Review “Unicorn”

Name: Wenhui Zhang

Paper Name :

Mannan, M., Kim, B. H., Ganjali, A., & Lie, D. (2011, October). Unicorn: two-factor attestation for data security. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 17-28). ACM.

Contribution:

This paper implemented a Unicorn prototype using commodity software and hardware, and two Unicorn example applications (termed as uApps, short for Unicorn Applications), to secure access to both remote data services and encrypted local data. Each uApp consists of a small, hardened and immutable OS image, and a single application.

Unicorn prototype co-exists with a regular user OS, and significantly reduces the time to switch between the secure environment and general purpose environment using a novel mechanism that removes the BIOS from the switch time.

Motivation:

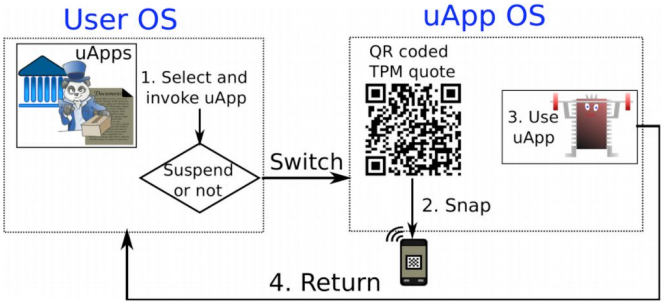
Phishing, malware, and malicious users leads to a need for a protection system that guarantees security policies. Phishing solved by token, malwares are solved by TPM.

Related works:

Secure kiosk computing [Garriss et al.]; Lockdown is a small hypervisor that provides one environment for regular tasks and another for all sensitive web transactions; Bumpy [21] is designed to secure sensitive user inputs (e.g., online passwords), by processing them in a separate Flicker [20] module, which can be loaded ondemand bypassing the untrusted user OS; Immutability of uApps images is similar to the root of trust installation (ROTI) system; Terra enables users to simultaneously use open-box VMs (with a commodity OS and user applications) and closed-box VMs.

Methodology:

Unicorn combines tokens with TPM. It uses a token to verify attestation and prevent phishing. The Personal Security Device holds authentication credentials that only released when passed attestation. Unicorn apps are called uApps. Control is transferred to trusted, closed uApps.



Results:

About 25s of overhead.

Take away:

Won’t be able to detect runtime vulnerabilities, has to preassign accounts and such.