2020 SunTrust Fellowship Grants

KENNESAW STATE UNIVERSITY

INSTITUTE FOR CYBERSECURITY WORKFORCE DEVELOPMENT

Introduction and Thanks

On behalf of the 2020 SunTrust Fellowship Grant Awards committee, I would like to congratulate the recipients of the 2020 Grants, recognizing them as SunTrust fellows. This year the Grant program was made available to a much larger audience, resulting in a significant increase in the number of proposals submitted. The proposals highlighted in this year's awards notice span a range of topics related to Cybersecurity. We hope they provide valuable contributions to the field of Cybersecurity knowledge.

I would also like to extend a special thank you to SunTrust Banks, now Truist, for the generous multi-year gift, providing funding for these proposals. There is one more year of support pledged in their gift, so we look forward to reviewing the proposals for next year, as well as reviewing the findings from awards in previous years.

A special thanks to Seth Walker of the KSU Foundation and Dr. Herb Mattord of the Department of Information Systems for their assistance in coordinating the gift, and to the awards committee.

Michael E. Whitman, Ph.D., CISM, CISSP, Executive Director, ICWD

2020 SunTrust Fellowship Grant Awards Committee:
Rebecca Rutherfoord, Ph.D., Chair, Department of Information Technology
Dawn Baunach, Ph.D., Chair, Department of Criminal Justice
Dominic Thomas, Ph.D., Assoc. Professor, Department of Information Systems
Stephen Gay, Executive Director (OCS) and Chief Information Security Officer

2020 SunTrust Fellowship Grants

1. *“Federated Learning for Effective Intrusion Detection System in IoT Mobile Attacks” (p. 6)*

Reza M. Parizi, Ph.D., Assistant Professor,
Department of Software Engineering
and Game Development

Seyedamin Pouriyeh, Ph.D., Assistant Professor,
Department of Information Technology

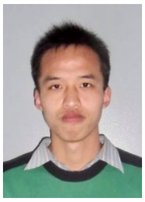
2. *“One size fits all? An IS use model of Cybersecurity” (p. 10)*

Saurabh Gupta, Ph.D., Professor,
Department of Information Systems

Adriane Randolph, Ph.D., Professor,
Department of Information Systems

Humayun Zafar, Associate Professor,
Department of Information Systems

3. *“Building Containerized Services with Security Assurance in the Edge Infrastructure” (p. 14)*



Kun Suo, Ph.D., Assistant Professor,
Department of Computer Science

Yong Shi, Ph.D., Associate Professor,
Department of Computer Science

2020 SunTrust Fellowship Grants

"IoT-related Attack Platforms" (p. 19)

Xiaohua Xu, Ph.D., Assistant Professor,
Department of Computer Science

"Building Secure Software Development with Data Leakage Detection and Analysis Plugins" (p. 24)

Hossain Shahriar, Ph.D., Associate Professor,
Department of Information Technology

Chi Zhang, Ph.D., Associate Professor,
Department of Information Technology

"Collaborative Guided Learning Pedagogy for Information Security Topics" (p. 27)

Xin (Shirley) Tian, Ph.D., Assistant Professor,
Department of Information Technology

Zhigang Li, Ph.D., Assistant Professor,
Department of Information Technology

2020 SunTrust Fellowship Grants

"Privacy Protection among Three Antithetic-Party for Context-Aware Service" (p. 31)

Yan Huang, Ph.D., Assistant Professor,
Department of Software Engineering
and Game Development

Donghyun Kim, Ph.D., Associate Professor,
Department of Computer Science

"Promoting Information Security Policy Compliance – An Action Research Enabled Empirical Study" (p. 35)

Lei Li, Ph.D., Professor and Assistant Chair,
Department of Information Technology

Meng Han, Ph.D., Assistant Professor,
Department of Information Technology

“Federated Learning for Effective Intrusion Detection System in IoT Mobile Attacks”

Reza M. Parizi, Ph.D., Assistant Professor, Department of Software Engineering and Game Development
Seyedamin Pouriyeh, Ph.D., Assistant Professor, Department of Information Technology

In recent years, we have witnessed the dramatic growth of mobile devices in the IoT domain, which enables people and services to interconnect and exchange information constantly. The number of IoT mobile users even tends to grow larger in the near future (as shown in Fig. 1). As many IoT mobile devices are vulnerable due to insecure design, implementation, or configuration, the networks that are based on such IoT mobile devices are therefore exposed to misuse and cyberattacks [1].

To safeguard mobile IoT networks, Intrusion Detection Systems (IDSs) have been widely used to monitor the network traffic and identify suspicious activities within the traffic. IDS systems are often regarded as a critical component in protecting IoT nodes and networks as well as mitigating adverse effects of cyber attack targeting IoT. In general, IDSs are categorized as signature-based or anomaly-based defense mechanisms [2]. Signature-based IDSs recognize intrusions (or suspicious activities) by finding the relationship between previously learned rules/signatures of known attacks’ rules. Anomaly-based IDSs monitor network traffic and compare the traffic with previously learned patterns to spot malicious activities. Despite their wide adoption, IDS-based methods are, however, not very effective in detecting new and unknown adversarial attacks (signature-based IDSs are unable to detect new attack unless they have the latest version of all attack signatures). Anomaly-based methods have shown to be able to recognize known and new attacks to some degree, but they often arise high false-positive rates hindering the accuracy [3]. Given the massive scale and heterogeneous networks of the IoT mobile devices, the effectiveness of the Intrusion Detection System (IDS) in detecting attacks is questionable.

Machine Learning (ML), as cutting-edge technology for designing and implementing robust intelligent systems, has been greatly contributing to cybersecurity solutions. The past decade has witnessed the release of several approaches utilizing ML for different aspects of cybersecurity ranging from malware detection and threat intelligence to forensic investigation and privacy-preserving. Deep Learning (DL) is one of the emerging topics of ML, which is generally related to a capable learning model that includes several layers, and each layer contains enormous computational nodes. DL models have demonstrated their suitability and competency for different data-driven problems including cybersecurity.

“Federated Learning for Effective Intrusion Detection System in IoT Mobile Attacks”

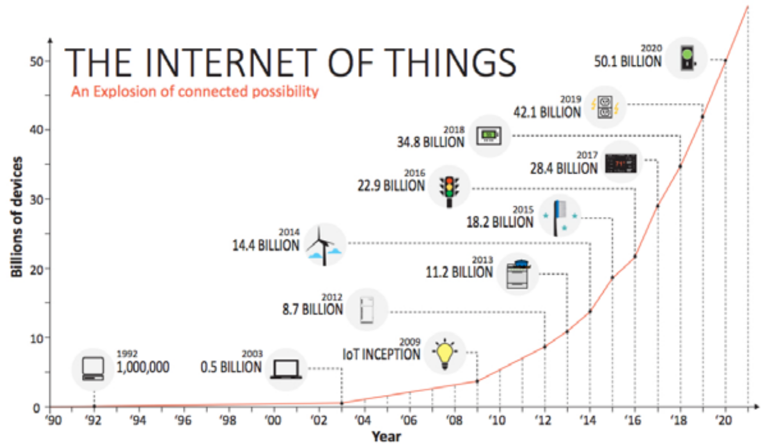
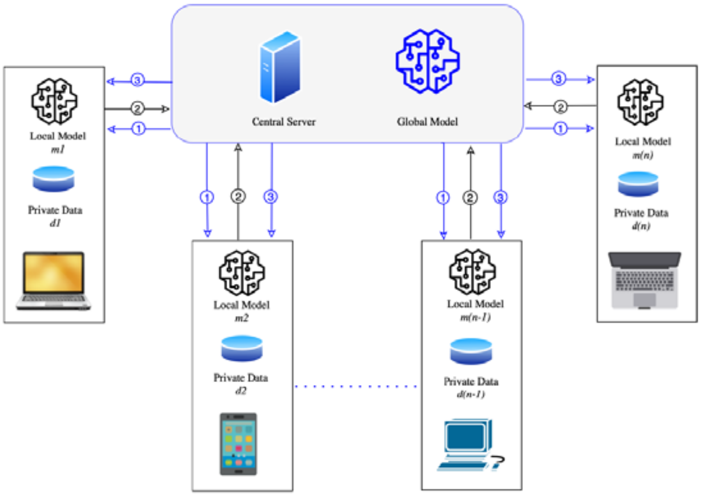


Fig. 1: Forecast number of IoT devices

Recently, recurrence neural networks have been used in different IDS based on anomaly-detection techniques. Lately, Malhorta et.al in [4] apply Long Short-Term Memory (LSTM) for detecting anomalies in time series data. Opera et al. [5] utilize the deep neural network to analysis DNS log data in order to detect anomaly patterns in enterprise networks. The recent proposed approaches mostly operate in an off-line manner while there is high demand for a real-time data analysis platform to detect zero-day vulnerabilities and anomaly attacks. In this project, we aim to propose a new effective anomaly detection model to differentiate benign pattern of behavior from malicious activities in mobile-based networks. To tackle the aforementioned challenges, we will utilize the Federated Machine Learning (FML) technique to develop anomaly detection patterns for IDSs. To the best of our knowledge, this work will be one of the first kind to use FML for IoT attack detection.

Methodology

While traditional Machine Learning models mainly rely on computational power and training dataset of a centralized server, Federated Machine Learning (FML), which has gained many attentions recently in different domains, is defined as a combination of federated and machine learning techniques [4]. FML implements different machine learning techniques in a decentralized environment where the machine learning models are developed based on the datasets distributed across different devices. Although, we still have the concept of central server in the FML, the training procedure is mainly done by mobile devices. In the first step, each mobile device in FML environment downloads a machine learning model from a central server, then it runs the model locally on the mobile device and improves it by learning from data stored on end device (i.e. edge). Ultimately, the mobile device summarizes the results, typically containing the model parameters and corresponding weights and send to the central server [5]. The updates from all mobile devices across the network is averaged by the central server and the improved model will be sent to the mobile devices for the next iteration (Fig. 2). The key point in FML is that all the training data remains on mobile devices which preserve the privacy property as well.



Step 1: Central Server shares initial model parameters with all the clients.
Step 2: Clients train their local model with initial parameters and share local model with central server.
Step 3: Central Server Aggregates the local models and shares global model with the clients.

Fig. 1: FML Process Flow

In this project, we aim to use FML to develop a global machine learning based IDS model from many local IDS running at each IoT mobile device. While applying anomaly detection techniques in IoT environment is associated with some challenges such as resource limitations and heterogeneity of IoT devices, and the current approaches are still dealing with those, we plan to target those issues and come up with an novel and efficient model for anomaly detection IDS using FML. In our model, the light version of the IDS (local IDS) is running on each IoT device. The local IDS is trained and the improved version of the model is sent to the main server to contribute to the global IDS. In the training procedure the IoT device collects local information, incorporates the data into the local model, refining and learning the decision boundary between benign pattern of behavior and malicious activities. The central server, generally, average all of the updates to calculate the improved global model. Then the updated model, which is the most accurate IDS, is pushed to the IoT mobile devices. Using FML to implement anomaly detection based IDS, enables all IoT devices to cooperate in training and improving the global model, dealing more effectively with unknown attacks. Additionally, FML technique features the IDSs to operate in real-time manner what we have not noticed in the current ML-based IDSs.

“Federated Learning for Effective Intrusion Detection System in IoT Mobile Attacks”

In this project, we aim to use FML to develop a global machine learning based IDS model from many local IDS running at each IoT mobile device. While applying anomaly detection techniques in IoT environment is associated with some challenges such as resource limitations and heterogeneity of IoT devices, and the current approaches are still dealing with those, we plan to target those issues and come up with an novel and efficient model for anomaly detection IDS using FML. In our model, the light version of the IDS (local IDS) is running on each IoT device. The local IDS is trained and the improved version of the model is sent to the main server to contribute to the global IDS. In the training procedure the IoT device collects local information, incorporates the data into the local model, refining and learning the decision boundary between benign pattern of behavior and malicious activities. The central server, generally, average all of the updates to calculate the improved global model. Then the updated model, which is the most accurate IDS, is pushed to the IoT mobile devices. Using FML to implement anomaly detection based IDS, enables all IoT devices to cooperate in training and improving the global model, dealing more effectively with unknown attacks. Additionally, FML technique features the IDSs to operate in real-time manner what we have not noticed in the current ML-based IDSs.

References available on request

“One size fits all? An IS use model of Cybersecurity”

Saurabh Gupta, Ph.D., Professor of Information Systems
Adriane Randolph, Ph.D., Professor of Information Systems
Humayun Zafar, Associate Professor of Information Security and Assurance

The rapid transformation of critical organizational information to the digital format has drastically increased the importance of information security (Moody, Siponen, & Pahnila, 2018), with expected spending to reach $133.8 billion in 2022 (IDC, 2019). However, despite the increase in spending on organizational initiatives to secure information, security incidents continue to occur, and their damaging effects continue to increase (Ab Rahman & Choo, 2015; Safa, Von Solms, & Furnell, 2016; Willison & Warkentin, 2013).

A key organizational mechanism used to manage IT security relates to security policies and procedures. Such procedures then to very prescriptive and assume all individual use of technology to be similar. However, recent research in information use identifies three clear and distinct types of IT use depending of the technology familiarity and task at hand (Burton-Jones, Stein, & Mishra, 2017; Williams & Gupta, 2018; Williams, Sinha, & Gupta, 2019). The three types of uses (initial, continued and novel use) draw on different types of cognitive load.

Researchers in IS have recently called on more focus on the user, and thus, highlight the importance of cognition in behavior (Davern, Shaft, & Te'eni, 2012). In this research, we content that such cognitive load is one of the key reasons for users to ignore security policies and fall prey to security threats (Mascha & Smedley, 2007; Pacauskas & Rajala, 2017). Consistent with calls for research to converge IS reference fields (Wynn & Hult, 2019), this research draws on the theory of cognitive load from education to understand the impact on behavior / performance of actions (Sweller, 1988; Sweller, van Merriënboer, & Paas, 2019). Our primarily focus is on post- adoptive (continued and novel use) behavior, since that is what most users tend to do.

In subsequent sections, we outline the underlying theoretical concepts used, method proposed and key implications.

Cognitive load and IT use

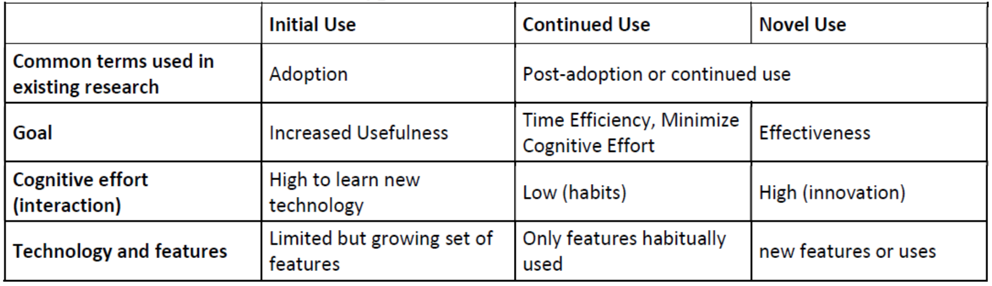
Cognitive load theory proposes that human brain a limited working memory and virtually unlimited long-term memory (Sweller, 1988). Consequently, only a limited number of items at a time (approximately seven) can be processed by individuals at a given time.

The theory also outlines the use of Schemas, which categorize information by the manner in which it will be used, are acquired over time and repeated exposure to related problems, are automated as rules, and stored in the long-term memory for recall when needed. The theory argues that the intrinsic nature of the task at hand, determines the level of cognitive load an end-user of technology may be dealing with.

IT Use types

Over time, multiple use constructs have been conceptualized with many different theoretical groundings. These many conceptualizations can be merged into three distinct types (See Table 1). Since this research focuses on post adoptive use, we focus only on the two use types involved.

Table 1. Characteristics of Use Types



	Initial Use	Continued Use	Novel Use
Common terms used in existing research	Adoption	Post-adoption or continued use	
Goal	Increased Usefulness	Time Efficiency, Minimize Cognitive Effort	Effectiveness
Cognitive effort (interaction)	High to learn new technology	Low (habits)	High (innovation)
Technology and features	Limited but growing set of features	Only features habitually used	new features or uses

Continued Use

Continued use refers to use of an advanced technology for its intended purpose after overcoming the initial learning curve of the technology and generally occurs before novel use. A user in the continuous use phase has become adept enough at using the technology such that the use of at least some features are habitual. The user’s goal in this phase of use is to minimize his/her cognitive effort required to use the technology and gain time efficiencies by tweaking the processes used since initial use to be more productive. This is generally done through three means: a) using the current knowledge, perhaps via training received earlier and independent and peer-based learning gained during initial use, to efficiently execute tasks using the IT (Burton-Jones & Straub Jr, 2006); b) habitual use, or well-learned actions sequences (De Guinea & Markus, 2009); and/or c) engaging in system 1 thinking i.e. automatic, fast and often unconscious way of thinking (Kahneman, 2003).

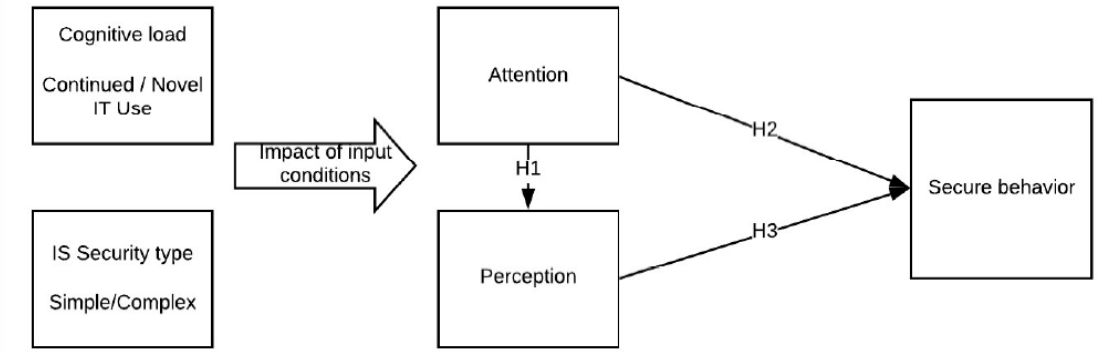
Novel Use

Continued use stands in contrast to novel use. Novel use occurs when users try to innovate what tasks they are able to do with the technology (Ahuja & Thatcher, 2005). Such use often involves the appropriation of more technology features and may occur after either initial or continued use. Novel use, we argue, exhibits higher cognitive load as compared with continued use. The higher cognitive effort stems from an increase in system 2 thinking (Kahneman, 2003)(Sun, 2012).

“One size fits all? An IS use model of Cybersecurity”

Research Design and Research Method.

Figure 1 outlines the research model, as well as the key hypothesis. The constructs outlined in the model will be manipulated as follows. The research method used for the study is an experiment.



Sample: A set of end-users with reasonable computer experience and usage need throughout the day would be part of the sample frame. Sample size is estimated to be around 30.

Manipulation: The experiment uses a 2X2 design. The first dimension would differentiate between continued use and novel use task. The second dimension would differentiate based on the complexity of the IT security threat.

Measurement: The key measure here is the use of NeuroIS tools to measure perception and attention.

These are through EEG and eye-tracking tools. Participants will have their EEG or brain waves recorded non-invasively using a standard electrode cap while they engage with technology of varying, pre-identified categories. During their engagement, eye-tracking technology will be used to confirm that the user’s attention is on the intended construct for which cognitive load is being measured. Post-hoc, cognitive load will be assessed according to a published engagement index (Pope et al., 1995) calculated from the recorded EEG.

The second measure relates to the actual measurement of the secure behavior. This would be captured by the system. Finally, a debriefing will be done with each participation to understand their cognition and the schemas used.

Time: Each session per participant is expected to take around 1 hour.

Context: A dedicated research assistant would participate in the collection of data for each of the participants.

“One size fits all? An IS use model of Cybersecurity”

Benefits of the research

The research provides three key benefits.

a) It provides evidence regarding the dark side of attacks i.e. provides evidence of where IT attacks should be done. We hypothesize that attacks on novel IT use tasks are likely to be more successful. We are seeing some of this with recent reports of researchers being targeted.

b) It provides guidelines to security designers on where to focus their efforts on. The key component here is that they need to focus on different IT use types to design their security policies rather than treating as “one size fits all”

c) Finally, the research provides guidelines to practice in terms of application design. Depending on the outcome of the study, one of the types of use should be done in a higher secure setting than others.

In terms of theory development, this study has the potential of moving beyond attitude-based models of IT security to a cognitive load model. This can then influence training as well as other knowledge mechanics used by practice.

References available on request

“Building Containerized Services with Security Assurance in the Edge Infrastructure”

Kun Suo, Ph.D., Assistant Professor, Department of Computer Science
Yong Shi, Ph.D., Associate Professor, Department of Computer Science

Overview:

1. Traditional virtualization technology

Virtualization technology is one of the most important technical means to realize the full utilization, reasonable allocation as well as effective scheduling of hardware infrastructure resources in today’s datacenters. For example, in a typical Infrastructure as a service (IaaS) based on OpenStack, the cloud service providers can virtualize the underlying resources such as servers, storage, and networks and build a cluster resource pool to provide elastic services to tenants. Traditional virtualization technology adopts virtual machines (VM) as the unit. Each VM has an independent operating system kernel and does not share software stack with other VMs on the same host. Therefore, it has good isolation and is suitable and secure for multi-tenant scenarios in a cloud environment.

2. Containers and containerized services

In recent years, as a lightweight virtualization technology, container [11] is becoming increasingly popular as it packages applications and necessary execution environments into images such that containerized applications and services can run independently on the physical or virtual hosts, and migrate easily across the machines. Compared to the traditional application development and deployment, containerized services do not need to consider the compatibility of execution environment. Different from hardware virtualization, container virtualizes the resources at the operating system level and multiple virtualized environments can run on the host kernel, which achieves higher efficiency and resource utilization.

With the advent of 5G era and Internet of everything, including smart cities, smart transportation, smart homes, etc., tens of billions of devices will access to the network and generate massive of data. The traditional cloud is difficult to meet the new demands of large bandwidth, low latency, and massive connections in the new era of the Internet of Things (IoT), and the edge computing emerges. Due to its lightweight, lightning startup and portability, containers are widely adopted to suit various edge computing scenarios.

“Building Containerized Services with Security Assurance in the Edge Infrastructure”

3. Container virtualization security risks

Compared with traditional virtual machines, containers do not have completely independent software stack and do not achieve isolation at the operating system level. Therefore, there exist security risks caused by incomplete resource isolation and insufficient resource restrictions, especially for the untrusted workloads. Because the container shares hardware resources, e.g., CPU, memory, and disk space with the host, and container runtime such as Docker does not have a default limit on the resources used by containers, the host or other containers might have denial of service (DoS) if a single container exhausts the host computing or storage resource, such as idle CPU time and free memory. Here we list some examples of DoS attacks on container virtualization:

3.1. Computational DoS Attack on Container

Fork bomb [10] (also called rabbit virus or wabbit) is a DoS attack wherein a process continually replicates itself to deplete available system resources, slowing down or crashing the system due to resource starvation. As the total number of processes that the host operating system can support is limited, the host resource could be exhausted and it cannot create more processes if one container is subject to a Fork bomb attack, which creates too many processes within the container in a short period of time.

3.2. Memory DoS Attack on Container

In general, the container runtime, e.g., Docker, does not set limit for the containers, which means all containers can use the entire memory of the host. It is significantly dangerous and might cause the host to run of memory, therefore making the service unavailable, if the container is running malicious memory consuming software or there exists memory leak in the source code. One possible solution is set the memory limit for each container. However, as the datacenters host diverse workloads, it is prohibitively expensive to devise application specific memory limit mechanism. In addition, it may also harm the services inside the container. For instance, if the memory limit is set too small, the services might be killed by out of memory (OOM) when it’s still running normally.

3.3. Storage DoS Attack on Container

Many container runtimes, such as Docker, achieves file system isolation through mounting namespace in order to make each container only see its own files. However, it does not limit the storage resources of a single container on the AUFS file system. Therefore, the security risks could still exist if the containers adopt AUFS as the storage driver. For instance, if one malicious container continuously writes files to the AUFS file system, the storage of the host machine could run out of space and cannot meet the data storage requirements of itself and other containers.

“Building Containerized Services with Security Assurance in the Edge Infrastructure”

3.4. Network DoS Attack on Container

Due to its unique network virtualization, container networks face different security risks from DoS attacks than traditional networks. The containers on the same host form a local area network (LAN). Therefore, the hacker can launch a DoS attack, such as ARP spoofing, sniffing, broadcast storm, from one container to the others and reduce their network data processing capacity. Besides, as all containers on the same host share the same network hardware, an external attacker can send large number of packets to a target container for DDoS attack, which exhausts the host network bandwidth and causes denial of service for the other containers.

3.5. Temperature Attack on Container

As the density of electronic components used in modern electronic devices keeps increasing, the thermal stress has become one of the most significant factors affecting application performance as well as system reliability. For instance, the Power Wall [12, 13, 14] is becoming one of critical obstacles to design modern CPUs. Many studies [15, 16, 17] also revealed that the reliability of some hardware, such as chip circuits, is almost entirely dependent on the thermal environment. Based on the Arrhenius equation, the life of components will be reduced by about 30%-50% if the ambient temperature increase by 10 ℃. A potential temperature attack could be the hackers inject some codes into the one container and keep it consuming the CPU resources, which not only harms the neighbor container performance due to the underclocking for avoiding overheat, but also could damage the electronic components inside the IoT devices.

4. Methodology: Building Containerized Services with Security Assurance for the Edges

4.1. Idea 1: Leveraging Hardware with Advanced Features

In recent years, many studies have demonstrated that it is effective to improve the container security by using advanced hardware. For instance, Intel has proposed SoC chip, Atom E3900 [1], for the IoT gateway. Samsung also introduces ARTIK secure IoT modules [2], which combine hardware-backed security with pre-integrated memory, processing, and connectivity, to deliver comprehensive device-to-cloud protection for IoTs. Also, ARM has released Cortex-M23 [3] and Cortex-M33 [4] chips for IoT devices with ARMv8-M and TrustZone security. Hardware techniques are fundamental and effective for container security running at the edge. We will leverage the advanced hardware to build trust and secure edge infrastructure but also will explore software solutions which can be widely adopted for various types of edge platforms and works for more hardware platform.

“Building Containerized Services with Security Assurance in the Edge Infrastructure”

4.2. Idea 2: Container Resource Isolation and Limitation

In traditional virtualization architecture, the hypervisor or virtual machine monitor is responsible for resource management and scheduling. The container architecture does not have the hypervisor layer and thus it is necessary to rely on the operating system to implement the resource isolation. In Docker, it uses the namespace mechanism of the Linux kernel to achieve independent resources between containers and hosts, or between containers. By creating its own namespace for each running container, it is guaranteed that the running of processes in the container will not affect the processes in other containers or the host. To avoid unnecessary kernel interaction, we can also control Linux system calls from the container through seccomp [5].

To implement resource limits, Docker provides Cgroups [6] for the resource control and audit on CPU, memory, I/O, etc. We can adopt Cgroups to prevent a single container from exhausting all resources and causing other containers or hosts denial of service in order to ensure the normal operation of all containers. For instance, the container can use all the memory on the host by default. To solve that, we can use memory throttling mechanisms to avoid that one container consumes all host resources. Similarly, limiting processor and network bandwidth can prevent attackers from running processes that consume large amounts of resources, such as bitcoin mining or torrent peers. As Cgroups does not implement restrictions on disk storage resources, we can create separate user for each container and limit the disk usage of each user. We can also create a separate virtual file system for each container or adopt file system such as XFS which supports disk usage restrictions for directories.

4.3. Idea 3: Interaction between Container and Applications

Although isolation at the operating system level and enforcement of least privilege are critical, the resource control also needs to be tied to application logic. Without knowledge of the applications running on the host, isolation at the operating system level may not be effective by itself. To achieve that, an isolated, per-container view of available resources is necessary for attaining high efficiency and preventing erroneous behaviors, such as out-of-memory (OOM), in containerized applications. The adaptive resource view is continuously updated to reflect the effective capacity of a container based on resource limits, shares, and the actual usage from other containers.

4.4. Idea 4: Container Resource Monitoring and Secure Runtime

In order to ensure the security of container operation and realize immediate alarm and emergency response to security risks, real-time monitoring of various performance indicators of containers is required. Currently, many tools and industrial solutions have been proposed including cAdvisor [7], Scout, DataDog [8], Sensu, etc. Besides, many researchers proposed optimizations of container runtime for improved security. For instance, Google has proposed gVisor [9], which isolates non-secure system calls by implementing independent user-mode kernels to recapture and proxy all system calls for applications. However, compared to the traditional OS containers, its application compatibility and system call performance is much worse. Another representative solution is microVM, which is a lightweight and simplified solution of traditional virtual machine. Due to the complete kernel inside, it has high application compatibility. Nevertheless, the cost are its higher overhead and relatively slow startup speed compared to the Docker containers. We plan to design a lightweight container resource monitoring system to trace the utilization at real time. We also plan to characterize the existing solutions and propose new designs to address the overhead of secure container runtime.

5. Summary

Compared to traditional virtualization, containers are much more agile and lightweight as the cloud infrastructure, which is irreplaceable in promoting IoT and edge computing applications. However, despite for the high efficiency, container also has significant flaws on security such as resource isolation. As the 5G, high speed network, and IoT become more popular, the study of container security is becoming increasingly important. In this project, we try to explore the possible solutions to improve the security of the containers and propose our ideas to advance the reliability of the containerized application infrastructure.

References available on request

“IoT-related Attack Platforms”

Xiaohua Xu, Ph.D., Assistant Professor, Department of Computer Science

The jamming resistant for mobile devices in fifth-generation (5G) networks has been well studied recently. However, most of the existing work simply assumes the a single resource constraint [9] or an even simpler model. We investigate interference aware opportunistic spectrum scheduling in 5G networks subject to imperfect channel state information under the multiple resource constraint model. Let us use the channel state of a communication link to indicate the probability that the channel is good for that link. The channel state of each communication link is not fully observed due to unpredictable primary user activities. The channel state of each link evolves as an independent discrete time Markov chain. Multiple communication links may transmit simultaneously and links that did not transmit last time are also allowed to change channel states. The objective is to select links under the multiple resource constraint model to transmit sequentially to maximize the jamming resistant throughput over an infinite time horizon.

There is a challenging gap between a single resource constraint such as the protocol interference model [9] and the multiple resource constraint model. The solutions under the protocol interference model cannot be applied to the multiple resource constraint model directly. Most scheduling problems become very hard with multiple resource constraints. To the best of our knowledge, we are the first to address the jamming-resistant communications under the multiple resource constraint model.

Under the 5G networks, we consider the jamming-attack against mobile device scenario and propose jamming-resistant communications. Given a collection of communication pairs, at each step, we select a subset of devices to activate. The reward of activating a device depends on its transmission state. The exact state is only revealed when the corresponding device is activated. The objective is to maximize the expected average reward over the infinite horizon. The problem has two challenges. First, the communications are vulnerable to jamming attacks. The jammers are unpredictable around each communication pair. Second, the channel state of each device fluctuates over the long time horizon. To address these challenges, we consider a reinforcement learning paradigm called Multi-Armed Bandit (MAB) [5] paradigm. The MAB paradigm can capture a trade-off between exploration and exploitation for sequential allocations.

There is a large literature on MAB. However, existing works consider a simple network while in this proposal, we consider a radically different paradigm which integrates wireless interference into the MAB framework.

“IoT-related Attack Platforms”

Task 1: Design jamming-resistant communications via the MAB framework.

We plan to conduct testbed experiments. We will deploy a testbed which consists of several nodes and one access point. We connect all smart devices to form a home area network via Bluetooth. We then test the performance of the proposed methodologies in this testbed.

Task 2: Testbed setup and performance evaluation.

To simulate a 5G network, we construct a 5G network with different system parameters. Under such setting, the simulation results will be used to verify the validity of our analytical models, so that we can predict the performance of our system in a real-world application.

The next step will be to implement our system and evaluate it in practice. we will deploy a testbed will consist of several real links. We will study different scenarios and evaluate the performances. The initial testing will be performed by bringing a couple of devices close to each other and verifying the correctness of the 5G communications. We then deploy the app on multiple devices (PI and research students) and experiment in an actual 5G environment. We will test different scheduling algorithms in this project and find the success data rate and the energy consumptions. We will consider several metrics such as the total throughput in a certain period, the fairness between different nodes, and the packet delivery ratio.

Literature Review

MAB belongs to the paradigm of reinforcement learning. In [22], Whittle suggested extending the multi-armed bandit (MAB) [5, 12] to Restless MAB. The special structure of Restless MAB has led to the discov-ery of “index-type” algorithms. The index structure for a Restless MAB problem is a priority index that is assigned to each channel state, and the optimal action each time is to activate the channels whose indices are the largest. In [2], the authors studied the optimality of the myopic algorithm for stochastically identical and independent channels, under the assumption of single-channel sensing. In [1], the optimality of the myopic algorithm was proved for selecting multiple channels each time. In [13], Liu and Zhao provided a comprehensive study on the indexability and optimality of the Whittle index for multichannel access. Wang et.al. [20, 21, 19, 18] address the Restless MAB from the perspective of myopic algorithm for both two and multiple state Restless MAB. Comprehensive surveys on Restless MAB are available in [14, 15, 4]. However, their work either cannot provide a performance guarantee or simply assume all links have the same transition probabilities. Guha and Munagala [7, 8] investigated the Restless MAB problem from a novel approximation algorithm perspective. In [17], Wan and Xu designed approximation algorithms for a weighted version of Restless MAB. In [23], Xu and Song proposed an interference-aware approximation algorithms for Restless MAB. The difference between their work and this study is that they either did not address wireless interference or use a over-simplified graph-based interference model.

“IoT-related Attack Platforms”

Methodology

Given a set of communication links in a two-dimensional plane, each link has a sender and a receiver. At each time, each link is associated with a channel state for transmitting along this link considering the possible jamming attacks. The channel state space of each links is {good, bad}. Assume time is divided into time-slots. The channel state of each link evolves independently and stochastically across time-slots.

Let r_i be the bandwidth of the channel associated with the link *i*. If a link transmits without interference along a channel which is in a good state, a throughput of r_i is obtained. Assume that the complete state information of each channel is not known. The state of each link can be estimated by exploiting the memory along with feedbacks from the activated channels.

We propose a method where the scheduler maintains a variable $\pi_i[T]$ for each communication link. $\pi_i[T]$ is defined as the probability that the channel for link i is in the good state at time-slot T . The accurate channel state is revealed only after the data are transmitted. If each channel has a stronger potential to stay in its previous state than to jump to another, then this scenario is called positive auto-correlation of state evolution. This scenario occurs when $\alpha_i + \beta_i < 1$ for each link *i*. Otherwise, the scenario is called negative auto-correlation of state evolution and occurs when $\alpha_i + \beta i \geq 1$ for each link *i*. The system starts to operate from time-slot T =0. Each link has an initial state of either good or bad. We define a scheduling algorithm as selecting a subset of links to play each time over the infinite horizon. For an algorithm, let ai[T] denote whether link i is scheduled to transmit ($a_i[T]=1$) or not ($a_i[T]=0$) at time-slot *T*. The objective is to design an algorithm that maximizes the expected average reward over the infinite horizon, i.e.,

$$\lim_{\mathcal{T}\to+\infty} E\left\{\frac{\sum_{T=0}^{\mathcal{T}}\sum_{i=0}^{N} a_i[T]\cdot\pi_i[T]\cdot r_i}{\mathcal{T}}\right\}$$

such that the links selected each time form an independent set.

We will design a scheduling policy to maximize the infinite horizon average reward. In the jamming-resistant communications, the state transition of each communication pair i can be represented by a probability transition matrix. Due to the dynamic nature of the state, the transition matrix may be unknown. For example, if either α_i or β_i is unknown, it is challenging to design a scheduling policy for optimization.

We consider a dynamic system with M random processes. The state of the i-th process at time n, denoted by $x_i[n]$, evolves according to a dynamic model,

$$x_i[n+1] = \beta_i x_i[n] + v_i[n], i = 1, \cdots, M(1)$$

where β_i is a known constant, and $v_i[n]$ is the noise following some normal distribution $N(0, \sigma_v^2)$. We define a non-decreasing reward function *g(x)* for state *x*, and without loss of

“IoT-related Attack Platforms”

generality, we assume a range space [0, 1]. At each decision period *n*, denote I_n as the arm chosen to observe. The expected regret can be expressed as

$$R(n) = E[\sum_{\ell=1}^{n} \max_{i=1,\cdots,M} g(x_i[\ell]) - \sum_{\ell=1}^{n} g(x_{I_\ell}[\ell])] i = 1, \cdots, M$$

where the expectation is taken with respect to random realizations of the *M* dynamic processes. Our goal is to select I_n at each time period to bound the expected regret as *n* increases (will linearly increase as *n*.)

Due to the system dynamics, there exists no single optimal option. Rather, based on the process evolution model, one could predict the state of all the dynamic processes based on past observations on each individual process. Denote $x^i[n]$ as the predict of $x_i[n]$ and denote $P_i[n]$ as the corresponding prediction variance. The process to be observed at time n can be chosen as

$$I_n = \arg\max\{\hat{x}_i[n] + \frac{1}{M}\sqrt{\alpha P_i[n]}\}$$

where α is a design paranode. Similar to the UCB scheduling policy [3], the second term is a bias (needs fine tuning) to achieve an optimal tradeoff between exploration and exploitation.

Integration of Research and Education

Curriculum Development PIs will use the project for educational purposes and integrate interdisciplinary research and education. This project aims to enhance the department’s curriculum, by integrating our research results in existing courses, particularly in the areas of wireless communications such as CS 2123 (C Programming), 4322 (Mobile Software Development), and 7030 (Mobile Device Application Development). Moreover, PIs will develop a new course on prediction, learning, and games in mobile networks to promote education in theory and practice. The syllabus will cover 5G communications and Restless MAB. One of the course objectives is to expose students to 5G communications and Restless MAB and educate students on how to schedule for 5G communications. After this course, the students have developed critical research skills. The theoretical and experimental results from this project will be brought to classroom and discussed. Both PIs will measure the students’ feedbacks and the teaching efficacy. Both PIs will use the Likert-type scale.

Task 3: Develop two new courses regarding IoT attack platform and 5G.

Capstone Projects The project expects to have two undergraduate and two graduate students per semester working on the proposal. Particular emphasis will be placed on recruiting female students and students from under-represented minorities.

“IoT-related Attack Platforms”

The leading PI Xu is currently managing a lab with two graduate research assistants. The project will provide opportunities for involving undergraduate and graduate students to participate in research activities including methodology design, testbed implementations, experiments, and mobile application development.

We encourage and support female and minority students to participate in research and professional organizations and will continue to do so. We encourage them to attend academic conferences, to present research, and network with other researchers. Dr. Xu has supported three female students through his previous NSF project.

Task 4: Directed capstone projects for students.

References available on request

“Building Secure Software Development with Data Leakage Detection and Analysis Plugins”

Hossain Shahriar, Ph.D., Associate Professor of Information Technology
Chi Zhang, Ph.D., Associate Professor of Information Technology

As access to software and services through mobile devices have increased, protecting data on the mobile devices is becoming increasingly important. A recent study found that 84% of applications have security flaws that pose threat of private data being exposed or the device being compromised [17]. We have witnessed numerous major cyberattacks, resulting in stolen personal credit card numbers, leakage of classified information vital for national defense, industrial espionage ending up major financial losses, and many more detrimental outcomes [19, 20]. Early elimination of security vulnerabilities can mitigate or reduce the potential damages through data losses or service disruptions caused by malicious attacks. However, software developers may not have enough security knowledge and skills required to apply tools to mitigate security vulnerabilities during development time [6, 7, 8]. Furthermore, secure mobile software development is not well presented in the curriculum despite high demand career options on information security [1].

If all the mobile applications are built with security in mind and have minimum security flaws and vulnerabilities, the security threat risks will be greatly reduced for the mobile systems as well as the connected cyber systems. Such efforts require support from both the education and training communities to improve software assurance, particularly during the secure code writing phase.

Related work: Many open source static Java code analysis tools help developers maintain and clean up the code through the analysis performed without actually executing the code such as Eclipse IDE [9], IntelliJ IDE [10], and FindBugs Plugin [11]. These tools focus on finding probable bugs such as inconsistencies, helping improve the code structure, conforming source code to guidelines, and providing quick fixes, but not the security vulnerability checking as it is not their major task. A literature review [12] provides a complete list of state-of-the-art tools. However, none of the listed tool allows mobile developers to analyze their project code for detecting security flaws in the development environment (e.g., Android Development Studio).

FindSecurityBugs (FSB) is a code analysis plugin that has been ported to IntelliJ IDE [11]. It only specializes in finding security issues in traditional Java applications instead of Android

"Building Secure Software Development with Data Leakage Detection and Analysis Plugins"

Specific security bugs (e.g., data leakage through inter process communication). FlowDroid [13] and Droidsafe [14] are two popular static analysis tools for Java-based applications only. Many other efforts have been made to enhance the secure software development in recent years. Application Security IDE (ASIDE) plug-in for Eclipse can warn programmers of potential vulnerabilities in their code and assists them in addressing these vulnerabilities [15, 16]. However, it cannot identify Android-specific security flaws. Moreover, ASIDE only works with Java Eclipse IDE.

Methodology: The planned tool will be built by leveraging some of the available open source Java program analyzers (e.g., Soot [21]). The tool will analyze a given Android apk generated during development time by accepting list of data sources and destinations (that may lead to data leakage) in the development environment. It will obtain a call graph (i.e., list of API calls within applications spanning from the defined sources to all possible sinks) and then generate a report showing a list of possible data leakage (between input sources and output sinks).

Figure 1 shows a high level architecture of the tool implementation plan. The tool development is based on researching and integrating the library sources (e.g., android-jar). It is planned to create the default source/sink APIs as text input files for users/classroom learners within the Android project directory. A user would be able to conveniently edit source and sink lists, to discover new malware, spyware, or adware within an analyzed application.

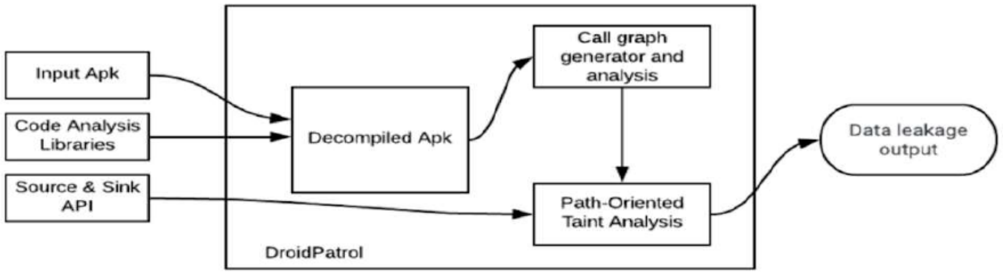


Figure 1: Architecture of Plugin

The plugin is intended to identify security bugs that have been identified in best practice resources [4, 5] such as OWASP top 10 security risks and top software security design flaw (e.g., SQL injection, unintended data leakage, insecure communication, and insecure data storage). Table 1 shows the examples of malicious leakage through APIs (input sources, output sinks) for insecure data storage, insecure communication, and insecure authorization. The tool is expected to identify the suspected data flow and warn users on the implication.

“Building Secure Software Development with Data Leakage Detection and Analysis Plugins”

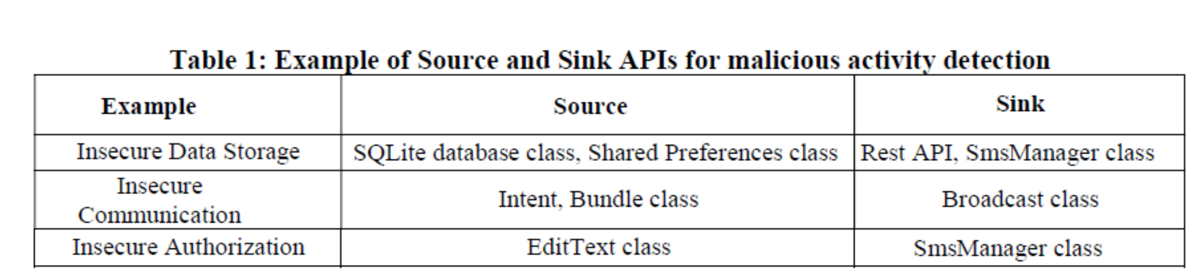


Table 1: Example of Source and Sink APIs for malicious activity detection

Example	Source	Sink
Insecure Data Storage	SQLite database class, Shared Preferences class	Rest API, SmsManager class
Insecure Communication	Intent, Bundle class	Broadcast class
Insecure Authorization	EditText class	SmsManager class

The flaw detection accuracy is vital for any newly developed Code Analysis tool assessment. A tool may miss a true flaw and in some other cases it may mislead developers with fake flaw reports. A False Negative (FN) indicates an overlooked vulnerability and a tool fails to identify or detect a serious security threat. On the other hand, a False Positive (FP) indicates that a tool falsely identifies acceptable pattern as a security flaw, which misleads or confuses users or result in unnecessary development delay. We plan to assess the effectiveness of our implemented tool using FN and FP. We expect our developed tool to have close to zero FN while the least FP rate (e.g., <3%). We plan to use a benchmark dataset (Contagiodump [3]), which includes 1260 samples of malware, spyware and adware applications. To collect samples of benign (good) apps, we will crawl Google Marketplace. The developed hands-on labware will be integrated into security related course (e.g., IT4863, IT6533) in Fall 2020/Spring 2021; and we plan to assess the effectiveness of the resources using pre- and post-lab surveys. The responses will be collected in a scale of 1-5 [5: Strongly agree, 4: Agree, 3: Neutral, 2: Disagree, 1: Strongly disagree], and analyzed. Open-ended questions will also be asked to collect students’ comments and suggestions toward the tool and the use of the tool.

The project will benefit the cybersecurity industry through a needed malware tool detection in the Android Studio environment. It also potentially opens the door for students and faculty to adopt the tool and learning resources into their courses for hands-on learning and development. The developed tool will support security vulnerability detectors for Android Apps following OWASP and related industry guidelines to enhance the security capability for mobile software development in Android Studio IDE. The effort will address one of the focused cyber workforce role based on the NICE guidelines to prepare students for high-demand jobs in the cybersecurity industries.

References available on request

“Collaborative Guided Learning Pedagogy for Information Security Topics”

Xin (Shirley) Tian, Ph.D., Assistant Professor, Department of Information Technology
Zhigang Li, Ph.D., Assistant Professor, Department of Information Technology

This project aims to develop a repository of instructional materials and assessment tools related to information security using a collaborative guided learning pedagogy. Each of these developed materials focuses on a particular security-related issue to help students achieve a better understanding of such a topic. The developed repository will cover a wide range of security-related topics that can be integrated into existing curriculum. The objective of this research project is to determine the effectiveness of the collaborative guided learning pedagogy for information security related topics. The focus of this project is the development and implementation of collaborative guided learning materials for Business Email Comprise Attacks (BEC), as well as contingency operations for ransomware attacks. We’d also take the opportunity to expand beyond these two topics and further develop learning materials to cover a wide range of security topics such as input validation, buffer-overflow attack, SQL injection, and cross-site scripting attack that can be integrated into a broad range of curriculum.

Literature

Literature has shown that collaborative and cooperative learning methods are effective in improving student learning and helping them develop key skills in both domain knowledge and “soft skills” in communication, problem-solving, teamwork/collaboration, and so on [1], [2]. As a result, more and more instructors are adopting collaborative and cooperative learning methods in their teaching, which have changed teaching styles away from the traditional lecture format to student-centered active learning [2], [3]. [4] suggests that teachers can increase student success by replacing content laden lectures with team-based learning that promotes conceptual understanding and skill development.

The National Science Foundation (NSF) has funded several projects to study active learning and student-centered learning approaches in STEM that promote higher student involvement in the learning process. The guided collaborative learning approach were found to have a positive effect on the learning experiences for students who are new or have limited prior knowledge in chemistry [6]. A meta-analysis done by [7] has suggested that process oriented guided inquiry learning (POGIL), which is a form of guided collaborative learning approach can substantially increase students’ odds of passing a course. In recent years, this guided collaborative learning process has been introduced to the field of computer science education to help students develop professional skills and prepare them for team-based upper level courses such as capstone courses [8]. [8] also suggest that the challenges, choices, options and approaches vary based on the class size, class modes, background of students, and the instructor preference. In a most recent study, [9] conducted interviews with instructors who adopted the POGIL method in their computer science curriculum and the feedback from faculty suggest that POGIL helps with student retention, attendance and engagement, reduces isolation and improves student performance.

Project Plan

This project has two primary components. The first component is the development and implementation of instructional materials and assessment tools for information security related topics following the collaborative guided learning pedagogy. The second component is the development and implementation of a web-based repository so that the instructional materials and assessment tools can be hosted and openly shared. Both components will proceed in parallel starting in Summer 2020.

Development and Implementation of Collaborative Guided Learning Materials

This project will follow an iterative approach for the development and implementation of collaborative guided learning materials. The iterative process consists of four steps:

1. Collection of information security related topics suitable for the collaborative guided learning pedagogy from both within the existing curriculum and external online resources.

2. Development of instructional materials and assessment tools following the collaborative guided learning pedagogy.

3. Integration and implementation of the developed instructional materials and assessment tools into appropriate courses. This can be either a security-focused course such as introduction to cybersecurity or a regular course with a security component. For instance, the materials for both Business Email Comprise Attacks and contingency operations for ransomware attacks can be integrated into the Information Security Administration and Privacy course in the undergraduate IT program and potentially other courses as well.

4. Evaluation of the effectiveness of collaborative guided learning pedagogy for

"Collaborative Guided Learning Pedagogy for Information Security Topics"

information security related topics. This includes the evaluation of students' understanding of the topics, attitude, motivation, etc.

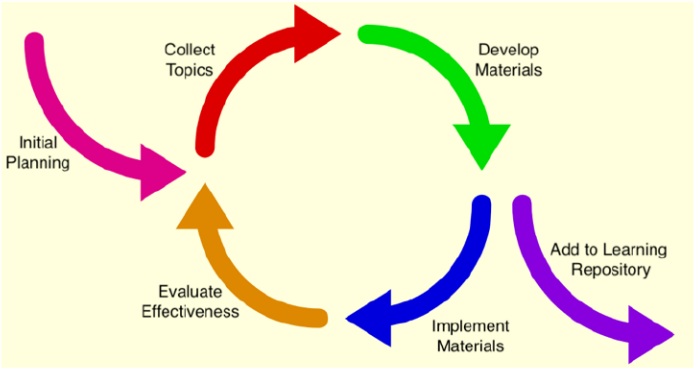


Figure 1. Iterative Process

The above figure is a graphical representation of the iterative process detailed earlier. This process will kick start in July 2020 with an initial implementation of the collaborative guided learning pedagogy in an information security course in Fall 2020. Further materials will be developed and implemented during Spring and Summer 2021 in a variety of courses.

A preliminary study on the effectiveness of collaborative guided learning pedagogy on information security related topics based on the data collected from Fall 2020 will be submitted to ITiCSE 2021 for publication. A more completed study using the data collected from all three semesters (Fall 2020 to Summer 2021) will be submitted to the Journal of Information Security and Applications for publication in Fall 2021. Furthermore, the research findings from this project will also be used in an NSF grant proposal under Improving Undergraduate STEM Education: Education and Human Resources (IUSE: HER) in September 2021.

Development and Implementation of Learning Repository

The purpose of the learning repository is to openly host the developed instructional materials and assessment tools for information security related topics so that they can be shared, used, and integrated into various IT or cybersecurity curriculum. Companies can also adopt the collaborative guided learning pedagogy and use the materials for workforce training. The web-based repository will be hosted on a server provided by the Kennesaw State University. For faster development, the possibility of adopting a content management system such as WordPress or Joomla will be evaluated. The development will kick off in Summer 2020, with a projected completion date in Summer 2021.

“Collaborative Guided Learning Pedagogy for Information Security Topics”

Assessment of Student Learning

To test the effectiveness of the collaborative guided learning pedagogy on information security related topics, we will assess student learning outcomes, learning experience, student attitudes and motivations in the courses that use the developed instructional materials and assessment tools. At the beginning of the semester, each student will complete a pre-survey asking about their demographic information, their background in information security, prior knowledge of security topics to be introduced. Students will then complete the learning activities as teams during the semester. At the end of the course, students will be given a post-survey to test their knowledge of the security topics introduced, their learning experience with the teaching method, their attitudes and their motivation in learning the topics.

References available on request

“Privacy Protection among Three Antithetic-Party for Context-Aware Service”

Yan Huang, Ph.D., Assistant Professor, Department of Software Engineering and Game Development
Donghyun Kim, Ph.D., Associate Professor, Department of Computer Science

Thanks to the rapid development and popularity of context-aware services, such as recommendation, navigation, and social network, individuals' lives have become more comfortable and convenient than ever before. We can use Yelp to find a popular restaurant, use Facebook to keep up with our friends, and use Google Map to find the way to a destination. When enjoying such personalized services, end-users need to provide service/application platforms with personal data, e.g., locations, weights, ages, and incomes. Unfortunately, there is a paradox between service quality and privacy protection level. On one hand, more personal data is needed if we ask for higher quality of service, resulting in that more private/sensitive information could be inferred from our submitted data. On the other hand, end-user’s privacy protection setting, and corresponding policies are influenced not only by platforms but also by adversaries because end-users' personal data may be revealed via data sell, malicious attacks. Users are suffering joint threats of privacy leakage from untrusted platforms as well as adversaries, which can be described in Figure 1.

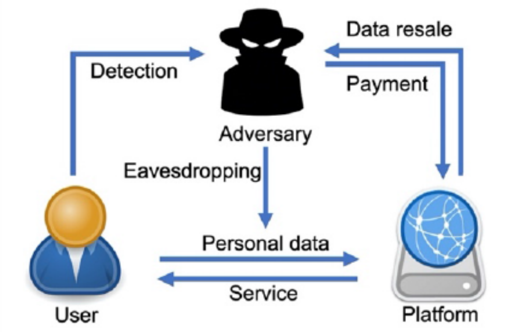


Figure 1. Structure of Three-Party Game Model

There is no doubt that, in the era of information, the collection and the use of personal data are major privacy concerns for end-users, and such concerns only grow over Figure 1. Structure of Three-Party Game Model time. Thus, the ongoing progress of context-aware services, the increasingly serious privacy leakage, and the growing privacy concern together make data privacy preservation imperative for users.

“Privacy Protection among Three Antithetic-Party for Context-Aware Service”

In the past years, privacy-preserving mechanisms have been paid a lot of attentions from researchers. Besides cryptography, game theory has been widely applied as a strategic methodology to search for optimal strategies balancing the trade-off between the benefit of sharing data and cost of privacy disclosure. Notice that most of the existing research only focuses on the interaction between two opposite parties, i.e., defender-attacker game model. In [1-5], various three-party game models are proposed. But, the game models of [1-5] are not “real”' three-party models because they fail to depict the interaction between any two of the three parties (i.e., they considered either data resale from platform or attack from adversary), and the schemes in [2-4] just figure out whether to defend (or cooperate with) opponents rather than showing the fine-grained strategy to defend (or cooperate with) opponents.

Furthermore, More and more applications are promoting customized or personalized services. In order for these applications to provide meaningful output, it collects users’ personal information over time. Some personal information (e.g. education level or income level) can only be captured by users actively updating their profile to reflect these changes, rather than the application being able to extract or infer the data. We refer to these as long-term time series data, as they do not change frequently. If applications are able to keep up to date on a diverse and large set of personal features, then it is better able to provide higher quality service. However, this quality of service comes at the cost of the user sacrificing their privacy. To set a proper privacy preservation level and corresponding privacy policies, there has been numerous researches on protecting privacy of time series data for context aware services, but these have mainly focused on short-term time series data (e.g. location, retail purchases, and activities). The privacy leakage of personal information updates during the whole lifecycle of the series has received only scant attention. More and more applications are promoting customized or personalized services. In order for these applications to provide meaningful output, it collects users’ personal information over time. Some personal information (e.g. education level or income level) can only be captured by users actively updating their profile to reflect these changes, rather than the application being able to extract or infer the data. We refer to these as long-term time series data, as they do not change frequently. If applications are able to keep up to date on a diverse and large set of personal features, then it is better able to provide higher quality service. However, this quality of service comes at the cost of the user sacrificing their privacy. To set a proper privacy preservation level and corresponding privacy policies, there has been numerous researches on protecting privacy of time series data for context aware services, but these have mainly focused on short-term time series data (e.g. location, retail purchases, and activities). The privacy leakage of personal information updates during the whole lifecycle of the series has received only scant attention.

Therefore, further exploring the mutual relationships among end-user, platform, and adversary would be more helpful for the end-users to defend both the untrusted platform and the adversary. For this purpose, we aim to design a three-party game among the three antithetic parties for end users to simultaneously resist untrusted service platforms and adversaries. Such practical and complicated game challenges us in the following aspects:

(i) **Complicated game structure.** As shown in Figure 1, the interaction occurs between any two of the three parties, increasing difficulty in addressing the three parties' different concerns -- how does the user assess the potential risk of privacy loss and determine the granularity when submitting personal data, how does the platform determine data resale with consideration of the risk of reputation loss, and how does the adversary make a choice between purchase and eavesdropping?

(ii) **Joint threats**. In such a complicated game, the user has to defend the joint threats from both the platform and the adversary, which may be hard to accomplish.

(iii) **Long-term data life cycle**. As shown in Figure 2, end-users’ information will change at different points in the long-term data life cycle, uploaded data will decay as time if no fresh data is updated.

(iv) **Theoretical analysis and solution.** Designing, analyzing, and solving the proposed three-party game are destined to be very difficult due to the complexity of the game structure, especially when the user's dataset contains multiple data attributes.

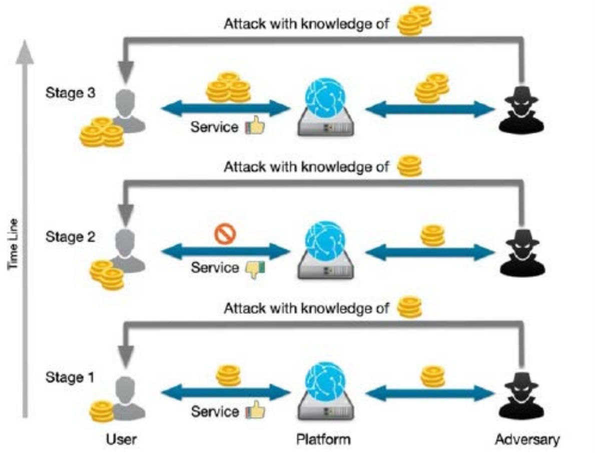


Figure 2. Long-term data updates with influence of services

“Privacy Protection among Three Antithetic-Party for Context-Aware Service”

Our research will endeavor on overcoming the above challenges is briefly introduced as follows. Firstly, in our game model, the three parties are linked by elaborately quantifying their concerns and mutual interactions such that they are inseparable. Secondly, based on our game model, a profound theoretical analysis will be performed to rigorously prove the optimal strategies of the three parties, including the optimal data release granularity for the end-user. Finally, simulations with real datasets will been well conducted under various settings to validate the effectiveness of our proposed game model.

Currently, we have proof the Nash Equilibrium exist in the general three party game scenario and also validate that with simulation results as shown in Figure 3. It shows how end-users and platforms utility change with their strategy changes. We can see that the optimal utility exists for both end-users and platforms. Therefore, the Nash Equilibrium exists in the proposed game model. In the future work, we want to improve the formulation accuracy and facticity of the interactions among three parties. Besides, we will dig into some real scenario to make the proposed framework more realistic and practical.

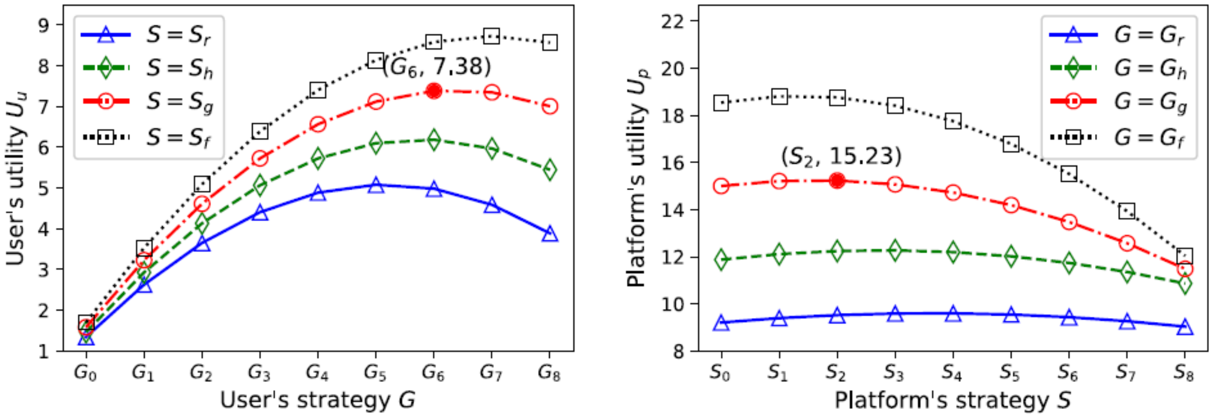


Figure 3. Strategy vs. Utility

References available on request

“Promoting Information Security Policy Compliance – An Action Research Enabled Empirical Study”

Lei Li, Ph.D., Professor and Assistant Chair, Department of Information Technology
Meng Han, Ph.D., Assistant Professor, Department of Information Technology

The widespread use of the technology has powered the economic growth and innovations in the world for the past decades. A side effect of the technology advancements is the exponential increase of cybercrimes. Hacks and data breaches have become daily news and the damages caused by those attacks have risen dramatically. It was estimated that the global cost of cybercrime for 2017 to be around $600 billion and by 2021 the figure will be $6 trillion per year (Security First 2019).

It has become increasingly important to protect organizations’ digital assets from cyber threats and attacks (Peltier 2016). One important component of an organization’s security program is the development of information security policy which defines a list of guidelines and rules an employee should follow in order to ensure the information security in an organization (Straub et al. 2008, Puhakainen and Siponen 2010). However, studies show that employees generally don’t take appropriate actions prescribed in the information security policy and often become the weakest link in information security (Puhakainen and Siponen 2010, Bulgurcu et al. 2010). Understanding why individuals in organizations engaging in insecure behavior has been become a major area in IS research (Moody et al. 2018).

There is a wealth of studies investigated the reasons behind individuals’ incompliance with information security policy (Puhakainen and Siponen 2010, Bulgurcu et al. 2010, Moody et al. 2018). Researchers draw theories from related disciplines such as criminology, psychology, social psychology and health psychology and developed more than ten different models to explain employees’ incompliant behaviors toward information security policy (Moody et al 2018). As illustrated in figure one, Moody et al. (2018) reviewed 11 theoretical models on information security policy compliance and proposed a unified model of information security compliance (UMISPC) which was supported by their empirical study.

Moody et al. (2018)’s study took the initial and important step on unified model for information security compliance research. Their study used three information security behavior identified by Siponen and Vance (2010) and the participants of their empirical study are from Finland. In their article, Moody et al. call for more study to empirically validate the UMISPC and examine other types of information security violation behaviors

"Promoting Information Security Policy Compliance – An Action Research Enabled Empirical Study"

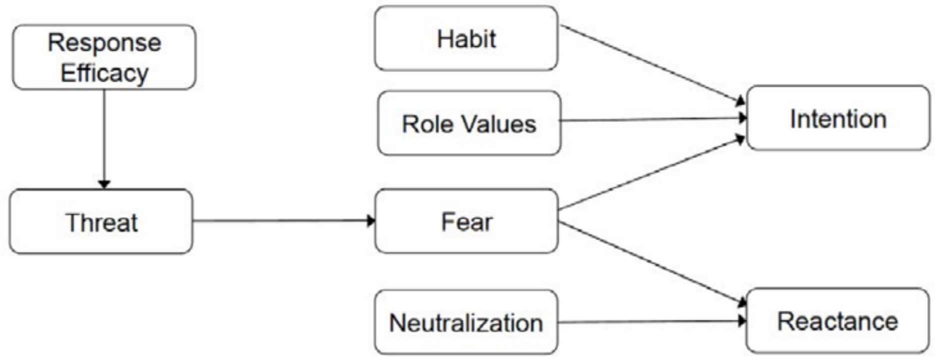


Figure 1. Unified Model of Information Security Policy Compliance (Moody et al. 2018)

There are many factors in an organization that could impact information security compliance, such as the industry the organization is in, the type and size of the organization, and management style and the culture of the organization, etc. A unified information security compliance model is still applicable as there are also many common attributes across organizations, and such a model can be easily adopted by industry practitioners. However, we argued that the most effective method in promoting security compliance in a given organization is an approach specifically designed for the organization. Action research, a clinical method that enables theory refinement in practice and solves organizational problems through research (Baskerville 1999, Baskerville and Myers 2004), is an ideal method for apply information security compliance theory/model in an organization. Grounded in action research and inspired by Moody et al. (2018)'s research, we propose a customizable framework for promoting information security compliance in a given organization (see figure 2).

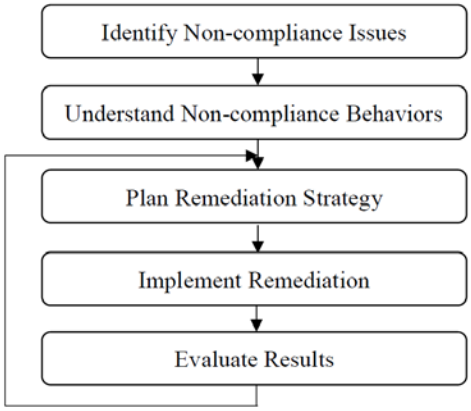

Identify Non-compliance Issues
Understand Non-compliance Behaviors
Plan Remediation Strategy
Implement Remediation
Evaluate Results

Figure 2. A Framework for Promoting Information Security Compliance

“Promoting Information Security Policy Compliance – An Action Research Enabled Empirical Study”

The proposed framework includes three major phases: 1) Identify the non-compliance issues; 2) Understand why non-compliance behavior; 3) Take a remediation action and evaluate the result. The remediation action may be repeated until desired outcomes are achieved. Survey will be used as the main method for data collection. Interviews and observation will be used as an additional means to collect data in phase three. The survey instrument and research methods are adopted from existing literature in information security compliance research.

Identify non-compliance issues. The objective of this phase is to identify the top three information security policy non-compliance issues in the participating organization. The personnel in charge of policy compliance will be interviewed and surveyed. The survey instrument is adapted from Siponen and Vance (2010) study.

Understand non-compliance behaviors. We propose to use UMISPC model (Moody et al. 2018) to understand the reasons behind employees’ non-compliance behavior. A questionnaire-based on Moody et al. (2018) will be developed and distributed to all employees in the participating organization. The top three non-compliance issues identified in phase one will be used to develop the security scenarios for the survey.

Remediation actions. Based on the discoveries in phase two, we will plan appropriate actions to remediate employees’ non-compliance. The actions could include revision of existing or creation of new security training, educational program or communication strategy. We will implement the remediation strategy and evaluate its effectiveness. Additional remediation actions may be needed based on the evaluation results of the first one. Puhakainen and Siponen (2010)’s research method will be adopted in this phase.

In the proposed framework, we adopt the proven theories and research methods from leading security policy researchers. The approach not only allows us to validate theoretical models in the field empirically, but also is highly effective in understanding and remediating security policy noncompliance issues for the participating organization. On the other hand, the customizable and action research nature of the proposed framework will require access to the participating organization. The whole process may take a longer time to implement and may not generalizable to other organizations.

References available on request