Hardware, Languages, and Architectures for Defense Against Hostile Operating Systems (DHOSA)

Vikram Adve, Krste Asanović, David Evans, Sam King, Greg Morrisett, R. Sekar, Dawn Song, David Wagner (PI)

http://www.dhosa.org/

The Problem

Can we defend applications from buggy and even malicious host operating systems?

- OS's contain ~50M lines of code.
  1 bug/Kloc $\Rightarrow$ ~50K bugs?

Reality: must assume OS will be compromised.

Exploring New Territory

- Conventional wisdom: If the OS is malicious or subverted, you are hosed.
- Our goal: Survive a malicious OS, perhaps with degraded functionality or availability.

The Approach

Advances that cut across traditional disciplines:

- new hardware architectures
- new techniques for binary rewriting
- new OS and software architectures
- new advances in formal methods
- new cryptographic techniques

Vikram Adve
(UIUC)

Krste Asanović
(UC Berkeley)

David Evans
(U Virginia)

Sam King
(UIUC)

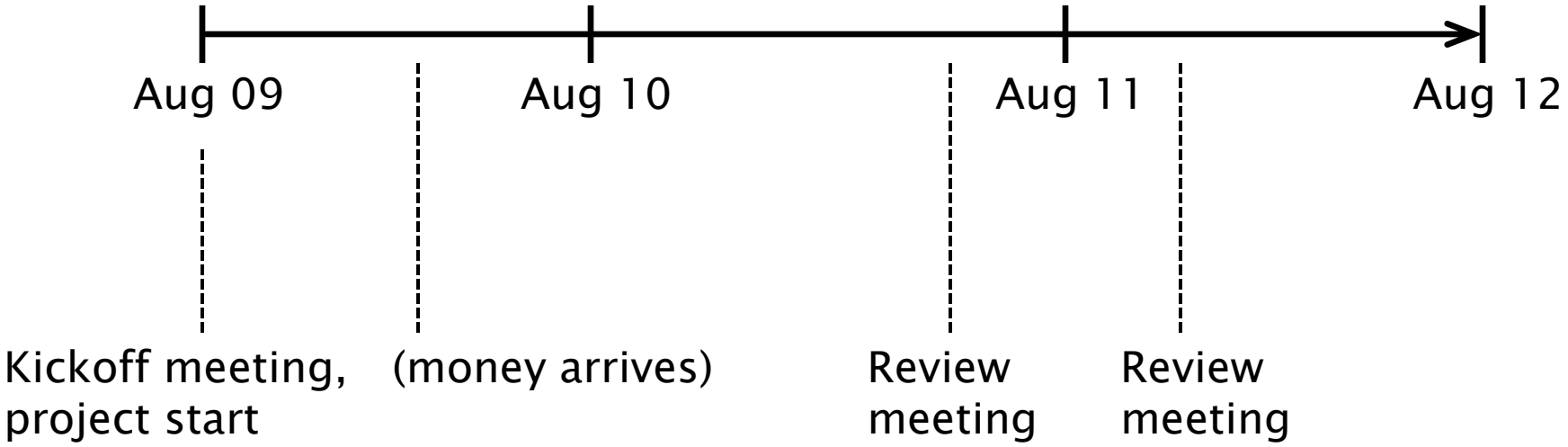
Greg Morrisett
(Harvard)

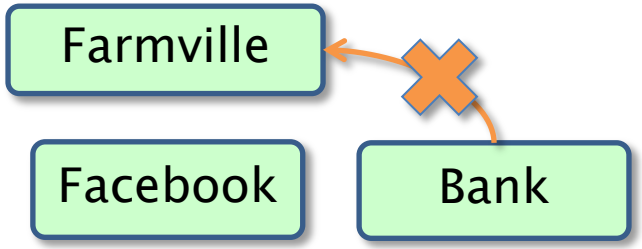
R. Sekar
(Stony Brook)

Dawn Song
(UC Berkeley)

David Wagner
(UC Berkeley)

Timeline


Aug 09
Aug 10
Aug 11
Aug 12
Kickoff meeting, project start
(money arrives)
Review meeting
Review meeting



What must you trust to prevent unwanted flows?

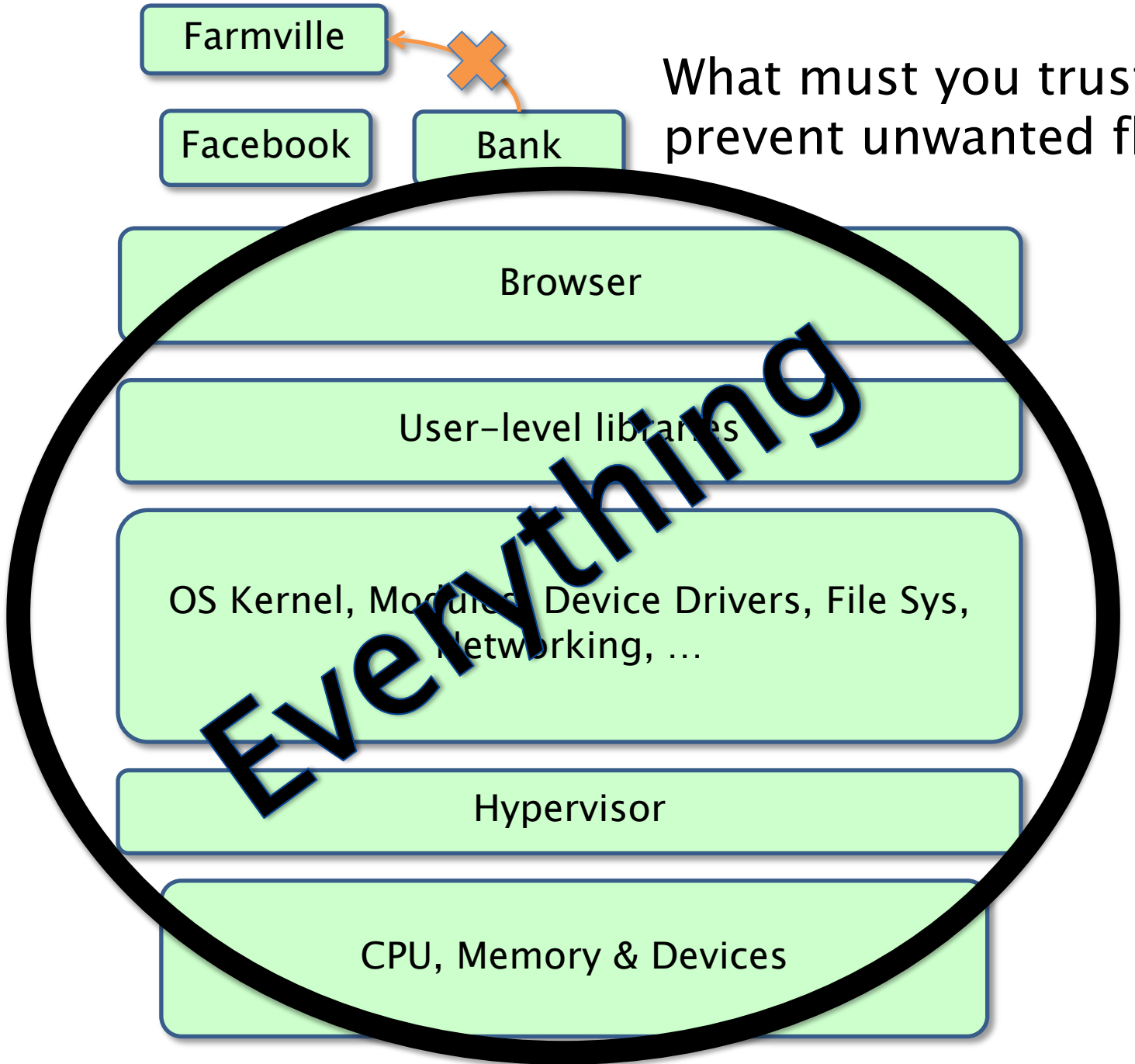
Browser

User-level libraries

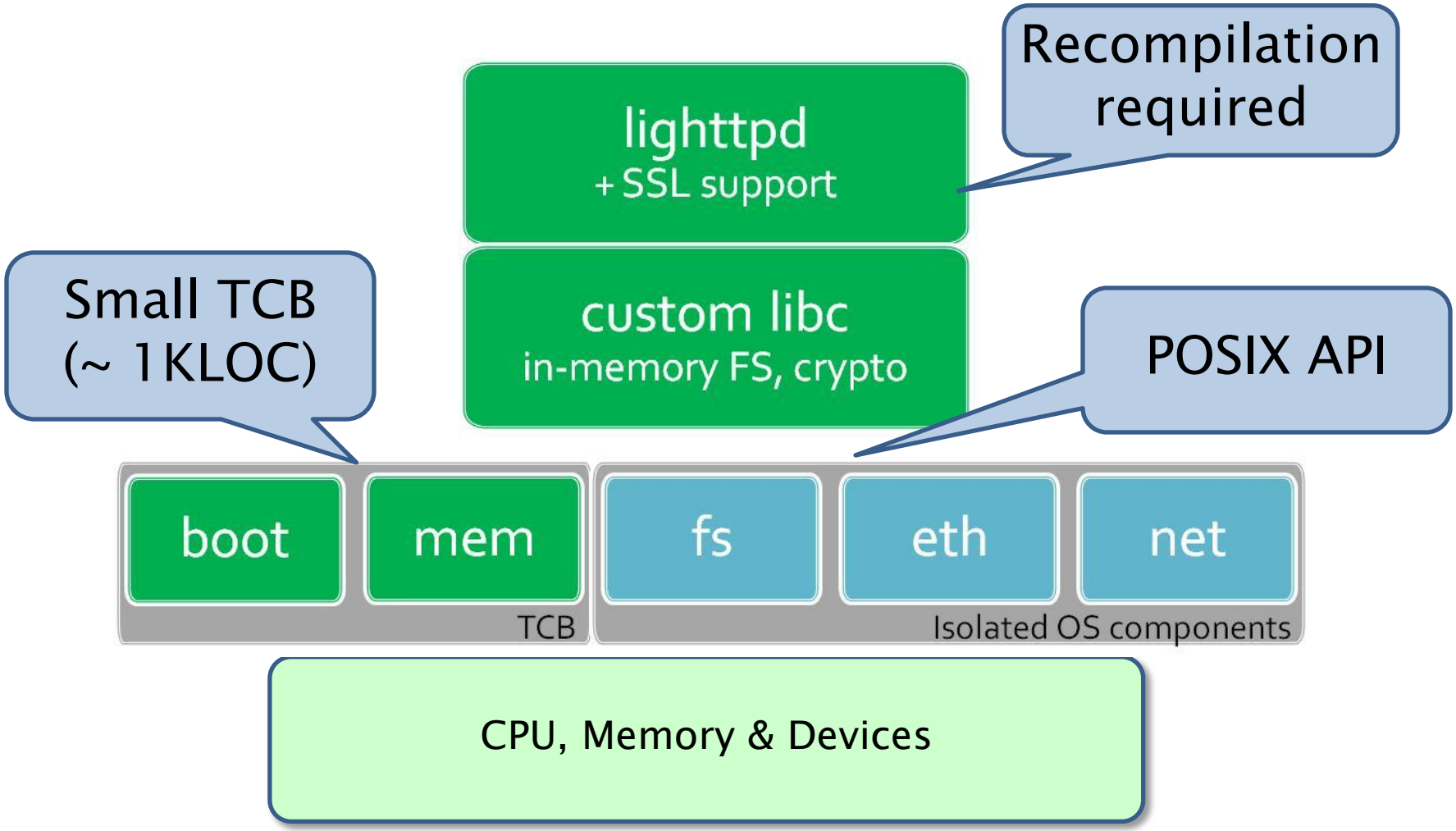
OS Kernel, Modules, Device Drivers, File Sys, Networking, …

Hypervisor

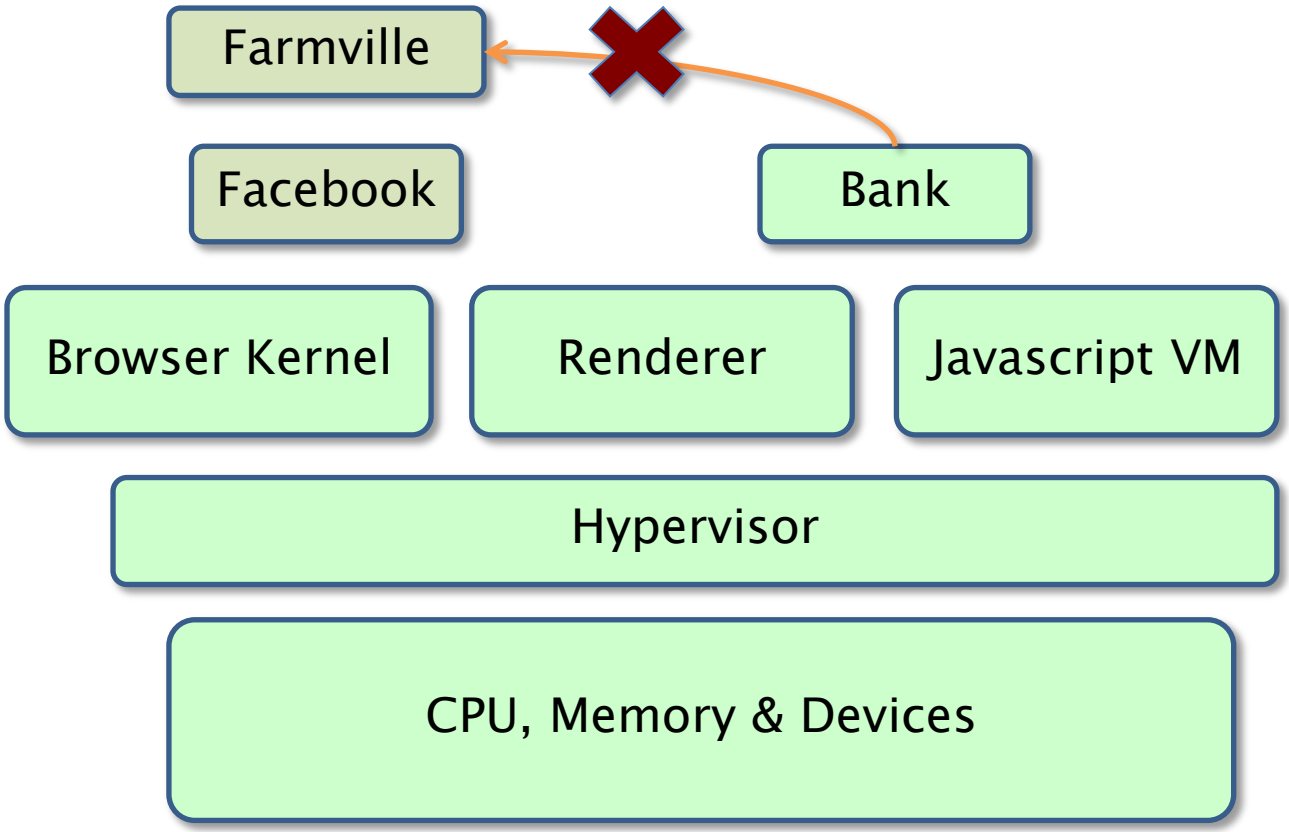
CPU, Memory & Devices


Farmville
Facebook
Bank
What must you trust to prevent unwanted flows?
Browser
User-level libraries
OS Kernel, Modules, Device Drivers, File Sys, Networking, …
Hypervisor
CPU, Memory & Devices
Everything

An alternative world?



Another alternative world?

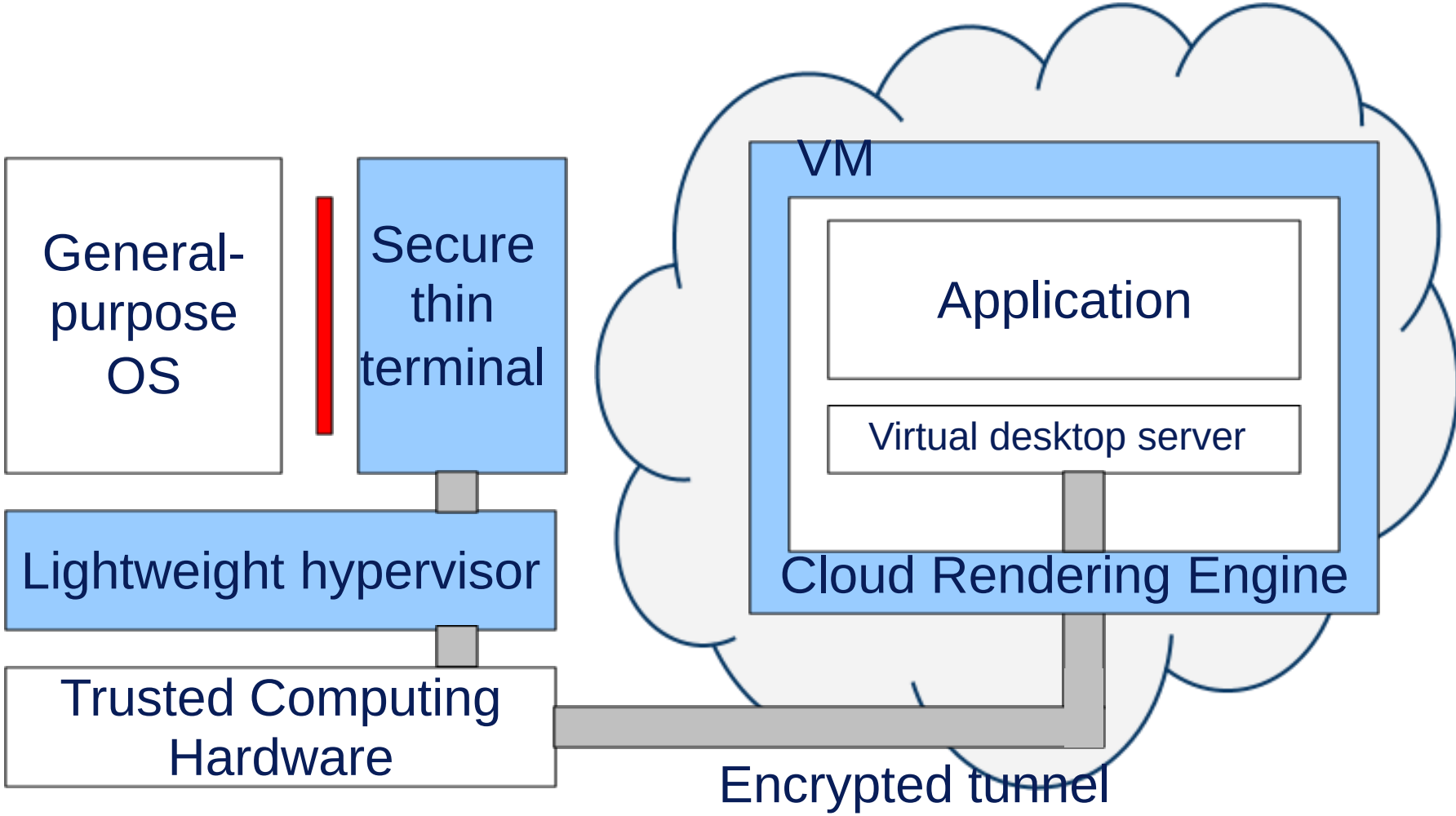


Illinois Browser Operating System (IBOS)

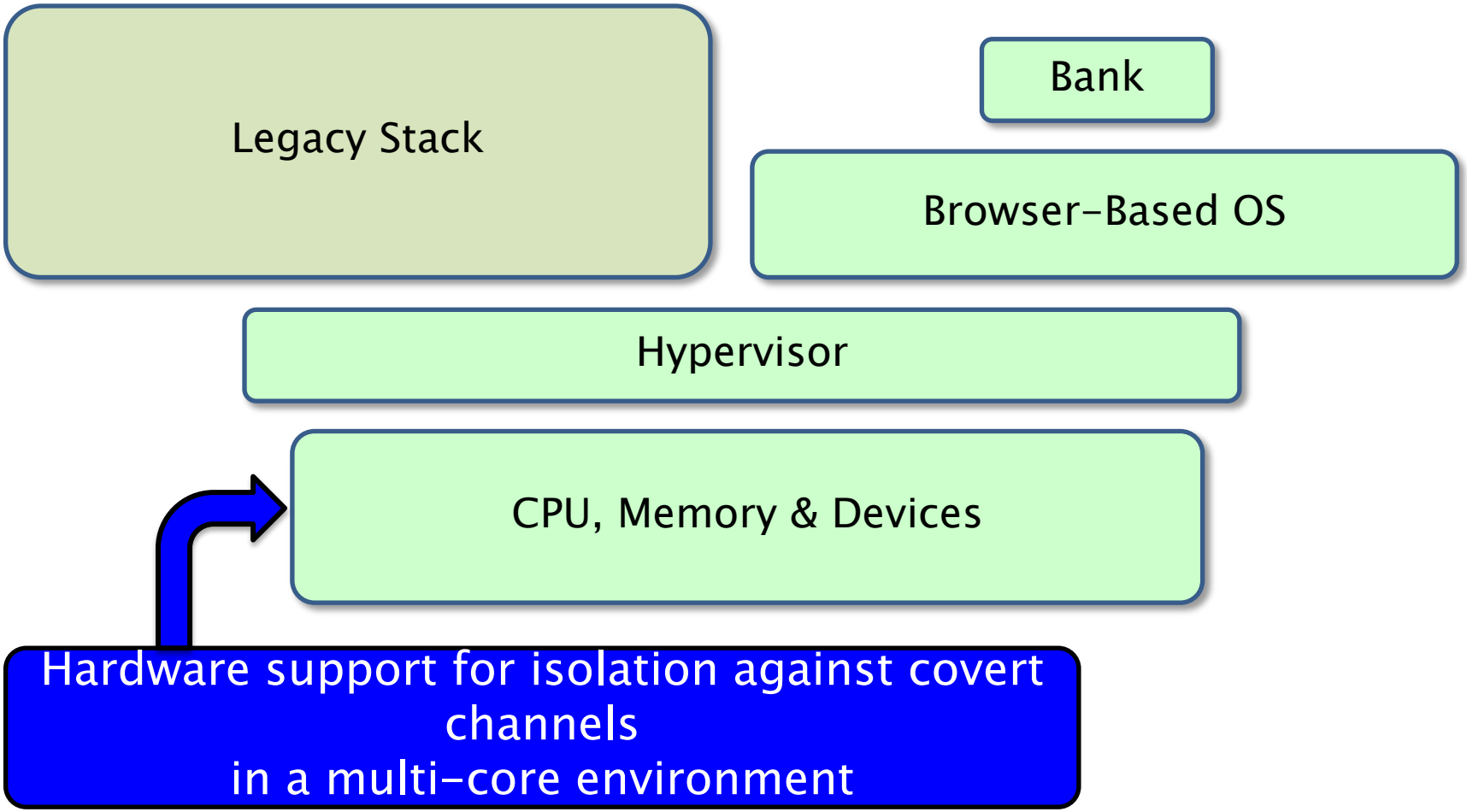
Data-centric Security

- Protect the data directly instead of network or host-based protection
- Three examples:
  - Cloud-terminal: providing trusted input/output
  - Platform for private data
  - Secure web applications: Guardrails

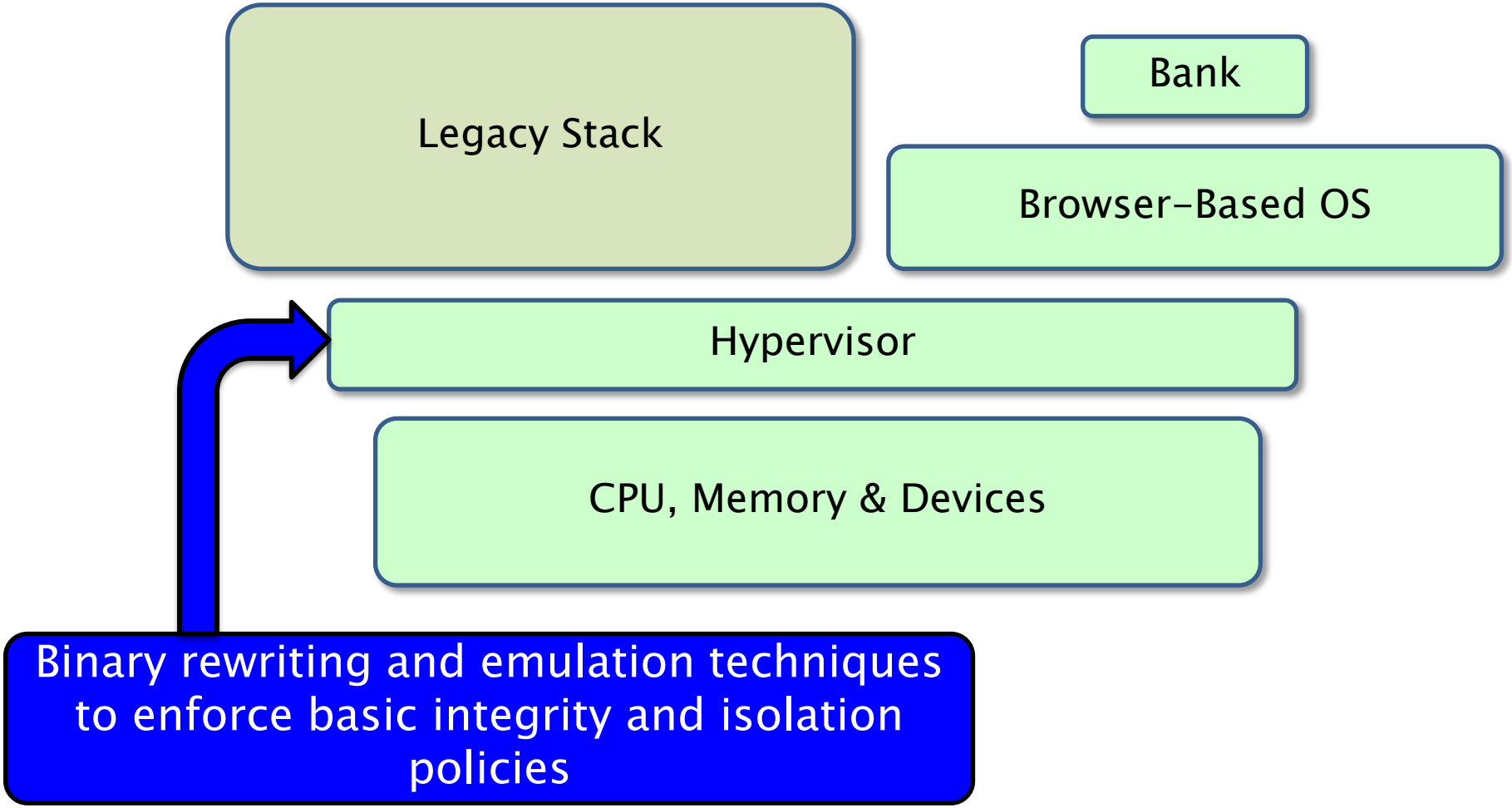
Cloud-terminal architecture



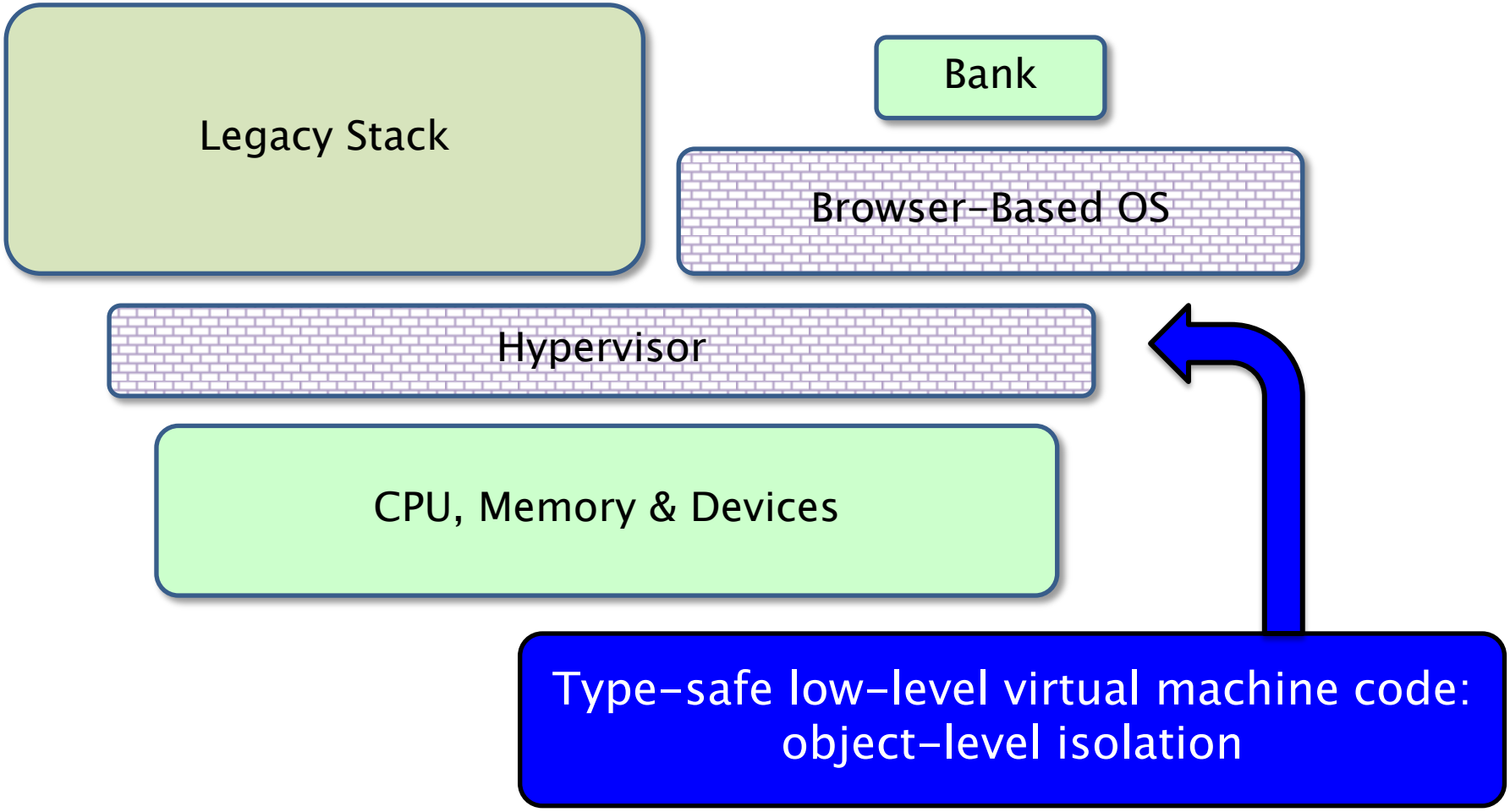
Hardware


Legacy Stack
Bank
Browser-Based OS
Hypervisor
CPU, Memory & Devices
Hardware support for isolation against covert channels
in a multi-core environment

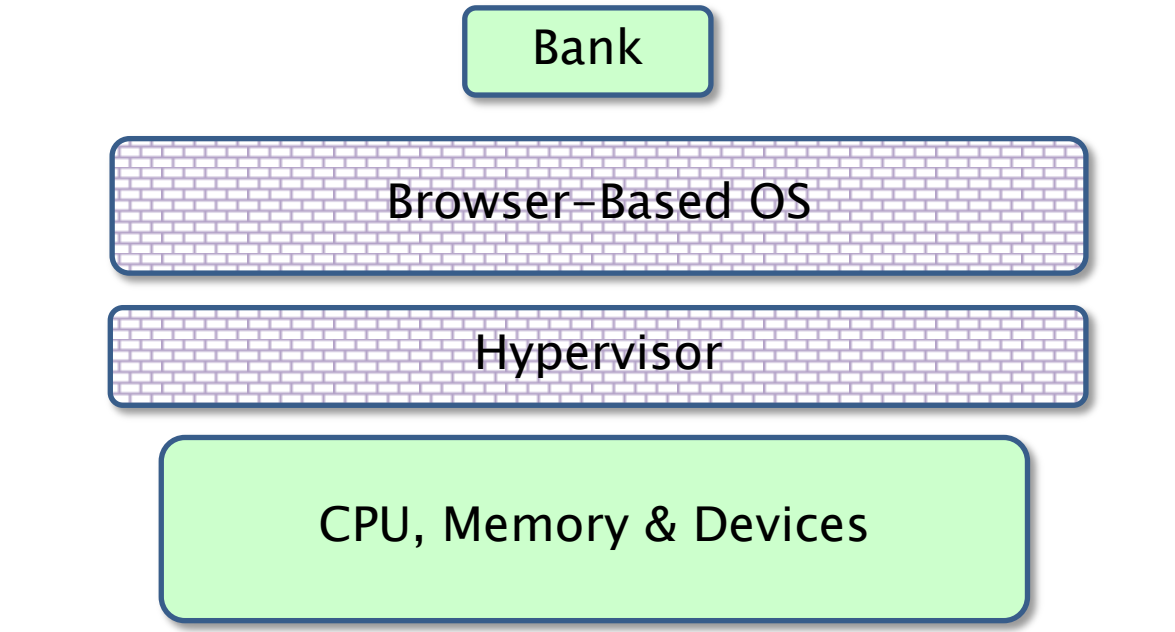
Binary rewriting



Language-based safety

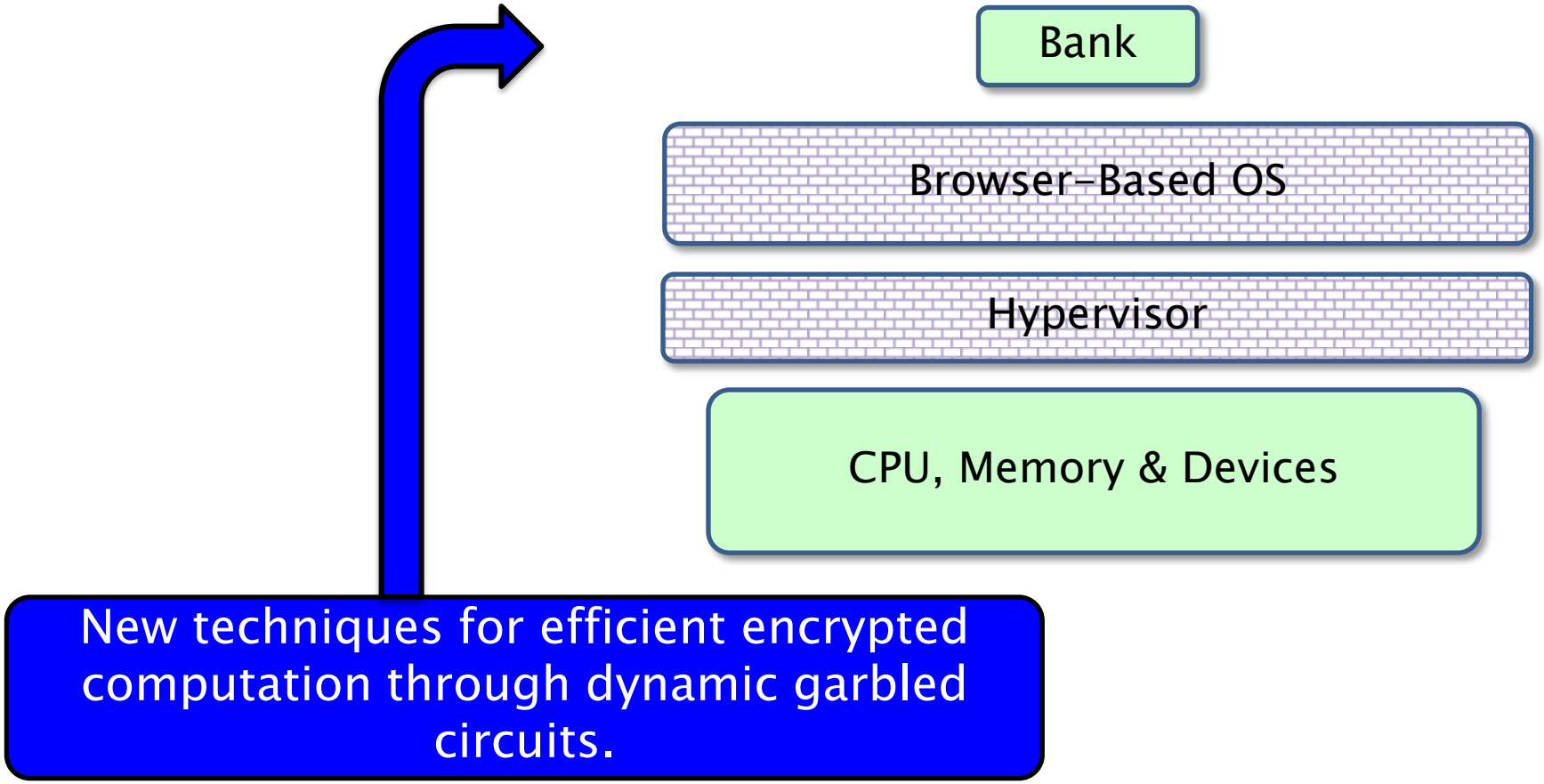


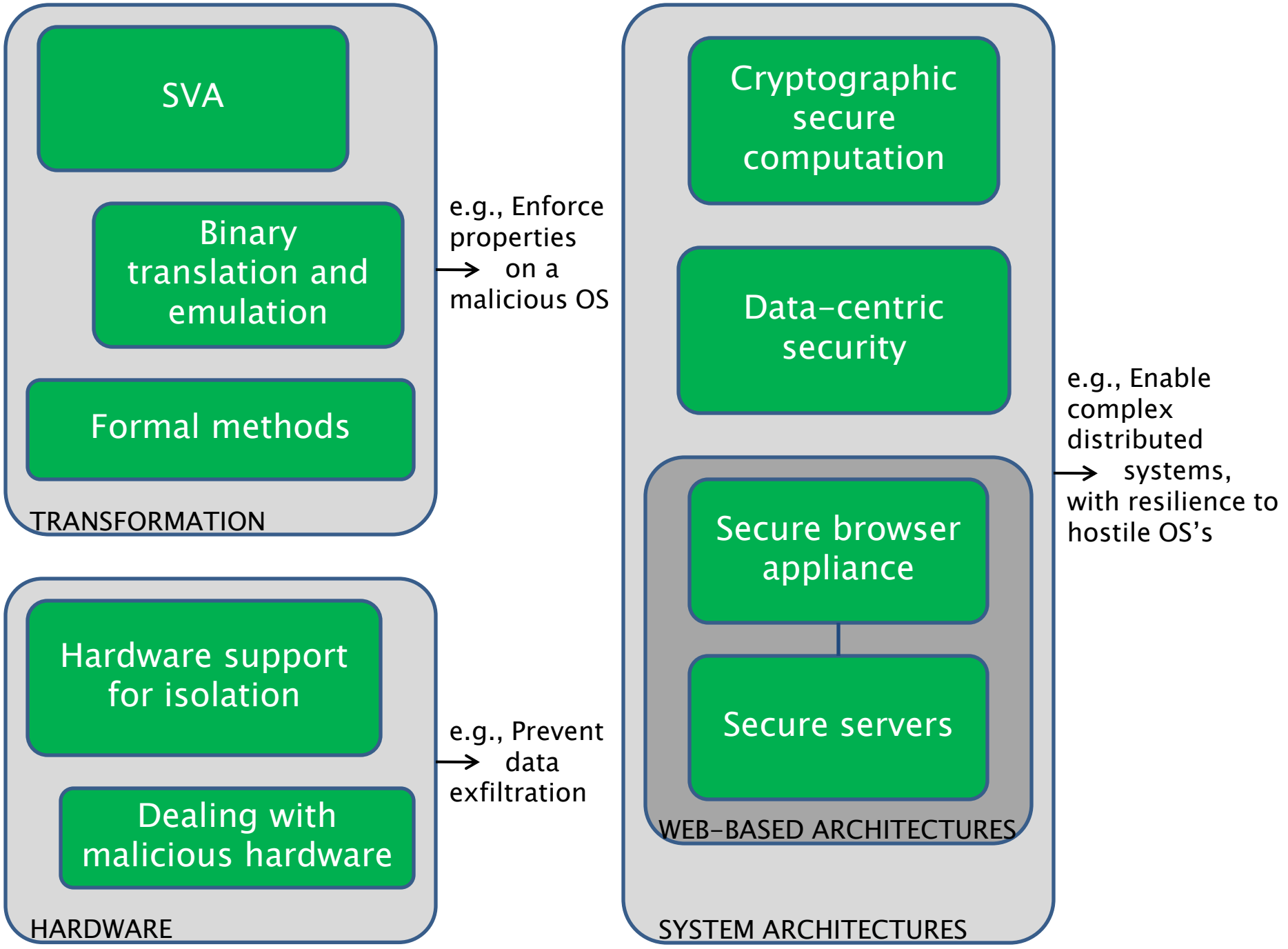
Formal methods



New techniques for scalable verification of enforcement technologies.

Cryptographic techniques




SVA
Binary translation and emulation
Formal methods
TRANSFORMATION
e.g., Enforce properties on a malicious OS
Hardware support for isolation
Dealing with malicious hardware
HARDWARE
e.g., Prevent data exfiltration
Cryptographic secure computation
Data-centric security
Secure browser appliance
Secure servers
WEB-BASED ARCHITECTURES
SYSTEM ARCHITECTURES
e.g., Enable complex distributed systems, with resilience to hostile OS's

Agenda

9:30- 9:45	Welcome + Overview
9:45-10:10	CPU emulators: improving their assurance
10:10-10:35	Formal modeling of x86 binaries
10:35-11:00	Data-centric security: Platform for Private Data
11:15-11:35	Binary rewriting
11:35-12:00	Secure Virtual Architecture
12:00- 1:00	Lunch
1:00- 1:25	Trust, protection, & performance with Valkyrie
1:25- 1:50	When semi-honest is only semi-good-enough
1:50- 2:30	Visitor feedback

http://www.dhosa.org/