Ontology in Cyber Defence and Computer Networks

Josef KADERKA[1]

[1] Dept. of Communication and Information Systems, University of Defence, Kounicova 65, 612 00 Brno, Czech Republic

josef.kaderka@unob.cz

Abstract. *The contribution covers some current issues of computer networks and their security and tries to find the trend of future development. Selected recent Cyber Attacks examples are also mentioned and simple example of Cyber Defence taxonomy is given. This area is developing dynamically, and it is not easy to even keep track of the current situation. Therefore, ontology can be prominently used here.*

Keywords

Cyber defence, security, ontology, knowledge management.

1. Introduction - cyber problems

The terms beginning with the word "Cyber" and implying the activity of military nature are extremely popular and widely used in the past few years. The examples are Cyber Attack, Cyber Defence, Cyber War, Cyber Warfare, Cyber Terrorism, and many more. Particular problems are caused by not fully settled definitions. One example is a definition of the term "Cyberterrorism", which according to Wikipedia [1] is: „ ... a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.“ It is evident that this definition covers, with slight modifications, any other above-mentioned terms. Moreover, the "Cyber Defence", for example, will logically represent the counterpart of Cyber Terrorism.

Above all, for the success of Cyber Defence, it is necessary to understand and describe those attacks, where ontological methods can be used. Of course, there are several circumstances or Cyber Attack levels. Some of them are so common, as a sniffing or port scanning, that they are normally ignored [2]. Only when something very unusual happens, more attention is paid to it. The botnet Chuck Norris mentioned below is an example.

One possible variant of the basic model Cyber Defence in the computer networks environment is outlined below. This model is intentionally depicted only as a simplified version` it would be much more complicated in real life.

We can see that the trends develop from conventional ways, first passive and active afterwards, to the proactive measures.

The basic idea of proactive Cyber Defence is to anticipate an attack against computers or networks and to adopt the necessary measures in time [3]. This proactive Cyber Defence lies between strictly defensive and offensive (remember, the attack is the best defence) measures. Proactive Cyber Defence can take the form of searching for potential attack preparations (for example trends in monitoring, botnets searching etc.) and organization countermeasures which are activated if necessary. An important role is played by telecommunications service providers, applications, sophisticated intrusion detection systems, etc. In the military coalition environment the operators of backbone networks and satellite connections play the same role.

2. Cyber attacks examples and their new opportunities

Cyber Attack against U.S. Forces

Probably one of the most serious Cyber Attack cases hit U.S. Forces in the autumn of 2008. Precise details are not yet available, but at least some partial aspects were published in August 2010. The worm (called agent.btz) had spread into internal systems of the U.S. Armed Forces, both classified and non-confidential, through a USB stick (storage media - flash drive). The probable source of the primary penetration was a laptop computer on a U.S. base in the Middle East. This worm spread rapidly and deliberately gave very limited opportunities for local systems administrators to stop it. The immediate ban of the use of USB sticks was repealed only in February 2010. Complete cleanup of all systems in the network took nearly 14 months. It is interesting, that the author of the worm does not seem to know what happened or how successful his product was. There are still some speculations regarding its real purpose, namely whether it was created specifically with the aim of attacking concrete

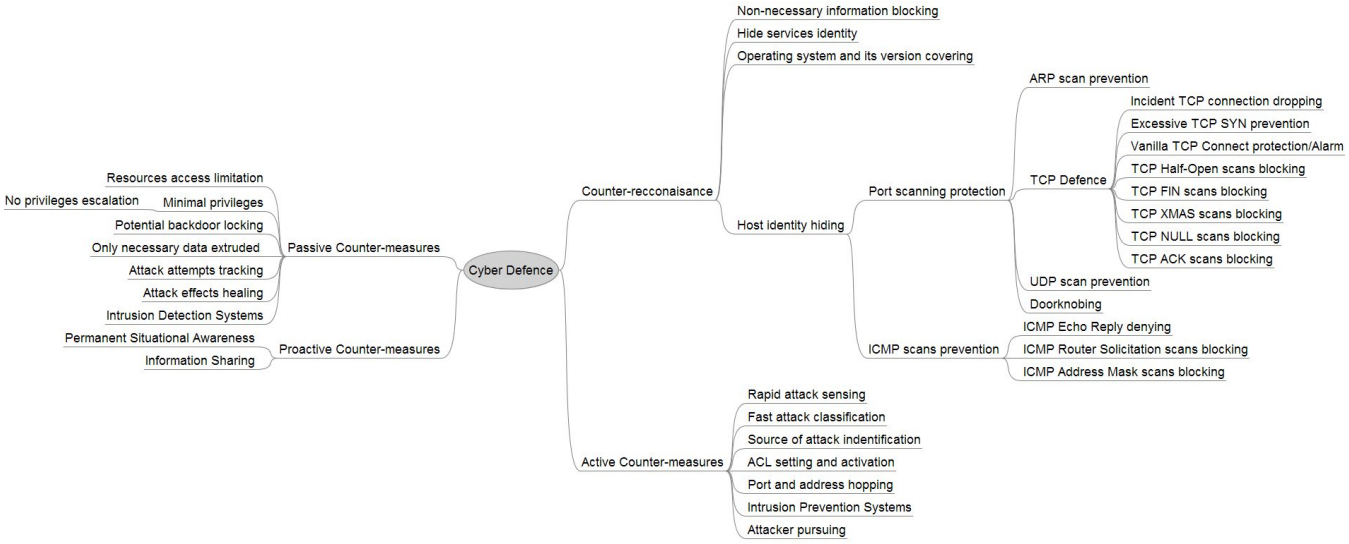

Figure 1. En example of selected areas of Cyber Defence in computer networks

networks, or whether it just found a convenient breeding ground; of course, some sources claim that it was the intention of targeting foreign intelligence services [4].

No disclosure of sensitive or even secret information probably occurred because those networks are, as indicated above, separated from the outside world and thus the way to export potentially acquired information out, at least in this case, lacked. The author of the worm perhaps did not know about the fact that (and to what extent) her/his piece was effectual from the beginning.

This example underscores the need to address proactively and systematically all aspects of cyber warfare. The ontologies can be developed to improve the quality of decision process.

Botnet Chuck Norris

Another example is the botnet Chuck Norris which was revealed less than year ago. That discovery was done by virtue of its unusual (but necessary) activity. Among other, it scanned IP addresses ranges, trying to find open port 23 (telnet). If such port was found, the attempt to connect to this port followed using simple login/password. Although botnets are not uncommon, in this case it was something entirely new. Individual members of that botnet did not dwell in regular computers as usually, but in various special purpose devices, especially the type of SoHo as ADSL modems and routers, but also in a satellite set top box with the connection to the Internet. These devices are often run by very simplified, outdated and unmaintained Linux distribution operating systems which contain known errors; the main goal of their vendors is achieving the lowest possible price. Therefore, the appropriate action can gain direct access to the operating system and its service and then completely dominate the device, install their own software modules into it, etc.

The botnet is still a subject of our interest, because although it was shut down several months after revealing it, it was not definitely turned off. Its creators are surely alive and active. For example, their latest activity has been targeted at DNS misuse by the way that resembles the Man In The Middle attack.

The rudimentary threat is the possibility of botnets to virtually endanger any area of modern life, as almost all existing control systems rely on computer networks. The targets may be components such as electrical distribution systems, intelligent buildings, transportation systems, etc. These victim components can be quite subtle and implausible such as door control modules, web IP cameras, rack power distribution units, UPS, maybe home refrigerators in the near future, etc.

Botnets could endanger military networks, where there are numbers of embedded devices suitable as objectives. These networks have strict security policies, which significantly limits the users. This is the positive side of the thing; on the other hand, , it can make it difficult to identify what is actually happening. Again, the space for the application of ontological approaches is open here.

Sensor networks

Sensor networks are significant challenges for the future in terms of security. These include for example the mesh type networks, where individual sensors can work together. Sensors (called motes) are often placed in operationally demanding, harsh environment (ambient networks), while being powered only by their own battery, and they must endure even several years of work. The basis for such networks is the IEEE 802.15.4 standard, which defines the physical and MAC sublayer; the Zigbee is the upper protocol.

The understanding of this area is still in the beginning, at least among the public. Probably everybody knows the anti-theft tags used in shops. The next generation will be based on RFID chips, which allow not only to locate hidden items, but also to make a bill without taking out goods from the shopping cart. The military personnel can use that type of sensors and especially sensor networks for supply and spare parts tracking, but also for any other purposes like motion detection in sparse settled areas etc.

2.1 Cyber Defence and NATO

NATO and NATO Nations are heavily dependent on CIS, which, to varying degrees, are vulnerable to threats from different adversaries through their network connections and also from access by authorized and/or unauthorized insiders. The rapid and explosive growth of commercial Information Technology (IT) and its penetration into almost every part of the world is significantly affecting the military community.

The NATO Consultation, Command and Control Agency (NC3A) has been formed in 1996. One of its missions is "Cyber Defence and Assured Information Sharing - supporting the build-up of NATO's Cyber Defence; enabling coalition interoperability; developing machine-understandable standards; industrialization of the metadata registry; creation of ontologies to further interoperability and the ability to share information; information assurance research and development, experimentation and expertise; procurement of information assurance products (mostly cryptography)." [5]

NC3A can provide Cyber Defence engineering and technical expertise covering a wide range of services, like:

- Expertise Description
- Cyber Defence Engineering (e.g., deployment of Intrusion Detection and Prevention devices, setting up of a Centralized Event Management capability).
- Expertise in Incident Management procedures (e.g., Incident Reporting, Incident Response,
- Coordination of Action).
- Static and Dynamic Malware Analysis.
- Computer and Network Forensics.
- Risk and Vulnerability Assessment of CIS (e.g., Macro Assessments, Operational Site Assessments, Penetration Testing, Online remote Assessments).
- Coordination and Technical support to Cyber Defence Exercises and Training.
- Security configuration guidance for virtualization infrastructure.

Conclusion

Cyber Attacks are today's reality. For that reason the Cyber Defence will play fundamental role in the future conflict, both latent and hot. There are many examples of that attack during last two or three years. This topic is now fortunately quite famous among decision makers. The ontologies and ontogical approach can significantly contribute to the improving of their tasks. Another sphere of using ontologies as regards of Cyber Defence is the specialist training, research etc.

References

[1] [online]. http://en.wikipedia.org/wiki/Cyberterrorism

[2] Chappell, L. *You're Being Watched: Cyber-Crime Scans*. March 2001. [online]. http://support.novell.com/techcenter/articles/nc2001_03.html

[3] Kotenko, I. *Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks.* In: Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC'03). October 20-23, 2003. Shanghai, China. ISBN: 0-7695-2033-2.

[4] Lynn, W. J. III. *Defending a New Domain*. The Pentagon's Cyberstrategy. In: Foreign Affairs Magazine. August 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[5] NC3A C4ISR Catalogue of Expertise. http://www.nc3a.nato.int/SiteCollectionDocuments/KeyAgencyDocuments/NC3ACatalogueOfExpertiseMay2010.pdf

About Authors ...

Ing. Josef Kaderka, Ph.D.

Assistant Professor at University of Defence, Faculty of Military Technology, Communication and Information Systems Department, Brno.

Graduated from the Military Academy, Computer Science, 1987.