JOY ASICO

INTRODUCING

ANGELOS STAVROU

- Professor, George Mason University, 2017-2020
- Associate Professor, George Mason University, 2012-2017
- Assistant Professor, George Mason University, 2007-2012
- Ph.D., computer science, Columbia University, 2007
- M.S., electrical engineering, Columbia University, 2002
- M.S., algorithms, computability and logic, National University of Athens, 2001
- B.S, physics, University of Patras, 1997

NEW FACULTY MEMBER

Mounting a Large-Scale Cyberdefensive

Malicious agents can worm their way into vulnerabilities planted in a pre-installed app or remote access network, downloaded with new software, hidden in a regular update, and even built into the hardware itself. As we increasingly rely on connected systems in our daily life, cyberattacks are more critical and pervasive. Professor Angelos Stavrou, who recently joined ECE in Arlington, is investigating large-scale attacks that disrupt critical infrastructure—some of which play a crucial role in our everyday lives like the power system or water purification stations.

A co-founder of mobile security company Kryptowire and a George Mason University professor for more than a decade, Stavrou was drawn to Virginia Tech's ECE department because of its robust critical infrastructure programs. These include power systems, wireless and next generation communications, space science, civil engineering and other areas where security and reliability are crucial for their operations.

IN THE SUPPLY CHAIN

Some pernicious large-scale attacks have been propagated through weak points in the supply chain of a product. Android devices, for instance, are shipped to consumers with pre-installed privileged apps in their firmware that users cannot disable.

One of Stavrou's recent projects focused on the "alarming" number of Android firmware apps that contained privilege-escalation vulnerabilities. These allowed attackers to execute arbitrary commands, record the end-users through device audio and screen, and access personal data without the user's permission or knowledge.

To uncover these vulnerabilities, Stavrou and his team built a static and dynamic program analysis system that inspected Android firmware to expose unwanted functionality in pre-installed apps. Their system used context-sensitive, flow-sensitive, field-sensitive, and partially object-sensitive taint analysis among other binary analysis techniques affecting mobile and Internet of Things (IoT) devices produced globally.

"These are deeper attacks against a much broader slice of society—everyone who buys a particular product," explained Stavrou. "The problem is already there. It has been distributed to all of us. Then later, the attackers can pick and choose whom they want to target."

ON THE LARGE SCALE

Until recently, cyberattacks have not greatly disrupted critical infrastructure, said Stavrou. But that's starting to change. "We've seen attacks against the supply chain of popular software like SolarWinds that can affect power generation and water purification systems, power grids, and other systems that have a physical impact—not only on our quality of life, but on our lives themselves."

Stavrou's team is currently investigating techniques to combine technologies like 5G

and nextG communications with critical infrastructure systems like smart communities and power systems.

"High-capacity networks are bringing together systems that were never designed to be interconnected, are deeply embedded in critical infrastructures, and are equipped with low resources," said Stavrou. "But they need the connectivity. How can we make them work together without increasing security risks?"

To answer this, Stavrou is involved in a research project sponsored by the Defense Advanced Research Projects Agency (DARPA) called Open, Programmable, Secure 5G (OPS-5G). The project, which kicked off in October 2020, aims to develop a portable standards-compliant network stack for 5G mobile that is open source and secure by design.

"We want demonstrate how the next generation of 5G systems can be built with components that are not necessarily trustworthy," said Stavrou. "Using a plug-and-play zero-trust approach to software components, we can reduce reliance on untrusted technology sources."

The signature security advantage of open-source software is increased code visibility, explained Stavrou, meaning that code can be examined, analyzed, and audited by many people. In addition, the portability of open source decouples the hardware and software, making supply-chain attacks more difficult.

TOMORROW'S CYBERSECURITY EXPERTS

As technologies advance and expand, so too must our cybersecurity and our cybersecurity education, according to Stavrou.

"Our electrical and computer engineering students are in a good position to defend against evolving attacks because they are learning how to transcend the gap between software and hardware, and combine knowledge from more than one field," said Stavrou.

Between creating systems robust to cyberattacks and training students to carry on tomorrow's cybersecurity research, Stavrou is contributing to many aspects of our cybersecure future.

> "Our electrical and computer engineering students are in a good position to defend against evolving attacks because they are learning how to transcend the gap between software and hardware, and combine knowledge from more than one field,"
>
> –Angelos Stavrou