Research Statement
Angelos Stavrou

I enjoy networking and systems research because of its experimental nature. Influenced by my Physics background, I am interested in applied research that involves the design, implementation and deployment of real-word, large-scale distributed systems. Such systems have many similarities with physics experiments: generating a model that describes the behavior and interactions of each individual component requires both extensive experimentation and theoretical modeling. This balance between modeling and experimentation is what I appreciate most about computer and network systems research.

Throughout my academic life, I have always preferred collaborating with other students and faculty, because research is more fun when sharing and arguing about one's ideas. I was lucky enough to have more than my fair share of colleagues and mentors that helped diversify my research, extending to areas beyond the immediate focus of my dissertation.

My thesis research is aimed at producing mechanisms that boost the security and resilience of distributed, large-scale systems. These systems are composed of large numbers of untrusted and unreliable components that communicate using the existing network infrastructure. Unfortunately, security mechanisms typically have a negative impact on the performance of a system, and some proposed techniques are not feasible because they represent a prohibitive cost. Exploring the tradeoffs between performance, usability and security is therefore of paramount importance. In my dissertation work, I proposed mechanisms that can protect a wide range of services while maintaining or even improving their performance characteristics, including end-to-end network latency and throughput.

1 Security Mechanisms For End-to-End Service Availability

Today’s Internet is clearly a successful communication vehicle providing connectivity for a wealth of ubiquitous and diverse services that are increasingly become part of our everyday life. My thesis addresses one of the main challenges that the Internet currently faces: ensuring service security and availability in a manner that is transparent to both the existing infrastructure and the end-users. To this end, I first developed PROOFS [1, 2], a system to alleviate disruption of availability of online objects due to Internet flash crowds. Flash crowds represent a sudden, unpredicted increase in demand of a web page or any other online object’s popularity, resulting in denial of service (DoS) experienced by end-users. PROOFS is a simple, lightweight peer-to-peer (P2P) system that uses randomized overlay construction and randomized, scoped searches to efficiently locate and deliver objects under heavy demand to all users that request them. PROOFS’ distributed nature takes advantage of the user’s bandwidth, transforming them into servers for the popular objects that have already received. Our approach does not depend on any network level or server side modifications. Unlike Bittorrent and other recent P2P distribution networks that focus solely on object dissemination, PROOFS offers distributed mechanisms to both locate and retrieve objects. Thus, it does not depend on the existence of a centralized, per object tracker to coordinate the download process among nodes. Maintaining a tracker for each web object requires resources making Bittorrent impractical for distribution of a large number of small files including web pages. For small files, locating the file is more crucial than its fast retrieval. In addition, unlike paid overlay distribution services such as Akamai, our system can scale without requiring extra resources or network presence and can operate in an extremely adverse environments. Moreover, we do not impose any economic burden on any of the protected sites, providing protection for even small sites.

However, PROOFS cannot be used when trusted or dynamic content (e.g., real-time communications) is involved. Furthermore, PROOFS cannot guarantee that a client will be able to obtain the latest version of the requested object without flooding the network. To improve network performance and to allow the protection of web services that offer dynamic or trusted content, we introduced WebSOS [3, 4]. WebSOS
was the first overlay-based architecture that enabled the protection of web servers that offer dynamic and trusted content against DoS attacks without any network requirements or modifications. Its design was based on the theoretical foundations laid by the Secure Overlay Services (SOS) work, but is geared toward web services. By filtering and dropping all connections toward the web server other than the ones originated from a very small set of overlay nodes, we managed to guarantee service availability even when the server was the victim of a DoS attack. One of our main contributions is complete transparency to the underlying network; creating an overlay of firewalls guarantees access to a web server for a large number of previously unknown users without requiring pre-existing trust relationships between users and the system. This was the first time that reverse Graphical Turing Tests were employed to thwart denial of service attacks by differentiating humans from malicious automated scripts (often referred to as “bots”).

With the MOVE [5] architecture, we further increased the attack and failure resilience of Internet services. When under attack, MOVE employs a lightweight process migration mechanism to relocate the service to another site informing the overlay of the new location. The migration is transparent to legitimate users because they use the overlay to reach the service. However, attackers are not aware of the new service location and thus they cannot disrupt the service. MOVE is the first truly End-to-End protection mechanism that can be deployed without relying on any network level support including firewalls and capacity reservation mechanisms. We deployed our prototypes on PlanetLab, a distributed network of nodes with global presence. We quickly realized that protection comes at a price: there was a significant end-to-end latency increase (by a factor of 2 or more) that was caused by packet indirection inside the overlay.

Although appropriate for web applications, WebSOS and MOVE cannot effectively protect time-critical or latency-dependent services, including Thin Clients and Voice over IP (VoIP) communications. Furthermore, we showed that all connection-oriented overlay-based systems that use connection state (i.e., all such mechanisms to date) are vulnerable to a new class of targeted DoS attacks. Our attacks exploit the fact that clients communicate with the service through a single, static connection with the overlay network. By severing that connection (e.g., through a targeted DoS attack), the user is forced to reconnect and re-authenticate, rendering the overall architecture impractical. To address all the latency issues and the new vulnerabilities, we proposed a stateless, spread-spectrum-like protocol that enhances the communication of the client with the overlay [6]. This novel approach allows the client to communicate with the end-server using multiple disjoint paths through the overlay, treating the overlay as a whole as a stateless pipe. The striking difference between this approach and the one used in WebSOS, MOVE, and other overlay-based networks, is the distribution of client traffic to all overlay nodes (and paths) instead of choosing individual paths per client. By taking advantage of multi-path and by aggressively using packet replication, we eliminate the latency overhead imposed by the overlay indirection. At the same time, we boost the resiliency of the system against failures and attacks that target the communication network, the overlay nodes or the end server itself.

2 Future Research Agenda

I would like to continue applying my experience in designing, implementing, testing and modeling of large complex systems beyond the scope of my dissertation. Applying my research results to wireless and sensor networks seems a natural next step; my approach is network-agnostic and thus can be adapted to protect all services deployed in a wireless or sensor network. Furthermore, modern networking systems still lack a comprehensive and unifying approach to deal with security and availability. In addition, legacy software and hardware systems are important and pervasive components of many networks. This reality makes it difficult to design and advocate solutions that ignore or fail to make use of current infrastructure. Having these limitations in mind, I would like to investigate further the following research areas.

Security through mixing of trusted and untrusted components. The security and resiliency of systems that are composed of a mixture of trusted (or controlled) and untrusted components has been the target of my recent research. There are numerous systems where such mixing can be used to prevent attacks
and faults from disrupting the normal operation of the system. For example, the presence of trusted nodes in swarming Bittorrent-like P2P distribution networks can prevent malicious participants from abusing the system for free file sharing. My preliminary work shows that even a small portion of trusted nodes can curb information leakage, which can lead to out-of-band file trading [7]. In general, analyzing the security and privacy properties of hybrid overlay networks where only a small fraction of the nodes are trusted is an exciting problem. Another potential application of this method can be in securing Inter-domain Internet routing: having a portion of routers that are trusted might be able to prevent BGP black-holing and illicit route announcement from propagating to the rest of the network.

**Behavioral profiling and detection of malware.** Malware is an emerging threat for network and host security. The increasing size, complexity and sophistication of malware, including botnets, spyware, and worms, has promoted them to an effective tool for profit-motivated online crime. Current methods dealing with bots and infected hosts seem crude and ineffective. I am interested in examining the inner structure of malware by examining their behavior. In [8], we present a logical progression in botnet evolution and future exploitation mechanisms.

**Application and network anonymity and Privacy.** Currently, operating systems and applications provide rudimentary support or mechanisms for data and user anonymity and privacy. The lack of such inherent mechanisms, combined with the ever increasing use of computing devices and services in our everyday life, will drastically increase demand for systems that provide anonymity and protect privacy. Furthermore, there is a new trend to use computers as thin clients, storing all user data to remote site locations or centralized servers. Moreover, email, blogs, documents and spreadsheets are among recent online services that utilize remote user data storage raising concerns about data privacy and anonymity. Our work on W3bcrypt [9] was a first exploration of the privacy concerns and possible approaches that can be used to address such problems.

**Security for mobile and wireless devices.** Mobile devices continuously evolve, becoming ever more pervasive and “smart”. Unfortunately, this has given rise to a new set of threats: cellphone viruses, cell hacking and hijacking are only the most visible. Providing security and at the same time preserving usability is very challenging. The majority of computer and network security mechanisms cannot be directly applied to mobile devices. Incorporating security to mobile and wireless devices is a very exciting research topic that I would like to pursue further in the future.

**Designing novel measurement methods and tools.** Experiments are a vital phase in the design and deployment of a distributed, large-scale system. The goal of an experiment is to measure the system’s characteristics. This requires precise and non-invasive measurement tools that need to be installed in as few machines as possible. To that end, I have developed a new single-end measurement tool for Internet path characterization called LinkWidth [10]. With this tool, we were able to determine the installed and available capacity of Internet paths, without requiring control of two endpoints on that path. As a next step, I would like to employ our tool to detect traffic congestion and infer path behavior under heavy load.

Given my expertise in building software systems, I believe that my current focus in security systems can be easily transposed to other research areas. I am eager to apply my system building methods to address interesting open problems through interdisciplinary collaboration.

**References**


