Using Secure Coprocessors

Bennet Yee

May 1994
CMU-CS-94-149

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Thesis Committee:
Doug Tygar, Chair
Rick Rashid
M. Satyanarayanan
Steve White, IBM Research

Keywords: authentication, coprocessor, cryptography, integrity, privacy, security

Abstract

How do we build distributed systems that are secure? Cryptographic techniques can be used to secure the communications between physically separated systems, but this is not enough: we must be able to guarantee the privacy of the cryptographic keys and the integrity of the cryptographic functions, in addition to the integrity of the security kernel and access control databases we have on the machines. Physical security is a central assumption upon which secure distributed systems are built; without this foundation even the best cryptosystem or the most secure kernel will crumble. In this thesis, I address the distributed security problem by proposing the addition of a small, physically secure hardware module, a *secure coprocessor*, to standard workstations and PCs. My central axiom is that secure coprocessors are able to maintain the privacy of the data they process.

This thesis attacks the distributed security problem from multiple sides. First, I analyze the security properties of existing system components, both at the hardware and software level. Second, I demonstrate how physical security requirements may be isolated to the secure coprocessor, and showed how security properties may be bootstrapped using cryptographic techniques from this central nucleus of security within a combined hardware/software architecture. Such isolation has practical advantages: the nucleus of security-relevant modules provide additional separation of concern between functional requirements and security requirement, and the security modules are more centralized and their properties more easily scrutinized. Third, I demonstrate the feasibility of the secure coprocessor approach, and report on my implementation of this combined architecture on top of prototype hardware. Fourth, I design, analyze, implement, and measure performance of cryptographic protocols with super-exponential security for zero-knowledge authentication and key exchange. These protocols are suitable for use in security critical environments. Last, I show how secure coprocessors may be used in a fault-tolerant manner while still maintaining their strong privacy guarantees.

Contents

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.