GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

Online and offline (data) privacy

by **Spiros Antonatos, Lead Engineer at Aegis Technologies, Singapore**

March 1st, 2021 16:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

We live in an era where almost everyone speaks about privacy or at least is aware of. The latest developments in GDPR and CCPA have raised the awareness of netizens and have sparked interesting discussions. But what does it really mean privacy? What are the elements that constitute our profile and how we can protect ourselves from revealing too much? In this presentation we will scratch the surface of what means online privacy and what constitutes data privacy (offline or on-the-fly anonymisation). We will give a walkthrough of the technologies involved and hopefully de-mystify some of the hypes around privacy.

Short Biography

Spiros Antonatos is currently a lead engineer at Aegis Technologies, a Singapore-based cybersecurity company. His role includes the research and development of high-scale threat intelligence products. Prior to that, he was a research manager at Tenable and before that he was a research scientist and manager at IBM Research – Dublin where he worked on security and privacy at scale. He was the Principal Investigator for intellectual property deals with external customers as well as internal joint programs, mostly in the healthcare and financial space. During his IBM tenure he authored 4 conference papers and 12 patents, was awarded an invention plateau for authoring 12 patents and received multiple achievements for his contributions to Watson Health and Truata (the first company worldwide to act as a GDPR data trust). During his 8-year experience at the Institute of Computer Science, Foundation for Research and Technology Hellas(FORTH), he has authored and co-authored 24 conference papers and 4 journal papers regarding Web security, privacy and anonymization issues and network monitoring. He has received his PhD from Computer Science Department, University of Crete.

GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

Baggy bounds checking: an efficient and backwards-compatible defense against out-of-bounds errors

by **Periklis Akriditis, CTO Niometrics, Singapore**

March 8th, 2021 16:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Attacks that exploit out-of-bounds errors in C and C++ programs are still prevalent despite many years of research on bounds checking. Previous backwards compatible bounds checking techniques, which can be applied to unmodified C and C++ programs, maintain a data structure with the bounds for each allocated object and perform lookups in this data structure to check if pointers remain within bounds. This data structure can grow large and the lookups are expensive.

In this work we present a backwards compatible bounds checking technique that substantially reduces performance overhead. The key insight is to constrain the sizes of allocated memory regions and their alignment to enable efficient bounds lookups and hence efficient bounds checks at runtime. Our technique has low overhead in practice—only 8% throughput decrease for Apache— and is more than two times faster than the fastest previous technique and about five times faster—using less memory—than recording object bounds using a splay tree.

Short Biography

Periklis serves as Niometrics' CTO, where he helped engineer key pieces of the company's technology stack to analyse one of the most voluminous data sources in our world today: the massive network-level information from telecommunications networks. Leading Niometrics' teams across all technology functions, Periklis is constantly looking for talented and like-minded systems engineers with a knack for high-performance, high-end hardware, and tough engineering challenges – solving the coding puzzle on our website is the fastest way to reach out to him directly.

Prior to Niometrics, Periklis was involved in research projects at the University of Cambridge, Microsoft Research Cambridge, and the Distributed Computing Systems (DCS) Lab of ICS/FORTH, with a focus on systems, network, and programming language security.

Periklis holds a PhD in Computer Science from the University of Cambridge, and a Master of Science and Bachelor in Computer Science from the University of Crete.

https://www.niometrics.com/niometrics-leadership/periklis-akritidis/

GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

SAuth: protecting user accounts from password database leaks

by **Elias Athanasopoulos, Assistant Professor, University of Cyprus**

March 10th, 2021 16:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Password-based authentication is the dominant form of access control in web services. Unfortunately, it proves to be more and more inadequate every year. Even if users choose long and complex passwords, vulnerabilities in the way they are managed by a service may leak them to an attacker. Recent incidents in popular services such as LinkedIn and Twitter demonstrate the impact that such an event could have. The use of one-way hash functions to mitigate the problem is countered by the evolution of hardware which enables powerful password-cracking platforms. In this work we propose SAuth, a protocol which employs authentication synergy among different services. Users wishing to access their account on service S will also have to authenticate for their account on service V, which acts as a vouching party. Both services S and V are regular sites visited by the user everyday (e.g., Twitter, Facebook, Gmail). Should an attacker acquire the password for service S he will be unable to log in unless he also compromises the password for service V and possibly more vouching services. SAuth is an extension and not a replacement of existing authentication methods. It operates one layer above without ties to a specific method, thus enabling different services to employ heterogeneous systems. Finally, we employ password decoys to protect users that share a password across services.

Short Biography

Elias Athanasopoulos is an assistant professor in Computer Science with the University of Cyprus. He received his BSc in Physics from the University of Athens and his Ph.D. in Computer Science from the University of Crete. Before joining University of Cyprus, he was an assistant professor with Vrije Universiteit Amsterdam. His research interests are systems security and privacy. Elias is a Microsoft Research PhD Scholar and he has interned with Microsoft Research in Cambridge. Elias is also a Marie Curie fellow with Columbia University and FORTH. He has several publications in IEEE Security and Privacy, ACM CCS, Usenix Security and ATC, NDSS, and EuroSys.

GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

A Retrospective on an Overlay-based DDoS Defense Mechanism

by **Angelos Keromytis, Professor, Georgia Tech**

March 22nd, 2021 17:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Denial of service (DoS) attacks continue to threaten the reliability of networking systems. Previous approaches for protecting networks from DoS attacks are reactive in that they wait for an attack to be launched before taking appropriate measures to protect the network. This leaves the door open for other attacks that use more sophisticated methods to mask their traffic. We propose an architecture called Secure Overlay Services (SOS) that proactively prevents DoS attacks, geared toward supporting Emergency Services or similar types of communication. The architecture is constructed using a combination of secure overlay tunneling, routing via consistent hashing, and filtering. We reduce the probability of successful attacks by (i) performing intensive filtering near protected network edges, pushing the attack point perimeter into the core of the network, where high-speed routers can handle the volume of attack traffic, and (ii) introducing randomness and anonymity into the architecture, making it difficult for an attacker to target nodes along the path to a specific SOS-protected destination. Using simple analytical models, we evaluate the likelihood that an attacker can successfully launch a DoS attack against an SOS-protected network. Our analysis demonstrates that such an architecture reduces the likelihood of a successful attack to minuscule levels.

Short Biography

Dr. Angelos D. Keromytis is Professor, John H. Weitnauer, Jr. Chair, and Georgia Research Alliance (GRA) Eminent Scholar at the Georgia Institute of Technology. His field of research is systems and network security, and applied cryptography. He came to Georgia Tech from DARPA, where he served as Program Manager in the Information Innovation Office (I2O) from 2014 to 2018. During that time, he initiated five major research initiatives in cybersecurity and managed a portfolio of nine programs, and supervised technology transitions and partnerships with numerous elements of the Department of Defense, the Intelligence Community, Law Enforcement, and other parts of the U.S. government. For his work, he received the DAPRA Superior Public Service Medal, and the Results Matter Award. Prior to DARPA, he served as Program Director with the Computer and Network Systems Division in the Directorate for Computer and Information Science & Engineering (CISE) at the National Science Foundation (NSF), where he co-managed the Secure and Trustworthy Cyberspace (SaTC) program and helped initiate a number of cross-disciplinary and public-private programs. Prior to his public service tour, Dr. Keromytis was a faculty member with the Department of Computer Science at Columbia University, where he founded the Network Security Lab. Dr. Keromytis is an elected Fellow of the ACM and the IEEE. He has 53 issued U.S. patents and over 250 refereed publications. His work has been cited over 20,000 times, with an h-index of 72 and i10-index of 229. He has founded two new technology ventures, StackSafe and Allure Security Technology. He received his Ph.D. (2001) and M.Sc. (1997) in Computer Science from the University of Pennsylvania, and his B.Sc. in Computer Science from the University of Crete, Greece. He is a certified PADI Master Instructor, with over 500 dives.

GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

Software Specialization for Attack Surface Reduction

by **Michalis Polychronakis, Associate Professor, Stony Brook University**

March 29th, 2021 16:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Attack surface reduction through the removal of unnecessary application features and code is a promising technique for improving security without incurring any additional overhead. In this talk I will present our work on software specialization, the goal of which is to restrict the operations an attacker can perform as part of vulnerability exploitation. Our techniques use various static code analysis techniques to remove code and functionality at the library, system call, and function level. I will present use cases of applying software specialization for server applications and Docker containers, demonstrating how restricting the operations an attacker can perform limits the capabilities of exploit code, and neutralizes Linux kernel vulnerabilities that could lead to privilege escalation attacks.

Short Biography

Michalis Polychronakis is an associate professor in the Computer Science Department at Stony Brook University. He received the B.Sc. ('03), M.Sc. ('05), and Ph.D. ('09) degrees in Computer Science from the University of Crete, Greece, while working as a research assistant in the Distributed Computing Systems Lab at FORTH-ICS. Before joining Stony Brook, he was an associate research scientist at Columbia University. His main research interests are in the areas of network and system security, network monitoring and measurement, and online privacy. He has published more than 100 peer-reviewed papers, many of them in top venues such as IEEE S&P, USENIX Security, ACM CCS, ISOC NDSS, EuroSys, and USENIX ATC, and is the recipient of the NSF CAREER Award (2018) and the DARPA Young Faculty Award (2018).

GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

Stop tracking me Bro!

Differential Tracking of User Demographics on Hyper-Partisan Websites

by **Panos Papadopoulos, Researcher, Telefonica Research**

April 19, 2021 16:00

https://zoom.us/j/95001863724?pwd=a3h1eitCMTJ5RGtEU3dTQ2haVlczQT09

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

Websites with hyper-partisan, left or right-leaning focus offer content that is typically biased towards the expectations of their target audience. Such content often polarizes users, who are repeatedly primed to specific (extreme) content, usually reflecting hard party lines on political and socio-economic topics. Though this polarization has been extensively studied with respect to content, it is still unknown how it associates with the online tracking experienced by browsing users, especially when they exhibit certain demographic characteristics. For example, it is unclear how such websites enable the ad-ecosystem to track users based on their gender or age. In this work, we take a first step to shed light and measure such potential differences in tracking imposed on users when visiting specific party-line's websites. For this, we design and deploy a methodology to systematically probe such websites and measure differences in user tracking. This methodology allows us to create user personas with specific attributes like gender and age and automate their browsing behavior in a consistent and repeatable manner. Thus, we systematically study how personas are being tracked by these websites and their third parties, especially if they exhibit particular demographic properties. Overall, we test 9 personas on 556 hyper-partisan websites and find that right-leaning websites tend to track users more intensely than left-leaning, depending on user demographics, using both cookies and cookie synchronization methods and leading to more costly delivered ads.

Short Biography

Panagiotis (Panos) Papadopoulos is a Research Scientist at Telefonica Research. Before that, he was a Security Researcher at Brave Software and a Assistant Researcher at FORTH-ICS, Greece. He holds a MSc and a Ph.D. in Computer Science from the University of Crete, Greece. His interests lie in the area of Network Privacy and Security, Transparency in Digital Advertising, and Fraud Detection. Results of his research have been published in top tier venues such as IEEE INFOCOM, ACM TOIT, USENIX NDSS, ACM WWW, ACM IMC, Springer ESORICS and more.