



Scientific Discoveries and Accomplishments

CyLab Researcher Adrian Perrig

Securing SSL/TLS/SSH communication: Perspectives Project

Perspectives helps users detect attacks in protocols that use the "Trust-on-first-use" model commonly associated with SSH and HTTPS with self-signed certificates. Widespread use of "Trust-on-first-use" (tofu) host authentication, most commonly associated with protocols like SSH and SSL with self-signed certificates, demonstrates significant demand for a host authentication mechanism that is low-cost and easy to deploy. While tofu applications are a clear improvement compared to completely insecure protocols, they can leave users vulnerable to even simple network attacks. Our system, Perspectives, thwarts such attacks using a network overlay that observes a server's public key via multiple network vantage points (detecting localized attacks) and keeps a record of the server's key over time (recognizing short-lived attacks). Clients that receive an unauthenticated key can contact this overlay and check the key against these records, detecting many common attacks. The Perspectives design explores a promising part of the host authentication design space: tofu applications gain significant attack robustness while retaining the basic ease-of-use that makes "Trust-on-first-use" so popular. We present a full network overlay and client design, analyze the security provided by the system, and describe our experience building and deploying a publicly available implementation.

Secure Computing on Untrusted Computer Systems: The SecVisior Proect

Computer systems are under attack from increasingly sophisticated malware, which operate stealthily and selectively target sensitive information such as passwords and financial data. Defenses, such as anti-virus scanners, are unable to cope with such malware. The situation makes it difficult to say with confidence that any given computing device is not compromised by malware. We made significant progress towards securely on malware compromised computing devices through our SecVisior project. SecVisior is a tiny hypervisor that guarantees code integrity for commodity OS kernels over the system lifetime. The attacker can control all hardware and software on the system, other than the CPU, the memory controller, and the memory chips, and can have the knowledge of zero-day kernel exploits. SecVisior defends against a wide variety of attacks including several kinds of kernel rootkits, hardware-based DMA attacks, and code injection via kernel buffer overflow exploits. Further, its small code size makes SecVisior amenable to formal verification and manual code audit.

Message in a Bottle (MiB) System

Existing protocols for secure key establishment all rely on an unspecified mechanism for initially deploying secrets to sensor nodes. However, no commercially viable and secure mechanism exists for initial setup. Without a guarantee of secure key deployment, the traffic over a sensor network cannot be presumed secure. To address this problem, we developed the Message-in-a-Bottle (MiB) system, a user-friendly protocol for the secure deployment of cryptographic keys in sensor networks. We propose a collection of five techniques to prevent an attacker from eavesdropping on key deployment. To demonstrate feasibility for real-world use, we implement our protocol on Telos motes and conduct a user study.