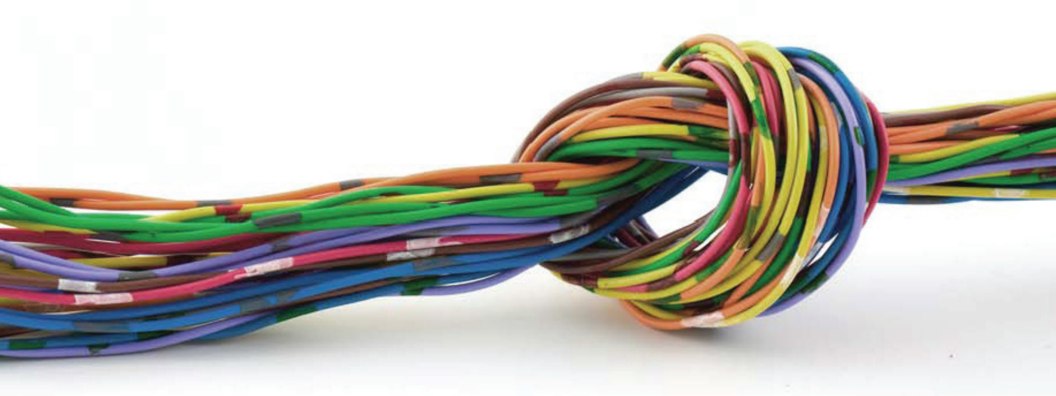
EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

30 YEARS

SECOND WORLDWIDE CYBERSECURITY SUMMIT



The Cyber 40
Mobilizing for International Action

The Queen Elizabeth II Conference Centre, **London, June 1-2, 2011**

In partnership with

London First

Technical co-sponsors

IEEE

IEEE COMMUNICATIONS SOCIETY

Call for Papers and Poster Session

INTRODUCTION

The Worldwide Cybersecurity Summit is a unique event that convenes experts, stakeholders and decision-makers from industry, government and academia to advance international policy to promote the security, stability and safety of cyberspace. The Summit is sponsored by the EastWest Institute, in partnership with its technical co-sponsor, the IEEE.

Consistent with EWI's reputation as a "think and do tank," the Summit fosters problem solving and solution recommendations for difficult international and consequential policy gaps in cyberspace, i.e. the internationally-focused Agreements, Standards, Policies and Regulations (ASPR) gaps. Ultimately, the Summit's format takes on the issues of mistrust and the confidence building necessary for global cooperation.

Papers were sought for international policy-related aspects of cybersecurity, including:

- Worldwide Governance, Frameworks and Protocols for the day-to-day behavior, in cyberspace, policing cyberspace and the conduct of cyber conflict.
- Worldwide reliability and resilience of the supply chain, infrastructure and emerging capabilities (e.g., the mobile ecosystem).
- Worldwide response to cyber crisis (e.g., international priority communications, and trusted information sharing).
- Worldwide issues, awareness and education (e.g., protecting youth, spam and the private public partnerships need to secure the global economy).

As a crucial component of the Call for Papers process, all of the authors will present their complete papers in the form of a poster at the Poster Session on both June 1st and 2nd.

PROGRAM COMMITTEE

Honorary Co-Chairmen
Scott Charney
Byeong Gi Lee
Harry Raduege Jr.
John Stanke
David Veness

GENERAL SESSION COMMITTEE

Greg Austin, *Chair*

Maria Livanos Cattaui
Melissa Hathaway
Terry Morgan
James Lash
Vartan Sarkissian
Deborah Taylor -Tate

ASPR PROGRAM COMMITTEE

Karl Frederick Rauscher, *Chair*

Salma Abassi, E-Worldwide Group
Mark Adams, Cox Communications
Massoud Amin, Univ. of Minnesota
Koichi Asatani, Kogakuin Univ.
Scott Borg, Cyber Consequences Unit
Manuel Pedrosa de Barros, ANACOM
Chi-Ming Chen, AT&T
Hsiao-Hwa Chen, Cheng Kung Univ.
Richard D. G. Cox, Spamhaus
Tariq Durrani, Univ of Strathclyde
Gib Godwin, Northrop Grumman
Stu Goldman, Bell Labs Fellow (ret.)
Marsali Hancock, iKeepSafe
James Isaac, IEEE CS
Luis Kun, U.S. NDU

Andrey Korotkov, Moscow State Institute
Yuxiao Li, Beijing Post & Telecom Univ.
Ramses Martinez, VeriSign
Jack McGourty, Columbia Univ.
Paul Nicholas, Microsoft
Michael O'Rierdan, MAAWG
Wayne Pacine, U.S. FRB
Steve Purser, ENISA
Andrea Rigoni, GCSEC
Mohammed Sabunchi, DIFC (ret.)
Phyllis Schneck, McAfee
Andrea Servida, European Commission
Shannon, Greg, US CERT
Amit Sharma, Ministry of Defense, India
Curtis Siller, IEEE
Abhishek Vaish, Indian Institute of IT
Dean Veverka, ICPC
Yonglin Zhou, Internet Society of China
Richard Zhao, NSFocus

PROCEEDINGS COMMITTEE

Andrew Nagorski, *Chair*

John M. Howell, IEEE Commun. Society
Tracy Larsen, EWI
Franz Stefan-Gady, EWI
Jason Pontin, MIT Technology Review
Abigail Rabinowitz, EWI
Dragan Stoganovski, EWI

Thank you to all of the ASPR Committee members, who contributed their valuable time and expertise to the review process for all of the papers!

Contents

1. Youth Protection

Digital Citizenship – Principles & New Resources

David Miles
Director – Europe, Middle East and Africa
Family Online Safety Institute
London, United Kingdom
e-mail: dmiles@fosi.org

Abstract—This paper explores the need to teach our children to become digital citizens, creating a culture of responsibility which will enable them to navigate the various risks inherent in using the Internet. FOSI's Global Resource and Information Directory (GRID) is the first of a new generation of online global resources that aggregate and track the progress citizens around the world are making as they embrace the challenges and opportunities that this digital age has brought. Its evidence-based approach provides an important counter-balance to the negative, fear-based approach that sometimes pervades the cyber security debate. By educating children and the professionals who work to protect them, all parties can be better equipped to deal with the ever-changing digital world in which we now live.

Keywords-component; children; cybersecurity; digital; Internet; literacy; media; online safety; professionals; responsibility; youth

2. New approaches to dealing with online child pornography

John Carr
Children's Charities' Coalition on Internet Safety
CHIS, London, UK
ukchis@btinternet.com
www.chis.org.uk

Abstract—This paper shows how the arrival of the internet has completely transformed and hugely expanded "the market" for child abuse images. The paper makes links between the production and distribution of child pornography and the activities of organized crime. It also suggests the continued availability of these kinds of images on the internet also contributes to a wider sense that the internet is a lawless place. This in turn encourages more diverse criminal elements to think of it as an attractive or easy environment in which to operate. The paper concludes by showing that, in relation to the web, there is an efficient system of "notice and take down" which operates very well in many countries but it argues similar systems need to be deployed in many more.

Keywords: child pornography, child abuse images, notice and take down, organized crime

3. Telecommunications Supply Chain Integrity

Mitigating the Supply Chain Security Risks in National Public Telecommunications Infrastructures

John Kimmins
Telcordia Technologies
Piscataway, New Jersey USA
+1 732-699-6188
jkimmins@telcordia.com

Abstract— Across the globe, many national telecommunications infrastructures are at a crossroads. Incumbent suppliers are increasingly relying on off-shore component sourcing, while new suppliers   some from countries with strong geopolitical tensions   have taken significant actions to position themselves to be major suppliers to various nations' telecommunications operators. Collectively, these factors have brought a sharp focus to the need for a more in-depth review of the integrity of national telecommunications infrastructures and the supporting foreign product supply chains. This paper delineates the above factors and their related risk implications for national and global communications infrastructures. In doing so, the paper reflects an enhanced risk management model and process Telcordia has developed that accommodates both government and private sector issues and builds upon current security practices.

Keywords-Supply Chain, Network Security, Telecommunications

4. The FATF as a Model for Internet Governance

Kevin P. Newmeyer
Assistant Professor
Center for Hemispheric Defense Studies
Washington, DC
Kevin.newmeyer2@ndu.edu

Abstract— To date, traditional diplomatic instruments and structures have only been marginally effective in combating cybersecurity risks. Perhaps it is time to use model that has been effective in another challenging international arena, money laundering. The Financial Action Task Force (FATF), which started as an effort among the economic leaders in the world, uses an intergovernmental policy group to build political will to counter a network threat in money laundering. With its best practices, regional subgroups and threat of blacklisting, it is effective in bringing pressure to bear on recalcitrant nations. A FATF style cyber security body offers a means to improve the global governance regime for the Internet by leveraging the will of interested governments. This paper offers an outline of how the FATF model could be applied to the Internet and thereby improve governance and security.

Keywords- cybersecurity ,internet governance; international cooperation; security

5. IPv6 Forum Cybersecurity Task Force

Create a Worldwide IPv6 Secure Network

Latif LADID
IPv6 Forum
Luxembourg
latif@ladid.lu

Junaid ISLAM
VIDDER
San Jose, USA
Junaid.islam@vidder.com

Abstract—With the growing rate of cyber attacks on government and commercial networks, policy makers are looking for a cost effective strategy to enable trusted communications. IPv6 has built-in IP security (IPSec)

which enables all traffic to be encrypted without the need for special hardware. Subsequently IPv6 enables the creation of large scale encrypted networks which are very resilient to cyber attacks. Unfortunately most network professionals are unaware of the integrated encryption and authentication features of IPv6.

The IPv6 Forum's Cyber Security Task Force is studying on how to mitigate cyber attacks thru the deployment of Internet scale VPN architectures. A summary of the group's findings will be published in a white paper. Individuals interested in volunteering for the Steering Committee should email their background to IPv6Forum@vidder.com

Note: Currently membership to the Cyber Security Task Force is strictly limited to network & security experts. Tutorial material will be created for those interested in learning about IPv6 based security at a later date.

Keywords-component; IPv6, Cybersecurity

- Background

The Internet is the most important communications network today. High value transactions such a banking that once took place in guarded offices now happen on browsers. Mission critical Enterprise applications are now hosted at publicly accessible clouds. Power distribution systems, which were not even networked in the past, are being connected via the Internet. For organizations that depend on the Internet, the rapidly increasing rate and sophistication of cyber-attacks is a major concern. Cyber attackers take advantage of the sheer size of the Internet to hide their presence, hijack PCs and attack network infrastructure without warning.

Unfortunately, the current cyber-attack counter-measures don't work. Browser-based SSL, intended to ensure that selected information is kept private as it traverses the Internet, is being compromised more and more every day. The ideal solution would be to leverage IPSec VPNs for all traffic. Unfortunately hardware based VPN are too complex and costly to deploy. Subsequently the IPv6 Forum has formed a Cyber Security Task Force to explore the creation of a distributed Internet scale public VPN.

Internet scale Public VPN

The key proposal of the Cyber Security Task Force is that end-to-end IPsec VPNs be used for all communications. That concept in itself is not revolutionary as IPsec VPNs are widely used by government and commercial organizations. However since IPsec VPNs use expensive hardware they are not used for on a large scale. To enable scalable IPsec VPNs, IPv6's integrated encryption, auto-configuration, and trillion size addressing properties seem ideal. IPv6 enables every network element to be individually addressed and secured via a dedicated VPN connection.

To create an Internet scale VPN, the Task Force will study and make recommendations on how best to activate the integrated IPSec features of IPv6 using open key management system. As IPv6 is still in the early deployment phase, the Task Force will also explore leveraging overlay as well as native deployment models. To simplify deployment of large scale VPNs, auto-configuration technologies such as Mobile IPv6 will be studied. Additionally the group will also develop a set of recommendations for a scalable key management and efficient block ciphers to secure large public networks.

6. Malaysia National Cyber Security Policy

The Country's Cyber Defence Initiatives

Mohd Shamir b Hashim
Government & Multilateral Engagement Div
CyberSecurity Malaysia
Kuala Lumpur, Malaysia
Shamir@cybersecurity.my

Abstract— The launching of Malaysia's Vision 2020 mark the country's journey towards becoming a developed nation and embracing the knowledge-based economy as a mean of achieving it. By consciously choosing to utilize the information and communication technology as a tool for development, it has resulted in the increasing use of digital information systems throughout the industry, the private and public organizations and the society at large. However, the dependency on digital information systems bring with it escalating vulnerabilities and risks, especially to the Critical National Information Infrastructure (CNII) which among others include cybercrimes such as Hacking, Intrusion, Fraud, Harassment, Malicious Code and Denial of Service Attacks.

Acknowledging the growth of cyber threats that are endangering the e-Sovereignty of the nation, a cyber security policy was put in place.

The National Cyber Security Policy (NCSP) is Malaysia's comprehensive cyber security implementation to be done in an integrated manner to ensure the CNII is protected to a level that commensurate the risks faced. Cutting

across the government machineries, the implementation has drawn in various ministries and agencies to work together to meet the vision of having a CNII that is secured, resilient and self reliant that will eventually promote stability, social well being and wealth creation for the country.

After 4 years of the NCSP implementation, the Malaysia's cyber security is now being looked as something to be reckon with. Much has been done and more need to be done as the landscape of cyber threats changes with the development of new technologies and tools.

Successfully implemented, Malaysia's CNII will be better placed to meet the challenges and opportunities that technological advancement brings and that it will help to achieve the objectives of Vision 2020 and beyond.

7. The Organisation of Islamic Conference – Computer Emergency Response Team (OIC-CERT)

Answering Cross Border Cooperation

Rahayu Azlina Ahmad
Multilateral Engagement Department
CyberSecurity Malaysia
Kuala Lumpur, Malaysia
rahayu@cybersecurity.my

Mohd Shamir Hashim
Government & Multilateral Division
CyberSecurity Malaysia
Kuala Lumpur, Malaysia
shamir@cybersecurity.my

Abstract-The rapid growth of the Information & Communication Technology (ICT) systems and network infrastructures have cause the Internet to be borderless and inevitably given rise to the issues in mitigating cross border cyber crimes. Realizing the danger and the huge impact of this matter, the Computer Security and Incident Response Teams (CSIRT) or the Computer Emergency Response Team (CERT) have developed international and regional collaborations to deal with cross borders cyber threats. Sharing intelligence, research, best practice, challenges and learning from other's mistakes as well as helping to formulate and drive international policy direction and initiatives will help member countries to protect their own critical information infrastructure.

Acknowledging this new trend of collaboration and the threats in the cyber world, the Organization of Islamic Conference (OIC) has agreed to

the establishment of inter CSIRT/CERT collaboration among its member countries. The OIC - CERT was established in 2009 with the status of an affiliated institution to the OIC. Presently, 18 OIC countries are members of this collaboration and various activities are being conducted with the main objective being to facilitate the development of CIRST capabilities, information sharing on views and issues in cyber security.

From the economic perspective, information security is currently considered as one of the factors to lure foreign investment to a country. Thus strengthening the nation's information security will help improve international recognition.

8. Multi-dimensional Challenges Facing Digital Youth and their Consequences

Salma Abbasi
CEO, e Worldwide Group, London, UK
Sr. Associate Fellow,
King's College London, UK
salma@e-wwg.com

Myra Manawar
e Worldwide Group, London, UK
myra@e-wwg.com

Abstract—The Internet continues to be a dynamic and incredibly powerful source of information with almost limitless capabilities for improving access to knowledge and connecting people around the world. It is also seen as a solution to addressing many social development issues by providing access to healthcare, remote learning opportunities, access to e-government services and innovative and higher paying jobs. With advancements in ICTs resulting in the transformation of the technological, economic, social, political, cultural, and educational realms, the world is fast becoming the proverbial 'global village'. The children and youth who are the major beneficiaries of this technology boom, who are the subject of this paper, are referred to as 'young digital citizens'. The emergence and widespread adoption of ICTs has greatly influenced the lifestyles of these young digital citizens, given the plethora of information on the Internet to which they have access. While the cyber world acts as a great resource on one side, it also has a sinister aspect, to which vulnerable and trusting digital youth can be subjected, both intentionally and unintentionally. The impact of the Internet can be extrapolated into four main aspects, namely: social, physical, psychological and moral (including ethical and religious). It is the aim of this paper to discuss the impact of these potential threats and the challenge they present to society and governments in creating a safe and secure environment.

Keywords – Internet; digital youth; challenges; cyber threats

9. Primer on the International Aspects of International Priority Communications Policy

(All packets cannot be equal)

Stuart Goldman
Bell Labs Fellow (ret)
Phoenix, AZ USA
familygoldman@gmail.com

Abstract—If this “Primer on the International Aspects of International Priority Communications (IPC) Policy” establishes a common understanding of what IPC is and is not, so that the other contributed papers to this Summit can then consistently build on that foundation, then it purpose has been achieved.

It is imperative that high priority critical communications must be served across international boundaries. Under severe conditions such as a disaster or crisis, the communications networks may well be offered much more communication traffic than the bandwidths can support. In such cases some, or most, traffic must be shed allowing other communications proceed. Rather than a random or arbitrary mechanism for discarding a subset of the communications, a system may have a means of marking critical communications such that a higher level of probability of completions exists for such communications as compared with other message attempts on the same network.

This paper addresses aspects of such Priority Communications when the origination and destination points are in different nation’s networks (international). This paper does not address the selection and transmission mechanisms used within a national network as this is a matter of local policy.

Keywords-component; Policy, International, High priority communications, wireline, wireless, Internet, future communication protocols & networks, crisis, disaster

10. Architectural Solution Integration to Contain ICT Supply Chain Threats

Xiaofeng QIU
Beijing University of Posts and Telecommunications
Beijing,P.R.China
qiuxiaofeng@gmail.com

Liang ZHAO
NSFOCUS
Beijing, P.R.China
Richard.zhao@nsfocus.com

Abstract—ICT (Information Communication Technology) , which has been more and more critical in the modern economy and society , means more than IT and traditional Telecom. The integrity of ICT Supply Chain has slightly different meaning than the traditional security and assurance. Partly for the sake of difficulties to technically testify the increasingly complicated modern ICT products, it's by no means to figure out an end to end integrity assurance program and methodology, letting alone test cost and timing factors.

This paper investigates the threats of ICT supply chain integrity, including covert channel. An architectural approach, named as Architectural Solution Integration, is given out to assure the integrity of ICT system and contain the potential threats from supply chain. The quantitative assessment of ICT supply chain integrity is discussed as well, followed by the future works.

Keywords—ICT Supply Chain Integrity Assurance Security Covert Channel

11. IVDA: International Vulnerability Database Alliance

Chen ZHENG[1,2], Yuqing ZHANG[1,2*], Yingfei SUN[2], Qixu LIU[1,2]
[1]National Computer Network Intrusion Protection Center, GUCAS
[2]School of Information Science and Engineering, GUCAS
Beijing 100049, PR China

Abstract—Vulnerability is one of the important factors that cause security incidents and has become a major international threat to network security. Previous work like Common Vulnerabilities and Exposures (CVE) and vulnerability databases has been offered to manage vulnerability. However, they have significant disadvantages in coverage and regional differences. International Vulnerability Database Alliance (IVDA) is proposed as an alliance model which consists of security organizations from different countries. IVDA provides systematic policies and standards to manage vulnerabilities of software in different languages, and achieves agreement with its members to enhance international cooperation and communication. The evaluation of IVDA shows that the international alliance is rational and effective in vulnerability disclosure.

Keywords-Network Security; Vulnerability; CVE; IVDA

12. A Brief Study of SNMP Protocol and its role in Network Management

Waqqas ur Rehman Butt
Centre of Excellence in Water Resources Engineering
University of Engineering & Technology,
Lahore, Pakistan
E-mail: wkbutt@hotmail.com

Sohail Abbas
MIS, Department
Head Office Sui Northern Gas Pakistan Ltd.
Lahore, Pakistan
E-mail: sohailabbas_19@hotmail.com

Abstract— In the modern era Network Management is hot issue. Number of accessories, methods and tools exists to support network and network device management. Simple Network Management Protocol (SNMP) is widely acceptable protocol for network management since 1988. It is typically developed for monitoring and controlling the communication systems as well as generates alerts to network administrator to problems. This paper shows that network management techniques and how the Network Management perform with SNMP. SNMP is applicable to TCP/IP networks, as well as other types of networks. SNMP is also available in Gateway should be configured properly as desired. Gateway device provides a shared Internet connection and workgroup services to a networked. Information retrieves from devices in network and information stored in (MIB) Management Information Base. SNMP uses this information to perform monitoring, controlling and management functions in the Network. SNMP is very useful in different management activities in communication system but in this paper focus will be on monitor the communication system and devices to ensure that system is working properly. It gives the some basics techniques for checking, controlling and maintain the devices in proper working. SNMP is a standard protocol of Internet protocol (IP) and used to control the network devices in very easy because it uses application level. Agents and manager retrieve information from MIB. In this paper, brief study of SNMP including working, architecture, functions in Gateway, advantages and disadvantages. Agent implemented, describe relation between agent and manager and network management system NMS. An agent is a mediator between the manager and the device.

Keywords- SNMP, MIB, TCP /IP, Manager, Agent

13. Is the future Web more insecure? Distractions and solutions of new-old security issues and measures

Stefano Zanero
Dipartimento di Elettronica e Informazione
Politecnico di Milano
Milano, Italy
zanero@elet.polimi.it

Federico Maggi
Dipartimento di Elettronica e Informazione
Politecnico di Milano
Milano, Italy
fmaggi@elet.polimi.it

Abstract— The world of information and communication technology is experiencing changes that, regardless of some skepticism, are bringing to life the concept of “utility computing”. The nostalgics observed a parallel between the emerging paradigm of cloud computing and the traditional time-sharing era, depicting clouds as the modern reincarnation of mainframes available on a pay-per-use basis, and equipped with virtual, elastic, disks-as-a-service that replace the old physical disks with quotas. This comparison is fascinating, but more importantly, in our opinion, it prepares the ground for constructive critiques regarding the security of such a computing paradigm and, especially, one of its key components: web services. In this paper we discuss our position about the current countermeasures (e.g., intrusion detection systems, anti malware), developed to mitigate well-known web security threats. By reasoning on said affinities, we focus on the simple case study of anomaly-based approaches, which are employed in many modern protection tools, not just in intrusion detectors. We illustrate our position by the means of a simple running example and show that attacks against injection vulnerabilities, a widespread menace that is easily recognizable with ordinary anomaly-based checks, can be difficult to detect if web services are protected as they were regular web applications. Along this line, we concentrate on a few, critical hypotheses that demand particular attention. Although in this emerging landscape only a minority of threats qualify as novel, they could be difficult to recognize with the current countermeasures and thus can expose web services to new attacks. We conclude by proposing simple modifications to the current countermeasures to cope with the aforesaid security issues.)

Keywords-component; Cloud Computing, Distributed Systems, Network operating systems, General Security and protection, Anomaly Detection.

14. HawkEyes: An Advanced IP Geolocation Approach

IP Geolocation using semantic and measurement based techniques

Art Dahnert
Overwatch Systems Ltd.
Austin, Texas, United States of America
adahnert@overwatch.textron.com

Abstract—Hawkeyes is an advanced implementation of IP Geolocation utilizing measurement-based geolocation techniques along with a semantic-based approach. The accuracy of the result is directly related to the detection of nearby “landmarks” that can be referenced in the measurement of the target from a well known location. By developing a reliable, fast, current and accurate mapping of IP addresses to physical locations it is possible to provide advanced capabilities to international law enforcement agencies as well commercial organizations.

Keywords- IP Geolocation; Constraint Based Geolocation; TopologyBased Geolocation; postal codes

15. Hybrid Elicitation of Latent Intent in Open Societies

(HELIOS)

John Palmer
Overwatch Systems, Ltd.
Austin, Texas, United States of America
jpalmer@overwatch.textron.com

Abstract— The reach of ubiquitous social networking tools enabled through new technology is evident in the recent regime change and the increased unrest within the Middle East. Such rapid dissemination of information may engender an equally rapid emergence of virtual communities of interest -- some with potentially hostile intent. Twitter's accessibility and popularity have attracted a large number of automated programs, known as bots, which can serve as a double-edged sword within Twitter. While legitimate bots generate a large amount of benign tweets delivering news and updating information, malicious bots spread misinformation with potentially virulent results. This paper blends methods from traditional statistical classification methods with latent Dirichlet allocation with techniques of social network analysis to underpin threat assessment based upon similarities discerned among topic sets that have distilled by semantic analysis of Twitter intercepts.

Keywords: Centrality, Cyber information, Dirichlet, document clustering, Gibbs sampling, Kullback-Leibler, multinomial, text extraction, twitter, social networks, unsupervised learning.

16. Emerging Social Media Threats: Technology and Policy Perspectives

R. Chandramouli
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, New Jersey

Abstract—Traditional cyber threats or attacks have targeted information and communication infrastructure that usually result in economic losses. Typically, launching these attacks requires an advanced skill level. Governments around the world have a good understanding of these threats and therefore have put in place many policies to deal with them.

The rapid growth of social media is giving rise to new types of threats that spill over from the cyber world to real-life. These threats profoundly alter the psychological, social and cultural dynamics of vulnerable social media users. Also, it is becoming increasingly easy even for an average user to exploit social media for malicious purposes. Organizations and governments are finding it difficult to accurately detect, identify, predict, and prevent the malicious exploitation of social media. Quantifying the socio-psychological effect of social media vulnerabilities is another major challenge. Due to these reasons there is a lack of policies to deal with this issue. In this paper, we discuss several challenges in this emerging area, from technologies to policies.

Keywords-social media security; deception detection; pycho-linguistics, regulatory policies.

17. Current Realities of Cyber Conflict

The “Open Secret” of the Global Cyber Arms Race

Eli Jellenc
Head of International Cyber Threat Intelligence
VeriSign, Inc. (iDefense Cyber Security Research; EMEA Office)
London, UK
ejellenc@idefense.com

Abstract- This paper offers new perspectives on global cyber conflict dynamics through comparative analyses of states’ policy developments and a set of actual cases of cyber conflict events. Moreover, this research shows how existing theoretical work in political science, sociology and information science can lend new rigor to the study of cyber security as a geopolitical issue. The outcome of the analysis is robust set of evidence-based conclusions which show that the reality of cyber conflict is much different than conventional wisdom suggests: the current reality is a very active and rapidly escalating cyber arms race.

Nearly all existing research or commentary on cyber conflict up to the present consists either in speculations on how cyber conflict might develop with scant evidence or otherwise in narrow technical descriptions cyber conflict events generally with little contextual analysis provided. In very few pieces of publicly available research are known cases of cyber conflict systematically, comparatively analyzed in order to test hypotheses about the principles of cyber conflict as it is actually developing (rather than how it might or "should" develop). This research seeks to address these shortcomings through reference to robust existing theories:

- Manuel Castells's theory of "communication power" provides a coherent underlying framework
- Models of arms races and the security dilemma (from international security studies) aptly explain current cyber security dynamics among states
- "Conflict theory" and "securitization" models from political sociology explain much government policy development
- Col. John Boyd's Observe-Orient-Decide-Act ("OODA") Loop models go far in explaining relative successes and failures in strategic cyber security interaction

Drawing on the models above, this effort fills gaps in cyber conflict research through two interconnected streams of analysis. First, I develop a structured, comparative analysis of the different information security and cyber conflict programs of various nation-states, including the roles played by commercial sectors and hacker undergrounds. This analysis reveals three essentially different models of cyber conflict development, with each specific nation's efforts varying along the main dimensions that constitute the models. Second, I structure analyses of a series of actual cases of politico-strategic cyber security incidents to discern the operative principles at play and to highlight development trends; a counterintuitive result is that "cyber conflict" and "cyber espionage" appear to be functionally integrated, not separate, classes of activity.

The primary conclusions to which this research leads are three:

- First, the treatment of cyber conflict by the world's major powers (and many of the minor ones) exhibits all the features of a novel, multilateral arms race…a cyber arms race. It is highly improbable that anything short of revolutionary legal or diplomatic means will prevent dramatic increases in cyber conflict in the near future.

- Second, the robust nature of the arms race dynamic and the very nature of information technology itself strongly suggest that deterrence (and, indeed, defense) will not always be possible for most significant variants cyber conflict. In short, no organization (governmental, military, commercial) has demonstrated the capacity to reduce the uncertainties of cyber conflict to a degree allowing its use as an instrument of national policy.
- Third, the deep uncertainty and asymmetry surrounding the cascading effects of cyber attacks against interconnected IT systems overshadows what little understanding of cyber conflict now exists. As the complexity of the global information grid increases, so will these uncertainties, which will have unprecedented implications for the development of the strategy and conduct of cyber conflict.

Keywords: cyber warfare ; cyber espionage ; information security ; communications theory; strategy; arms races

18. DevEyes Insider Threat Detection

Art Dahnert
Overwatch System Ltd
Austin, Texas, USA
adahnert@overwatch.textron.com

Dr. Stanley Young
Overwatch Systems Ltd
Austin, Texas, USA
syoung@overwatch.textron.com

Abstract—The DevEyes framework provides a system for detecting insider threats aimed at manipulating the software development process, based on analysis of vulnerabilities and interactions between people, other people and system artifacts.

Keywords: insider threat, vulnerabilities, interactions

19. The Analysis of Youths' Searching Behavior

Chao li, Bin Wu
Beijing Key Laboratory of Intelligent Telecommunications
Software and Multimedia
Beijing University of Posts and Telecommunications
Beijing, China

Abstract—In order to create a safe and harmonious online environment for youth and protect them from the impact of bad information such as pornography, violence and gambling, most of the current solutions are to shield the bad sites that reported by the public. However some youth will take the initiative to seek for these bad information. In this paper we propose a method to analyze the searching behavior of youth and then to shield those keywords that may impact their health in time. Parents of youth can provide their IP address to the operators depending on the circumstances to allow operators to set their IP within the scope of monitoring. Firstly we collect the keywords that youth search in the websites .Secondly we count and classify these keywords to know the trend of their searching behavior and the areas that they often concern.Lastly we cluster the keywords in each category to get the main clusters and the frequent keywords in each cluster. Using this method we can grash youths' searching behavior effectively.

Keywords- classify; cluster; searching behavior;shield

20. Comparing Twitter and Chinese Native Microblog

Wenhao Wang, Bin Wu
Beijing Key Laboratory of Intelligent Telecommunications
Software and Multimedia
Beijing University of Posts and Telecommunications
Beijing,China

Abstract- Microblog is a mixture of web media and social network. It has been becoming prevalent in recent years. This new web member in different countries does not only appear with different languages, but also contains other distinctions. In this paper, we conduce a throughout comparison between Twitter, the most popular microblog service, and ShuoKe, a Chinese native microblog service. On one hand, we analyze the content in both services using text clustering to reveal what kind of topic is hot and how long a topic can exist. One the other hand, we depict the social network of the two services through the relationships among microblog users. Our findings enable us to understand the underlying contrast of miroblogs in different countries.

Keywords- miroblogs; comparision; social network.

21. Worldwide Security and Resiliency of Cyber Infrastructures: The Role of the Domain Name System

Andrea Rigoni, Igor Nai Fovino,
Salvatore Di Blasi
Global Cyber Security Center
GCSEC, Rome, Italy
{andrea.rigoni, igor.nai, salvatore.diblasi}@gcsec.org
Emiliano Casalicchio
Dep. of "Informatica, Sistemi e Produzione"
Università di Roma "Tor Vergata"
Rome, Italy
emiliano.casalicchio@uniroma2.it

Abstract— The pervasiveness of Information and Communication Technologies in the control and governance of Critical Infrastructures (CIs) (e.g. power plants, energy grids, oil pipelines etc.) makes the Cyber Security problem a matter of citizen protection and safety. Today, CIs are exposed not only to traditional safety and availability problems, but also to new kinds of security threats related to the inevitable use of IP networks (and related routing protocols) and the Domain Name System (DNS). While these two worldwide infrastructures have been generally operated in a reliable and robust fashion for decades, the pervasiveness problem above mentioned and the growing number of cyber threats and attacks raise new challenges at political, governance and technical level.

In this work we concentrate our attention on the core role of the DNS in the secure and resilient operation of CIs.

Keywords: DNS Security, Stability, Resiliency, Critical Infrastructure Protection, Cyber Warfare

22. Making the Internet Clean, Safe and Reliable

Asia Pacific Regional Collaboration Activities

Yurie Ito
Chair, Asia Pacific Computer Response Teams (APCERT)
Tokyo, Japan

Abstract— This paper introduces Asia Pacific Regional Collaboration activities for making the Internet Clean, Safe and Reliable. Internet ecosystem faces significant challenges and we need to begin to think of solving problems at a global level and using strategies and approaches that work to improve the ecosystem and its health in addition to protecting against and reacting to specific threats and incidents. Paper introduces APCERT members' national level Internet Clean up activities from Australia, Japan, Korea and China. APCERT supports good practices and sharing among members. Additionally, we seek to define what is meant by a "clean" Internet and how to measure whether the Internet is actually becoming "cleaner" due to the conduct of clean up activities. Also the paper introduces good practice of confidence building measure to limit cyber conflict between China, Japan and Korea. This approach demonstrates public-private partnerships on both sides addressing participant needs and incentives are key to the success of these conflict management arrangements.

23. Information Security Practices Followed in the Indian Software Services Industry – An Exploratory Study

Sanjay Bahl
Microsoft Corp
(India) Pvt Ltd
New Delhi, India

O P Wali
Indian Institute of
Foreign Trade
New Delhi, India

Ponnurangam Kumaraguru
Indraprastha Institute of
Information Technology
New Delhi, India

Abstract—India tops the global IT outsourcing supply chain world ranking. While there are numerous benefits, there are also perceived risks of IT outsourcing to India. The service quality gaps model encompassing the business model for information security has been applied on Indian Software Services Providers practices around information security while they deliver software service to their customers. This exploratory study employs data, theory and methodological triangulation to enhance confidence in the findings. The results have been mapped onto the business model for information security in the overall context of service quality gaps model. The study concludes that from information security perspective there are service design and service performance gaps impacting service delivery of Indian Software Service Providers. However these gaps still put India at par with various countries, if not ahead with respect to information security practices, since the service quality gaps model is primarily customer driven. From a trade perspective the study concludes that information security gaps at Indian software Service Providers side will not impact Indian software exports growth adversely as long as the customer gap which is the gap between perceived and expected service, remains within customer defined tolerance limits.

Keywords-supply chain; IT outsourcing; Indian software service providers; business model for information security; service quality gaps model

24. Establishing the Baseline: A Framework for Organizing National Cyber Strategies

Aadya Shukla
Science, Technology and Public Policy Fellow
The Kennedy School at Harvard University
Cambridge, Massachusetts

Abstract- The nature of cyberspace is not the same as the approaches taken to tackle the challenges within the cyberspace. Therefore, an effort to understand the cyberspace requires a ‘separation of concerns’.

The question of ‘what is cyberspace’ requires the conceptualization of the entities (actors and processes) within the domain (ontology construction). This lies more in the realm of Computer Science. But the question of how to govern the interaction between different actors and processes belongs to the policy-making domain. In the recent past, different nation states have released their cyber strategy documents to address this concern. With increased consensus among various stakeholders (nation states) that tackling the cyberspace challenges will require improved interoperation in cyber policy making, there is an immediate need to characterize the cyber strategies of various nation states. An integrated framework to understand various strategies is currently missing from the domain. We think that interoperation can not be achieved unless weight of the stakes for each stakeholder is clearly understood in terms of their domestic and international commitments.

The research presented here aims to fill this gap by presenting a framework to discuss priorities, concerns and models for various national cyber strategies (EU, UK, Dutch, German, and French) in a coherent manner. We

hope that characterization and analysis presented within the framework will answer three important questions. Firstly, what measures have been proposed to respond to cyber incidences; secondly, what is the gap between theory and practice by looking at the actual incidence response deployed by the nation states discussed here; thirdly, a comparative study of the strategy documents of a number of European states will highlight the degree of interoperation (or lack of it).

The paper proposes models of various cyber strategies at a meta-level to keep the analysis platform independent. By which we mean that analysis presented here separates attributes of the Information Technology being employed to implement the cyber strategy from the attributes of the cyber strategy itself (different types of technologies may or may not address the concerns at the policy level given its specific constraints and nature). The components of meta model map onto three main aspects of a given cyber strategy i.e., mitigation, response and evolution.

A common framework will help us to establish a more standardised vocabulary to understand the parameters and associated constraints to facilitate the meaningful dialogue among the cyber policy makers. This research will help the practitioners to understand the gap between deployment of these policies at a practical level, before and after the incidence takes place. Added value of this research stems from the fact that it will help us to understand the generic and specific policy-making concerns of the nation state actors. How the local laws place different weights on a number of components of cyber incidence response policy will be clarified. Furthermore, how the boundaries of the cyberspace do not map onto boundaries in conventional international relations can be understood by analysing the cross-agency cooperation required to tackle the cyber-incidences. We also hope to extend the framework by comparing the cyber strategies of developed and developing nations.

25. The Study on the Communication Mechanism of New Media Event

Yiwen Zhang[1], Qixing Qu[2], Jiayin Qi[3], Binxing Fang[4]
[1, 2, 3.] School of economics and management, Beijing University of posts and telecommunication, 100876, Beijing, China.
[4.] School of computing, Beijing University of posts and telecommunication, 100876, Beijing, China.

Abstract— With the development of the internet, there is a new kind of event beginning to emerge. Researchers call them" new media event, which has great social influence and every person in society, has the chance to participate in it, making the thing change. To compare with the traditional media event, the new media one empowers the Grass-roots not only have the right to know the event, but also have the power to change the developing process of it. So many researchers consider that the new media has the function to settle disputes between the government and the public. In conclusion, research on the emerging mechanism and communication rules of the new media event is significant. In this paper, after the contrast between the concept of "media event" and one of "new media event", we describe the communication mechanism of the new media event, and build the model to explain the deep relationship of the variables such as the number of topics, the number of network news and the number of doubt posts. Finally, we use the case study method to verify the reliability of the model.

Keywords- new media event; deviation; doubt degree; number of topics.

26. Cybersecurity Principles for Industry and Government A Useful Framework for Efforts Globally to Improve Cybersecurity

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council
Washington, DC, United States
dkriz@itic.org

Abstract— Cybersecurity is rightly a priority for governments globally. The phenomenal expansion of cyberspace has brought unprecedented economic growth, opportunity, and prosperity. However, it also presents bad actors with completely new threat and crime opportunities. The interests of industry and governments in securing and facilitating cyber-based transactions and activities are fundamentally aligned. All companies want a secure digital infrastructure for commercial transactions. To ensure the continued viability of the infrastructure and growth of their sector, technology compa-

nies are highly motivated to design and build security into the DNA of their products and systems. Governments need a secure global digital infrastructure for economic growth, prosperity, efficiency, and protection.

To better inform the public cybersecurity discussion, the Information Technology Industry Council (ITI) developed a comprehensive set of cybersecurity principles for industry and government. ITI's six principles aim to provide a useful and important lens through which any efforts to improve cybersecurity should be viewed. To be effective, efforts to enhance cybersecurity must:

- Leverage public-private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today's cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;
- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

The growth of cyberspace will continue to advance if interoperability, openness, stability, resiliency, economic growth, and risk mitigated by security guide its development. In the right policy environment, we can increase security while maintaining cyberspace's overall benefits. A host of tools and approaches are available to consumers, businesses, governments, infrastructure owners and operators, and the IT industry to meet our shared security challenges and goals. These evolving tools include information sharing, risk management models, technology, training, and the development of globally accepted security standards, guidelines and best practices. Public policy will play an important role in encouraging the use and improvement of these tools and helping to shape the expectations and actions of stakeholders on cybersecurity.

ITI's principles can guide policymakers in developing and facilitating an effective public policy framework that enhances security while maintaining the overall benefits of cyberspace.

Keywords-Information Technology Indusrtry Council; ITI; principles.

27. Legislation Concerning the Protection of the Right to Online Privacy in China:

A comparative study with EU

Yuxiao Li
School of Humanities
Beijing University of Posts and Telecommunications
Beijing, People's Republic of China
liyuxiao@bupt.edu.cn

Jinghong Xu
School of Humanities
Beijing University of Posts and Telecommunications
Beijing, People's Republic of China
xujinghong@bupt.edu.cn

Abstract—Triggered by a spat between China's two top Internet firms, this paper explores the legal system concerning the protection of the right to online privacy in mainland China by an international and comparative study, with special reference to that of EU. The authors point out that all the problems of existing laws and regulations concerning the protection of the right to online privacy should be regarded as the combined results of both the legal system building and the current stage characteristic of rapid development. The authors offers suggestions for China to better the legislation concerning the protection of the right to online privacy systematically, such as the constitutional protection of the right to privacy should be strengthened; the protection of the right to privacy in civil law system should be unified and be more detailed; the protection of the right to privacy in criminal law should be promulgated and be more updated; the protection of the right to privacy in administrative law should be strengthened and the special law protecting the right to online privacy should be enacted.

Keywords- legislation; online privacy; the right to online privacy; China; EU

28. Metrics for Measuring the Robustness of the Undersea Cable Infrastructure

A Road to Standardization

Spilios E Makris
Telcordia Technologies
Red Bank, New Jersey,
USA
smakris@telcordia.com

Nicholas Lordi
Telcordia Technologies
Red Bank, New Jersey,
USA
nlordi@telcordia.com

Melvin G. Linnell
Telcordia Technologies
Red Bank, New Jersey,
USA
mlinnell@telcordia.com

Abstract—The Undersea Cable Infrastructure (UCI) is a critical component of the global telecommunications infrastructure. No universally accepted metrics currently exist to assess and track the resiliency, reliability, and growth of the UCI. Standards are needed to ensure the continued development of a resilient and reliable UCI. This paper highlights current standards efforts at the Alliance for Telecommunications Industry Solutions (ATIS) Performance, Reliability, and Quality Committee (PRQC) to standardize such metrics in an effort to ensure a resilient UCI and the end-to-end integrity of the global telecommunications network infrastructure.

This paper highlights a need to complement the ATIS Standards Outage Index currently used for wireline, cable TV, wireless, & satellite telecommunications service outages, with metrics to incorporate the UCI environment, thus fulfilling a related recommendation from the IEEE ROGUCCI Global Summit in Dubai (27-29 October 2009). This paper also discusses (i) a set of factors that influence the resiliency, reliability and growth of the UCI metrics associated with these factors, and (ii) a method of visualizing (based on an ITU-T international standard) these metrics in a single diagram, which could be used by assorted interested parties.

Keywords- resiliency, undersea cable infrstructure, submarine cable; metrics; outages.

Thank you to our sponsors

Leader's Forum

Deloitte.

Goldman Sachs

Microsoft®

Platinum Sponsors

HUAWEI

KNIGHTSBRIDG
CYBERSYSTEMS

Gold Sponsors

AKIN GUMP
STRAUSS HAUER & FELD LLP

at&t

vodafone

Silver Sponsors

BAE SYSTEMS

VERISIGN

UNISYS

CHERTOFF
GROUP

FT
FINANCIAL
TIMES

MEDIA PARTNER

NEW EUROPE

RESOURCE PARTNER

TeleGeography

Institute for Security
& Resilience Studies
University College London

IN PARTNERSHIP WITH

DSCI
PROMOTING DATA PROTECTION

intellect
REPRESENTING THE UK TECHNOLOGY INDUSTRY

NASSCOM®

UK Investment Banking
Information Security SIG

EastWest Institute
Forging Collective Action for a Safer and Better World

30 YEARS

Founded in 1980, the EastWest Institute is a global, action-oriented, think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe, and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) non-profit organization with offices in New York, Brussels and Moscow. Our fiercely-guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
Belgium
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka Street
7/5, Building 1, 6th Floor
Moscow, 125009
Russia, +7-495-2347797

EWI New York Center
11 East 26th Street
20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100

www.ewi.info