial of service or root compromise. The defense are the steps that may be taken beforehand that would remediate or mitigate the attack. Informational impact is the effect on sensitive information such as disclosure or destruction. AVOIDIT does not attempt to classify physical attacks.

An excellent and much more extensive survey of computer taxonomies was published by Igure and Williams [4]. In addition to providing an extensive discussion of security taxonomies they identified the common basic dimensions for attack classification: impact, target, source, and vulnerability. Additionally they list the basic properties of an efficiently organized taxonomy, the two most important being that classes need not be mutually exclusive, and that taxonomies must be layered or hierarchical.

4. Taxonomy overview

Our taxonomy is divided into two dimensions. The first dimension is the event vector. This vector can be thought of as describing the threat agent and different abstract levels of objectives and methods by which the event occurs. The second dimension of our taxonomy is the effect vector. The effect vector describes what critical infrastructure is affected, the reason it is affected, and what the effects are on the community.

It is important to point out that when considering a large scale attack on a community, the overall attack may be comprised of several event vectors. Additionally, an attack with one or more event vectors may have multiple associated effect vectors. In Section 7.1 we give an example of an event with multiple related effect vectors.

5. Event vector

The event vector is shown in Figure 1. The event vector describes a threat agent and the different levels of abstraction that lead a threat agent to cause a cyber event. The high level objective of a threat agent may be sabotage, but at a lower level of abstraction the objective might be to overload the available network resources.

5.1. Threat agent

The threat agent is the threat faced by the community. The threat agent describes who or what is primarily responsible for the cyber event. The possible threat agents are as follows:

- Malicious Individuals work alone or in a small group. They are severely lacking in organization and funding. Individuals range in skill level from uneducated through highly trained.
- Organisations are entities such as corporations or organized crime. They have a significant amount of training, organization, and funding.
- Foreign Governments have virtually unlimited funding and are a highly organized threat.
- Natural Disasters are environmental disasters over which humans have no control.
- Human Errors are unintended accidents or mistakes either in the real world or in cyberspace. Human error is a concept and should not be interpreted to mean that an individual making an error is the threat agent.

5.2. Motivation

Motivations are a high level abstraction of the goals of the threat agent. The motivation describes what the overall goal of the threat agent is, in respect to cyberspace and the community in general. The possible motivations of a threat agent are as follows:

- Service Theft occurs when a service is used in an unauthorized manner.
- Sabotage is the disruption or destruction of services or information. Sabotage is usually part of a larger overall goal such as terrorism, political posturing, revenge, or a prelude to invasion.
- Intelligence Gathering is the motivation of an entity attempting to gain access to information for which that entity is not authorized.
- Extortion is the motivation of threat agents seeking to extort money out of the community.
government, community members, or the community as a whole.

- **Zombie Propagation** is the motivation to increase the number of systems under the threat agent’s control. Zombie computers are computers that are part of a botnet and are used for other motives such as spamming or DDoS attacks.

- **Widespread Destruction** is seeking to cause damage without discriminating against the target type or location.

- **Identity Theft** is attempting to gain access to personal information in order for the threat agent to make a financial gain.

- **No Motivation** exists when the threat agent is incapable of reasoning as in the case of nature or the concept of human error.

5.3. **Objective**

The objective is an abstract idea of how the threat agent will attempt to achieve its motivation. The objective can be thought of as the goal of the threat agent in respect to resources such as information, service availability, and long term system control. The possible objectives are as follows:

- **Information Corruption** is attempting to modify information such as files stored on a computer or in transit.

- **Information Fabrication** is attempting to create information masquerading as legitimate information. The information may be fabricated either as files stored on a computer, or as information in transit coming from a legitimate host.

- **Information Destruction** is attempting to destroy information owned by another entity.

- **Information Disclosure** is gaining the ability to read information known to exist, for which the threat agent is not intended to have read access to.

- **Information Discovery** is searching for and gaining access to important information without

<table>
<thead>
<tr>
<th>Threat Agent</th>
<th>Motivation</th>
<th>Objective</th>
<th>Method</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Individual Organizations</td>
<td>Service Theft</td>
<td>Information Corruption</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td>Foreign Government</td>
<td></td>
<td></td>
<td>Protocol Compromise</td>
<td>Targeted Exploit of Social Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Fabrication</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Protocol Compromise</td>
<td>Targeted Exploit of Social Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Sabotage</td>
<td>Service Disruption</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Resource Exhaustion</td>
<td>Overload Network Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hardware Failure</td>
<td>Physical Damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software Crash</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Destruction</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hardware Failure</td>
<td>Physical Damage</td>
</tr>
<tr>
<td></td>
<td>Intelligence Gathering</td>
<td>Information Disclosure</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information Discovery</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Extortion</td>
<td>System Subversion</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Zombie Propagation</td>
<td>System Subversion</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Widespread Destruction</td>
<td>Information Destruction</td>
<td>System Compromise</td>
<td>Autonomous Self Propagating Malware</td>
</tr>
<tr>
<td></td>
<td>Identity Theft</td>
<td>Information Disclosure</td>
<td>System Compromise</td>
<td>Autonomous Self Propagating Malware</td>
</tr>
<tr>
<td>Nature</td>
<td>None</td>
<td>None</td>
<td>Hardware Failure</td>
<td>Physical Damage</td>
</tr>
<tr>
<td>Human Error</td>
<td></td>
<td></td>
<td>Software Crash</td>
<td>Unintentional Exploit of System Vulnerability</td>
</tr>
</tbody>
</table>

*Figure 1. Event vector*
the threat agent having foreknowledge of what exactly the intended information is.

- **System subversion** is the process by which the entity brings systems under its control, usually for a separate, long term future purpose.
- **Service disruption** is the objective of disrupting the correct operation or usability of a electronic or physical service.
- **No Objective** exists when the threat agent is incapable of reasoning as in the case of nature or the concept of human error.

### 5.4. Method

This category classifies the abstract method in which the cyber event occurred. The possible abstract methods by a cyber event could occur are as follows:

- **System Compromise** is when the objective is carried out by gaining unauthorized access to a system.
- **Protocol Compromise** is when a vulnerability exists within a utilized protocol allowing for the unauthorized fabrication and modification of information in transit.
- **Resource Exhaustion** occurs when a finite amount of resources, such as network bandwidth or open network connections, are completely consumed.
- **Hardware Failure** occurs when cyber related hardware, such as microchips, circuits, or wires, are no longer able to carry out its intended function.
- **Software Crashes** occur when the software programs running on a system, such as applications, operating systems, or embedded software, cease to function as they are intended to do when operating correctly.

### 5.5. Technique

Technique is the specific technique used to achieve the threat agent’s objective. The possible techniques are as follows:

- **Targeted Exploitation of System Vulnerability** is the use of an exploit to gain unauthorized access to a system specifically targeted by the threat agent.
- **Targeted Exploitation of Social Vulnerability** is the use of social engineering to gain unauthorized access to a system specifically targeted by the threat agent.
- **Targeted Exploit of Protocol Vulnerability** is the use of an exploit to take advantage of a protocol vulnerability in order to modify information going to or from a specific target.
- **Overload of Network Resources** is a technique

### Effect Vector

<table>
<thead>
<tr>
<th>Cause</th>
<th>Service Affected</th>
<th>Disruption Impact</th>
<th>Evaluation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Event within Service</td>
<td>Energy</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Government Impact</td>
<td>% Government Effectiveness Reduced</td>
</tr>
<tr>
<td></td>
<td>Telecommunications</td>
<td>Population Impact</td>
<td>% Population denied access to service</td>
</tr>
<tr>
<td></td>
<td>Finance</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Water Supply</td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Healthcare</td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Transportation</td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Law Enforcement</td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Government Impact</td>
<td>% Government Effectiveness Reduced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Govt. Administration</td>
<td>Government Impact</td>
<td>% Government Effectiveness Reduced</td>
</tr>
<tr>
<td></td>
<td>Shipping</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Agriculture</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Commercial Facilities</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Population Impact</td>
<td>% Population Denied Access</td>
</tr>
<tr>
<td></td>
<td>Critical Manufacturing</td>
<td>Economic Impact</td>
<td>% Revenue Lost, %GDP Lost</td>
</tr>
</tbody>
</table>

*Figure 2. Effect vector*
such as a Distributed Denial of Service (DDoS) attack or a Smurf attack used to consume all available bandwidth.

- **Overload of System Resources** is a kind of denial of service attack in which a finite system resource is completely consumed such as a syn flood.
- **Physical Damage** occurs when hardware is modified from its original state until it no longer functions properly. Physical damage may be caused in a variety of ways including water, scissors, lightning, explosives, or blunt trauma.
- **Autonomous Self Propagating Malware** includes all forms of malware that use techniques to spread autonomously without the need for the direct involvement of the threat agent in selecting targets. This includes worms, viruses, spyware, scareware, drive-by downloads, and email viruses just to name a few.
- **Unintentional Exploitation of System Vulnerabilities** occur when the conditions are met that allow a software bug to manifest itself through the incorrect operation of software. This may have the unintentional effect of crashing or hanging the system or application, as well as corrupting or deleting information.

### 6. Effect vector

The effect vector is shown in Figure 2. The effect vector describes the community sector affected, the cause of the effect, the impact of the affected sector, and metrics that can be used to further evaluate the impact.

#### 6.1. Cause

Cause is a category useful for differentiating between an effect directly caused by a cyber event, and an effect caused by the disruption of another service. The two possible causes are as follows:

- **Cyber Disruption within Service** occurs when a service is affected by a cyber event directly caused by a threat agent. In this case the disruption to the service originates from within the service itself.
- **Cascade Disruption from <Service>** occurs when a service is affected through a dependency on another affected service. In this case the disruption to the service originates from another service, an example would be: Cascade Disruption from Energy Services.

### 6.2. Services affected

We have surveyed government documents and have come up with an appropriate list of community sectors and critical infrastructures [17]:

- **Energy** services include the production and transportation of electrical energy, as well as gas and oil production, storage, transportation, and refining.
- **Telecommunications** services are services facilitating the electronic transfer of information such as phone companies and internet service providers, as well as the hardware infrastructure used by these services.
- **Finance** services are organizations that manage monetary assets. Finance services include banks and stock exchanges as well as hardware such as ATMs.
- **Water Supply** services are services that maintain, store, pump, and process water used primarily for drinking. Water supplies may also be critical for industrial activities such as oil refining.
- **Healthcare** services provide medical care to the population as well as the production of critical medical supplies and equipment.
- **Transportation** services facilitate transit within communities or between communities. This includes roads, traffic lights, the airline industry, public transportation, and railways.
- **Law Enforcement** services are tasked with maintaining the laws of the community. These services include the police departments and the criminal justice system.
- **Fire and Emergency Response** services are tasked with preventing and responding to fires, chemical attacks, biological attacks, and explosive devices. Emergency ambulatory services are included as part of emergency response and not healthcare.
- **Government Administration** services are responsible for running the day to day operations of the government. This includes various government departments such as treasury, education, tax collection, and tourism as well as various regulatory and legislative offices.
- **Shipping** services are responsible for the physical transportation of goods. This includes private companies that are responsible for the transportation of packages, resources, and manufactured goods over road, rail, water, or air transportation. Shipping services also includes government agencies such as the postal service.
- **Agriculture** services are concerned with the production and harvesting of food and goods through farming. This includes the farming, harvesting, and production of basic agricultural
products such as crops, livestock, and dairy products.

- **Commercial Facilities** are businesses within a community that provide goods and services to the community.
- **Critical Manufacturing** is the manufacturing of chemicals and hazardous products as well as the products critical to our nation.

### 6.3. Disruption impact

The disruption impact describes the effect on the community. The disruption impact may be one of the following:

- **Economic Impact** is a detrimental impact on the production of goods or a monetary loss.
- **Population Impact** occurs when a community citizen is denied the use or access to goods or services provided by the affected sector.
- **Government Impact** occurs when the effectiveness of the government is reduced.

### 6.4. Impact metrics

Impact metrics attempt to provide a measure of how much the community was impacted. The possible impact metrics are as follows:

- **Economic Impact** may be measured as a percent of revenue lost or as a percentage of reduction in GDP.
- **Population Metrics** may be measured as a percent of the population denied access to a service.
- **Government Metrics** may be measured as a percentage of reduction in its effectiveness.

### 7. Examples

In Figure 3, we provide examples of how to apply our taxonomy to real world cyber events. The first event vector and effect vector make up example 1. Similarly examples 2 and 3 are the second and third event and effect vector combinations respectively.

#### 7.1. Example 1

In the first example ten fiber optic cables, with over 500 total strands, were sliced in San Jose and San Carlos, California in April of 2009 [18]. It is unknown what threat agent carried out the attack or what their motivation was. However, their objective was clearly to cause a service disruption. They went about causing a hardware failure in the fiber optic lines by inflicting physical damage to the fiber optic lines themselves. This event had the effect of causing a cyber disruption within the telecommunications infrastructure. The disruption to the telecommunications service had a

---

**Event Vector (1)**

<table>
<thead>
<tr>
<th>Community</th>
<th>Threat Agent</th>
<th>Motivation</th>
<th>Objective</th>
<th>Method</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Jose/San Carlos</td>
<td>Unknown</td>
<td>Sabotage</td>
<td>Service Disruption</td>
<td>Hardware Failure</td>
<td>Physical Damage</td>
</tr>
</tbody>
</table>

**Effect Vector (1)**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Service Affected</th>
<th>Impact</th>
<th>Evaluation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Event within Service</td>
<td>Telecommunications</td>
<td>Population Impact</td>
<td>Unknown Percentage of Population</td>
</tr>
<tr>
<td>Cascade Disruption from Telecommunications</td>
<td>Finance</td>
<td>Population Impact</td>
<td>Unknown Percentage of Population</td>
</tr>
<tr>
<td>Cascade Disruption from Telecommunications</td>
<td>Emergency and Fire Response</td>
<td>Population Impact</td>
<td>Unknown Percentage of Population</td>
</tr>
<tr>
<td>Cascade Disruption from Telecommunications</td>
<td>Healthcare</td>
<td>Population Impact</td>
<td>Unknown Percentage of Population</td>
</tr>
</tbody>
</table>

**Event Vector (2)**

<table>
<thead>
<tr>
<th>Community</th>
<th>Threat Agent</th>
<th>Motivation</th>
<th>Objective</th>
<th>Method</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>Organized Crime</td>
<td>Extortion</td>
<td>System Subversion</td>
<td>System Compromise</td>
<td>Targeted Exploit of System Vulnerability</td>
</tr>
</tbody>
</table>

**Effect Vector (2)**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Service Affected</th>
<th>Impact</th>
<th>Evaluation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Event within Service</td>
<td>Energy</td>
<td>Economic Impact</td>
<td>Unknown Revenue, GDP Lost</td>
</tr>
</tbody>
</table>

**Event Vector (3)**

<table>
<thead>
<tr>
<th>Community</th>
<th>Threat Agent</th>
<th>Motivation</th>
<th>Objective</th>
<th>Method</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Houston</td>
<td>Unknown</td>
<td>Zombie Propagation</td>
<td>System Subversion</td>
<td>System Compromise</td>
<td>Autonomous Self Propagating Malware</td>
</tr>
</tbody>
</table>

**Effect Vector (3)**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Service Affected</th>
<th>Impact</th>
<th>Evaluation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Event within Service</td>
<td>Law Enforcement</td>
<td>Government Impact</td>
<td>Unknown Reduction in Government Efficiency</td>
</tr>
</tbody>
</table>
direct population impact as people were denied use of telecommunications services such as the Internet or the ability to make phone calls. The disruption within the telecommunications service had a cascade effect on financial services, fire and emergency response, and healthcare. An unspecified percentage of people were affected by being denied access to all four services. Additionally, the disruption to the financial services had an unspecified economic impact on the community as well.

7.2. Example 2

The second example deals with the suspected extortion attempts made against power plants in Brazil [19]. In this example organized crime is the threat agent and their motive is extortion. The threat agent has an objective of system subversion in order to set the stage for their extortion demands. In order to subvert systems the threat agent compromises the systems using the technique of executing exploits targeting specific systems and their corresponding vulnerabilities.

The effect of this event is the attempted extortion of the energy sector. The community suffers an economic impact from this event, as revenue is spent on fixing the problem and possibly complying with the extortion demands. Conversely if the extortion demands are not met and the power is shut off the community suffers an economic impact of lower GDP and possibly additional cascading effects to other critical infrastructure.

7.3. Example 3

The third example occurred in February of 2009, when the Conficker worm infected 475 computers belonging to city of Houston [20]. In this case, author’s motivation for deploying Conficker worm is the unknown threat agent. The motivation of Conficker at the time of the event was to propagate and enlist new zombie machines. In order to create zombie machines the objective of the worm is system subversion. The systems were compromised using autonomous self propagating malware.

The effect of this event was the almost complete shutdown of the court system. Because of this minor arrests were suspended as well. The cause of the effect was a cyber event within the law enforcement infrastructure. This event had an effect of severely reducing the effectiveness of law enforcement.

8. Discussion

8.1. Usefulness

As the examples demonstrate our taxonomy is useful to e-government and industry for classifying cyber events and their effects on communities. Existing taxonomies do an adequate job of classifying a vulnerability or an attack on a single computer system. However, our taxonomy is much more capable of describing the motivation and methods for attacking a community, and the results of an attack on a community. These aspects are not considered by previous taxonomies.

Additionally, we believe our taxonomy will be useful in providing insights into the cyber events that threaten communities and critical infrastructures as discussed in the following section.

8.2. Future work

This research is the first step towards real time detection of cyber attacks on a community by the community government. This work is important because it leads to other very important work that must be done to work towards this goal.

First, we hope this taxonomy will prove useful by helping us to define exactly what constitutes an attack on a community, and how that differs from other types of cyber attacks or cyber events. Additionally, using this taxonomy we hope to identify what important metrics are needed to be gathered in real time to detect a cyber event. With a scientific definition of an attack on a community, and real time metrics detecting cyber events, we hope to develop a system that can analyze and detect attacks on a community in real time.

9. Conclusion

In this paper we have introduced a new taxonomy that is useful for classifying cyber events affecting communities. We focus on the motivations for attacking a community’s critical infrastructure and the effects on that community, two important ideas that have not been part of any previous computer security taxonomy.

Although we believe our taxonomy is useful to e-government and industry as it is, we hope that it will be of further use as it leads to greater insights into what constitutes an attack on a community, how an attack on a community might be detected in real time, and possible defenses against the different types of events affecting communities and critical infrastructure.
10. References


