2017-03

Naval Postgraduate School Cyber Academic Group Compilation of Abstracts

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/55247

Naval Postgraduate School
Cyber Academic Group

Compilation of Abstracts

Unrestricted Theses, Dissertations, and
Capstone Project Reports

Naval Postgraduate School
Monterey, California • www.nps.edu

This compilation of abstracts highlights the breadth of cyber-related student research at NPS in Winter Quarter 2017 and reinforces the importance of cyber as an integral aspect of today's Naval enterprise. The abstracts provided represent publicly releasable theses completed by March 2017 graduates. They are the product of the NPS Cyber Academic Group (CAG) students, which is a national resource for the interdisciplinary study and design of secure and resilient cyber systems and the conduct of cyber operations.

Cyberspace is now a primary warfare area. Establishing U.S. Tenth Fleet/Fleet Cyber Command, combined with the Deputy Chief of Naval Operations for Information Dominance (N2N6), created an enterprise able to address the opportunities and challenges for cyber systems and operations (CSO) within the Navy's vision for the information warfare community (IWC). Reflecting a growing cognizance of the importance of cyber operations, other elements of the U.S. military and U.S. government, such as the Department of Homeland Security, have created similar or complementary organizations.

Optimizing military and U.S. government cyber assets for future operations will require leaders who both understand how to defend our networks from penetration and employ cyber capabilities to ensure an advantage in future operations. This objective cannot be reached without a cadre of officers able to address a broad range of cyber operations: computer network attack, defense, and exploitation; cyber analysis, operations, planning, and engineering; and cyber intelligence operations and analysis.

The CAG is an interdisciplinary association of two dozen faculty members, including those holding named chairs, representing eight distinct academic disciplines. Established by the Naval Postgraduate School (NPS) on 23 September 2011, the CAG has responsibility for oversight and management of the Cyber Systems and Operations curriculum. Graduate-level instruction and research support in interdisciplinary programs is delivered by members of this academic group and by faculty primarily from the following academic departments: Computer Science, Electrical and Computer Engineering, and Information Sciences.

For more information, please contact the following individuals or visit our website at: http://my.nps.edu/web/cag/.

Dr. Clark Robertson, Chair, Cyber Academic Group
crobertson@nps.edu

CDR Zachary Staples, Director, Center for Cyber Warfare
zhstaple@nps.edu

DEVELOPING SIMULATED CYBER ATTACK SCENARIOS AGAINST VIRTUALIZED ADVERSARY NETWORKS

Luis E. Aybar–Lieutenant, United States Navy
Master of Science in Cyber Systems and Operations
Advisor: Alan Shaffer, Department of Information Sciences
Co-Advisor: Gurminder Singh, Department of Computer Science

Cyberspace is now recognized as a critical center of gravity for modern military forces. The ability to maintain operational networks, while degrading the enemy's network capability, is a key consideration for military commanders. Conducting effective cyber-attacks against sophisticated adversaries requires the ability to develop, test, and refine cyber-attack scenarios before they are used operationally, a requirement that is not as well defined in the cyber domain as it is in the physical domain. This research introduces several concepts to address this need and creates a prototype for cyber-attack scenario development and testing in a virtual test environment. Commercial and custom software tools that provide the ability to conduct network vulnerability testing are reviewed for their suitability as candidates for the framework of this project. Leveraging the extensible architecture of the Malicious Activity Simulation Tool (MAST) custom framework allowed for the implementation of new interaction parameters and provided temporal specificity and target discrimination of cyber-attack scenario tests. The prototype successfully integrated a virtualized test environment used to simulate an adversary network and the enhanced MAST capability to demonstrate the viability of a cyber-attack scenario development platform to address the needs of modern offensive cyber operations. Based on these results, we recommend continued development of MAST with the intent to ultimately deploy to Department of Defense cyber operations teams. Full Text

Keywords: offensive, malware, cyber, virtualization, attack, simulated, modeling, MAST, MAVNATT

IN-NETWORK PROCESSING ON LOW-COST IOT NODES FOR MARITIME SURVEILLANCE

Andrew R. Belding–Lieutenant Commander, United States Navy
Master of Science in Computer Science
Advisor: Gurminder Singh, Department of Computer Science
Co-Advisor: John H. Gibson, Department of Computer Science

The effective distribution of offensive weapon capabilities to naval units at the tactical edge is a critical focus for Navy leaders. A direct byproduct of this priority is the need to employ sensor and data collection systems that can effectively guide the targeting of that offensive capability. In the recent past, wireless sensor networks have received limited use in the maritime domain due to the exploratory nature of technology, high system complexity, and the high cost of system deployment. With the Internet-of-Things revolution, commercially available hardware and software components can be used to build low-cost, reliable, disposable wireless sensor networks that can leverage in-network processing schemes to greatly expand the intelligence collection footprint.

In this research, a technology demonstrator composed of low-cost wireless sensor nodes leveraging in-network processing for the gathering of wireless transmitter data was investigated. The sensor nodes were created using consumer electronic components, open-source software libraries, and networking protocols used commercially to support distributed sensors organized in a network. The network demonstrates that, for a fraction of the cost associated with conventional persistent surveillance systems, a complete sensor network can be implemented at the tactical edge and provide valuable intelligence from a variety of sources. Full Text

Keywords: wireless sensor networks, internet-of-things, intelligence, surveillance and reconnaissance, in-network processing

BLIND DATA ATTACK ON BGP ROUTERS

Joseph W. Catudal–Major, United States Army
Master of Science in Cyber Systems and Operations
Advisor: Robert Beverly, Department of Computer Science
Second Reader: J. D. Fulp, Department of Computer Science

Transport Communication Protocol (TCP) implementations may not properly implement blind attack protection, leaving long-standing connections, such as Border Gateway Protocol (BGP) sessions, vulnerable to exploitation. This thesis aims to understand the efficacy of a blind data attack on BGP sessions. This thesis examines BGP, the protocols BGP relies on, and the effectiveness of safeguards against BGP blind attacks. A series of blind attack tests are performed against various production BGP implementations to determine how dangerous and feasible a blind attack is on BGP routing information integrity. Blind data attacks can inject and temporarily propagate erroneous routing information; however, on the routers tested, the complexity required to brute force connection-specific values makes blind data attacks difficult. Also, there is a high probability that a blind data attack will desynchronize a BGP session without modifying routing information. Protective measures are available that could further safeguard BGP sessions, but older router images may not implement some of the most vital protections recommended today. Organizations responsible for routing infrastructure and network security must carefully weigh the risk of not implementing more strict protection measures should a discovered vulnerability reduce attack complexity. Full Text

Keywords: BGP, TCP, blind attack, blind data attack

IDENTIFICATION OF LOW-LATENCY OBFUSCATED TRAFFIC USING MULTI-ATTRIBUTE ANALYSIS

Kevin R. Dougherty–Lieutenant, United States Navy
Master of Science in Cyber Systems and Operations
Advisor: Shelley Gallup, Department of Information Sciences
Co-Advisor: Thomas Anderson, TRAC Monterey

There is no process or system capable of detecting obfuscated network traffic on Department of Defense (DOD) networks, and the quantity of obfuscated traffic on DOD networks is unknown. The presence of this traffic on a DOD network creates significant risk from both insider-threat and network-defense perspectives. This study used quantitative correlation and simple network-traffic analysis to identify common characteristics, relationships, and sources of obfuscated traffic. Each characteristic was evaluated individually for its ability to detect obfuscated traffic and in combination in a set of Naive Bayes multi-attribute prediction models. The best performing evaluations used multi-attribute analysis and proved capable of detecting approximately 80 percent of obfuscated traffic in a mixed dataset. By applying the methods and observations of this study, the threat to DOD networks from obfuscation technologies can be greatly reduced. Full Text

Keywords: Tor, onion routing, obfuscation, network traffic analysis, multi-attribute analysis

HIGH-FREQUENCY MAPPING OF THE IPV6 INTERNET USING YARRP

Eric W. Gaston–Information Systems Technician First Class, United States Navy
Master of Science in Applied Cyber Operations
Advisor: Robert Beverly, Department of Computer Science
Advisor: David Plonka, Akamai Technologies

Both the number of hosts using Internet Protocol version 6 (IPv6), as well as the volume of IPv6 traffic, have increased exponentially since 2012. With this adoption, the IPv6 routed infrastructure becomes an increasingly important component of global critical infrastructure and network policy. Unfortunately, the tools and techniques used to perform active network topology discovery were designed for Internet Protocol version 4 (IPv4), leading to a potentially opaque view of the IPv6 Internet. In this thesis, we extend nascent work on stateless high-speed IPv4 active topology probing to develop a new IPv6 traceroute method "Yelling At Random Routers Progressively version 6" (Yarrp6). Yarrp6 randomly permutes the set of IPv6 targets and hop counts to distribute load, thereby helping to avoid IPv6 response rate limiting. Further, we encode state in the IPv6 payload to permit Yarrp6 to both match responses with probes and use different probe transport protocols. Via active experimentation on the public IPv6 Internet, we compare the results obtained from Yarrp6 against the current state-of-the-art IPv6 topology mapping tool. We show that Yarrp6 can discover topology at more than an order of magnitude faster than previously possible. Finally, we conduct a study of the effect of transport layer protocol on forward Internet Protocol (IP) path inference to determine what protocol is best used for active IPv6 topology discovery. Full Text

Keywords: IPv6, active topology mapping

DETECTING TARGET DATA IN NETWORK TRAFFIC

Aaron Haycraft–Civilian, Federal Reserve Bank of San Francisco
Master of Science in Computer Science
Advisor: Michael McCarrin, Department of Computer Science
Advisor: Robert Beverly, Department of Computer Science

Data exfiltration over a network poses a threat to confidential information. Due to the possibility of malicious insiders, this threat is especially difficult to mitigate. Our goal is to contribute to the development of a method to detect exfiltration of many targeted files without incurring the full cost of reassembling flows. One strategy for accomplishing this would be to implement an approximate matching scheme that attempts to determine whether a file is being transmitted over the network by analyzing the quantity of payload data that matches fragments of the targeted file. Our work establishes the basic feasibility of such an approach by matching Transmission Control Protocol payloads of traffic containing exfiltrated data against a database of MD5 hashes, each representing a fragment of our target data. We tested against a database of 415 million fragment hashes, where the length of the fragments was chosen to be smaller than the payload size expected for most common Maximum Transmission Units, and we simulated exfiltration by sending a sample of our targeted data across the network along with other non-target files representing "noise." We demonstrate that under these conditions, we are able to detect the targeted content with a recall of 98.3% and precision of 99.1%.
Full Text

Keywords: exfiltration, information, flows, hashes

EFFECTIVENESS OF A LITTORAL COMBAT SHIP AS A MAJOR NODE IN A WIRELESS MESH NETWORK

Joshua B. Hicks–Lieutenant, United States Navy
Ryan L. Seeba–Lieutenant, United States Navy
Master of Science in Network Operations and Technology
Advisor: Alex Bordetsky, Department of Information Sciences
Co-Advisor: Wayne Porter, Department of Defense Analysis

The Littoral Combat Ship (LCS) is an evolving platform capable of performing missions in a variety of environments worldwide. One theoretical mission area—the performing advanced command, control, communications, computers, intelligence (C4I) with wireless networking technology in a littoral environment—brings new aspects to the level of versatility this platform can provide. The Navy relies heavily upon networks for information sharing between deployed assets; there is therefore a need for a more reliable means of communicating with these systems. The LCS's adaptability makes it a prime candidate for experimentation with wireless networking technology used for communications with multiple assets. Continuous improvements in Wireless Mesh Network (WMN) and Mobile Ad-Hoc Network (MANET) technologies are producing capabilities that satisfy the need for greater bandwidth and reliability between interconnected manned and unmanned systems. This thesis proposes to virtually model and simulate the operation of an LCS equipped with WMN and MANET technologies intended to

enable the LCS to manage these networks and to communicate with surrounding assets reliably. Standard thresholds for network reliability are used to determine the network effectiveness. Based on results from network simulation software, the research findings demonstrated the LCS is capable of performing as a major node in a WMN. Full Text

Keywords: mesh networking, littoral operations, network management, simulations

NATURAL LANGUAGE PROCESSING OF ONLINE PROPAGANDA AS A MEANS OF PASSIVELY MONITORING AN ADVERSARIAL IDEOLOGY

Raven R. Holm–Lieutenant, United States Coast Guard
Master of Science in Computer Science
Advisor: Mathias Kölsch, Department of Computer Science
Advisor: Justin Jones, United States Marine Corps (ret.)

Online propaganda embodies a potent new form of warfare, one that extends the strategic reach of our adversaries and overwhelms analysts. Foreign organizations have effectively leveraged an online presence to influence elections and distance-recruit. The Islamic State has also shown proficiency in outsourcing violence, proving that propaganda can enable an organization to wage physical war at very little cost and without the resources traditionally required. To augment new counter-foreign propaganda initiatives, this thesis presents a pipeline for defining, detecting, and monitoring ideology in text. A corpus of 3,049 modern online texts was assembled, and two classifiers were created: one for detecting authorship and another for detecting ideology. The classifiers demonstrated 92.70% recall and 95.84% precision in detecting authorship, and detected ideological content with 76.53% recall and 95.61% precision. Both classifiers were combined to simulate how an ideology can be detected and how its composition can be passively monitored across time. Implementation of such a system could conserve manpower in the intelligence community and add a new dimension to analysis. Although this pipeline makes presumptions about the quality and integrity of input, it is a novel contribution to the fields of Natural Language Processing and Information Warfare. Full Text

Keywords: data mining, natural language processing, machine learning, algorithm design, information warfare, propaganda

A CYBER SITUATIONAL AWARENESS MODEL FOR NETWORK ADMINISTRATORS

Huseyin Karaarslan–Captain, Turkish Gendarmerie
Master of Science in Information Technology Management
Advisor: Alan Shaffer, Department of Information Sciences
Co-Advisor: John Gibson, Department of Computer Science

Although there are many well-established cyber security tools and techniques available to network administrators for managing and defining their systems, attackers still succeed in penetrating their

systems. Defending these systems' confidentiality, integrity, and availability is the responsibility of network administrators; however, protecting these systems becomes more difficult when one considers the volume and velocity of data provided by many of these cyber security tools. Often, this data may actually indicate a cyber-attack, but is hard to discern among the bulk of data provided. The purpose of this research is to propose a cyber situational awareness (CSA) model to provide network administrators with better situational awareness of cyber security threats to their systems. This research examines an established situational awareness model and surveys cyber security practices and tools to extend this knowledge to actual cyber situational awareness. This research further develops a model for CSA in three hierarchical levels: configurational awareness, operational awareness, and special conditions awareness. The research concludes that if network administrators manage their systems with awareness of these three levels, they would be able to decrease the amount of unnecessary data and focus on the most important information that can help them better guarantee cyber security of their systems.
Full Text

Keywords: network administrator training, network management, network configuration, cyber situational awareness, operational awareness, configurational awareness, cyber situational awareness pyramid, cyber-security tools, cyber-security techniques

IMPLEMENTATION OF A PARAMETERIZATION FRAMEWORK FOR CYBERSECURITY LABORATORIES

Jean Khosalim–Civilian, Department of the Navy
Master of Science in Computer Science
Advisor: Cynthia E. Irvine, Department of Computer Science
Co-Advisor: Michael F. Thompson, Department of Computer Science

Computer Science courses often include laboratory exercises to make sure certain concepts are experienced hands-on by the students. These courses sometimes are taken by a large number of students, and each assignment needs to be graded. Instructors or teaching assistants responsible for grading assignments are presented with the tedious task of verifying students' work. Besides making sure that each student performs the assignment correctly, the assignment grader may also be concerned that students do not cheat on the assignment by copying and submitting work from other students.

The objective of this thesis is to investigate and develop a framework for Linux-based cybersecurity laboratory exercises performed on individual student computers. The purpose of the framework is to provide the designer of laboratory exercises with tools to parameterize labs for each student, and to automate some aspects of the grading of laboratory exercises. A prototype of this framework was implemented by making use of the Linux Containers, which provide an additional benefit of standardizing execution environments utilized by students and instructors. Full Text

Keywords: automated assessment tool (AAT), parameterization framework

MULTIPATH TRANSPORT FOR VIRTUAL PRIVATE NETWORKS
Daniel Lukaszewski–Lieutenant, United States Navy
Master of Science in Computer Science
Advisor: Geoffrey Xie, Department of Computer Science
Co-Advisor: Justin Rohrer, Department of Computer Science

Virtual Private Networks (VPNs) are designed to use the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) to establish secure communication tunnels over public Internet. Multipath TCP (MPTCP) extends TCP to allow data to be delivered over multiple network paths simultaneously. This thesis first builds a testbed and investigates the potential of using MPTCP tunnels to increase the goodput of VPN communications and support seamless mobility. Based on the empirical results and an analysis of the MPTCP design in Linux kernels, we further introduce a full-multipath kernel, implementing a basic Multipath UDP (MPUDP) protocol into an existing Linux MPTCP kernel. We demonstrate that the MPUDP protocol provides performance improvements over single path UDP tunnels and, in some cases, MPTCP tunnels. The MPUDP kernel should be further developed to include more efficient scheduling algorithms and path managers to allow better performance and mobility benefits seen with MPTCP. Full Text

Keywords: MPTCP, multipath TCP, MPUDP, multipath UDP, VPN, OpenVPN, mobility

A HIGH POWERED RADAR INTERFERENCE MITIGATION TECHNIQUE FOR COMMUNICATIONS SIGNAL RECOVERY WITH FPGA IMPLEMENTATION
Geoffrey R. Meager–Civilian, Raytheon (SAS) Corporation
Master of Science in Electrical Engineering
Advisor: Ric A. Romero, Department of Electrical and Computer Engineering
Co-Advisor: CDR Zachary Staples, Department of Electrical and Computer Engineering

In this thesis, we investigate the demodulation of a communications signal that is interfered with by a high-powered radar signal. We choose quaternary phase-shift keying (QPSK) modulation for illustration. The radar phase offset is initially assumed to be fixed. Later, a practical phase sequence is added to the phase offset. A least-squares estimator (LSE) is used to estimate the amplitude and fixed-phase offset of the interfering radar signal to be used for interference cancellation. Then, we utilize a maximum-likelihood detection (MLD) receiver. We show that the QPSK symbol error ratio (SER) improvement in the radar interference depends on collection time. The variance of the estimate increases as the QPSK signal-to-noise ratio (SNR) increases. The increase in variance affects SER. SER results approach the ideal with increasing collection times. For the case where the phase offset includes a phase sequence, the original LSE technique is modified. Later, a system is created in Simulink and converted to hardware-description language (HDL). The SER performance of the HDL implementation in hardware is compared to those of the signal model. SER performance is somewhat degraded in the hardware implementation. Full Text

Keywords: parameter estimation, matched-filter detection, QPSK, radar, interference, LSE, cyber, electronic warfare

THREE IF BY INTERNET: EXPLORING THE UTILITY OF A HACKER MILITIA
Matthew S. O'Loughlin–Lieutenant, United States Navy
Master of Science in Defense Analysis
Advisor: Leo Blanken, Department of Defense Analysis
Co-Advisor: Zachary Davis, Department of National Security Affairs

Recent cyber exploits have highlighted the ever-growing complexity of the threats challenging our national security today. The surge of cyberattacks against both U.S. and allied targets has rapidly increased due to technological convergence and the accessibility of cyber tools that once were the sole domain of highly skilled hackers. The potential consequences of cyberattacks on national critical infrastructure, illustrated by state-sponsored encroachments of sovereignty in the cyber realm, underscore a growing list of "cross-domain" capabilities. The significant destructive potential of non-state actors in the cyber realm, however, pales in comparison with the sophistication, number, and consequence of those originating from China and Russia.

Understanding the tools of these new adversaries and leveraging emerging technologies to combat them asymmetrically in the digital environment may provide the foundation for forging a new kind of strategy based on partnerships, in which civilian technologists and government leaders unite against malicious cyber actors with the potential to inflict destabilizing effects worldwide. Collaborative efforts are already underway in government, private industry, and the civilian population. This thesis examines how the U.S. government might effectively incorporate unconventional cyber entities to help improve national cybersecurity via nontraditional means. Full Text

Keywords: counterproliferation, collaboration, militia, national defense, unconventional, asymmetric battlespace, hacking, hacktivists, cyber space

KEY TERRAIN: APPLICATION TO THE LAYERS OF CYBERSPACE
Nicholas T. Pantin–Captain, United States Army
Master of Science in Cyber Systems and Operations
Advisor: Wade Huntley, Department of National Security Affairs
Co-Advisor: Duane Davis, Department of Computer Science

The concept of key terrain is a common fixture in military strategy and tactics. The emergence of cyberspace, with characteristics unseen in any warfighting domain, challenge the concept's value. This work is a conceptual analysis that examines the applicability of key terrain in the cyber domain. To determine if key terrain applies in cyberspace, we examine key terrain in traditional physical warfighting domains to understand the concept and draw comparisons. Each of the three layers of cyberspace is examined to determine if the concept of key terrain applies and to identify challenges presented when applying the concept. The result of this work finds key terrain to hold value and applicability within cyberspace. Key terrain can be found at each layer of cyberspace but with some considerations. Cyber key terrain requires constant reassessment, exists only under certain conditions, and can present difficulties in terms of measuring seizure and retention of terrain in cyberspace. The conclusion additionally finds that while cyberspace is unique, it does not require a cyber-specific key terrain definition. We recommend that changes be made to future doctrine, institutional education, and leader development in an effort to provide clarity when using traditional military concepts such as key terrain in cyberspace. Full Text

Keywords: key terrain, cyber, doctrine, cyber key terrain

MAPPING AD HOC COMMUNICATIONS NETWORK OF A LARGE NUMBER FIXED-WING UAV SWARM

Alexis Pospischil–Lieutenant, United States Navy
Master of Science in Computer Science
Advisor: Duane Davis, Department of Computer Science
Co-Advisor: Justin Rohrer, Department of Computer Science

In 2015, a group of Naval Postgraduate School (NPS) professors and students set a record when they flew 50 fixed-wing unmanned aerial vehicles (UAVs) simultaneously as a self-organizing swarm. These vehicles were able to execute behaviors based on message notification from a single ground station and then decide within their swarm group how to order themselves. They were able to accomplish this by communicating over their 802.11n wifi connections. Understanding the strengths and weaknesses of this network will be essential to scaling the swarm to larger sizes or even creating partitioned sub-swarms. The work covered in this thesis is to build a model of the NPS swarm's communication network in ns-3 simulation software and use popular network metrics to illustrate the performance of the network as swarm size increases. It also applied four routing protocols to the swarm and compares their performance to the broadcast protocol. The swarm's communication network was not very tolerant of overhead. This thesis concludes that any routing protocol applied to the (NPS) swarm in the future should consider protocols that reduce or strictly manage overhead generated by either routing tables or multiple message copies. Goodput and packet delivery ratio were the quantitative metrics used. While they illustrate reliability, they do not give a good picture of latency. It would be useful to add latency as a quantitative metric to future work because some swarm messages are more time-sensitive than others. It may be that more than one routing protocol or a protocol with variable settings would be best for this swarm and its various message priorities. Full Text

Keywords: UAV communications network, swarm communications network, UAV swarm, fixed-wing UAV swarm, UAV, swarm

CYBER INDICATORS OF COMPROMISE: A DOMAIN ONTOLOGY FOR SECURITY INFORMATION AND EVENT MANAGEMENT

Marsha D. Rowell–Lieutenant, United States Navy
Master of Science in Computer Science
Advisor: J. D. Fulp, Department of Computer Science
Advisor: Gurminder Singh, Department of Computer Science

It has been said that cyber attackers are attacking at wire speed (very fast), while cyber defenders are defending at human speed (very slow). Researchers have been working to improve this asymmetry by automating a greater portion of what has traditionally been very labor-intensive work. This work is involved in both the monitoring of live system events (to detect attacks), and the review of historical system events (to investigate attacks). One technology that is helping to automate this work is Security Information and Event Management (SIEM). In short, SIEM technology works by aggregating log information and then sifting through this information, looking for event correlations that are highly indicative of attack activity—for example, Administrator successful local logon and (concurrently) Administrator successful remote logon. Such correlations are sometimes referred to as indicators of compromise (IOCs). Though IOCs for network-based data (i.e., packet headers and payload) are fairly mature (e.g., Snort's large rule-base), the field of end-device IOCs is still evolving and lacks any well-defined go-to standard accepted by all. This report addresses ontological issues pertaining to end-device IOCs development, including what they are, how they are defined, and what dominant early standards already exist. Full Text

Keywords: IOCs, events, rules, incident, SIEM, CANES, NetIQ

SELECTION OF THE BEST SECURITY CONTROLS FOR RAPID DEVELOPMENT OF ENTERPRISE-LEVEL CYBER SECURITY

Oleksandr Tytarenko–Major, Armed Forces of Ukraine, Army
Master of Science in Computer Science
Advisor: J. D. Fulp, Department of Computer Science
Advisor: Gurminder Singh, Department of Computer Science

State-supported cyber attacks, cyber espionage campaigns, and hacktivist movements have forced many states to accelerate their cyber defense development in order to achieve at least a minimum level of protection against expanding threats of cyber space. As with any other development effort, cyber capability development requires resources of time, money, and people, which in most cases are very restricted. To rapidly build up "the first line of defense," enterprises should select the most efficient cyber controls and measures.

This thesis sought out the top 10–20 cyber security controls, where ranking was based upon a return on investment (ROI) assessment. This ROI assessment entailed consideration of both the likely/expected security benefits of each candidate security control (the "R" numerator) and the likely/expected cost

associated with each security control (the “I” denominator). The primary references for security controls and their specifications are NIST Special Publication 800-53, revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” and publications of the SANS Institute, NSA, ISACA, the Centre for the Protection of National Infrastructure, and other organizations dealing with cyber security. The selected security controls are presented in a standardized form, with sections for description, expected ownership cost, expected security provided, and general implementation recommendations.
Full Text

Keywords: cybersecurity, security controls, capability development, ROI, resource constraints