Topic Area: Transparency and alternative certification, distribution or confirmation of key information

Authors: Ms. Alexandra Grant, Dr. Charles Palmer, Dartmouth College

Title: The Search for Trust

Abstract:
The security of the broadly deployed and universally relied upon X.509 Public Key Infrastructure for browsers and SSL web servers has come under scrutiny in response to Certification Authority (CA) compromises in the recent past. These compromises resulted in the circulation of fraudulent certificates which could and have been used to execute Man-in-the-Middle attacks and gain access to users' sensitive information. In wake of these events, the focus of online security professionals has turned to enhancing the current Internet PKI system, as a flurry of proposals to replace the system altogether have also emerged. The primary goal of such efforts is to aid in the prevention and detection of MITM attacks and improve the trust infrastructure for online users. This presentation will provide details of on-going a research from Dartmouth College that lays the foundation for evaluating the primary proposed technologies by defining new metrics that rank each proposal according to a set of well-identified criteria. The proposals evaluated by the research to date include: Certificate Transparency, Public Key Pinning or HTTP Strict Transport Security (HSTS) pinning, CAA Records in DNSSEC, DNS-Based Authentication of Named Entities (DANE), Perspectives, Convergence, Mutually Endorsed Certificate Authority Infrastructure (MECAI), and Sovereign Keys. Building upon Dartmouth's ranking system, this presentation will highlight which of the proposals found to warrant further discussion, and will consider the potential strengths and weaknesses of their design. A practical review of what each of these systems might provide for future online trust – systems which are delineated by the Internet Engineering Task Force (IETF) in RFCs or drafts – will be presented.

Thanks,
Charles

CTO Security & Privacy, IBM Research
Member, IBM Academy of Technology
M: 914-954-2466
Twitter: @DrCyberSecurity
http://researcher.ibm.com/person/us-ccpalmer