Emerging Technology Space: Transparency and alternative certification, distribution or confirmation of key information

Speaker: Joseph Bonneau, Google

Title: Transport Security Policies: A broad framework for new proposals in server trust on the web

Abstract: Several protocols are emerging which allow servers to declare "Transport Security Policies" defining the conditions under which clients should trust a connection to them. Traditionally, all sites on the Internet inherited the default HTTPS security policy, allowing them to present certificates from any of a wide range of public CAs. New protocols allow servers to replace this permissive default policy with more restrictive and secure "TSPs" such as HSTS ("disallow non-TLS connections"), "pinning" (specifying additional constraints on the certificate chains), or opting-in to new trust signals such as Certificate Transparency or DNSSEC. Several languages are being developed to allow servers to assert these choices via DNS assertions or HTTP headers (e.g. DANE, HPKP, TACK). Infrastructure is also being developed to securely transport TSPs to clients (e.g. TSP discovery during web browsing, delivery via "preloaded" trust lists and introduction via secure links). The TSP framework clarifies the relationships between these new protocols, points out how they share common challenges in reliability and efficiency, and highlights the importance of designing new primitives to to work together in a holistic TSP infrastructure. It also points out common challenges within the browser security model to deploying and managing TSPs.