CSDS 500 and ECSE 500
Fall 2020 Colloquium

11:30AM to 12:30PM
Tuesday, November 24, 2020

Zoom Webinar ID: 862 815 806
Passcode: 914464

"Next-generation Public Key Infrastructure (PKI): Goals, Solutions and Challenges"

Public Key Infrastructure (PKI) provides an essential foundation to applications of public key cryptography, and crucial for security in open networks and systems. Since its introduction in 1988, the PKI landscape was dominated by the X.509 standard, widely deployed by many protocols and systems, most notably TLS/SSL, used to secure connections between web server and browser.

Unfortunately, the web-PKI deployment has inherent weaknesses, and over the years, we have seen many failures of this trusted-CA approach. PKI failures allow attackers to issue fake certificates, launch website spoofing and man-in-the-middle attacks, possibly leading to identity theft, surveillance, compromises of personal and confidential information, and other serious security breaches.

These failures motivated efforts to develop and adopt next-generation, improved-security PKI schemes, i.e., PKI schemes that ensure security against corrupt CAs. During the recent years, there have been extensive efforts toward this goal by researchers, developers and the IETF. These efforts focus on additional security goals such as {\em transparency}, {\em non-equivocation}, {\em privacy} and more.

This talk will provide a concise review of this important area, and give the highlights of our research toward well-defined security goals for PKI schemes, and toward practical, efficient and yet provably-secure PKI schemes.

Some parts of the presentation would require basic understanding of applied crypto, mainly public-key cryptography, collision-resistant hashing, and Merkle trees.

Amir Herzberg, University of Connecticut

Dr. Herzberg's is the Comcast professor for Cybersecurity Innovation in the department of Computer Science and Engineering, University of Connecticut. His research areas include: network security (esp. routing/DNS/transport, Denial-of-Service, Web), privacy and anonymity, applied cryptography, usable security, security for cyber-physical systems, and social, economic and legal aspects of security.

Dr. Herzberg earned his Ph.D. in Computer Science in 1991 from the Technion in Israel. From 1991 to 1995, he worked at the IBM T.J. Watson Research Center, where he was a research staff member and the manager of the Network Security research group. From 1996 to 2000, Dr. Herzberg was the Manager of E-Business and Security Technologies at the IBM Haifa Research Lab. From 2002 to 2017, he was a professor in Bar Ilan University (Israel). Since 2017, he is professor at University of Connecticut.

Dr. Herzberg is the author of many papers in different areas of cybersecurity as well as 24 patents, and is now writing a textbook on cybersecurity (draft available online). He has served in numerous program committees and delivered multiple keynote and plenary talks in conferences, and served as program chair for IEEE CNS'19, editor of PoPETS and ACM TISSEC/TOPS. Dr. Herzberg is recipient of the Internet Society's Applied Networking Research award, 2017.

This is to certify that ______________________________attended this seminar. Certified by ______________________________.
Certificates of attendance and other evidence of CPD activity should be retained by the attendee for auditing purposes.

CASE SCHOOL
OF ENGINEERING
CASE WESTERN RESERVE
UNIVERSITY