AMCIS 2011 Proceedings - All Submissions

8-5-2011

NG Augmented Ontology on shared cloud attack dimension Proceedings of the Seventeenth Americas Conference on Information Systems, Detroit, Michigan August 4th-7th 2011 1 Americas Conference on Information Systems AMCIS 2011 Detroit "Augmented Ontology to discover Shared Attack Dimension in Cloud Computing for Information Warfare Prediction"

Daniel CHINGWA NG
C-PISA, Daniel@c-pisa.info

Americas Conference on Information Systems AMCIS 2011 Detroit “Augmented Ontology to discover Shared Attack Dimension in Cloud Computing for Information Warfare Prediction”

NG, CHINGWA Daniel
C-PISA
Daniel@c-pisa.info

ABSTRACT (REQUIRED)

There are several small countries adjacent to Russia. One is Estonia on the west and Georgia on the south east. The national computer network incident in Estonia dated 2007, and Georgia dated 2008 sparkled an rising concern in both Europe Council and Interpol on the vulnerabilities, integrity and sustainability of any government totally relying on computers and network, especially, opening up the whole national information assets to the global public information network. This paper takes a discovery journey from the allegation against China Telecom Internet traffic hijacked in April 2010, which later revoked by Investigation Committee in US Congress, to sparkle the gradual adoption of “METHONTOLOGY”, a special format of Ontology, in North American Internet traffic surveillance and Extensible Messaging Presence Protocol, or XMPP real time communication in North Atlantic Treaty Organization or NATO , to counteract major weaknesses in global Internet structure, says Border Gateway Protocol or BGP Leaking. This distillation of auto ontology exchange evolves shared attack dimensions for ongoing cyber warfare incidents. This paper attempts to shrine the rising role of semantic technology in Cyber Security cradle.

Keywords (Required)

Ontology, Attack Dimensions, Cyber Attack, Information Warfare.

I. CYBER CRIME CONTEMPORARY SITUATION

The final down counting of Global Internet infrastructure towards Internet Protocol Standard version 6, or IPv6 actually has three empirical challenges to those financial-oriented internet hackers, and organized cyber criminals:

- The absence of network address translation or NAT construction in IPv6 mandates hackers to integrate more intra data packet exploits to facilitate the initiation of respective malicious software payload. In the good old days of Internet Protocol version 4 or IPv4, malicious payload can be hidden through the use of network address translation or NAT.
- Mobile radio networks, like Long Term Evolution or LTE and High Speed Packet Access or HSPA, are replacing landline data and voice networks remarkable in Nordic regions, and British Isles such that any cyber information warfare, or cyber storms can be launched through handheld devices. Many internet online videos are highly available to knowledge transfer jailbreak skills converting the mobile data networks into a team of hand launch able “cyber-missiles”.
- Stuxnet, a specialized computer virus, outbreak in 2010 marks a new era in offline computer robot network, or BOTNET control to shake up Law Enforcement in their Incident Response or IR arrangement not solely on connected networks, but a total rethinking on data in motion through mobile storage. Apparently, cyber criminals can hijack some intelligent buildings in prominent cities to demand huge ransom from states’ government. Even more scarily, high speed trains system in Europe and Asia could be a national cyber attack targets similar to the proven case in Stuxnet, a specialized computer virus. This rocks the stability of many developed countries, as stories pictured in famous 007 James Bond movie “Royale Casino”.

Long Tail Effect is generated in the rising of Amazon web presence (Easley, D., Kleinberg, J. and Ebrary, I. 2010) to describe the targeting of all individual consumers’ needs. This effect starts to emerge in cyber criminals as the core objective is to get financial rewards. Due to the absence of boundary in Cyber Space or Internet space, and the participation of individuals around the clock, a new way of track taxonomy should be in place to cater this phenomenon of self-organization in Cyber Defense.

II . FIRST ATTEMPT ON CYBER DEFENCE ONTOLOGY

Ontology is a seaming difficult word, but the literal meaning is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents. This definition is consistent with the usage of ontology as set-of-concept-definitions, but more general. And it is certainly a different sense of the word than its use in philosophy, a.k.a. mean a specification of a conceptualization.

Security Asset Vulnerability Ontology, or SAVO (Vorobiev A and Bekmamedova N 2007) is considered to be the main stream with the following features supported:

1. ability to specify security information for different types of resources and environments;
2. reusability and extensibility; and
3. mapping between high-level and low-level security requirements and capabilities.

It is a high level security ontology depicting information security in a simplified manner for non-security professionals, but striving on industry expertise and knowledge of information security. Nonetheless, here are security jargon elaboration crucial for better understanding of Figure 1:

A. Threat refers to any occurrence that may cause any unwanted outcome for a company. A threat agent uses a threat to exploit vulnerability, while vulnerability is the absence or the weakness of defense;

B. Risk is the possibility for a threat agent exploiting vulnerability to damage an asset whereas exposure reveals the possibility that vulnerability will be exploited by a threat agent.

C. A safeguard or defense is utilized to resist attacks using security techniques, i.e. security function, and mechanisms or security algorithm standards.

D. An asset refers to anything within any environment needing protection, i.e. data, software, accounts, resources . Then, asset can be subdivided into client data and system data ; component and services for software implementation while such subclasses as central processing unit, memory, and storage encompass available resources;

E. Further, any asset may contain vulnerability which is explored with other vulnerabilities. Vulnerability has three attributes, i.e. vulnerability name, an attribute, and associated values. A patch removes vulnerability by a supplier.

F. A threat agent may use a threat to attack to penetrate the asset. The attack can be peer-to-peer.

Those connected words are special terms to describe the objects in Figure-01. Explanations are given in above clauses A to F. In Figure 1 below, a casual looping diagram is drawn to connected all identified key security taxonomy class and sub-classes showing the inter-dependency as well.

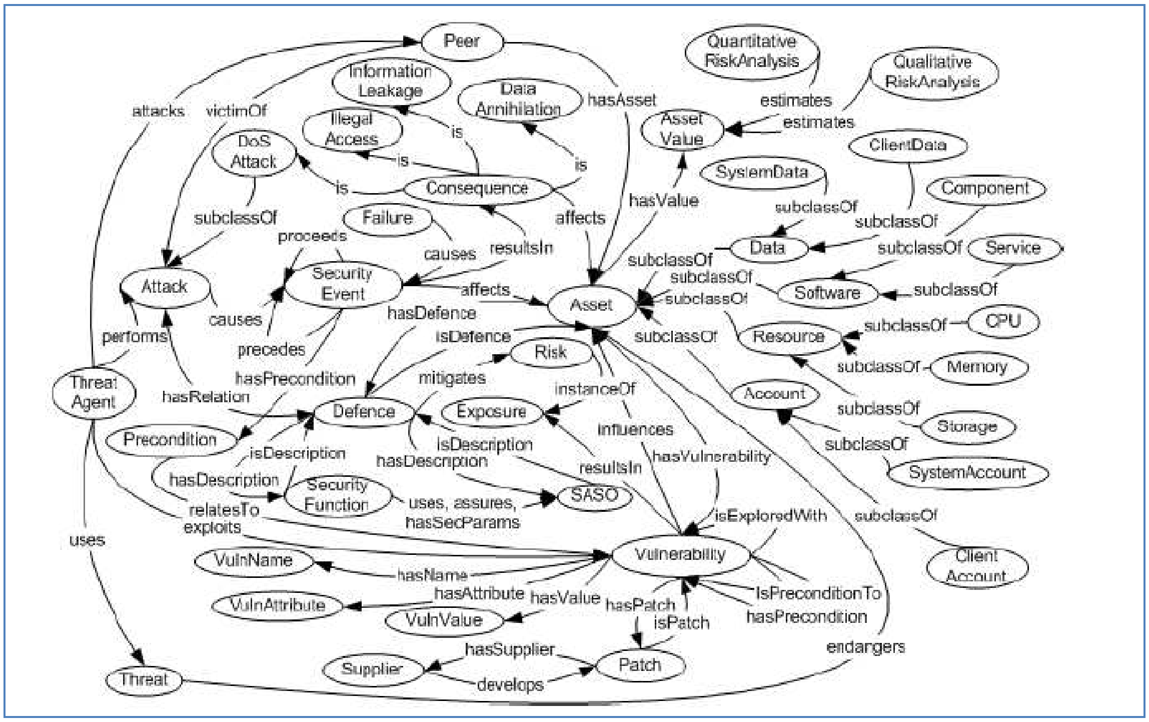

Figure 1. Security Asset Vulnerability Ontology or SAVO

Security Attack Ontology, like Cross Site scripting , Security Defense Ontology, like Intrusion Detections, and Defensive Components, like firewalls, can be inserted into common vocabulary to expand the Cyber Defense Ontology. Acting on this baseline, a cyber security ontology (ITU-T SG 17 2009) is built above.

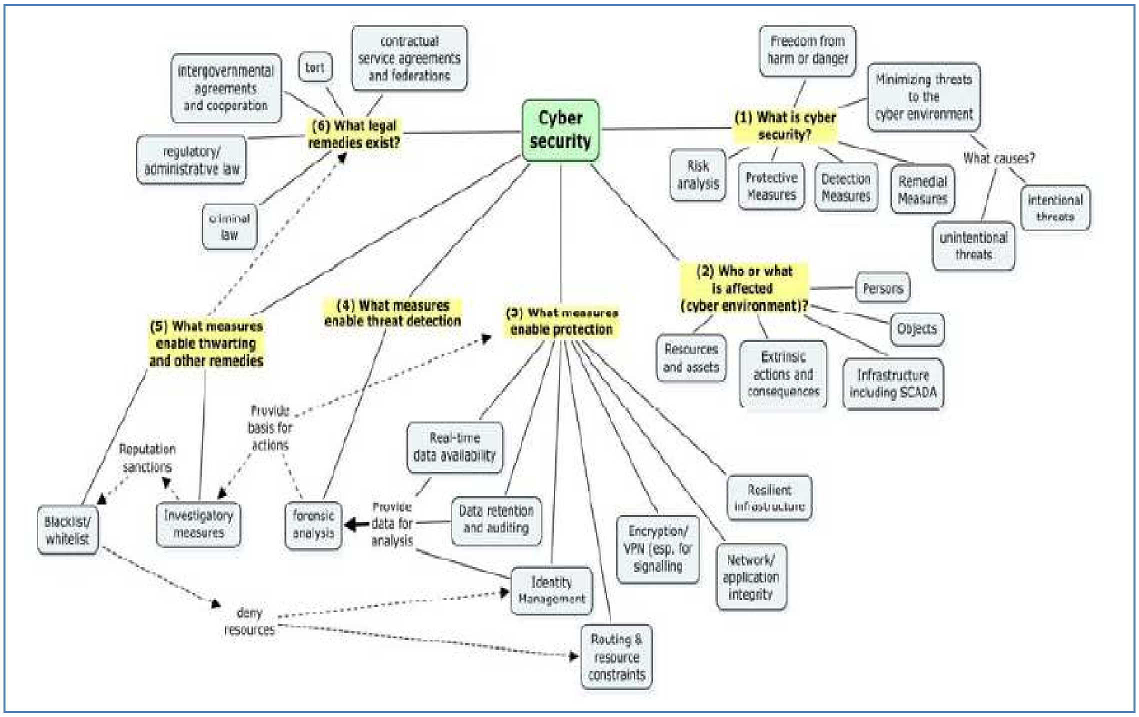
contractual service agreements and federations
intergovernmental agreements and cooperation
tort
Freedom from harm or danger
Minimizing threats to the cyber environment
(6) What legal remedies exist?
Cyber security
(1) What is cyber security?
regulatory/ administrative law
What causes?
Risk analysis
Protective Measures
Detection Measures
Remedial Measures
intentional threats
criminal law
unintentional threats
(2) Who or what is affected (cyber environment)?
Persons
(4) What measures enable threat detection
(5) What measures enable thwarting and other remedies
(3) What measures enable protection
Objects
Resources and assets
Extrinsic actions and consequences
Infrastructure including SCADA
Provide basis for actions
Reputation sanctions
Real-time data availability
Resilient infrastructure
Blacklist/ whitelist
Investigatory measures
forensic analysis
Provide data for analysis
Data retention and auditing
Encryption/ VPN (esp. for signalling
Network/ application integrity
Identity Management
deny resources
Routing & resource constraints

Figure 2. Cyber Security Ontology

In principle, a highly de-coupling of data-asset classification (Takahashi T., Kadobayashi Y. and Fujiwara H 2010) is depicted, with a common grouping of cyber attack behaviors for forensics study to facilitate ongoing attack pre-emption. Key international cyber defense organizations adopt an self-organizing software agent driven common vocabulary development, which is not able to be handled manually. From an architecture stand point, some key strengths are noted to promote an agile technical implementations to cater for dynamic situation in cyber crime space:

- A conceptual information model comprised of a loosely-coupled federation of modular ontology that form the structural and semantic framework of an information domain;
- Ability to relate upper ontology to middle and domain level extensions;
- Extremely flexible to scale up and out when applying to large, dynamic, complex domains such as cyber-security in timely manner.

In the cyber security ontology, there is an underlying belief to assume Internet Infrastructure run without any issue. In reality, one biggest issue surfaces frequently these days is BGP Leaking (Scholl T 2006), Certain global internet infrastructure ontology item must be captured to ensure a full picture to run the Figure-2 Cyber Security Ontology Map.

III ONTOLOGY "CONFICKER" INTELLIGENCE EXCHANGE

CONFICKER（Threats Report from McAfee : Third Quarter 2010), is a dreadful computer malicious software dispatched by organized cyber criminals to compromise any vulnerable Microsoft Windows workstations since 2009. Some attempt is done to create an ontology model on its attack behavior to give the following schema:

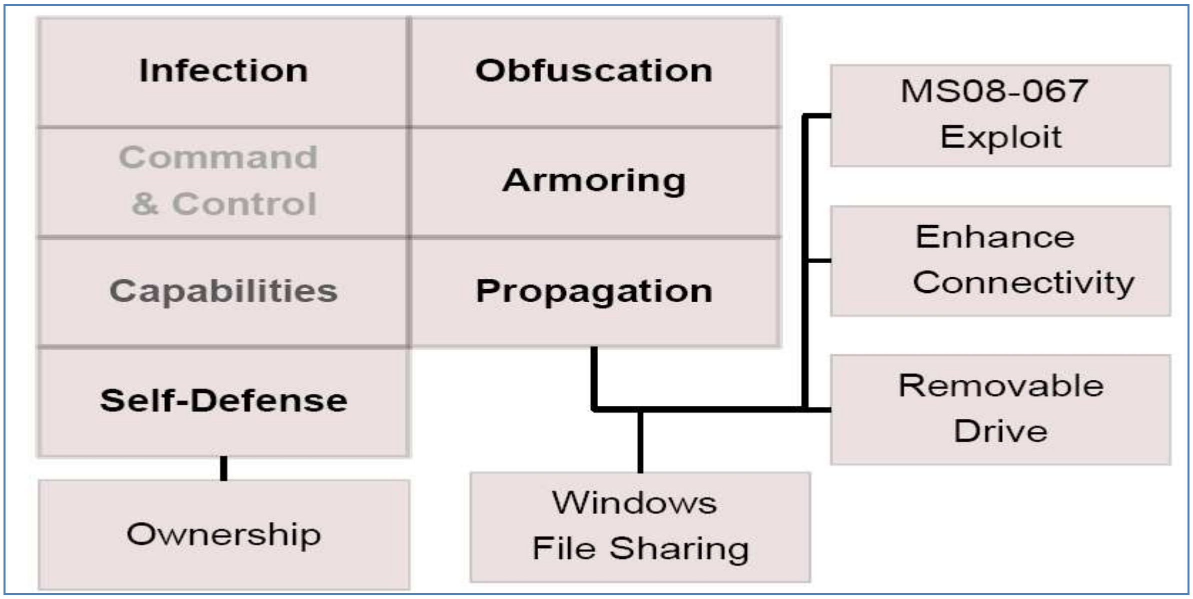

Figure 3. CONFICKER Conceptual Schema

Above ontology schema fairly contain all key evolution and proliferation of all variants in CONFICKER discovered so far that major cyber defense organizations communicating in the auto semantic exchange.

In reality, cyber attack occurs when a new piece of software product installed and exposed to internet. Taking the example of CONFICKER, there were many "pilot" versions throwing out to test against major tertiary institutions to trial out the ease of windows workstation exploitation and contamination.

Long tail approach is observed as a common practice in those cyber criminals to do victim search. Therefore, cyber security ontology should have a kind of machine-based intellectual mind to continuously refresh ontology metadata to ensure new attack matched.

According to North Atlantic Treaty Organization or NATO and some research institutes attached to US Congress, many international internet services providers or ISP, are forming cyber forensics alliance to surveillance their covered internet area for any attack-type scanning actions.

CONFICKER is a kind of organized computer crime to run a robotic network, or BOTNET, to either sub-lease for malicious commercial actions, like halting websites for revenges, or stealing passwords for cash embezzlement, or supporting any kind of black market's money laundry, which could foster a fundamental damage to global financial market.

A global effort is being done to mould out new malicious software, like CONFICKER, in order to frame out new taxonomy in a light-speed mechanical way so as to catch those cyber criminals once launching Internet attacks.

IV AUTO TAXONOMY FOR DIGITAL FINGERPRINT EXCHANGE

"METHONTOLOGY" is a promising land for ever changing cyber security and forensic ontology to work in a self-organizational, structural manner. Ontology is about classification of information components in a specification format. Cyber Space security taxonomy keeps on refreshing such that is it quite impossible to anticipate any new or merged information categories. In a holistic framework (Á.SABUCEDO L, RIFÓN L.A, PÉREZ R.M. and GAGO J.S 2009) for electronic government, a taxonomy life cycle approach is developed to cater for ever mutating taxonomy. The principle is using a semantic web analyzer to scan unclassified items using unstructured text-mining technique. Proximity score clusters new unclassified items to 95% fit taxonomy, or to extend the sub-taxonomy class. Then auto adjustment appears in ontology for cyber security.

Location based ontology system needs to communicate with other countries' cyber defense centre, and so Extensible Messaging Presence Protocol or XMPP is adopted at North Atlantic Treaty Organization or NATO (Richards T 2009) for real time cyber attack exchange. The Extensible Messaging and Presence Protocol or XMPP is an open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of Extensible Mark Up Language, or XML data. This new technology supports routing of captured attack data in real time manners for data stream, voice & video, and instant message. It connects any hardware server system loggings to another machine's requests, or human interaction.

Another question is how the meta data working with ontology auto-adjustment routines. One insightful method is performed in (Ishida T. and Cho H 2005) to exploit all known ontology on the World Wide Web to consolidate some template ontology for meta data development. Here are some procedures for references:

Firstly, domain specific existing ontology in familiar Web is analyzed. This is necessary because these ontology later constitute the design material's key terms of references. Unless those obtained ontology are over abundant in variety and in quantity to all referring tedious, a bare minimum benchmarking is needed. Secondly, process problems in metadata design process must be clarified to remove ambiguity. In particular, information needs that arise within a restricted setting, which prohibits any designer from referring to existing ontology, has to check out thoroughly to highlight what information support to make it useful. Thirdly, based on the understanding obtained from first and second, a step by step metadata design process which incorporates existing ontology as design material should be presented and executive in a holistic manner to give a detailed design flow. This will definitely addresses specific design difficulties.

An additional step should be included in auto taxonomy on those potential infrastructure wreck, in particular BGP Leak.(Ishida T. and Cho H2005). This could evade unnecessary misunderstanding in internet hijack, as in April 2010 allegation against China Telecom, but late revoked by US Congress' investigation committee. False alarm must be avoided through the inclusion of self-reported infrastructure ontology item to label out true attack..

CONCLUSION

Auto-taxonomy is a long sought-after in ontology development. The constant influx of trillions of data around the World in 7x24 manner demands a self-organized security and attack information schema to predict any new attack targets or

In the cyber defense world, every second shall have trillions of various attacks, from pure location scanning to attempt traffic suspension to the illegitimate computer access to the extraction of sensitive data. A standard, pre-planned taxonomy for information classification sounds impossible, as human effort cannot cater for the speed expected and volume encountered.

METHONTOLOGY is a holistic framework to develop an ontology cycle such that there is an interim aggregation with data clustering to either extend a particular taxonomy, or to discourage it. Cross summary checking is executed against real life output to validate all auto adjustment logic.

The scary cut-over of Internet Protocol version 6 or IPv6 in March 2011 may not be able to deliver the original peaceful promise to reduce cyber crime, as security features turned on natively. Cyber criminals can still find legacy Microsoft windows workstations in developing countries, like Iran, and India, to embed their secret weapon months before attack. This time bombs could be a kid toy for trading on black market, as there is Do-It-Yourself services offered by cyber criminals.

Meth ontology paves solid cornerstone to international community connected in cloud of cables and servers so as to continuously expand, extend and restructure the cyber security ontology map for information gathering and exchange.

Global village is moving from a single site with cables and computer hardware to split deployment of cables, hardware, software across time zone and location in order to arbitrage on a gold paradigm, "Competitive Advantage", which is a basis for the emerging cloud computing.

REFERENCES

1. Vorobiev A and Bekmamedova N (2007) "An Ontological Approach Applied to Information Security and Trust", *18th Australasian Conference on Information Systems Information Security and Trust via Ontologies*, 5-7 Dec 2007, Toowoomba, Australia

2. Easley, D., Kleinberg, J. and Ebrary, I.(2010), "*Networks, crowds, and markets*", Cambridge University Press, Cambridge; New York.

3. ITU-T SG 17 (2009) "*Collaboration in the work on global Cyber security*", INTERNATIONAL TELECOMMUNICATION UNION, Geneva, Switzerland, 11-20 February 2009

4. Á.SABUCEDO L, RIFÓN L.A, PÉREZ R.M. and GAGO J.S (2009), "A HOLISTIC SEMANTIC FRAMEWORK FOR THE PROVISION OF SERVICES IN THE DOMAIN OF eGOVERNMENT", *International Journal of Software Engineering and Knowledge Engineering* IJSEKE (2009) Volume: 19, Issue: 7, Pages: 961-993

5. Takahashi T., Kadobayashi Y. and Fujiwara H (2010), "Ontological approach toward cyber security in cloud computing", *SIN '10 Proceedings of the 3rd international conference on Security of information and networks*, ACM 2010

6. Threats Report from McAfee : (Third Quarter 2010), "Spam Slows, But Malware Still a Menace." *Channel Insider,* Nov 18, 2010 p. 1-3

7. Richards T (2009), *Location-based services handbook :applications, technologies, and security*, CRC Press, Boca Raton, FL;

8. Ishida T. and Cho H(2005), *Designing Metadata with Existing Ontologies*, Department of Informatics, Kyoto University, 9 Feb. 2005

9. Scholl T (2006), *"Maximum Prefix Tripping: A potential workaround for leaking on the Internet"*, AT&T Labs NANOG 38 October 9th, 2006.