Classifying Network Attack Scenarios using an Ontology

RP van Heerden[1,2], B Irwin[2], ID Burke[1]
[1]CSIR, Pretoria, South Africa
[2]Rhodes University, Grahamstown, South Africa
Keywords/ Key Phrases: Network attack, Taxonomy, Ontology, Attack Scenario
rvheerden@csir.co.za
b.irwin@ru.ac.za
iburke@csir.co.za

Abstract: This paper presents a methodology using network attack ontology to classify computer-based attacks. Computer network attacks differ in motivation, execution and end result. Because attacks are diverse, no standard classification exists. If an attack could be classified, it could be mitigated accordingly.
A taxonomy of computer network attacks forms the basis of the ontology. Most published taxonomies present an attack from either the attacker's or defender's point of view. This taxonomy presents both views. The main taxonomy classes are: Actor, Actor Location, Aggressor, Attack Goal, Attack Mechanism, Attack Scenario, Automation Level, Effects, Motivation, Phase, Scope and Target. The "Actor" class is the entity executing the attack. The "Actor Location" class is the Actor's country of origin. The "Aggressor" class is the group instigating an attack. The "Attack Goal" class specifies the attacker's goal. The "Attack Mechanism" class defines the attack methodology. The "Automation Level" class indicates the level of human interaction. The "Effects" class describes the consequences of an attack. The "Motivation" class specifies incentives for an attack. The "Scope" class describes the size and utility of the target. The "Target" class is the physical device or entity targeted by an attack. The "Vulnerability" class describes a target vulnerability used by the attacker. The "Phase" class represents an attack model that subdivides an attack into different phases.

The ontology was developed using an "Attack Scenario" class, which draws from other classes and can be used to characterize and classify computer network attacks. An "Attack Scenario" consists of phases, has a scope and is attributed to an actor and aggressor which have a goal. The "Attack Scenario" thus represents different classes of attacks. High profile computer network attacks such as Stuxnet and the Estonia attacks can now be been classified through the "Attack Scenario" class.

Section 1 Introduction

In Section 2 we define the research problem and the purpose of this paper. In Section 3 we discuss related research. In Section 4 we present a taxonomy of computer network attacks. In Section 5 we present an ontology that classifies network attack scenarios with respect to the taxonomy in Section 2.. In Section 6 we summarize our research and propose avenues for future research.

Section 2: The research problem

Computer networks are attacked on a daily basis. Attacks differ depending on different factors. Although each attack is unique, attacks share some commonalities. We classified computer network attacks into attack scenarios, and created a taxonomy to serve as a basis for a more full featured ontology that can be used to classify computer network attacks.

Section 3: Related research

Previous research on the use of ontologies in classifying computer network attacks is introduced in this Section. We discuss Taxonomies, Network Attack Ontologies and other research.

Ye et al designed an ontology for a Peer-to-Peer Multi-Agent Distributed Intrusion detection system. Using this ontology, a peer can detect suspicious activities from information received from other peers, and take action against future attacks (Ye, 2008).

Undercoffer et al designed an ontology that describes a model of computer attacks. The ontology is categorized according to target, attack strategy, attacker location and end result (Undercoffer, 2004).

More related research are listed in Section 3 and Section 4.

Section 4: Taxonomy

We developed a network attack taxonomy that describes a number of attack scenarios. The attack scenarios will be presented in Section 4.

Hansman listed requirements for a high-quality taxonomy (Hansman, 2003):

- Acceptable
- Comprehensible
- Completeness
- Determinism
- Mutually exclusive
- Repeatable
- Constant and defined Terminology
- Unambiguous
- Useful

Hansman also stated that a taxonomy cannot always meet all the requirements.

The taxonomy in this paper was created to form a basis for an ontology. It thus complies mainly with requirements for usefulness, mutual exclusivity, comprehensibility and unambiguity. The requirement for "Completeness" could not be achieved as the scope of network attacks is wide. The requirement for "Constant and defined terminology" could not be achieved as the ontology requires a broad definition of network attacks, and not minute detail as in a typical taxonomy.

4.1 Taxonomy detail

The main classes identified in the proposed taxonomy classes are discussed below:

- Actor
- Actor Location
- Aggressor
- Attack Goal
- Attack Mechanism
- Automation Level
- Effects
- Motivation
- Phase
- Scope
- Target
- Vulnerability

4.1.1 Actor

This class describes the entity executing the attack. Simmonds (2004) subdivided the Actor into "Script Kiddie", "Black Hat hacker", "Cracker", "Malevolent user" or "Malevolent sys Admin".

We expanded on Simmonds' work by adding "Commercial", "Criminal" and "Protest" subgroups. The "Hacker/Cracker/Malevolent" group is defined as "Hacker" or "Insider", with subclasses separating their effectiveness.

Rounds (2009) compiled a more comprehensive list that includes: "Script Kiddie", "Malware developer", "Hactivist", "Vigilante", "State Sponsored", "Thieves", "defensive hackers", "innocent hacker", "Enforcement DOS hacker" and "Terrorists".

We subdivide our Actor class as follows:

- Commercial Competitor
- Hacker
    - Script Kiddie Hacker
    - Skilled Hacker
- Insider
    - Admin Insider

    - Normal Insider
- Organised Criminal Group
- Protest Group

“Commercial Competitor” refers to an Actor that uses hacking for industrial espionage (Crane 2005). “Hacker” was subdivided into “Skilled” and “Script Kiddie” classes. “Script Kiddie” refers to hackers that use freely available tools without any in-depth knowledge of their inner workings.
“Script Kiddie” was also defined by Spitzner as “….someone looking for an easy kill ….not out for specific information or targeting a specific company ….goal is to gain root the easiest way possible …..by focusing on a small number of exploits and then searching the entire Internet for that exploit ….sooner or later they find someone vulnerable." (Spitzner, 2001)

“Insider” refers to a person with intimate access to the target computer’s infrastructure. This class is subdivided into “Admin” and “Normal”. “Admin” refers to the System Administrator or a person with elevated or full access. “Normal” refers to an employee or contractor with controlled access.

“Organised Criminal group” refer to criminal organisations that use hacking as an instrument for financial or other ill gain. Choo developed a typology that explores the different kinds of criminal groups in cyberspace (Choo, 2008).

“Protest group” refers to groups whose goals are driven by specific issues and that use hacking to effect change or spread propaganda. Taylor et al referred to this practice as "Hackticism" (Taylor, 2001).

4.1.2 Actor Location

This class refers to the country or state from whence an attack is launched, and derives from the "location of attack" class developed by Undercoffer.

Subclasses are:
- Foreign Actor Location
- Local Actor Location
- Indeterminate Actor Location

Lewis suggested that foreign militaries, criminals or terrorists can initiate cyber attacks and thus constitute a cyber threat (Lewis, 2002). The actor location can thus be outside the target’s national borders. The second subclass refers to an actor within the target’s national borders. Sometimes an actor location cannot be determined or spans different countries. In such cases the "Indeterminate Actor Location" subclass is used. Although the location of an attacking computer can be determined (Dickerson, 2000) it does not necessarily correspond with the actor’s physical location as the attack can be executed via the internet.

4.1.3 Aggressor

This class refers to the instigator of an attack, and differs from the Actor class in that it describes an association with an Actor, rather than a type of Actor.

Subclasses are:
- Individual Aggressor
- Commercial Aggressor
- State Aggressor
- Group Aggressor
    - Ad-hoc Group Aggressor
    - Organised Group Aggressor

"Individual Aggressor" refers to a single person instigating an attack without direct links to other persons or groups. "Commercial Aggressor" refers to a corporate entity for example the "News of the World" British tabloid that authorised other entities to hack celebrities’ cell phones (Myler 2011). “Group Aggressor” refers to an instigator with commercial or state associations, and can be either an organised group (for example Peta) or a "Ad hoc Group".

The SCO computer network was attacked in December 2003. Although no evidence exists, it is suspected that the attack was instigated following a lawsuit against IBM concerning IBM's use of Linux, and that open source activists were the attackers (Argyraki, 2005). The attack was not officially organised, and participants did not necessarily know each other.

"State Aggressor" refers to a nation or state that executes an attack. Brenner suggested that France, Russia, Japan, China, Germany, Israel and South Korea are actively engaged in economic espionage by means of the Internet and computer network attacks (Brenner, 2006).

4.1.4 Attack Goal

This class refers to the purpose of the attack, and is subdivided as follows:

- Change Data Attack Goal
- Destroy Data Attack Goal
- Disrupt Data Attack Goal
- Steal Data Attack Goal
- Springboard for other attack Goal

The first four goals correspond with the traditional CIA+ (Confidentiality, Availability, Integrity Authentication) information security principles. These goals are similar to Simmond's outcome class. The "Springboard for other attack" Goal represents instances where the network under attack is used only as a staging post for attacks on a different network.

4.1.5 Attack Mechanism

This class represents the attack methodology, and is linked to vulnerability maps (Simmonds). Attack mechanisms have been listed by Hansman.

Our subclasses are:

- Access
    - Brute Force
    - Buffer Overflow
    - Spear Phishing
    - Physical
- Data Manipulate
    - Network-based
        - Denial of Service
    - Virus-based
        - Trojan
        - Virus
        - Worm
    - Web Application-based
        - SQL Injection
        - Cross-site scripting (XSS)
- Information Gathering
    - Scanning
    - Physical

"Access" mechanisms refer to traditional hacking methods such as "Brute Force" and "Buffer overflow" methods (Cowan, 2000). "Spear Phishing" refers to targeted social engineering-type email attacks (Jagatic, 2007). "Physical" refers to manual methods to gain access, for example physically removing the hard drive or breaking the access door to enter a secure server room.

"Data Manipulate" mechanisms refer to attack methodologies that use data as an attack vector. The main vectors are network-based, virus-based or web application-based. "Network-based" refers to instances where the network itself forms part of the attack. The main methodology that uses this mechanism is "denial of service" attacks (Lau, 2000). Virus-based attacks can take the form of Trojans, Viruses or Worms.

Currently there is no clear scientific distinction between these attack methodologies. The most acknowledged definitions are (Yampolskiy, 2007):

- Virus: a self-replicating malicious program which requires a careless user or external software to replicate itself.
- Worm: a self-replicating program that automatically spreads through vulnerabilities.
- Trojan horse: a malware program posing as a legitimate program.

Web applications are most commonly attacked though SQL injection. SQL injection uses common escape characters to execute user-defined database queries, thus bypassing authentications and other security measures. Cross-site scripting (XSS) is a methodology that enables attackers to inject client-side script into Web pages. These pages can be viewed by unsuspecting users. Mookhey discussed techniques to identify Cross Site Scripting (CSS) and SQL Injection attacks (Mookhey, 2004).

“Information Gathering” refers to an attack that only assembles information. “Scanning” refers to port-scanning and other computer network-related scanning methodologies.

4.1.6 Automation Level

This class describes the degree to which network attacks are automated.

Our subclasses are:
- Manual
- Automatic
- Semi-Automatic

The subclasses were derived from Mirkovic’s taxonomy (Mirkovic’s, 2004). “Manual” refers to an attacker selecting the attack target and methodology by hand. “Automatic” refers to a system requiring minimum input from the attacker, even with regards to target selection. Mudge lists methods and tools that can be used to automate attacks. Most attacks are “semi-automatic” where some user interaction is required, but tools are used to execute attacks (Mudge, 2011).

4.1.7 Effects

This class refers to the impact of an attack. Mirkhovic discussed the impact of different attacks.

Our subclasses are:
- Null
- Minor Damage
- Major Damage
- Catastrophic

"Null" refers to no effect on the target, "Minor" to recoverable damage and "Major" to non-recoverable damage. “Catastrophic” refers to damage of such a nature that the target ceases to operate as an entity, for example declaration of bankruptcy.

4.1.8 Motivation

This class refers to an attacker’s motivation for an attack. Rounds listed possible motivations. The subclasses are:
- Financial
- Fun
- Ethical
- Criminal

"Financial" refers to hacking for financial or other gain such as stealing money or manipulation of the stock market. "Fun" refers to hackers looking for a challenging hack with no other evil intensions. "Ethical" refers to vigilantes or spies that work toward some national interest. "Criminal" motivation differs from "Financial" motivation, as some criminal organizations use network hacking to supplement to their operations.

4.1.9 Phase

This class represents different stages of an attack.

Grant et al identified nine stages: Footprinting, Reconnaissance, Vulnerability identification, Penetration, Control, Embedding, Data extraction, Attack relay and Attack dissemination (Grant, 2007). Brummell listed Footprinting, Scanning, Enumeration and System Hacking (Brummell, 2010).

Our subclasses are:

- Target Identification
- Reconnaissance
- Attack Phase
    - Ramp-Up
    - Damage
    - Residue
- Post-Attack Reconnaissance

”Target Identification” refers to the action of an attacker choosing a target. The motivation could be opportunistic, random, ideological or financial. The target identification phase ends when a specific device or entity (an individual, company or state institution) has been identified.

”Reconnaissance” refers to the action of an attacker probing a target for weakness. Probing consists of scanning, Google queries and other network-related activities. No computer or network system is changed or adversely affected. The goal is to identify avenues of attack whilst leaving network operations unaffected.

”Attack” refers to the action of compromising the target according to the CIA principles (Confidentiality, Integrity or Availability), and has three sub-phases.

The Ramp-Up sub-phase refers to the action of an attacker preparing to achieve a goal. The target may be affected but not necessary adversely. An example of the Ramp-Up phase is installation of a sniffer by an attacker on an unsuspecting user to harvest clear text passwords for later use to steal data.

The Damage sub-phase refers to the action of the attacker inflicting damage on the target. Damage may take the form of breached confidentiality, compromised integrity or disrupted service availability. Damage could be inflicted via data, physical means (computer-controlling hardware) or to the target’s reputation.

The Residue sub-phase refers to damage or artefacts of the attack that occur after the attack goal has been achieved, and occurs because the attacker loses control of some systems. For example after the launch of a DDOS (Distributed Denial of Service) attack, zombie computers may still connect to the target for some days following the attack.

”Post-Attack Reconnaissance” refers to actions undertaken by an attacker after the attack has occurred, and takes the form of inspections to verify if backdoors are still available, or scans to verify if security holes have been patched. The goal is not to inflict damage but to verify the target’s status.

4.1.10 Scope

This class refers to the size and type of entity that is targeted. The "Scope" class differs from the "Target" class in that it views the entity holistically, rather than looking at specific devices. Subclasses are:

- Corporate Network
    - Large Corporate Network
    - Small Corporate Network
- Government Network
    - Large Government Network
    - Small Government Network
- Private Network

Distinction between “Large” and “Small” corporate networks is not uniformly defined. Thus distinction between small and large networks must be defined for each entity classified in this class. The "Corporate Network" subclass refers to networks controlled by private companies. The "Government Network" subclass refers to networks controlled by the government. The "Private Network" subclass refers to a network that serves one person in his/her private capacity.

4.1.11 Target

This class refers to the devices that are targeted by an attack. Hansman proposed a taxonomy that listed the target as:

- Hardware
  - Network Equipment
  - Peripheral Devices
- Software
  - Operating Systems
    - Windows Family
    - Unix Family
  - Application
    - Server
    - User
- Network
  - Protocols
    - TCP
    - IP

Our proposed class refer to physical devices that are targeted, and subclasses are:

- Personal Computer
- Network Infrastructure Device
- Server

The "Personal Computer" subclass refers to PC's, Laptops, tablets and similar devices with a single user. "Network Infrastructure Device" refers to devices such as routers and switches that only enable data flow, but can still be attacked. The "Server" subclass refers to computers that are accessed by multiple users, such as web-server or database computers.

4.1.12 Vulnerability

This class refers to the weaknesses exploited by the attacker. Simmonds constructed a Vulnerability map:

- Security Policy & Short Term Time Scale
  - Social Engineering
    - Information phishing
    - Trojan
- Security Policy & Long Term Time Scale
  - Policy oversight
    - Poor planning
    - Poor control (weak passwords)
- Technology & Short Term Time Scale
  - Logic Error
    - Bugs
    - OS/Application vulnerabilities
    - Network Protocol Design
- Technology & Long Term Time Scale
  - Weakness
    - Weak password system
    - Old encryption standard

Undercoffer listed the following vulnerabilities: Input Validation Errors, Buffer Overflows, Boundary Condition Errors and other Malformed Input.

Our subclasses are as follows:

- Configuration
  - Access Rights
  - Default Setup
- Design
  - Open Access
  - Protocol Error
- Implementation
  - Buffer Overflow
  - Race Condition
  - SQL Injection
  - Variable Type Checking

"Configuration" vulnerabilities describe instances where vulnerabilities were exposed by incorrect configuration of a device or software. Two types of incorrect configuration are listed namely “Access Rights” and “Default Setup”.

"Access Rights" refers to an instance where incorrect access rights have been allocated to normal users. For example, Citygroup was hacked by thieves that penetrated the bank’s defences by first logging on to the site reserved for its credit card customers (Swhwartz, 2011).

"Default setup” refers to the use of default usernames and passwords to overcome the security of a system. This vulnerability is often caused by inexperienced or lazy users. Lancor and Workman described how Google can be used to hack systems by using default usernames and passwords (Lancor 2008).

"Design" vulnerabilities refer to a system that is insecure because of design errors. Design errors can be either in the protocol or in the access control. The "Ping-of-death" is an example of a protocol vulnerability (Karig, 2001).

"Implementation" vulnerabilities refer to vulnerabilities introduced by faulty coding or system construction. "Buffer Overflow" refers to the ability of injecting an attack code (Cowen, 2000). “Race Condition” is when a program creates a short opening for an attacker by opening a timed window of vulnerability. SQL Injection vulnerability is when an attacker takes advantage of flawed coding of web sites. An attacker usually injects SQL commands into a website to allow him access to a database (Razvan, 2009).

5 Proposed Ontology

Gruber described an ontology as ”*a specification of a representational vocabulary for a shared domain of discourse — definitions of classes, relations, functions, and other objects….”* (Gruber, 1993)

Noy and McGuinness defined an ontology as: “…. *a common vocabulary for researchers who need to share information in a domain …. includes machine-interpretable definitions of basic concepts in the domain and relations among them.*”(Noy, McGuinness 2001) .

They list the following motivations for developing an ontology:

- *Sharing a common understanding of the structure of information*
- *Facilitate reuse of domain knowledge*
- *Make domain assumptions clear*
- *Separate domain knowledge from operational knowledge*
- *Analyse domain knowledge*

Noy and McGuinness define an ontology as a formal explicit description of concepts of discourse classes, with the properties of each class describing various attributes of the concepts (slots) and their restrictions. Classes are the focal point of ontologies, and can be divided into subclasses which represent more detailed concepts.
They further state that developing an ontology requires:

- Definition of classes
- Arrangement of classes in a taxonomy

- Description of the attributes of slots
- Definition of allowed values for attributes
- Definition of events according to classes and slots

5.1 Defining classes and creating a taxonomy

The taxonomy in Section 3 forms the basis of the ontology. An "Attack Scenario" class supplements the taxonomy. The goal of this class is to present a type of network attack, providing a means through which the attack can be classified by the ontology. The list of attack scenarios presented in this paper is not comprehensive, but forms a basis from which to test the ontology's classification methodology.

The "Attack Scenario" class is subdivided as follows:

- Denial Of Service
- Industrial Espionage
- Web Deface
- Spear Phishing
- Password Harvesting
- Snooping for secrets
- Financial theft
- Amassing computer resources
- Industrial Sabotage
- Cyber Warfare

5.2 Describing attributes of slots

Classes and subclasses have a "is a" relationship. This relationship is similar for classes and subclasses. In Figure 1, the "is a" relationship for the "Actor" class is shown

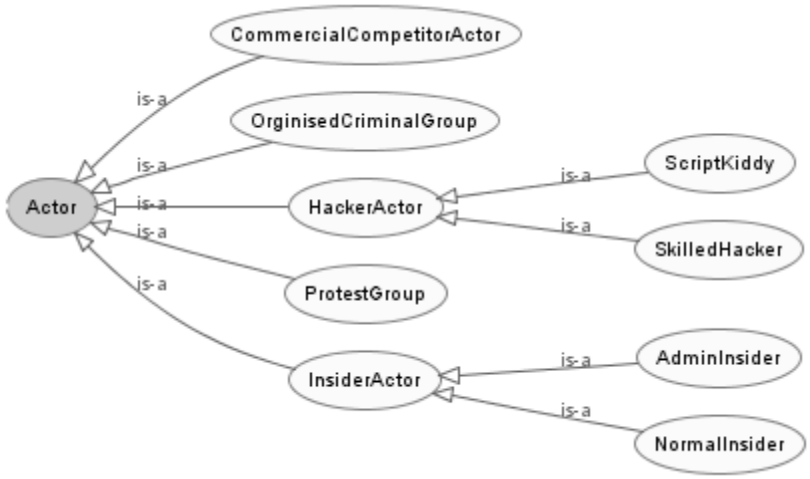

Figure 1: Actor class

Classes have inter-relationships as listed below:

- "Actor" has at least a "Actor Location"
- "Aggressor" must have some "motivation"
- "Attack Mechanism"
    - has a single "Target"
    - has one "Automation" level
- "Phase"
    - must have an "Attack Mechanism"
    - has one "Effect"
- "Target" must have a "Vulnerability"
- "Attack Scenario"
    - must have an "Attack Goal"
    - must have a "Phase"
    - has at least one "Actor"

- has at least one "Aggressor"

5.3 Defining the allowed values for attributes

Each "Attack Scenario" class has unique constraints that separate it from other scenarios. These constraints are listed in the following sections.

5.3.1 Denial of Service

This scenario represents an attack of the availability of computer services by overwhelming the available resources, and has the following constraints:

- "Attack Goal" must be "Disrupt"
- "Automation Level" must be "Automatic"
- "Vulnerability" must be "Design Vulnerability"
- “Attack Mechanism" of the “Damage Phase” must be "Denial of Service"

Needham discussed examples of Denial of Service attacks (Needham, 1994).
In February 2004, the SCO website was attacked by a distributed Denial of Service attack. This attack was generated by My-doom worm (Hurley, 2004).

5.3.2 Industrial Espionage

This scenario represents stealing industrial secrets through computer networks, and has the following constraints:

- "Attack Goal" must be "Steal Data"
- "Scope" must be "Corporate Network"
- "Aggressor" must be "Commercial" or "State"
- "Motivation" must be "Financial"
- "Attack Mechanism" of the “Damage Phase” must be "Access Attack"

"Operation shady rat" (Alperovitch, 2011) is the systematic industrial espionage operation sponsored by China and revealed in 2011.

5.3.3 Web Deface

This scenario represents altering websites without permission. Hacker groups even have competitions for who can deface the most websites [www.rankmyhack.com]. This scenario has the following constraints:

- "Attack Goal" must be "Change Data"
- "Actor" must be "Hacker"
- "Target" must be "Server"
- "Aggressor" must be "Commercial" or "State"
- "Motivation" must be "Fun" or "Ethical"
- "Effects" must be "Minor or Major"
- "Attack Mechanism" of the “Damage Phase” must be "Web Application-based"

5.3.4 Spear Phishing

This attack uses social engineering techniques to entice an individual to disclose information that can be used to attack his/her place of work. Most spear phishing attacks are not published to protect the targeted person and the company’s reputation (Brody, 2007). This scenario has the following constraints:

- "Attack Goal" must be "Steal Data"
- "Actor" must be "Hacker"
- "Automation Level" must be "Manual"
- "Target" must be "PC"
- "Motivation" must be "Financial"
- "Attack Mechanism" of the ‘Damage Phase” must be "Spear Phishing"

5.3.5 Password Harvesting

This scenario refers to collection of password lists for future attacks, and has the following constraints:

- "Attack Goal" must be "Steal Data"
- "Actor" must be "Hacker" or "Organised Criminal group"
- "Target" must be "Server"
- "Aggressor" must be "Individual Aggressor"
- "Motivation" must "Criminal" or "Financial"
- “Attack Mechanism” of the "Target Identification Phase" must be "Access"

The "MySpace.com" user and password database was breached. 50 000 passwords was released on the web soon after the breach. Kelley et al used these publicly available lists for testing password cracking algorithms (Kelley, 2011).

5.3.6 Snooping for secrets

This scenario represents curious individuals nosing around for secrets. Gary McKinnon, a UK citizen, is facing extradition to the US after being caught hacking NASA and other US state entities. McKinnon has been diagnosed with Asperger's Syndrome (Espiner, 2009). This scenario has the following constraints:

- "Attack Goal" must be "Steal Data"
- "Actor" must be "Hacker"
- "Automation Level" must be "Manual"
- "Target" must be "Server"
- "Aggressor" must be "Individual"
- "Motivation" must "Fun"
- "Effects" must be "Null" or "Minor"
- "Attack Mechanism" of the “Damage Phase” must be "Information Gathering"

5.3.7 Financial theft

This scenario refers to stealing money via computers. Computer networks in banks and other financial institutions can be compromised and money transferred electronically to criminals. Individuals can also be targeted and attacked through web banking interfaces. This scenario has the following constraints:

- "Attack Goal" must be "Change Data"
- "Actor" must be "Organised Criminal Group" or "Hacker"
- "Automation Level" must be "Manual"
- "Target" must be "Server" or "PC"
- "Aggressor" must be "Individual"
- "Motivation" must "Financial"
- "Attack Mechanism" of the “Damage Phase” must be "Data Manipulate"

In 1995 a Russian hacker broke into Citibank computer systems and stole more than $10 million. (Harmon, 1995)

5.3.8 Amassing computer resources

This scenario refers to act of controlling computers, so that the collection of computer recourses can be sold or used at a later date. For example millions of "zombie" computers are for sale on the black market on the internet (Markoff, 2007). This scenario has the following constraints:

- "Actor" must be "Organised Criminal Group"
- "Automation Level" must be "Automated"
- "Target" must be "PC"
- "Motivation" must "Financial"
- "Effects" must be "Minor Damage"
- The "Damage Phase" 's "Attack Mechanisms" must "Virus Attack"

5.3.9 Industrial Sabotage

This scenario refers to damaging industrial capability of commercial or state entities. The most famous industrial sabotage computer attack is the "Stuxnet" worm attack on the Iranian nuclear infrastructure(Falliere, 2010). This attack used computer networks attack the Programmable Logic Controllers of the Bashir Nuclear plant in Iran. This scenario has the following constraints:

- "Attack Goal" must be "Disrupt"
- "Actor" must be "Organised Criminal" or Commercial Competitor"
- "Scope" must be "Large Corporate Network"
- "Aggressor" must be "Organised group"
- "Motivation" must "Ethical" nor "Criminal"
- "Effects" must be "Catastrophic or Major Damage"
- The "Damage Phase" 's "Attack Mechanisms" must "Data Manipulation"

5.3.10 Cyber Warfare

This scenario refers to refer where nation states uses the Internet to leach an attack on other nation state. In 2008, Estonia computer networks was attacked. Information security specialists identify the attack as an unprecedented assault on the electronic infrastructure of a state (public and private), originating in Russia, which was angry over Estonia's relocation of a Soviet war memorial. Russian representatives rebuffed any official involvement (Finn, 2007).

- "Attack Goal" must be "Disrupt"
- "Scope" must be "Government Network"
- "Aggressor" must be "Organised Group"
- "Motivation" must "Ethical"
- "Effects" must be "Catastrophic or Major Damage"
- ""Actor Location" must be "Foreign Actor"
- The "Damage Phase" 's "Attack Mechanisms" must "Data Manipulation"

6 Future Work and Conclusion

From this Taxonomy and Ontology it is possible to classify a large range of computer network attacks. This paper is a preliminary attempt to classify the attacks from the viewpoints of the attacker and the target. For future work, the "Attack Scenario's" can be refined and expanded. The 10 scenarios listed does not represent a complete scope of network attacks. Once the Ontology has been refined, it can be used for network attack prediction. Intrusion Detection system concentrate only on specifics of network attack incidences, not in the overall scope or scenario of the attack. By combining the Ontology with attack sensors, a better understanding of the network attack can be formulated.

References

Alperovitch, D., & President, V. (2011). Revealed: Operation shady rat. *McAfee Inc, Santa Clara, CA, USA,* www.mcafee.com/us/resources/white.../wp-operation-shady-rat.pdf

Argyraki, K., & Cheriton, D. R. (2005). Active internet traffic filtering: Real-time response to denial-of-service attacks. *USENIX 2005,*

Brenner, S. W., & Crescenzi, A. C. (2006). State-sponsored crime: The futility of the economic espionage act. *Hous.J.Int'l L., 28*, 389.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal, 11*(3), 43-57.

Brummell, N. H., Tobias, S. M., & Cattaneo, F. (2010). *Dynamo efficiency in compressible convective dynamos with and without penetration* Taylor & Francis.

Choo, K. K. R. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime, 11*(3), 270-295.

Cowan, C., Wagle, P., Pu, C., Beattie, S., & Walpole, J. (2000). Buffer overflows: Attacks and defenses for the vulnerability of the decade. Paper presented at the *Discex,* 1119.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48*(3), 233-240.

Dickerson, J. E., & Dickerson, J. A. (2000). Fuzzy network profiling for intrusion detection. Paper presented at the *Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American,* 301-306.

Falliere, N., Murchu, L. O., & Chien, E. (2010). W32. stuxnet dossier. *Symantec Security Response,[Online], Accessed, 14*

Finn, P. (2007). Cyber assaults on estonia typify a new battle tactic. *Washington Post, 19*

Grant, T., Venter, H., & Eloff, J. (2007). Simulating adversarial interactions between intruders and system administrators using OODA-RR. Paper presented at the *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries,* 46-55.

Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition, 5*(2), 199-220.

Hansman, S. (2003). A taxonomy of network and computer attack methodologies. *Supervisor: Ray Hunt, Department of Computer Science and Software Engineering, University of Cantebury, Christchurch, New Zealand, November,*

Harmon, A. (1995). *Hacking theft of $10 million from citibank revealed.* Retrieved 10/10, 2011, from http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system

Hurley, E. (2004). *SCO site succumbs to DDoS attack.* Retrieved 10/10, 2011, from http://searchsecurity.techtarget.com/news/947481/SCO-site-succumbs-to-DDoS-attack

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Karig, D., & Lee, R. (2001). Remote denial of service attacks and countermeasures. *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002,*

Kelley, P., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., et al. (2011). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms (CMU-CyLab-11-008).

Lancor, L., & Workman, R. (2007). Using Google hacking to enhance defense strategies. *ACM SIGCSE Bulletin, 39*(1), 491-495.

Lau, F., Rubin, S. H., Smith, M. H., & Trajkovic, L. (2000). Distributed denial of service attacks. Paper presented at the *Systems, Man, and Cybernetics, 2000 IEEE International Conference on,* 2275-2280 vol. 3.

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. *Center for Strategic and International Studies,* 1-12.

Markoff, J. (2007). Attack of the zombie computers is growing threat. *New York Times,* http://www.nytimes.com/2007/01/07/technology/07net.html?pagewanted=all

McKinnon a cyber-terrorist, I. (2009). OBSESSED: Should a computer hacker with asperger syndrome go to prison?

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.

Mookhey, K., & Burghate, N. (2004). Detection of SQL injection and cross-site scripting attacks. Article from: http://www.Securityfocus.com/infocus/1768*,*

Mudge, R. (2011). Live-fire security testing with armitage and metasploit. *Linux Journal, 2011*(205), 1.

Myler, C., & Wapping, L. (2011). *News of the world.* Retrieved 10/06, 2011, from http://medbib.com/News_of_the_World

Needham, R. M. (1994). Denial of service: An example. *Communications of the ACM, 37*(11), 42-46.

Noy, N. F., & McGuinness, D. L. (2001). Ontology development 101: A guide to creating your first ontology. Stanford University, Stanford, CA, 94305

Razvan, R. (2009). Over the SQL injection hacking method. Paper presented at the *Proceedings of the 3rd International Conference on Communications and Information Technology,* 116-118.

Rounds, M., & Pendgraft, N. (2009). Diversity in network attacker motivation: A literature review. Paper presented at the *2009 International Conference on Computational Science and Engineering,* 319-323.

Schwartz, N. D., & Dash E. (2011). *Thieves found citigroup site an easy entry.* Retrieved 10/10, 2011, from http://www.nytimes.com/2011/06/14/technology/14security.html?_r=1

Simmonds, A., Sandilands, P., & van Ekert, L. (2004). An ontology for network security attacks. *Applied Computing Conference, AACC 2004, Kathmandu, Nepal, October 29-31,* 317-323.

Spitzner, L. (2001). Know your enemy. *Parts I, II, III." Available Online: www.Linuxnewbie.org/nhf/intel/security/enemy.Html.(for Parts II and III, Replace" Enemy" with" enemy2" and" enemy3," Respectively.),*

Taylor, P. A. (2001). Editorial: Hacktivism. *The Semiotic Review of Books, 12*(1)

Undercoffer, J., Joshi, A., Finin, T., & Pinkston, J. (2004). A target-centric ontology for intrusion detection. Paper presented at the *18th International Joint Conference on Artificial Intelligence,* 9-15.

Yampolskiy, R. V., & Govindaraju, V. (2007). Computer security: A survey of methods and systems. *Journal of Computer Science, 3*(7), 478-486.

Ye, D., Bai, Q., Zhang, M., & Ye, Z. (2008). P2P distributed intrusion detections by using mobile agents. Paper presented at the *Seventh IEEE/ACIS International Conference on Computer and Information Science,* 259-265.