Twizzler-Security
A Capability-Based Security System for Twizzler

BSc Thesis

written by

Surendra Jammishetti

under the supervision of **Owen B. Arden**, and submitted to the

Examinations Board in partial fulfilment of the requirements for the degree of

Computer Engineering B.S.

at the *University of California, Santa Cruz.*

Date of the public defence:	**Members of the Thesis Committee:**
August 28, 2005	Dr. Peter Alvaro
	Dr. Andi Quinn

Abstract

whatevea lowkey not even sure what to write Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

Contents

Chapter 1

Introduction

In mainstream operating systems, security policy is enforced at runtime by a omnicient and all powerful kernel. It acts as the bodyguard, holding all i/o and data protected unless the requesting party has the authorization to access some resource. This tight coupling of security policy and access mechanisms works great since the kernel is always **there** and the only way to access anything through it. However the enforcement of security policy starts getting complicated when we try to seperate the access mechanisms from the kernel.

1.1 Data Centric Operating Systems

Data centric operating systems are defined by two principles [Bit+20]:

1. Provide direct, kernel-free, access to data.
2. A notion of pointers that are tied to the data they represent.

Mainstream operating systems fail to classify as data-centric operating systems, as they rely on the kernel for all data access, and use virtualized pointers per process to represent underlying data. The benefit of this "class" of operating systems comes from the low overhead for data manipulation, due to the lack of kernel involvement. However our previous security model fails to operate here as, by defenition, the kernel cannot be infront of accesses to data.

1.2 Capability Based Security Systems

Capability based security systems utilize capabilities, a finegrained

1.3 Our Contributions

Chapter 2

Key Pairs

2.1 Abstraction

2.2 Compartmentalization

Chapter 3

Capabilities

3.1 Gates

3.2 Flags

3.3 Signature

Chapter 4

Security Contexts

4.1 Map

Chapter 5

Results

Chapter 6

Conclusion

Bibliography

[Bit+20] Bittman D, Alvaro P, Mehra P, Long DDE, Miller EL. Twizzler: a Data-Centric OS for Non-Volatile Memory. In:. 2020 USENIX Annual Technical Conference (USENIX ATC 20), USENIX Association; 2020, pp. 65–80.