Journal of Information Warfare

Volume 15, Issue 3

Contents

Authors

Dr. Jim Q. Chen is professor of Systems Management and Cybersecurity in the iCollege at the U.S. National Defense University (NDU). His expertise is in cybersecurity technology and cybersecurity strategy. He is a recognized cybersecurity expert.

Tiago Cruz is an assistant professor in the Department of Informatics Engineering at the University of Coimbra. He also serves as a senior researcher at the Centre for Informatics and Systems of the UC. His research interests include management of communications infrastructures and services, critical infrastructure security, and network function virtualization.

J. S. Hurley is the course manager for Cyberspace Strategies and co-manager of the Critical Infrastructure Protection Laboratory at the National Defense University (NDU). He has also worked as senior manager of Distributed Computing at the Boeing Company, directed three research centers, and served as the co-director of the Army Center of Excellence. He is also a 2014-2015 Seminar XXI Fellow.

Dr. Andre Karamanian is a consulting solutions architect at Cisco Systems, where he consults for Fortune 500 and enterprise clients. He is the author of *PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks*. He periodically speaks at Networkers and Cisco Live. He completed his doctoral dissertation at Capitol College in information assurance and has earned a dozen industry certifications including the CCIE and CISSP. He enjoys finding synergies between different areas of research and fields of study.

Marc M. Kolenko is a solutions-oriented Cyber Defense and Information Systems Security Engineering Professional with more than 30 years of notable success directing a broad range of Enterprise IT initiatives in both the private sector and government. He is currently the Senior Cyber Security Solutions Architect and Strategist at Information Innovators, Inc. (Springfield, VA). He is responsible for delivering Computer Network Defense (CND), Continuous Monitoring, Security Operations, Cyber Threat Intelligence, Information Assurance (IA) & Compliance, and Systems Security Engineering solutions that aid clients with meeting federal government cybersecurity mandates (i.e., RMF/FISMA, FedRAMP, ICD 503, CNSS 1253, and the Comprehensive National Cyber Security Initiative) through technology.

Christine MacNulty, FRSA, is the CEO of Applied Futures, Inc., which specializes in strategy, strategic planning and change, and understanding cultures. For the last twenty years, she has been a consultant for the Department of Defense and NATO. She has also worked with many Fortune Global 500 companies. She is the co-author of two books and a speaker at many conferences.

Edmundo Monteiro is a full professor at the University of Coimbra, Portugal, where he earned a doctorate in Electrical Engineering in 1996 and the Habilitation in Informatics Engineering in 2007. His research interests include computer networks, wireless communications, quality of service and experience, service oriented infrastructures, and security. He is the author of more than 200 publications including books, journals, book chapters, and has presented at international conferences. He is also co-author of nine international patents. He participated in many

European initiatives and projects. He is an editorial board member of *Computer Communications* and *Computer Networks*, and is involved in the organization of national and international conferences and workshops. He regularly serves as a reviewer of Portuguese and European projects. He is the Portuguese representative in IFIP-TC6, and senior member of IEEE Communication Society, and ACM Special Interest Group on Communications.

Njabulo Mkhonto is a researcher and software developer for the Cyber Defense team at the Council for Scientific and Industrial Research (CSIR). He has an interest in the applications of Artificial Intelligence research and techniques in solving real-world problems. He studied at the University of Johannesburg where he completed his BSc and BSc Hons in Information Technology, focusing on the use of swarming technologies for improved image processing. Since joining the CSIR, his focus has been on cyber security, where he has been involved in research efforts involving cyber threat intelligence, mobile security, and network security.

Dr. Jabu Mtsweni is a Research Group Leader for the Cyber Defense team at the Council for Industrial and Scientific Research (CSIR). He has research interests and technical expertise in Internet of services, software and firmware reverse engineering, malware analysis, threat intelligence, web security and general cyber warfare. He has more than 13 years of academic and industry experience and has published more than 38 peer-reviewed conference and journal papers/articles in both local and international forums. He has also publicly presented and actively contributed at various technology forums over the years, including the ITWeb Security Summit, TEDx, the SADC Cybersecurity Conference, IST-Africa, the South African Institute for Computer Scientists, the International Conference on Cyber Warfare and Security, and the Information Technologists and International Information Security South Africa Conference. He is a co-organizer of Random Hacks of Kindness (Pretoria) and a member of the Suganang Foundation, focusing of human capital and capacity development in the ICT space.

Muyowa Mutemwa is a Cyber Security Researcher for the Cyber Defence team at the Council for Industrial and Scientific Research (CSIR). He has research interests in Platform, Application and Network Security. He completed his master's degree in computer science at the University of the Western Cape with a specific focus in Information Communication Technologies for rural developments. He previously worked for Telkom SA as a Data Centre, Network Strategy Architect.

Jorge Proença is a PhD student in Information Science and Technology at the University of Coimbra. He earned his M.Sc. degree from the same institution in 2012. Since 2012 he has been a junior researcher in the Centre for Informatics and Systems of the University of Coimbra (CISUC), where he participates in research projects in the fields of network virtualization, security, and critical infrastructure protection.

Rui Queiroz is an M.Sc. student in the Department of Informatics Engineering at the University of Coimbra. He also serves as a research student at the Centre for Informatics and Systems of the UC. His research interests include management of communications infrastructures and critical infrastructure security.

Daniel J Ryan is a lawyer in private practice, an author, and an educator teaching cyberlaw and information security as an adjunct professor at George Washington University. He previously served as a faculty member at the National Defense University.

Julie JCH Ryan, D.Sc., is a professor at the National Defense University, teaching in the areas of cyber security and information assurance. Her service in academia follows a career in the private sector and service as a U. S. government civilian and as a U. S. Air Force officer. She has published three books – *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*, *Leading Issues in Information Warfare and Security*, *Detecting and Combatting Malicious Email*.

Dr. Char Sample is currently a visiting research fellow at the University of Warwick and is employed as a research fellow for ICF International at the Army Research Labs in Maryland. She has more than 20 years of experience in the information security industry, including roles as a developer, integrator, architect, product designer, and researcher. Most recently she has been researching the role of national culture in cyber security events. Presently she is continuing research on modelling cyber behaviours by culture, metrics, risk quantification, and modelling of other security issues.

Paulo Simões is a tenured assistant professor in the Department of Informatics Engineering at the University of Coimbra, Portugal, where he earned his doctorate in 2002. He regularly collaborates with Instituto Pedro Nunes as a senior consultant, leading technology transfer projects for industry partners such as telecommunications operators and energy utilities. His research interests include Future Internet, network and infrastructure management, security, critical infrastructure protection and virtualization of networking, and computing resources. He has more than 150 publications in refereed journals and conferences and is a member of the IEEE Communications Society.

Lanier Watkins is currently a Senior Professional Staff II member of the Asymmetric Operations Sector of the Johns Hopkins University Applied Physics Laboratory (JHU/APL) and an Associate Research Scientist at the JHU Information Security Institute. Prior to joining APL, he served as a senior engineer and product manager at the Ford Motor Company and AT&T.

Murdoch Watney is a professor in the Department of Public Law and head of the Private Law Department at the University of Johannesburg, South Africa. She holds the degrees BA, LLB, LLM (RAU), LLM (UNISA) and LLD. She previously worked as a prosecutor and is an admitted advocate of the High Court of South Africa. She has contributed to three textbooks and has published extensively in law journals – both nationally and internationally – on the law of criminal procedure, criminal law, law of evidence, and cyber law. Most of her research focuses on cyber law. She has delivered peer-reviewed papers at national and international conferences.

Shuang Xie is a software engineer at Alpine Electronics Research of America, Inc. He earned a bachelor's degree in Security Informatics from the Shanghai Jiao Tong University, Shanghai, China, in 2012, and a master's degree in Security Informatics from the Johns Hopkins University, Baltimore, Maryland, in 2014.

Tianning Yang is a security engineer at Nav Technologies, designing security schemes and protecting confidential data related to credit reports and personally identifiable information. She earned her bachelor's degree in Information Security and an LLB in Law from Nankai University in 2012, and a master's degree in Security Informatics from Johns Hopkins University in 2014.

Enhancing Cybersecurity by Defeating the Attack Lifecycle: Using Mobile Device Resource Usage Patterns to Detect Unauthentic Mobile Applications

LA Watkins[1], JS Hurley[2], S Xie[1], and T Yang[1]

[1]*Information Security Institute*
Johns Hopkins University, U.S.A.
E-mail: lanier.watkins@jhuapl.edu; super0xie@gmail.com; maria.tinayang5@gmail.com

[2]*Information Resource Management College*
National Defense University, U.S.A.
E-mail: john.hurley@ndu.edu

Abstract**:** *Attacks are usually orchestrated based upon the motivation of the attackers, who are becoming increasingly savvy, better resourced, and more committed. This article examines cyber threats and vulnerabilities through the eyes of the perpetrator. To begin, the authors discuss some counter approaches that have produced limited benefits at best, and then introduce a novel approach that details the use of mobile device resource usage to discern unauthentic mobile applications from authentic applications. This capability is indeed a step in the right direction to addressing the problem of intrusion detection in mobile devices without using traditional signatures or rule-based approaches.*

Keywords: *Cybersecurity, Attack Lifecycle, Information Assets, Deterrence, Intrusion Detection, Intrusion Prevention*

Introduction

It is advantageous to examine cyber threats and vulnerabilities through the eyes of the attackers, for this view can often provide perspective on the goals and targets of the perpetrators. As techniques have gotten markedly better at addressing some of the attack points within given environments, so have the techniques of those who seek to attack those environments. As such, many have started to rely more on security firms to protect their 'valuables'; and though the firms have gotten much better at 'qualifying' their capabilities, the misperception that they can indeed protect and defend against all attacks on information assets still exists. The perpetrators, increasingly becoming savvier, have significantly upped their game, as seen recently, and have decided to now target the security firms that organisations hire to protect their information assets. Security firms, for instance Lifelock (Federal Trade Commission 2010) and RSA (2011), have come under siege by attempts to access the information assets of their clients. In many cases, the 'keys to the castle' held by the security firms provide greater access to huge assets of some companies, including some of the major Fortune 500 companies—a great incentive to attackers seeking financial gain. The critical decisions that enable organisations such as the Fortune 500 companies to better protect and utilize their information assets to meet mission and organisation priorities come with a lot of risk (both short- and long-term). In this current Information Age,

senior leaders are reluctant to pursue bold strategies largely because the potential repercussions of bad decisions can have severe consequences (especially to the careers of the senior leaders). As a result, unfortunately, these leaders tend to be more reactive than pro-active because guarantees are few and far between. In cyberspace, it is very possible that attacks can go undetected and lead to the incorrect conclusion that environments are safe, secure, and protected. In reality, environments can be largely infected through vulnerabilities that have been stealthfully identified and utilized by attackers.

This study proceeds under the assumption that senior leaders defer to the status quo on cyber investments largely because of a lack of data to drive their decision making. Many of the decisions are driven by experience, intuition, and 'gut feelings', which are indeed valuable assets that surely have their place and should not be discredited. However, cyberattacks provide an entirely different dimension in terms of the speed in which attacks can occur, as well as the attribution to which they can be assigned. Hence, the collection and analysis of relevant data is selected as one of the few viable options available to senior leaders to provide more assurance about their cyber investments to better protect their organisations' information assets. This article begins with a more in-depth look at the economy and drivers that will remain major motivations, simply because of their potential payoffs. Even though an organisation may launch a series of attacks in which only very few are successful, the payoff for the few that work can be enormous.

Economy

The days in which the United States or any other country can operate in isolation are long gone. Countries are inextricably woven together through a tapestry that reflects a global economy that has redefined relationships around the world in ways that are dramatically different from those of just a decade ago. Within the United States, the economy sets its imprint on national security through three overlapping roles. First, the economy can serve as a source of funds, materiel, and personnel for the military. Second, the economy can serve as a provider of economic security and well-being for American citizens. Lastly, the economy can serve as the foundation for interaction with other countries and of building shared or competing interests. In particular, the spread of wealth can be generated by trade that allows countries to build their military and financial power, for instance, the steady flow of oil revenues into the Middle East and the large trade surplus by China. The economy can also enter into national security considerations in other ways, including economic sanctions, export controls, economic incentives, and expeditionary economics (Nanto 2011). The increasing data and analytics challenges facilitated by the markets are driven largely by the diverse and immense amounts of data that must be analysed. Relational technologies coupled with business intelligence tools have been the dominant instruments used by financial institutions to resolve some of the data and analytics challenges (*Financial services data management: big data technology in financial services* 2012). Top-tier global banks face the constant need to secure a 'horizontal view' of risk within their trading arms in response to new regulations. To facilitate this view, banks need to integrate data from different trade capture systems, each with its own data schema, into a central repository. It is not uncommon for traditional Extract, Transform, and Load (ETL)-based approaches to take several days. However, pressure from regulators requires that the entire process be done several times per day.

In addition, the simulations required for the different risk scenarios can generate terabytes of additional data each day. The challenges include the sheer volumes of data, variety of data, and the timeliness in which such varied data needs to be aggregated and analysed. Analysts estimate

that nearly 80-90% of the data that financial institutions possess is unstructured, for example, in the form of texts and documents (*Financial services data management* 2012). An enormous opportunity for improving business insight for financial institutions exists when such unstructured data can be enjoined with the structured content.

In addition, the Internet is considered to be the dominant and most decisive technology of the Information Age (Castells 2014). The Internet has moved economic concerns to the forefront because of how it has so connected the different segments of society. Also, the Internet has readily provided near real-time availability and access through mobile devices to financial institutions and markets in a way that is only now truly being appreciated. A better understanding of the impact of the mobile devices on e-commerce is emerging. The following section examines how access to information is driving government policies and modes of engagement with citizens and others.

Openness and Transparency

Openness and transparency of government pre-date the Internet. In efforts to provide efficient services, make policy, and be held accountable to their constituents, governments rely very heavily on the data that is produced, collected, and analysed (Heeks 1999). The efficient management of this information is essential to effective governance—a hallmark to a true democracy (Gant & Turner-Lee 2011). When the Internet revolution arrived in the 1990s, the U.S. government foresaw the important need to facilitate an anticipated shift in how people would consume and deliver information and services. The ongoing rise of mobile technologies and reduced cost of the devices have increased the citizens' demand for digital capabilities and services, with even greater demand expected in the future. Government agencies are increasingly exploring how new and emergent technologies such as social media, mobile apps, and data-access and data-visualization platforms can help improve their internal operations as well as the way information is exchanged with their own citizens and others abroad. In spite of the progress and efficiency that can result from services that can be delivered by electronic government (e-government), many challenges and complexities can exist that seriously limit the effectiveness of those services. The main challenge that e-government faces is that it is still largely perceived solely as a technological innovation, a tool, rather than a platform by which better government can be administered. Functioning democracies and market economies require openness and transparency to build accountability and trust (Gurria 2016). Security can play an important role in terms of how organisations can better position themselves against cyber-attacks and better protect their information assets.

Security

An Intrinsically Secure Architecture (ISA) is needed to better protect the information assets of organisations. An ISA refers to an IT architecture that establishes, provides, and maintains IT infrastructure and/or systems that ensure a state of inviolability from hostile acts or influences from both external and internal sources throughout all infrastructure and systems (Harrison 2016). Some of the current major challenges reflect the difficulties of maintaining architectures that are in sync with evolving systems. These systems enable new opportunities and platforms for sharing information, as well as operating in environments in which traditional security boundaries and pathways become increasingly blurred. These traditional security systems (including firewalls, intrusion detection systems [IDS]/intrusion prevention systems [IPS], and anti-virus software) are

not evolving quickly enough to keep pace with the evolving devices and other systems to adequately secure information sharing. For example, the use of non-signature-based attacks; standard Operating Systems (OS) and application ports for new attack vectors (such as SSL, SSH, and previously unknown functions system ports); and software built on secure-enabling patterns are increasingly gaining recognition as hallmarks of attacker strategies.

Security must be viewed in practical terms: specifically, perfect security is infinitely expensive. Hence, organisations, governments, and other entities must be practical in terms of understanding how cost constraints delineate between acceptable risk and desired performance. Recent FBI cyber threat reports have noted that

- The ratio of insider to outsider threats is changing;
- Over the last four years, the ratio was 80:20 (insider: outsider);
- The current ratio of attack is 18:73 (insider: outsider);
- 39% of data breaches implicate business partners;
- Insider data breaches have had a larger impact than previously reported;
- 59% of data breaches result from hacking and intrusions;
- Approximately 80% of attacks are opportunistic and not highly difficult;
- 87% of the attacks are considered to be avoidable with reasonable controls;
- 13% of the attacks use sophisticated technology and approaches. (Federal Bureau of Investigation 2016)

For law enforcement, data plays a very important role in terms of providing more effective and efficient investigations, responses, predictions, and detection and mitigation of criminal activities. The influence and relevance of data is also playing a very important role due to the fact that a number of law enforcement agencies are undergoing significant budget cuts. As Brewster *et al.* (2015) have noted, in some cases, almost 80% of police budgets are dedicated to personnel staffing. Hence, reductions that have hit staffing requirements have caused a number of different police forces to turn to data analytical tools to compensate for the loss of manpower. In addition, traditional crimes, often classified as 'physical', which include human trafficking among others, provide an opportunity to use data from open sources to identify factors that can be used in the detection of illicit activity. Lastly, the use of social media and other data media can enhance the situational awareness and decision-making capability of law enforcement to better address crimes even at their onset.

Though there are many models that discuss an attack ecosystem, the model in **Figure 1**, below, serves as the basis for the current discussion (Gilliland 2015). It represents the six distinct phases of the attack ecosystem: research, infiltration, discovery, capture, exfiltration, and the end game.

To counter adversaries, prevention and blocking techniques (for example, antivirus) and policy-based controls (for example, firewalls) have been the dominant 'tools' in their efforts (MacDonald & Firstbrook 2014). Unfortunately, traditional solutions such as these, however, have proven largely inadequate to handle the diverse and advanced attack mechanisms used by the perpetrators (MacDonald 2013).

Figure 1: Disrupting the attack life cycle

Organisations, in general, are overspending in the Infiltration Phase to block and prevent attackers (Gilliland 2015). However, given the inability to create and implement a perfect, impenetrable, 100%-effective defence solution against attackers, the distribution of how and where efforts and resources invested should be re-examined as follows:

1. Focus on security intelligence—be smart about finding the adversary after it penetrates an environment, but before data is stolen;
2. Disrupt the Capture Phase by placing data protections as close to the data as possible using encryption technologies and information protection mechanisms;
3. Do not focus on 1 or 2 phases of the Attack Ecosystem;
4. Use a defense-in-depth approach, which is better suited for the task;
5. Invest in capabilities at every step of the life cycle; and,
6. Manage the data with security in mind from the very beginning.

Leap-ahead Technology

The complexities that surround the different options for cyberattacks on different environments create within themselves complications that actually exacerbate the challenges. In Watkins and Hurley (2016), a novel Next-Generation Security Framework (NGenSeF) is proposed that aligns with the Obama administration's Comprehensive National Cybersecurity Initiative (CNCI), specifically the call for 'leap-ahead' technology, intrusion-detection and intrusion-prevention systems. The proposed framework is composed of novel modifications to traditional technologies: (1) inference-based intrusion detection—network-based systems that infer active process activity executing on end-point devices, (2) intrusion prevention systems—Software Defined Networking (SDN)-based infrastructure that uses threat intelligence sourced from the

previously mentioned inference-based system to wage an automated offensive campaign against cyber threats. This paper focuses next on the mobile device aspect of NGenSeF.

Intrusion Detection Systems

The new attack surfaces are mobile device networks and Industrial Control Systems (ICS), but this paper focuses specifically on mobile devices. The traditional security approach for enterprise Information Technology (IT) systems is defence-in-depth and thus has also become the standard for mobile devices; however, defence-in-depth is losing the battle against APT. One of the main reasons for this is the reliance on signature- and rule-based detection for traditional anti-virus protection and intrusion detection. APT remains untamed by traditional security measures for at least the following two reasons: APT has been known (1) to subvert signature- and rule-based host intrusion detectors such as anti-virus software (Virvilis & Gritzalis 2013), and (2) to evade signature- and rule-based network intrusion detectors by obfuscating or encrypting network traffic. The NGenSeF proposed by Watkins and Hurley (2016) fills in the gaps that exist within the defence-in-depth framework and provides an extra layer of protection against APT. In that article, Watkins and Hurley discuss how their work correlates network traffic and the internal state of hardware for mobile (that is, CPU speed and system input/output) and SCADA devices. The authors propose a security framework which uses a correlation between network traffic and mobile- and SCADA-device resource usage. This concept could lead to intrusion-detection systems that are capable of accurately and remotely inferring the hardware state of devices to identify when the distinct phases of the attack ecosystem are in play, and thus detect APT without the use of signatures or rules. This approach should be viewed very favourably since the impact of signatures or rules to impact APTs have been, at best, limiting. **Table 1**, below, represents this point in that this proposed form of intrusion detection essentially correlates the APT attack lifecycle with the complex state of mobile device CPU speed through network traffic. One of the contributions of the current paper worth noting is that results confirm the feasibility of an inference-based intrusion-detection system for mobile devices.

APT Attack Lifecycle	APT Activity On Device	Android CPU Speed
Infiltration Phase	External processes utilize resources	Hi to Low
Discovery Phase	Network scanning	Low
Capture Phase	File system traversal and network propagation	Hi to Low
Exfiltration Phase	File system traversal and transformed network traffic is sent	Low
End Game Phase	Transformed network traffic is sent	Hi to Low

Table 1: Translating APT attack lifecycle into mobile device resource usage

Case Study: Inference-based Resource Usage in Mobile Devices

In this example, the experimental setup in **Figure 2**, below, is used to (1) execute an authentic application on an HTC mobile device running an Android operating system, (2) ping the mobile device at a rate of 10 ms and capture the network traffic from the monitoring laptop, (3) execute an unauthentic version of the same application (specifically, Talking Tom Trojan), (4) repeat step 2 for the mobile device executing the unauthentic version of the same application, and (5) train the random forest tree machine learning algorithm running on the monitoring laptop to discern the authentic application from the unauthentic application using only the captured network traffic.

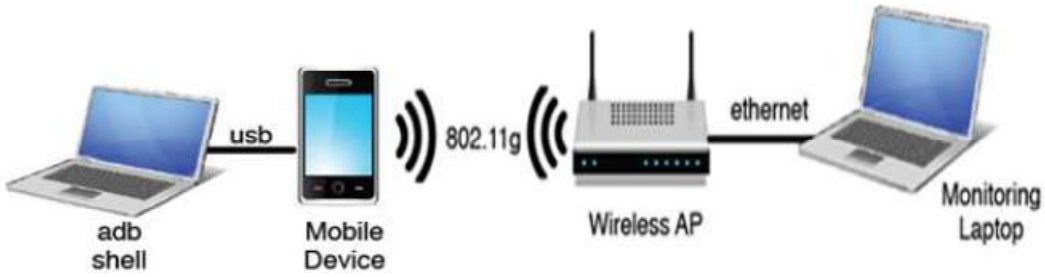
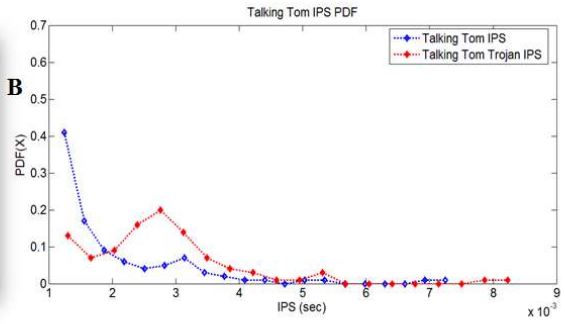


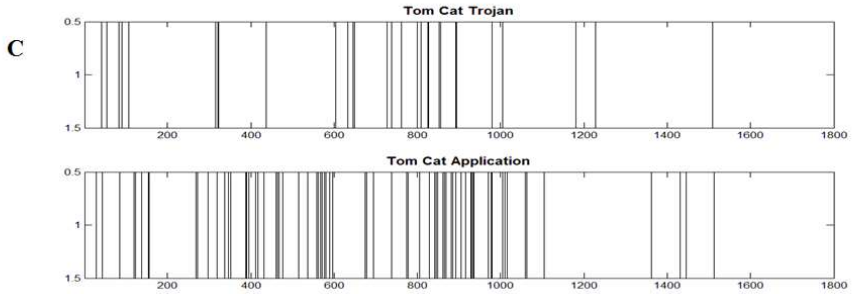
Figure 2: Experimental setup for mobile device resource usage inference example

Specifically, the Open System Interconnect (OSI) Layer 1 inter-packet spacing of the ICMP responses is used. The authentic Talking Tom application from Google Play and the unauthentic Talking Tom application from a third-party repository as verified by VirusShare are also used. **Figures 3A-3C**, below, illustrate statistical data for CPU and memory bound instructions, CPU speed and memory usage, inter-packet spacing of ICMP responses, and location of CPU bound instructions as compared to all other instructions.

A

	Talking Tom	Talking Tom Trojan
# of Executed CPU Bound Instructions	138	51
# of Executed Memory Bound Instructions	1151	1024
Average CPU Speed	935 MHz	442 MHz
Average Memory Usage	160 MB	132 MB





Figures 3A, 3B, 3C: Statistical analysis of (A) CPU and memory bound instructions, CPU speed and memory usage, (B) inter-packet spacing of ICMP responses, and (C) location of CPU bound instructions as compared to all other instructions

Table 2, below, illustrates the definition of CPU and memory-bound instructions. The CPU speed and memory utilization are measured while the mobile device is executing Talking Tom and then the unauthentic Talking Tom application.

CPU Bound	add,sub,mul,div,rem,and,or,shl,shr,cmp,if,not,neg, int-to,long-to,float-to,double-to
Memory Bound	move,return,const,aget,aput,array,iget,iput,sget,sput, instance
Other	goto,monitor,throw,invoke,execute

Table 2: Grouping of Dalvik virtual machine instructions

To get the number of executed instructions in **Figure 3A**, above, each application is decompiled using 'smali'; the command 'adb' shell 'dumpsys' is used to identify all Dalvik subroutines that are executed; and the Dalvik subroutines that lead to the instructions that are executed are manually traced. Finally, a Java program is used to group the instructions into CPU bound, memory bound, and other categories and to count the number of instructions per group. The graph in **Figure 3B**, above, was developed by calculating the Probability Distribution Function (PDF) for the inter-packet spacing values that came from the ICMP responses for both the authentic and unauthentic Talking Tom application. The DNA-type graph in **Figure 3C**, above, was developed by visualizing the locations of the CPU bound instructions (which appear as vertical lines) relative to all other instructions (which appear simply as spaces).

Per **Figures 3A** and **3B**, above, there is a correlation between CPU speed (specifically, mobile device resource usage) and average inter-packet spacing and possibly a correlation between the number of CPU-bound instructions and CPU speed. The probability distribution function in **Figure 3B**, above, illustrates that the CPU speeds required by the authentic application are much larger than for the unauthentic application. This point is explicitly stated in **Figure 3A**, above, which makes sense because it is conceivable that the unauthentic application has less game functionality than the authentic application since its main focus is not really game play. **Figure 3C**, above, illustrates that the CPU bound instructions for the authentic application (that is, 14 instructions apart) are on average closer together than those for the unauthentic application (32 instructions apart). This may also support the theory that the unauthentic application has less game play functionality than the authentic application (which is confirmed by actually playing both games). The IPS distributions in **Figure 3B**, above, are the result of the applications containing Dalvik instructions that throttle-up the CPU speed high in the unauthentic Talking Tom application, and even higher for the authentic Talking Tom application. As a result of these empirical truths, machine-learning tools can be trained using features from the raw baseline data to identify irregular application usage patterns (specifically, unauthentic applications).

In the confusion matrix in **Table 3**, below, the majority of the patterns are assigned to the right classes (True Negatives=26 of 30, and True Positives=23 of 30). It is assumed that the random forest tree machine-learning algorithm can properly discern the unauthentic application from the authentic application (the certainty percentage is 76%). Thus all correlations resulting from the analysis of this experiment should hold. This is a detailed example of how mobile device resource usage can be used to remotely infer application activity on the mobile device.

		Predicted Class	
		TomCat	TomCat Trojan
Actual Class	TomCat	26	4
	TomCat Trojan	7	23

Table 3: Confusion matrix which demonstrates the ability to discern between the Tom Cat application Trojan and non-Trojan for the HTC

Once NGenSeF (through the mobile device intrusion detection technology noted above) has determined that the mobile device is executing an unauthorized application, a Software Defined Networking (SDN) framework that monitors the enterprise network could be engaged to turn off the ports on the access point of the compromised mobile device. A direct result of this action is the elimination of the potential imminent threat posed by the unauthorized software.

Summary and Conclusion

Banks are targeted for the lucrative payoffs they can potentially make available. As with most other industries, however, they must also adjust their best practices to better protect themselves against cyberattacks. Financial institutions need to integrate data from different trade capture systems into a central repository. There is still also the issue of the sheer volume and variety of data that must be addressed.

Openness and transparency are hallmarks of a true democratic society that pre-dates the Internet. However, the transition from Web 1.0 (which represents the first stage in the World Wide Web constructed with the use of a set of static websites that were not yet providing interactive content) to the current version of the Web x.0 demonstrates how a one-way conversation has now blossomed into a collaborative environment that enables communication, interaction, and engagement between people, communities, and governments. The rise of mobile technologies has been a huge game-changer in that it has pushed the demand of digital capabilities and services to unexpected boundaries by the various user communities. The explosion of data is expected to also continue as governments continue to explore new platforms for data exchanging with the public, as well as in internal operations. However, there is the continued need to balance access and security.

It is very difficult to maintain intrinsically secure architectures in sync with the evolving systems, platforms, and applications because of how quickly things can change. Though the systems provide new opportunities for sharing information, traditional security solutions fall very short in terms of meeting the necessary demands. Organisations get a quick reality check when they seek to attain the most ‘secure’ systems because costs can be prohibitive. The cost constraints, when linked to the level of acceptable risk and desired performance, lead organisations to be more practical in terms of establishing where they must prioritize. One can see from the view of the Attack ecosystem or lifecycle as identified for this study and the recent statistics from the FBI that the ecosystem must be re-examined in order for cybersecurity to be improved. Statistics show that most of the resources are assigned to the blocking phase of the attack lifecycle, leaving very

little elsewhere to address the attackers that are likely getting in (or are already in) these environments.

Most of the security methods to this point have been dominated by defensive operations. In concert with the proposed new guidance from the executive branch, the authors have considered a more aggressive approach to better protect information assets. The technology detailed in the case study represents a specific capability of the Next-Generation Security Framework. For the Next-Generation Security Framework to be viable, it must solve some of the major issues facing a National Cyber Deterrence model, namely (1) attribution and (2) acceptable responses to cyberattacks. The model as constructed in theory could be used to respond to unauthorized applications executing on mobile devices, which in most cases are the precursors to cyberattacks; however, attribution is still an open question since any such solution will likely not be automated and will keep humans in the loop. The promise of NGenSeF is to detect and respond to unauthorized software and likely APT.

Within the context of this discussion, the authors have highlighted the decision-making requirements that are needed for senior leaders to be more comfortable with the ability to verify and validate solutions through the data. In addition, the authors have offered additional details to NGenSeF as a capability to launch offensive operations against the early stages of APT. This offensive approach to security may be a step in the right direction and an initial start toward an effective tactic to be used against APT.

References

Brewster, B, Kemp, B, Galehbakhtiari, S & Akhgar, B 2015. 'Cybercrime: attack motivations and implications for big data and national security', *Application of big data for national security: a practioner's guide to emerging technologies*, eds. B Akhgar, H Saathoff, R Rabnia, A Hill, A Staniforth & P Bayerl, Elsevier, Waltham, MA, U.S.A., pp. 108-13.

Castells, M 2014, *The impact of the Internet on society: a global perspective*, 8 September, Technology Review, <http://www.technologyreview.com/view/530566/the-impact-of-the-internet-on-society-a-global-perspective/>.

Federal Bureau of Investigation 2016, *Law enforcement cyber incident reporting*, 14 January, https://www.fbi.gov: https://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting>.

Federal Trade Commission 2010, *Lifelock to settle charges by the FTC and 35 states,* 9 March, <https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states>.

Financial services data management: big data technology in financial services 2012, Oracle, Redwood City, CA, U.S.A.

Gant, J & Turner-Lee, N 2011. 'Open government and transparency in the broadband age'*, Government transparency: six strategies for more open and participatory government* Aspen Institute, Washington, DC, U.S.A.

Gilliland, A 2015, *Outthinking the bad guys*, 6 February, viewed 6 February 2015, <https://www.brighttalk.com/webcast/1903/144605>.

Google Play 2015, <https://play.google.com/store/apps>.

Greenberg, A 2013, *Founder of stealthy security firm endgame to lawmakers: let U.S. companies "hack back",* 9 September, <http://www.forbes.com/sites/andygreenberg/2013/09/20/founder-of-stealthy-security-firm-endgame-to-lawmakers-let-u-s-companies-hack-back/>.

Gurria, A 2016, *Accueil de l'OCDE*, January, Openness and Transparency: Pillars for Democracy, Trust, and Progress, <http://www.oecd.org/fr/etatsunis/opennessandtransparency-pillarsfordemocracytrustandprogress.htm>.

Harrison, V 2016. *Cyber threats and vulnerabilities: a case for standards,* OMG, Needham Heights, MA, U.S.A.

Heeks, R 1999. *Re-inventing government in the information age: international practice in IT-enabled public sector reform*, Routledge, London, UK.

MacDonald, N 2013. *Prevention is futile in 2020: protect information via pervasive monitoring and collective intelligence,* Gartner, Stamford, CT, U.S.A.

——& Firstbrook, P 2014. *Designing an adaptive security architecture for protection from advanced attacks,* Gartner, Stamford, CT, U.S.A.

Nanto, D 2011. *Economics and national security: issues and implications for U.S. policy,* Congressional Research Service, Washington, D.C., U.S.A.

RSA FraudAction Research Labs 2011, '*Anatomy of an attack', blog,* <http://blogs.rsa.com/anatomy-of-an-attack/>.

Smali 2015, <https://code.google.com/p/smali/>.

VirusShare 2015, <https://virusshare.com/VirusShare139a553936b9a927c188ca987a9f3bd0>.

Virvilis, N & Gritzalis, D 2013, 'The big four: what we did wrong in advanced persistent threat detection', *Proceedings of the Eighth International Conference on Availability, Reliability, and Security (ARES)*, pp. 248-54.

Watkins, L & Hurley, J 2016, 'Enhancing cybersecurity by defeating the attack lifecycle', *Proceedings of the International Conference on Cyber Warfare and Security (ICCWS)*, March 2016.