Dimitrios Damopoulos
Assistant Teaching Professor
Computer Science Department, Stevens Institute of Technology
mobile: +1 551 248 2004
email: ddamopou@stevens.edu

Research Statement

The evolution of cyber-attacks and malwares is a continuous race between intruders and defenders. Both parties use the same hardware, programming methods, tools, and resources to create either a ***smart*** *attack or to develop* ***intelligent*** *protection mechanisms.*

Mobile devices have evolved and experienced an immense popularity over the last decade. As a result, this growth has exposed mobile devices to an increasing number of security threats. Despite the variety of peripheral protection mechanisms described in the literature and the (post)authentication and access control techniques imposed by the Operating Systems (OS) of such devices, integral protection against advanced intrusions cannot be adequately enforced. More specifically, sophisticated and powerful OSs, such as Android and iOS, and the increasing amount of services they can support, provide new opportunities for attackers to compromise the device and the data stored on it.

This is along with the rise of mobile and IoT malware which is anticipated to comprise a serious threat in the near future. Therefore, the research community is constantly seeking solutions to cope with these newly-introduced perils. Thus, a need for more **intelligent** and **sophisticated** security controls, such as *Intrusion Detection and Prevention Systems (IDPS*), that rely on **Machine Learning** and **Deep Learning** are deemed necessary. However, whilst much work has been devoted to mobile device IDPSs in general, research on **anomaly-based** or **behavior-based** *IDPS* has been limited leaving several problems unsolved.

My five-year goal is to fundamentally enhance **Machine Learning**, **Deep Learning**, **Human & System-Behavio**r and **Cyber Security** systems into a synergetic approach, ensuring confidentiality, integrity, availability, and authenticity with new intelligent **embedded** and **ubiquities** systems. These systems will be capable to continuously **learn**, **adapt** and make **decisions** based on **personalized models**.

Background and Ongoing Research

My past and ongoing research combines the security of smartphones and the Internet of Things (IoT) with Data Mining (DM), Machine Learning (ML) and Deep Learning (DL) to build a behavior-based Intrusion Detection and Prevention Systems. My research interests focus on smartphone OS security, mobile device intrusion detection & prevention systems, smartphone malware and service attacks, mobile forensics, authentication, privacy, mobile applications and services development, among others.

The Best of Both Worlds: A Framework for the Synergistic Operation of Host and Cloud Anomaly-based IDS for Smartphones

This is the core of my research as it supports ***four detection mechanisms*** running both on **host** and **cloud** and facilitate ***synergy***. The framework focusses on ***anomaly-based*** intrusion detection systems (IDS) used primarily for malware detection and privacy invasive software. The framework aims to decouple the IDS from where it is hosted, enabling the "movement" of mechanisms from host to cloud and vice-versa transparently, and without any modifications to the IDS. This means that an IDS component will be able to operate autonomously on the device (e.g., for run-time protection or when connectivity issues occur), as well as with the assistance of the cloud for relieving the device from sophisticated, but computationally expensive operations.

Ideally, our solution would automatically decide where to deploy a particular IDS by balancing resource ***consumption*** and ***security requirements*** such as the time required to detect a threat. Policies regarding resource allocation could also be applied, such as if the phone is fully charged, we might decide to run more (multiple?) IDS on the device, and as the battery depletes offload them to the cloud.

More specifically, we show that by monitoring: i) ***user's touch patterns,*** and ii) ***behaviors*** as they utilize popular mobile ***applications or services*** (e.g., SMS, Call, Internet), and/or iii) by ***profiling native system calls*** produced by an active (running) service, one is able to design powerful ***intelligent*** mechanisms that can be very reliable and ***accurate in detecting malicious behavior*** produced by malwares or unauthorized device use.

We concentrated on how to understand, explore and present how novel mobile device security threats can be exploited to violate confidentiality, integrity, availability, authenticity and privacy requirements imposed by such devices. By attacking modern smartphone platforms and popular services and considering the different attack vectors, we created proper IDS mechanisms for modern mobile devices.

- We utilized the framework to develop an IDS that combines ***four diverse anomaly-based detection mechanisms***. The combination of diverse techniques provides protection against a broader set of attacks.
- Our prototype was evaluated along three main axes: overhead in terms of ***CPU load, memory*** and ***battery consumption***, and ***timeliness***, i.e., the time it takes for the IDS to respond to an attack. The results provided insights on the actual advantages and disadvantages of hosting a defense on the device or the cloud and can be used as a reference for future work.

Location-Enhanced Authentication Using the IoT

The most recent work goes beyond smartphones to build a security system utilizing the ***Internet of Things (IoT). User location*** can act as an additional ***factor of authentication*** in scenarios where physical presence is required, such as when making in-person purchases or unlocking a vehicle. This work proposes a novel approach for **estimating user location** and **modeling user movement** using the ***IoT***. The goal is to utilize its scale and diversity to estimate location more robustly than solutions based on smartphones alone and stop adversaries from using compromised user credentials (e.g., stolen keys, pass- words, etc.) when sufficient evidence physically locates them elsewhere. To locate users, we **leveraged the increasing number of IoT devices** carried and used by them and the smart environments that observe these devices. We also exploited the ability of many IoT devices to "sense" the user. To demonstrate our approach, we built a system called Icelus.

Hands-Free One-Time and Continuous Authentication Using Glass Wearable Devices

This work is just published and aims to utilize wearable devices to support users with ***limited use of their hands***. These users ***face challenges*** when ***authenticating*** with computer terminals, especially with publicly accessible terminals such as ATMs. When authentication through a password or PIN is possible, these users often choose a short "easy" combination due to the difficulties involved with entering lengthy convoluted passwords, subjecting them to greater security risks. Access tokens, like smartcards, can be helpful, however, they require that the user can physically handle such a token and custom reading sensor would need to be installed in access terminals. Similar authentication challenges are also present in environments where users need to frequently authenticate and log out or require ***hands-free authentication***, like in ***hospitals***.

A new glass wearable device was recently re-introduced by Google and it was immediately welcomed by groups of users, such as the ones described above, as Google Glass allows them to perform actions, like taking a photo, using only verbal commands. This work investigates whether ***glass wearable devices*** can be used to ***authenticate users***, both to grant access (***one-time***) and to maintain access (***continuous***), in similar hands-free fashion. We do so by designing and implementing ***Gauth***, a system that enables users to authenticate with a service simply by issuing a voice command, while facing the computer terminal they are going to use to access the service. We found that authenticating using Gauth takes on average 1.63 seconds, while using username/password credentials takes 3.85 seconds and varies greatly depending on the computer-literacy level of the user.

This work is timely given the importance of accessibility and accommodating the differently-abled.

Next Steps/Looking Forward

I am currently exploring a few select universities as I am seeking an environment where I can continue to move my research forward over the next decade or more. While I have a clear vision of the direction of my work, the research process is evolutionary in nature. Please find below next steps that I intend to take over the next year:

A Blockchain-Based Mechanism as a Means of Authentication for "Networks-of-Things"

The IoT is an impending technological revolution poised to have a tremendous impact on the way humans interact with everyday industrial, energy, and home automation systems. Initially used solely within industrial settings, the use of IoT introduces advantages that expand beyond the mere self-regulation of "smart things". Essentially, IoT systems include processes like i) accurate monitoring of a wide range of phenomena in the physical world, ii) the multilevel analysis of the produced raw data, and iii) the automatic generation of responses. Thus, it is not an exaggeration to claim that IoT will drastically alter our level of understanding of physical procedures, including what used to be closed-control systems and the way we interact with them.

This research concentrates on the design and development of novel mechanisms for validating the authenticity across networks of mobile IoT devices. My major contribution is the design and prototyping of a novel ***lightweight blockchain-based protocol*** that, unlike the conventional schemes, is completely independent of heavy cryptographic operations (e.g., PKI) thus enabling even the most ***resource-constrained of the IoT devices to participate*** in the scheme. Therefore, the proposed mechanism provides ***proof-of-membership*** and ***automated auditing***. It is application-agnostic and may be integrated into of different administrative domains, e.g., from simple SOHO environments to complex industrial networks, energy systems, and critical infrastructures.

Detection and Mitigation of IoT Botnets and DDoS attacks

Recently, the Mirai botnet ***crippled the normal functionality of a significant portion of the Internet*** by infecting ill-configured IoT devices. It is my belief that similar but more sophisticated attacks will harness the numbers of IoT devices and exploit their limited protection to unleash unprecedented Distributed Denial of Service attacks. I have begun to study the evolution of Mirai and Mirai-like botnets with the purpose of the ***timely detection of infection attempts*** against IoT devices utilizing behavior-based machine learning and deep learning models.

Privacy-Preserving Machine Learning

Machine learning, deep learning, and big data analytics boost the success of many services such as self-driving cars, automatic personal assistants, and healthcare informatics. To design intelligent system a huge amounts of data collection targeted for machine learning applications. My goal is to build a ***data sharing and machine learning scheme*** that processes data in a ***privacy preserving*** way. My aim is to design an IoT platform capable to securely share information with a cloud service via a ***Blockchain-based*** network, in order to make decisions related to the ***automobile and self-driving*** car ecosystem. The decisions will be made by a ***deep neural networks*** system that preserves the privacy of user.

Security and Privacy in Mobile Health

Access to healthcare is one of the major social and economic problems around the world, particularly in an aging society which often requires tremendous labor resources and expenses. With the boom of multi-functional wearable devices and the widespread use of smartphones, mobile health has been envisioned as a promising IT-supported paradigm to foster wide-spread healthcare quality. It integrates miniaturized ***wearable and in-body sensors,*** heterogeneous mobile communication networks, and powerful cloud servers to continuously monitor a patient's health conditions, remotely diagnose phenomena, and share health information in real-time.

However, mobile health raises critical ***security and privacy issues*** as highly sensitive health information is collected and users may have diverse security requirements. Users may also worry about their critical health data to be tampered when their health data are stored in powerful but untrusted cloud servers. In addition, the costs of security and privacy protections vary with users' diverse demands and may ***impact users' experiences in healthcare*** applications. A **Blockchain-based** system may be the solution to ensure that ***sensitive data related to health will remain secure*** and the ***user privacy*** will be protected.

Security Considerations for CyberPhysical Systems (CPS)

The revamped interest towards CPS through the proliferation of IoT technologies has rendered these systems a primary target of adversaries. Indeed, CPS and IoT appear to be fertile environments where attackers can gain access to large amounts of private information or disrupt the service of large organizations in multiple ways. This is possible primarily due to the fact that many of the involved ***technologies*** are still in ***embryonic stage***, relying on building blocks that were ***not always designed to perform in adversarial environments*** and thus are harboring known and ***unknown vulnerabilities*** and because the majority of IoT devices have ***limited resources*** which in turn limits their capacity to enforce comprehensive security measures.

The ultimate goal of this research effort is to improve the security and privacy assessments of the CPS building blocks, as well as commercial IoT products. My plan is to i) formulate and define of the ***aspects of a CPS vulnerability***; ii) understand the ***systemic vulnerabilities of popular technologies*** used in this sector across multiple layers by taking into consideration the different use-case scenarios; iii) examine the applicability of certain types of ***CPS security defenses and technologies*** in various use cases; and iv) ***define*** a set of quantitative and qualitative ***metrics*** that can be employed to model and describe the ***security and privacy guarantees of CPS***.

Design and Implement an All in One Security Processing Unit (SPU)

Over the last few years, the smartphone industry has seen an unprecedented focus on processing hardware. Modern smartphones are equipped not only with powerful multi-core primarily processors (CPU), but they are also supported by dedicated ***co-processors*** able to i) take the heavy demands of visual processing away from the CPU through dedicated graphics chips (GPUs), ii) process information gathered by the digital compass, accelerometer and gyroscope (Motion CPU), iii) encrypting and decrypting data, and iv) perform predictions utilizing machine learning as a processing core.

Although the ***effectiveness*** in identifying intrusions is one of the most critical metrics when designing and evaluating a security system, two other attributes that indicate how the system behaves during the detection phase are of equal importance. Specifically, the ***Performance*** and ***Timeliness*** metrics are directly associated with the effectiveness of any detection system with regard to ***real-time detection*** of intrusions before significant damage occurs. Due to the fact that software can be more easily compromised than hardware, having security processes executed by a co-processor will not only ***increase the security*** of the device, but ***real-time detection*** will be possible.

Implementing an ***All-in-One*** Security Processing Unit (SPU) will improve the performance and decrease the timeliness for CyberPhysical Systems (CPS). With the experience I have gained the past eight years by working with mobile devices and designing detection systems based on machine learning, along with the aforementioned research projects, I am confident I will achieve my ultimate goal of designing and building a ***Security Processing Unit (SPU***) capable of enhancing machine learning, deep learning, human & system-behavior and security systems into a **synergetic approach**. In this way, confidentiality, integrity, availability, and authenticity of new intelligent, embedded, and ubiquitous systems will be ensured, enabling them to continuously learn, adapt and make decisions based on automated personalized models.

Grant Proposals - Strategic Plan

I am currently working with other researchers to write grant proposals for the NFS and DARPA, for both research and teaching grants. In my new position, I plan to strategically apply for two or three grants utilizing the strong collaborations I have established over the past years.

Collaborations with Senior Faculty Members

- Dr. Constantinos Kolias Assistant Professor in the CS Department at University of Iowa and Lead Engineer for the Internet-of-Things Laboratory at NIST, MD, USA
- Dr. Susanne Wetzel Associate Professor in the CS Department at Stevens Institute of Technology.

Collaborations with High-Performing PhD Students:

> I have co-mentored Ms. Lefkothea Spilitopoulou towards her PhD since 2014. Ms. Spilitopoulou is a PhD student from the Aegean University in Greece. So far, we have published a research paper at a tier one conference, and we are currently working on two other papers. Her research area is related to policy-making, text mining, sentiment analysis.

Mentoring Plan for Research

I will actively recruit students of all levels and talented postdoctoral researchers who all are able to make their own contribution. My approach and background directly benefit students in the following ways:

1. Funding from my startup
2. Immediate access to ongoing research projects
3. Joint project creation for students, when appropriate
4. Mentorship in the paper-writing process
5. Access to PhD positions, postdoctoral positions, internships, via my international network of colleagues and affiliates

Mentoring Postdoctoral Researchers

During the first year of my appointment, I am planning to utilize my startup to recruit and mentor a strong postdoctoral researcher to assist me with preliminary experiments and grant proposal writing. My goal is to strike a balance between fostering postdoc-level independence, while also striving to support their growth and round out any gaps in their experiences, skills, or knowledge.

Mentoring Undergraduates

I intend to continue to collaborate with undergraduate students to actively contribute to research projects through independent studies or senior theses, with topics ranging from developing prototype implementations to assisting with theoretical development.

Mentoring PhD Students

Mentoring PhD students is a tremendous opportunity to have a significant impact on the career and academic success of a young researcher. I intend to create an interdisciplinary group of PhD students to collaborate on research and real-world applications across the disciplines.