Security Operations Centre: Situation Awareness, Threat Intelligence and Cybercrime

Dr Cyril Onwubiko
Chair, Cyber Security Intelligence, Research Series, London, UK

Abstract

There have been longitudinal advances in both cybersecurity and cyber-threats in recent years. With cybersecurity, for instance, there are now mechanisms to geographically locate an entity; there are those that can intercept most forms of electronic communications, and those that can recover most types of hidden images and data in electronic devices. The pace of change and advancements has equally been astronomical and astonishing. Technology refresh cycles have been slashed, and are now estimated to between 12 to 18 months, while the number of cyber users or entities has quadrupled in the last five years. These continuous changes have left an ever increasing gap between cybersecurity, that is, control mechanisms (a.k.a. safeguards) that help protect, detect, respond and recover organisational or national cyber investment, and cyber-threats, that is, threats that aim to exploit, breach or circumvent the cyber controls. This gap between cybersecurity on one hand and cyber-threats on the other hand appears to widen even further in areas with far greater financial rewards for the criminals, or nation state political gains. Exploits are now common and frequent, and impacts far much greater than before. This situation is further exacerbated by the lack of adequate and well deployed security operations centres to monitor organizational cyber investments.

In this research cyber security operations centre deployment models are proposed to provide better and enhanced situational awareness in order to detect common and frequent exploits, and also sophisticated and cross-channel exploits.

Keyword: Cyber SA, CyberOps, Intelligence, Cybercrime, Situational Awareness, Cross-Channel Exploits (CCE)

Biography

Dr Onwubiko is Director, Cyber Security Intelligence, at Research Series Limited where he is responsible for directing strategy, IA governance and cyber security. Prior to Research Series, he had worked in the Financial Services, Telecommunication, Health, Government and Public services Sectors. He is a leading expert in Cyber Situational Awareness, and experienced in Cyber Security, Security Information and Event Management, Data Fusion, Intrusion Detection Systems and Computer Network Security; and vastly knowledgeable in Information Assurance, Risk Assessment & Management. He holds a PhD in Computer Network Security from Kingston University, London, UK; MSc in Internet Engineering, from University of East London, London, UK, and BSc, first class honours, in Computer Science & Mathematics. He has authored several books including "Security Framework for Attack Detection in Computer Networks" and "Concepts in Numerical Methods.", and edited books such as "Situational Awareness in Computer Network Defense: Principles, Methods & Applications", and Cyber Science 2015 – International Conference on Cyber Situational Awareness, Data Analytics and Assessment. He has over 30 articles published in leading and most prestigious academic journals and conferences.

Reference

[1] Onwubiko, C. (2016). Understanding Cyber Situation Awareness. *International Journal on Cyber Situational Awareness, Vol. 1, No. 1, pp11-30*, *DOI:* **10.22619/IJCSA.2016.100101**

Incorporating Situation Awareness into Workflow Models for Security Incident Response

Dr Andrew Lenaghan
Computer Security Specialist, Oxford University Computer Emergency Response Team (OxCERT), Oxford, UK

Abstract

Investigating and resolving information security incidents is a complex task. The nature of the threat constantly changes; and indicators of compromise can arrive spread over time, from multiple sources. There is time pressure to act, to protect users and assets, yet evidence can be incomplete and may contain both uncertainties and contradictions. Members of Incident Response Teams (IRT) must build and maintain their situational awareness as multiple incidents play out. To help in managing security incidents, standardised models have been proposed, for processes or workflows, to be adopted. These models capture the phases and activities for detecting, assessing and responding to threats.

We examine how these models can be extended to incorporate ideas about situational awareness; how it develops and how it breaks down, in individuals and in teams. We look at whether systemic weaknesses such as the risk of information overload or miscommunication can be identified; and if changes to workflows can lead to a more resilient incident management approach.

Keyword: SOC, CERT, OxCERT, Situational Awareness, Threat Intelligence, Incident Response Team (IRT)

Biography

Dr Andrew Lenaghan is a Computer Security Specialist at Oxford University. He is a member of the Computer Emergency Response Team (CERT) responsible for protecting the University's network infrastructure, and users, from attack. Prior to this, he was a Senior Security Consultant and Information Security Officer in the finance sector for 8 years, advising firms in the UK, Europe and the US. He has been a regular speaker and chair of the Electronic Money Association's Fraud and IT Security subcommittee; highlighting emerging fraud and IT security issues. As an academic at Kingston University, he was a Principal Lecturer in Data Communications and a founding member of the Networking and Communication research group. Andrew holds a degree in Computer Science, an MSc Human-Computer Interaction and has a doctorate in computer vision and pattern recognition

Searchable Encryption in the Modern Era

Professor Kevin Curran
School of Computing & Intelligent Systems, Ulster University, UK

Abstract

"Can we have perfect privacy in the Cloud?"
The concept of Cloud computing is now an accepted philosophy for computing. Cloud computing is a kind of grid computing and has evolved by addressing the quality of service and reliability problems. The benefits of Cloud computing are significant: reduced costs, high reliability, as well as the immediate availability of additional computing resources as and when needed. Despite such advantages, Cloud Service Provider (CSP) consumers need to be aware that the Clouds poses its own set of unique risks that are not typically associated with storing and processing one's own data internally using privately owned infrastructure. Perhaps the most severe risk facing CSP consumers at present is the threat of data disclosure or data loss. Recent years have seen several such incidents occur, whereby customer data hosted on the Cloud has been compromised. Despite being a relatively obscure form of Cryptography, Searchable Encryption is now at the point that it can be deployed and used within the Cloud to store data in encrypted form, while retaining the ability to search that data without disclosing the associated decryption key(s) to CSPs. This talk will outline this new paradigm for a Cloud centric world.

Keywords: Security Implications, Cloud Security, Data Privacy, FHE

Biography

Kevin Curran is a Professor of Cyber Security at Ulster University and group leader for the Ambient Intelligence & Virtual Worlds Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr Curran has made significant contributions to advancing the knowledge and understanding of computer networking and security, evidenced by over 800 published works. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to print, online, radio & TV news on computing & security issues. He was the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Public Visibility technical expert since 2008. He currently holds a Royal Academy of Engineering/Leverhulme Trust Senior Research Fellowship awarded in 2016. Prof. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He was the founding Editor in Chief of the International Journal of Ambient Computing and Intelligence and is also a member of numerous Journal Editorial boards and international conference organising committees. He has authored a number of books and is the recipient of various patents.

Protecting Critical National Infrastructures – A Case Study & Lessons Learned of the Norwegian Water Resources and Energy Directorate (NVE)

Dr Janne Hagen
Norwegian Water Resources and Energy Directorate (NVE), Norway

Abstract

The hydropower system supplies the vast majority Norwegians with electricity. Electricity supply is one of the most critical resources in a modern digitized society like Norway. Digitalization of the electricity infrastructure exposes however the infrastructure for cyber threats. The presentation gives a brief overview of how Norway handles the cyber risks that follows with digitalization of critical infrastructure like electric hydropower supply. The presentation draws attention towards how regulation and audits enforce a minimum-security level, and how awareness and knowledge-building activities towards the industry add value to security.

Keyword: National Critical Infrastructure, Norwegian Government, Electricity, Cyber security, Cyber-threats, Norway

Biography

Dr Hagen, from April 2016 is employed as Head Engineer at the Norwegian Water Resources and Energy Directorate (NVE), working on cybersecurity in the Energy Sector in Norway. She has previously worked as a Researcher and Consultant, most of the time employed at the Norwegian Defence Research Establishment (FFI) conducting research on societal security and protection of critical infrastructures. Since 2005, her scientific work focused primarily on cybersecurity, and the vulnerability of the digital society, lately with focus on the Energy Sector. She has been member of several expert groups in Norway, including the Norwegian Governmental Committee of Digital Vulnerabilities in Society that delivered an Official Norwegian Report (NOU) to the Ministry of Justice and Public Security in November 2015.

Game Theory Meets Security Risk Assessment - Overview and Current Developments

Dr Eckhard Pfluegel
Faculty of Science, Engineering & Computing, Kingston University, London, UK

Abstract

Security assessment is a crucial activity within the broader security management cycle, nowadays adopted by many organisations to analyse threats, assess vulnerabilities and respond to risk with appropriate security measures. Game theory models scenarios where participants have competing interests. It provides a way of predicting consequences if several people are making decisions at the same time, and if the outcome depends on the decisions of the others. Recently, applications of game theory to security - so-called security games - have been studied, analysing attacker-defender security scenarios using game theory, under the assumption that both attacker and defender are rational entities. In this talk, we will explain how game theory can be used to improve security assessment. We will start with reviewing and clarifying fundamental security terminology. We will present the basic approach of security assessment and discuss the most common methodologies and frameworks. We then focus on risk analysis and motivate how game theory can help with obtaining a better modelling of the overall security risk. Several important game-theoretic concepts will be introduced and the audience will understand how an equilibrium analysis of the security game can be used for the likelihood assessment of potential attacks. This yields a quantitative alternative to traditional, qualitative approaches for risk assessment.

Keyword: Game Theory, Security Risk Assessment, Cyber Situational Awareness

Biography

Dr Pfluegel obtained a Ph.D. in Computer Science at Université Joseph Fourier, Grenoble (France) in 1999 after graduating with a First Class degree ("Diplom") in Computer Science (Equivalent of UK Honours and Master's degree) in 1999 at Universität Karlsruhe (now known as KIT), Karlsruhe (Germany). An experienced Senior Lecturer with 3 years of industrial practice in software engineering and over 13 years of research expertise, teaching responsibilities and professional practice, his current main area of specialism is network and cyber security. He has an active and continuous portfolio of over 40 peer-reviewed international journal and conference publications, serves as member of several technical programme committees and regularly reviews for international journals. Dr Pfluegel is leading an educational programme in cyber and network security at postgraduate level and frequently gives public lectures and talks on the topic of cyber and computer security awareness. He particularly enjoys research-informed teaching in order to bring in cutting-edge knowledge from his research into his lectures.

Application of Cyber Situational Awareness and Cyber Security in Vehicular Networks

Dr Mahmoud Hashem Eiza
School of Physical Sciences and Computing, University of Central Lancashire, Preston, UK

Abstract

"Are you driving a smart connected car? If it has a software, it is hackable; and if it is connected, it is exposed." In an era where cars are no longer isolated mechanical machines that are solely used for transportation, a new cyber security challenge is born. With the introduction of telematics, vehicular communications, and the integration of smartphones and Bluetooth devices, connected vehicles represent an ecosystem that is part of a fully connected world. In fact, connected vehicles are an integral part of the smart city vision and a node in the world of Internet of Things. However, while brining many improvements in terms of functionality and convenience, connected vehicles become a new target for hackers. Recently, there are numerous news about hacks/attacks against smart connected vehicles. Given the variety of connections a smart vehicle has with the outside world, penetration points are numerous. Where do we start the battle with hackers? Which systems should we protect first? And how? This talk aims to illuminate the latest reported attacks, their grounds, and the latest attempts to defend them. This will cover malware attacks, on-board diagnostic (OBD) vulnerabilities, and automobile apps threats with an illustration of the in-vehicle network architecture. Finally, it will show how the application of cyber situational awareness would improve the defending mechanisms against vehicle cyberattacks.

Keyword: Connected Car Security, Vehicle Cyber Security, Vehicle Cyberattacks, Cyber Situational Awareness

Biography

Dr Mahmoud Hashem Eiza is a Lecturer in Computing (Computer and Network Security) at the School of Physical Sciences and Computing, University of Central Lancashire (UCLan), Preston, U.K. He received the M.Sc. and Ph.D. degrees in electronic and computer engineering from Brunel University London, London, U.K., in 2010 and 2015, respectively. He is the co-founder of the Laboratory of Security and Forensic Research in Computing (SAFeR) at UCLan. His research interests include computer and network security, with specific interests in QoS and wireless network security and privacy in Vehicular Networks, Smart Grids, Cloud Computing, and Internet of Things. Throughout his roles, he has been significantly engaged in the preparation and writing of numerous research grant proposals including H2020 and InnovateUK. Mahmoud has published several papers in prestigious IEEE conferences and journals and has served on the committees of several IEEE conferences and workshops such as IEEE GLOBECOM and IEEE CCNC.