## A computer network attack taxonomy and ontology

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

**Abstract:** Computer network attacks differ in the motivation of the entity behind the attack, the execution and the end result. The diversity of attacks has a consequence that no standard classification exists. The benefit of automated classification of attacks, means that an attack could be mitigated accordingly. The authors extend a previous, initial taxonomy of computer network attacks which forms the basis of a proposed network attack ontology in this paper. The objective of this ontology is to automate the classification of a network attack during its early stages.

Most published taxonomies present an attack from either the attacker's or defender's point of view. The authors’ taxonomy presents both these points of view.
The framework for an ontology was developed using a core class, the "Attack Scenario", which can be used to characterize and classify computer network attacks.

## 1. Introduction

Computer networks are attacked on a daily basis. Although each attack is unique and has different characteristics, attacks share some commonalities. The taxonomy and ontology presented in this paper exploit these commonalities to classify attacks. The authors classify computer network attacks into attack scenarios, extend their taxonomy in this paper, and use the taxonomy to serve as a basis for an ontology that can be used to classify computer network attacks. An ontology represents taxonomical information as well as relations between entities.

A significant body of research has been performed on the use of ontologies in classifying computer network attacks. An overview of taxonomies, network attack ontologies and other related research follow.

Hansman & Hunt (2003) developed a taxonomy which presents attack mythologies. Gandhi et al. (2011) aimed to thoroughly understand a cyber-attack by studying the nature and the motivation behind it, and then developed a taxonomy which classifies a hacker’s motivation into three classes: political, socio-cultural and economical. Lindqvist & Jonsson (1997) presented a classification of network intrusions. Their classification was build on intrusion experiments and used classes originally developed by Neumann & Parker (1989). Tutânescu & Sofron (2003) described active and passive computer network attacks. Simmonds et al. (2004) defined an extensible ontology for network security which followed from teaching a network security course at the University of Technology Sydney. They developed a map that demonstrates vulnerability relationships. Rounds & Pendgraft (2009) investigated the diversity in network attacker motivations and compiled a list of possible hacker agents. Debar et al. (1999) developed a taxonomy that defined families of intrusion-detection systems according to their properties. Undercoffer et al. (2004) designed an ontology that describes a model of computer attacks. This ontology is categorized according to target, attack strategy, attacker location and end result. Ye et al. (2008) 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.

In Section 2, we present a taxonomy of computer network attacks, followed in Section 3 by a framework for an ontology that classifies network attack scenarios with respect to the taxonomy. In Section 4 we summarize our research and propose avenues for future research.

Research related to specific classes in our taxonomy and ontology is mentioned in the subsequent sections.

## 2. Taxonomy

In this section the authors present an extended network attack taxonomy that describes a number of attack scenarios. The initial taxonomy was presented in van Heerden et al. (2012a). The detailed descriptions of the attack scenarios follow the next sub-section.

Hansman & Hunt (2003) listed the following requirements for a high-quality taxonomy. It must be

- Acceptable,
- Comprehensible,
- Complete,
- Deterministic,
- Mutually exclusive,
- Repeatable,
- Constant and contain a defined terminology,
- Unambiguous, and
- Useful

Hansman & Hunt 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 met since the scope of network attacks is too wide. The requirement to be constant and contain a defined terminology could not be met since the ontology requires a broad definition of network attacks, and not minute detail such as is contained in a typical taxonomy.

### Taxonomy detail

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

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

Each of these classes is discussed in a subsection below.

## Actor Class

The “Actor” class describes the entity executing the attack. Simmonds et al. (2004) subdivided the actor into “Script Kiddie”, "Black Hat Hacker”, “Cracker”, “Malevolent User” or “Malevolent Sys Admin”.

We expand on the work of Simmonds et al. and add "Group Actor" which includes "Organized Criminal Group", "Protest Group" and "Cyber Army". The “Hacker/Cracker/Malevolent” group is defined as “Hacker” or “Insider”, with subclasses addressing their effectiveness.

Rounds & Pendgraft (2009) compiled a more comprehensive list that includes: “Script Kiddie”, “Malware Developer”, “Hacktivist”, “Vigilante”, “State Sponsored”, “Thieves”, “Defensive Hacker”, “Innocent Hacker”, “Enforcement DOS Hacker” and “Terrorist”.

We subdivide our “Actor” class as follows:

- Group Actor
  - Organized Criminal Group
  - Protest Group
  - Cyber Army
- Hacker
  - Script Kiddie Hacker
  - Skilled Hacker
- Insider
  - Admin Insider
  - Normal Insider
- Unknown Actor

The sub-class "Organised Criminal Group" refers to organizations that launch network and computer attacks for financial and other gains. For example, in Russia criminal organizations have recruited hackers to launch attacks on their behalf

(Savona & Mignone, 2004). The "Organized Criminal Group" sub-class is not placed in the "Aggressor" class because the "Aggressor" class refers to criminal groups that who hire hackers perform their own attacks. Choo (2008) developed a typology that explores the different kinds of criminal groups in cyberspace.

Protest groups refer to groups that attack networks because of some ethical reason. This also include groups whose goals are driven by specific issues, and that use hacking to effect change or spread propaganda. Taylor (2001) referred to this practice as "Hacktivism". The hacking group *Anonymous* is an example of a protest group that launched network attacks not as a criminal group, but rather as a protest group (Schwartz, 2012).

The "Cyber Army" sub-class refers to military personnel who perform computer based attacks as part of their normal duties. The "Insider" sub-class refers to a person who is a member of a target organization or is in some trusted relationship with the target. Magklaras & Furnell (2001) defined three main insider groups: system masters, advanced users and applications users. The advanced and applications users are classified as "Normal" users and System masters as "Administrators". The distinction between advanced and application users is considered to be too vague for our taxonomy.

For this research it was decided to group "Hacker", "Cracker" and "Malevolent User" in the authors' "Hacker" sub-class. The hacker agents described by Rounds & Pendgraft (2009) were used to verify the possible classes, although some of their classes were used by the "Aggressor" class. The "Hacker" sub-class is subdivided into “Script Kiddie” and “Skilled Hacker”. "Script Kiddie" refers to hackers that use freely available tools without any in-depth knowledge of their inner workings. Spitzner (2001) defined a Script Kiddie 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.*

## Actor Location Class

This class refers to the country or state from where an attack is launched, and derives from the "Location of Attack" class developed by Undercoffer et al. (2004).

Sub-classes are:

- Foreign Actor Location
- Local Actor Location
- Indeterminate Actor Location

Lewis (2002) suggested that foreign militaries, criminals or terrorists can initiate cyber attacks and thus constitute a cyber threat. The actor location can thus be outside the target's national borders. The second sub-class above 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" sub-class is used. Although the location of an attacking computer can be determined (Dickerson & Dickerson, 2000), it does not necessarily correspond with the actor’s physical location because the attack can be executed via the Internet.

## Aggressor Class

This class refers to the perpetrator of an attack, and differs from the "Actor" class in that it describes an association with an Actor, rather than a type of Actor. The subclasses of the "Aggressor" class are:

- State;
- Commercial Aggressor
    - Organised Group Aggressor
    - Flash Mob
- Individual Aggressor
- Self Instigator
- Unknown Aggressor.

"State" refers to a nation or state that sanctions an attack. Brenner & Crescenzi (2006) 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. "Commercial Aggressor" refers to a corporate entity, for example, the "News of the World" British tabloid that authorized other entities to hack celebrities' cell phones (Myler & Wapping, 2011). "Commercial Aggressor" has the sub-classes "Organized Group Aggressor" and "Flash Mob". "Organized Group Aggressor" refers to a perpetrator with commercial associations. "Flash Mob" refers to attackers that are not officially organized, and participants do not necessarily know each other.

The SCO group 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 & Cheriton, 2005). When the "Aggressor" and "Actor" are the same entity, the "Self Instigator" sub-class is used. This sub-class refers to lone hackers that are not motivated by an external party. The "Unknown Aggressor" sub-class is used when the identity of the perpetrator is unknown. For example, up to 2010 the instigators and perpetrators of the Conficker worm attack had not been identified (Conficker Working Group, 2011).

## Asset Class

This class refers to the device class that is under attack. This class distinguishes between different assets that can be attacked. Examples of assets are information stored as data, the system that uses computers, or the network infrastructure itself. The "Asset" class is subdivided as follows:

- Network
- System
- Data
- Access.

Typically, the goal of a Denial-of-Service attack is to deny users access to their own computer resources, or as described by Specht and Lee (2004): "*A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource*". When an attack targets communication infrastructure, the affected asset is classified as "Network". When attacks affect information, "Data" is the asset under attack. This can include changing data, stealing data and removing data. The "Access" sub-class refers to when unauthorized access to computers/computer networks has been obtained. Some attacks make use of computer networks to attack physical assets outside the computer network. For example, with the Logic bomb a pipeline was affected, and with Stuxnet centrifuges were the affected. These attacks are classified as to affect the "System" asset.

## Attack Goal Class

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 the outcome class of Simmonds et al. (2004) 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.

## Attack Mechanism

This class represents the attack methodology, and is linked to vulnerability maps (Simmonds et al., 2004). Attack mechanisms have been listed by Hansman & Hunt (2003).

Our subclasses are:

- Access
    - Brute Force
    - Buffer Overflow
    - Spear Phishing
    - Social Engineering
- Data Manipulate
    - Network-based
    - Infective Malware
        - Trojan
        - Virus
        - Worm
    - Web Application-based
        - SQL Injection
        - Cross-site scripting (XSS)
- Information Gathering
    - Scanning

    - Open Information

“Access” mechanisms refer to traditional hacking methods such as "Brute Force" and "Buffer Overflow" methods (Cowan et al., 2000. “Spear Phishing” refers to targeted social engineering-type e-mail attacks (Jagatic et al., 2007). Social engineering is defined by Rouse (2006) as: *"Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures"*.

“Data Manipulate” mechanisms refer to attack methodologies that use data as an attack vector. The main vectors are network-based, infective malware 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 et al., 2000). Infective malware 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 & Govindaraju, 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 & Burghate (2004) discussed techniques to identify XSS and SQL injection attacks.

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

## Automation Level

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

Our sub-classes are:

- Manual
- Automatic
- Semi-Automatic

These sub-classes were derived from Mirkovic & Reiher'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 (2011) 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.

## Effects

This class refers to the impact of an attack. Mirkovic & Reiher (2004) discussed the impact of different attacks in their research.

Our sub-classes 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, the declaration of bankruptcy as a result of an attack.

## Motivation

This class refers to an attacker’s motivation for launching an attack. Rounds & Pendgraft  (2009) listed possible motivations that included classes from Gandhi et al. (2011).

Our sub-classes are:

- Criminal
- Financial
- Ethical
  - Political
  - Espionage
  - Vigilantism
- Fun

"Financial" refers to hacking for financial or other gain such as stealing money or manipulating the stock market. "Fun" refers to hackers looking for a challenging hack with no malicious intensions. "Criminal" motivation differs from "Financial" motivation, as some criminal organizations use network hacking to supplement to their operations. "Ethical" motivation refers to a motivation that has an ethical aspect. This ethical aspect can be national interests of spies, political reasoning or vigilantes.

## Phase

This class represents different stages of an attack.

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

Our sub-classes 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 can 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 weaknesses. 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 necessarily adversely. An example of the Ramp-Up sub-phase is the installation of a sniffer by an attacker on an unsuspecting user to harvest clear text passwords for later use such as the stealing of 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.

## Scope Class

This class refers to the 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. Our sub-classes for the Scope class are:

- Corporate Network
- Critical Information Infrastructure
- Government Network
- Individual Scope
- Military Network

- All networks

The "Corporate Network" sub-class refers to networks controlled by private companies. The "Government Network" sub-class refers to networks controlled by the government, and has two sub-classes: "Government Agency" such as a Department of Home Affairs corporate network, and "Government E-Business" that includes websites used by the public to access information. The "Private Network" sub-class refers to a network that serves one person in his/her private capacity.

## Scope Size Class

This class refers to the size of entity that is targeted. Our sub-classes for this class are:

- Global Network
- Large Network
- Medium Network
- Small Network
- Single

If an attack affects a large portion of the Internet or multiple countries, the scope size is referred to as "Global Network". "Large Network" represents large corporations or significant government networks such as state departments. There are no hard definitions that separate small, medium and large networks, and thus this separation is an subjective judgement. "Single" size is used to present attacks on a single person or single computer.

## Target

This class refers to the devices that are targeted by an attack. Hansman & Hunt (2003) 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 sub-classes refer to physical devices that are targeted:

- Personal Computer
- Network Infrastructure Device

- Server
- Industrial Equipment

The "Personal Computer" sub-class refers to PCs, 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" sub-class refers to computers that are accessed by multiple users, such as web-server or database computers. The "Industrial Equipment" sub-class refers to computerized automation equipment used in industrial plants. Such equipment is also referred to as Supervisory Control And Data Acquisition (SCADA) systems. A PC has a lot of useful information or other potential malicious uses that can be exploited by an attacker. Krebs (2012) compiled a list of all the methods that can be used to compromise a PC for monetary gain.

## Vulnerability

This class refers to the weaknesses exploited by the attacker. Simmonds et al. (2004) 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 et al. (2004) listed the following vulnerabilities: Input Validation Errors, Buffer Overflows, Boundary Condition Errors and other Malformed Input.

Our sub-classes are as follow:

- 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, Citigroup was hacked by thieves that penetrated the bank’s defences by first logging on to the site reserved for its credit card customers (Schwarz & Dash, 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 & Workman (2007) described how Google can be used to hack systems by using default usernames and passwords.

"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 & Lee, 2001).

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

## 3 The Network Attack Ontology Framework

This section describes what an ontology is and gives a short overview of requirements and motivations for developing an ontology. It is followed by a description of our network attack ontology's framework.

Gruber (1993) described an ontology as ”*a specification of a representational vocabulary for a shared domain of discourse — definitions of classes, relations, functions, and other objects….”*. Noy & McGuinness (2001) 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.*”. They further described 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 sub-classes which represent more detailed concepts.

Noy & McGuinness listed motivations (below) for developing an ontology and also requirements for the developing an ontology (in the second bulleted list below). 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; and
- Analyse domain knowledge.

Ontology development requirements:

- Definition of classes;
- Arrangement of classes in a taxonomy;
- Description of the attributes of slots;
- Definition of allowed values for attributes; and
- Definition of events according to classes and slots.

## Network Attack Ontology Framework

The taxonomy in Section 2 forms the basis of our 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 "Attack Scenario" class was developed by van Heerden et al (2012) by investigating famous and significant computer attacks.

The "Attack Scenario" class is subdivided as follows:

- Denial Of Service
- Industrial Espionage
- Snooping for secrets
- Financial theft
- Amassing computer resources
- Cyber Warfare
- Runaway Malware
- Web Deface
- Industrial Sabotage

The "Denial of Service" scenario is used to describe attacks that target accessibility by overloading a victim's capability to respond to a flood of interaction request. "Industrial Espionage" refers to the theft of commercial valuable data such as trade secrets, system blueprints or sales numbers. The "Snooping for Secrets" scenario differs from "Industrial Espionage" in that the goal of stealing secrets is not commercial in nature, and the secrets themselves may have no commercial value apart from the mere fact that the data is secret.

"Web Defacement" can be considered graffiti of the digital world. Web sites are the public face of commercial and other entities in the digital world, and their reputations are negatively affected when by defacing it.

Computers can be used for direct financial gain by stealing money directly from banks, individuals or other institutions. Computer attacks with a solely financial goal belong to the "Financial Theft" scenario. The goal of many malware applications is to control computer and networks. These controlled computers are also referred to as zombies. Zombie computers can be used for other scenarios, but the processes of collecting zombie computers belong to the "Amassing Computer Resources" scenario.

The "Industrial Sabotage" scenario refers to instances where computers are used to attack other industrial targets physically. The Logic bomb and Stuxnet attacks resulted in physical damage to industrial equipment. The next step is to use computers directly in war. This was done in the South Ossetia war where computer attacks were launched in conjunction with military operations.

Many malware applications that caused the most damage and financial losses were software that was written without any goal other than to see how far it could spread. These instances of "Runaway Malware" usually exploit come technical flaw that allows it to spread.

The ontology maps all the classes of the Network Attack taxonomy into a single concept, with the "Attack Scenario" as its base class. This mapping is presented in Figure 1 and it narrates the following story (The classes are in bold and within brackets):

> *An [**Actor**] based at [**ActorLocation**] location with the goal of [**AttackGoal**] sponsored by [**Aggressor**] with a [**Motivation**] motivation The attack effected [**ScopeSize**] [**Scope**] scope. A [**Target**] was attacked via [**Vulnerability**]. This attack affected [**Asset**] and resulted in [**Sabotage**] and having [**Effect**] effect During the [**Phase**] phase an [**AttackMechanism**] was used. This mechanism was automated to [**AutomationLevel**] level and used [**Vulnerability**].*

In Figure 1 the relationships between the formal classes are shown along with their uses in the story. Each of the attack scenarios can now be described with their sets of classes and sub-classes in a similar story as above. For example, a "Web Deface" attack can be narrated as follows:

> *An **Hacker** based at [**ActorLocation**] location with the goal of [**AttackGoal**] sponsored by [**Aggressor**] with a **Fun** OR **Ethical motivation.** The attack effected [**ScopeSize**] **Corporate OR Government Network** scope. A **Server** was attacked via [**Vulnerability**]. This attack effected the **Data** and resulted in **Reputation Loss** and having [**Effect**] effect During the **Damage an Data Manipulation Attack Mechanism** was used. This mechanism was automated to [**AutomationLevel**] level and used [**Vulnerability**].*

Specific attacks (or individuals) can also be described in the story form. For example, the defacement of *Apache.org* website story is as follows (Dede, 2010):

> *An **Hacker** (**Peter van Dijk and accomplices** based at **Foreign** location with the goal of **Changing Data** sponsored by **Self** with a **Fun** motivation The attack effected **Medium Network Corporate** scope. A **Web Server** was attacked via **Configuration Vulnerability**. This attack effected the **Data (Web Site)** and resulted in **Reputation Loss** and having **Minimal** effect During the **Damage** an **Data Manipulation Attack Mechanism** was used. This mechanism was automated to **Manual** level and used **Configuration Vulnerability**.*

## 4. Future Work and Conclusion

The authors describe a network attack taxonomy and ontology framework. It is possible to classify a large range of computer network attacks. This paper is an attempt to classify the attacks from the viewpoints of both the attacker and the target. For future work, the "Attack Scenario" class can be formally defined and expanded, as well as the relations between the various classes.

Once the ontology has been refined, it can be used for network attack prediction. Intrusion detection systems 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

Argyraki, K., & Cheriton, D. (2005). Active internet traffic filtering: Real-time response to Denial-of-Service Attacks. The Advanced Computing System Association's Annual Technical Conference (USENIX 2005), Anaheim, CA .

Brenner, S., & Crescenzi, A. (2006). State-Sponsored Crime: The Futility of the Economic Espionage Act. *Houston Journal of International Law, 28(2), 389-432.*

Brummell, N. H., Tobias, S. M., & Cattaneo, F. (2010). Dynamo efficiency in compressible convective dynamos with and without penetration (Vol. 104). Taylor and Francis.

Choo, K. K. (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. *DARPA Information Survivability Conference and Exposition (DISCEX '00)* (pp. 119-129). IEEE Computer Society.

Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer Networks, 31 (8),* 805-822.

Dede, D. (2010). Apache.org Defaced - Security Archive Case Study. Retrieved November 16, 2012, from http://blog.sucuri.net/2010/03/apache-org-defaced-security-archive-case-study.html.

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

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *Technology and Society Magazine, 30 (1)*, 28-38.

Grant, T., Venter, H., & Eloff, J. (2007). Simulating adversarial interactions between intruders and system administrators using OODA-RR. Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, (SAICSIT 2007) (pp. 46-55). ACM.

Conficker Working Group. (2011). Conficker Working Group: Lessons Learned Document. Retrieved 16 November, 2012 from http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/LessonsLearned#toc1

Gruber, T. R. (1993). A Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition, 5 (2),* 199-220.

Hansman, S., & Hunt, R. (2003). A Taxonomy of Network and Computer Attack Methodologies. Master's thesis. Department of Computer Science and Software Engineering University of Canterbury. Retrieved 16 November 2012 from http://citeseerx.ist.psu.edu/oai2.

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*. (Tech. Rep. No. CE-L2001-002). Princeton University, Department of Electrical Engineering.

Krebs, B. (2012). The Scrap Value of a Hacked PC, Revisited. Retrieved November 7, 2012, from *Krebs on Security*: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/ .

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*. 2000 IEEE International Conference on Systems, Man, and Cybernetics (pp. 2275-2280). USA.

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*. Washington, DC. Retrieved 16 November 2012 from http://csis.org/publication/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats.

Lindqvist, U., & Jonsson, E. (1997). How to Systematically Classify Computer Security Intrusions. *IEEE Symposium on Privacy and Security*, (pp. 154-163). Oakland, CA.

Magklaras, G., & Furnell, S. (2001). Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse. *Computers & Security, 21(1)*, 62-73.

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. *Symantic*. Retrieved 18 November 2012 from http://www.symantec.com/connect/articles/detection-sql-injection-and-cross-site-scripting-attacks

Mudge, R. (2011). Live-fire Security Testing with Armitage and Metasploit*. Linux Journal , 2011 (205).* Retrieved 18 November 2012 from http://www.linuxjournal.com/article/10973.

Myler, C., & Wapping, L. (2011). Phone Hacking Scandal. *News of the World*. Retrieved 10 June 2012 from http://medbib.com/News_of_the_world.

Neumann, R., & Parker, C. (1989). A summary of computer misuse techniques. Processings of the 12th National Computer Security Conference, (pp. 396-407).

Noy, N., McGuinness, D., & others. (2001). Ontology development 101: A guide to creating your first ontology. Stanford knowledge systems laboratory and Stanford medical informatics technical report. Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880.

Razvan, R. (2009). Over the SQL injection hacking method. Proceedings of the 3rd International Conference on Communications and information technology (pp. 116-118). World Scientific and Engineering Academy and Society (WSEAS).

Rounds, M., & Pendgraft, N. (2009). Diversity in network attacker motivation: A literature review. *2009 International Conference on Computational Science and Engineering* (pp. 319-323). University of Idaho, ID, USA.

Rouse, M. (2006, October). Definition: Social Engineering. *SearchSecurity*. Retrieved 18 November 202 from http://searchsecurity.techtarget.com/definition/social-engineering.

Savona, E., & Mignone, M. (2004). The fox and the hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research, 10(1),* 3-26.

Schwartz, M. J. (2012, July). Who Is Anonymous: 10 Key Facts. *InformationWeek Security*. Retrieved 18 November 2012 from http://www.informationweek.com/security/attacks/who-is-anonymous-10-key-facts/232600322.

Schwartz, N. D., & E., D. (2011). Thieves Found Citigroup Site an Easy Entry. Thieves Found Citigroup Site an Easy Entry. (13 June 2011). *The New York Times*.

Retrieved 18 November 2012 from http://www.nytimes.com/2011/06/14/technology/14security.html?pagewanted=all.

Simmonds, A., Sandilands, P., & van Ekert, L. (2004). An Ontology for Network Security Attacks. *Applied computing: Second Asian Applied Computing Conference, AACC 2004* (pp. 317-323), Kathmandu, Nepal.

Specht, S., & Lee, R. (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, (pp. 543-550). Atlanta, USA.

Spitzner, L. (2001). Know your enemy. Parts I, II, III. Retrieved 18 November 2012 from http://rootprompt.org/article.php3?article=159.

Taylor, P. A. (2001). Editorial: Hacktivism. *The Semiotic Review of Books , 12(1)*. Retrieved 18 November 2012 from http://projects.chass.utoronto.ca/semiotics/srb/Hacktivism.html.

Tutânescu, I., & Sofron, E. (2003). *Anatomy and Types of Attacks Against Computer Networks*. 2nd RoEduNet International Conference, Iassi.

Undercoffer, J., Joshi, A., Finin, T., & Pinkston, J. (2004). *A Target-centric Ontology for Intrusion Detection*. 18th International Joint Conference on Artificial Intelligence (pp. 9-15). San Francisco, LA.

van Heerden, R. P., Pieterse, H., & Irwin, B. (2012). Mapping the Most Significant Computer Hacking Events to a Temporal Computer Attack Model. Human Choice and Computers (HCC10) International Conference: ICT Critical Infrastructures and Society. Amsterdam.

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*. The Seventh IEEE/ACIS International Conference on Computer and Information Science, (pp. 259-265). Portland, Oregon.