中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

Distinguished Lecture Series

Why has computer security failed to scale, and what we can do about it?

Wednesday, April 03, 2019 10:30am

Auditorium 106,
Institute of Information Science, Academia Sinica

Mr. Paul Kocher

Abstract

The costs of insecurity are growing rapidly, undermining the benefits of technological advances. In this talk, I will review several underlying trends and their implications for the future. Using my work on the Spectre vulnerability as example, I will explore how computer architectures and hardware implementations are particularly important, both as a source of risk and as an opportunity to implement effective security solutions.

To address these challenges, designers will increasingly need to address messy real-world problems, such as side channels and fault attacks. Likewise, security models need to reflect realistic assumptions about the fallibility of the humans who architect, implement, test, and administer systems. The cultural challenges ahead may be even more difficult than the technical ones, since today's companies and engineering leadership developed in an era where security was insignificant compared to the economic importance of performance gains. As a result, the transition to an environment where security risks dominate creates both major challenges and opportunities.

Biography

Paul Kocher is an entrepreneur and researcher focused on cryptography and data security. Areas of interest include trade-offs between complexity/performance and security, as well as how computer systems could be architected to reduce the likelihood and severity of exploitable security vulnerabilities. His technical work also includes discovering differential analysis, co-authoring the SSL/TLS v3 protocol, architecting numerous security hardware cores, and co-discovering the Spectre vulnerability.

Paul founded Cryptography Research in 1995 and grew the company organically until its acquisition by Rambus for $342M, then led the Cryptography Research division until 2017. Today, Paul is an advisor to Rambus and investor/advisor to a range of security-related start-ups. He is also a member of the U.S. National Academy of Engineering, a member of the National Academies' Forum on Cyber Resilience, a Fellow of the International Association for Cryptologic Research (IACR), and a frequent speaker on security topics.

For more information: http://www.iis.sinica.edu.tw/