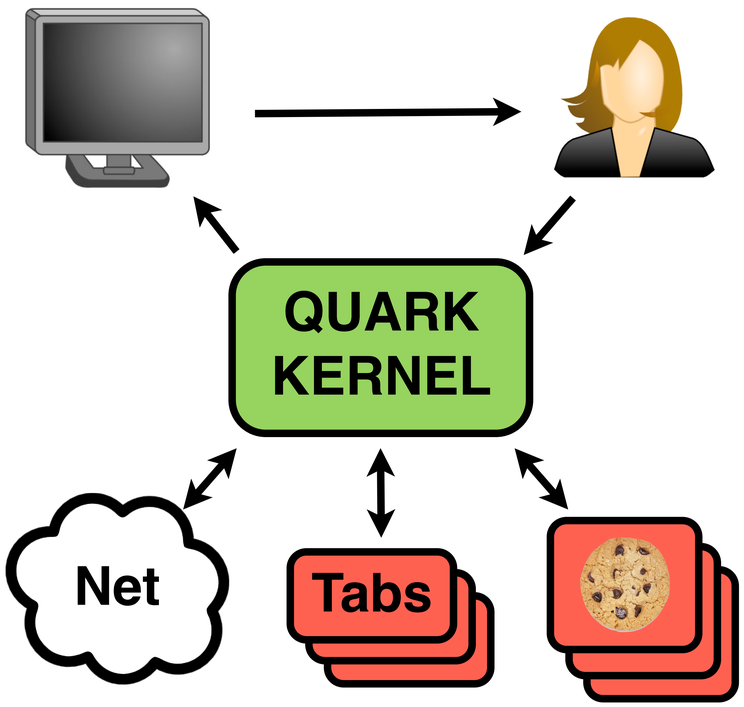
QUARK: Formally Verified Web Browser

Zachary Tatlock, Dongseok Jang, Sorin Lerner

Design



Privilege Separation

Components run with minimal privilege

Sandbox complex, vulnerable parts (■)

Impl. and verify trusted kernel in Coq (■)

Simple Interfaces

Kernel orchestrates messaging over pipes

Components access resources via kernel

Simple kernel; state-of-the-art tabs (WebKit)

Shim Verification

Kernel as Restrictive Wrapper

Guarantee behavior of entire system

Only reason about tiny fraction of code

*Thin **shim** restricts even exploited components to only approved actions*

Enables us to use off-the-shelf rendering engine

Trace Based Reasoning

Formalize behavior as seq of syscalls

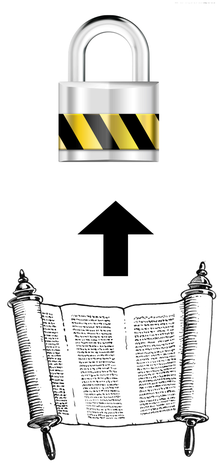
Chain of recv / send to process messages

Security Guarantees

Tab Isolation

Cookie Integrity

Address Bar Integrity



Specification

Enum. valid exchanges

Abstract impl. details

Implementation

Message exchange

Resource management

Written in Coq + YNot

QUARK KERNEL

Evaluation

Verification Effort

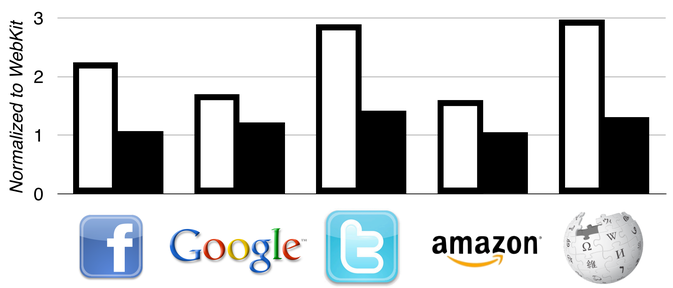
165 lines sec. props

4k line Coq proof

Spec eases mods

Base for new policies

Performance



Optimizations reduce overhead to 20%

Robustness

Support rich apps:

Gmail by Google

Google maps

YAHOO! FINANCE

ebay