Security Leaders to Convene at 20th Annual Network and Distributed System Security Symposium

Groundbreaking research on the latest security topics, including a security comparison of the top mobile platforms and the safe use of postMessage by popular websites

CISSP credentialed attendees eligible for continuing professional education credits

[Washington, D.C., and Geneva, Switzerland, XX February 2013] -- The Network and Distributed System Security (NDSS) Symposium, February 24-27 in San Diego, will bring together security researchers, technology experts, and practitioners from the private and public sectors who design, develop, exploit, and deploy the technologies that define network and distributed system security.

In its 20th year, NDSS will feature keynotes from industry leaders Joe Sullivan, Chief Security Officer, Facebook; Stephen Smalley, Trusted Systems Research Group, U.S. National Security Agency; and Richard Kemmerer, Computer Science Leadership Chair and Professor, University of California Santa Barbara. Attendees will also hear presentations of more than 50 solution-oriented scientific and technical papers, as well as debates on new and practical approaches to security problems.

Original paper presentations will cover a broad range of topics, including security and privacy of mobile devices, distributed systems and networks, web security and privacy, malware and spam, and intrusion detection and attack analysis. The paper titled "Comparison of Mobile Privacy Protection through Cross-platform Applications" features a security comparison between the two most popular mobile platforms. The authors investigated applications that run on both Android and iOS and examined the difference in usage of their security sensitive APIs (SS-APIs). Results of the analysis of over 2,600 applications will demonstrate how one platform's application vetting process was more effective, particularly in protecting sensitive resources from third-party applications.

Another paper, "The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites," will highlight a large-scale empirical study of how popular websites use the postMessage mechanism in HTML5. The authors collected postMessage receivers from the Alexa top 10,000 websites and studied how origin checks were performed. Attendees will hear how vulnerabilities were exposed and learn patterns for the safe use of postMessage.

The Internet Society is now an official CPE Submitter of the International Information Systems Security Certification Consortium, Inc., (ISC)²®. Security professionals holding the CISSP credential will be eligible for up to 24 continuing professional education credits for participating in NDSS 2013.

Organized by the Internet Society in cooperation with Usenix, the NDSS 2013 event is sponsored by Internet2, Qualcomm, FishNet Security, Afilias, the San Diego Supercomputer Center, Google, Microsoft Research, and IEEE Security & Privacy Magazine. Additional details are available at: http://www.internetsociety.org/ndss2013

About the Internet Society
The Internet Society is the trusted independent source for Internet information and thought leadership from around the world. With its principled vision and substantial technological foundation, the Internet Society promotes open dialogue on Internet policy, technology, and future development among users, companies, governments, and other organizations. Working with its members and Chapters around the world, the Internet Society enables the continued evolution and growth of the Internet for everyone. For more information, visit www.internetsociety.org

Media Contact: Wende Cover, cover@isoc.org, +1-703-439-2773