System Storage as a Service

Michael Orlov, SCE/SE
noexec.org

CSCML 2017, BGU/CS
28.06.2017

Secure Storage as a Service (SSaaS)

- Secure computing environment
- Complete separation between computation and storage
- Improves user-friendliness / security dichotomy
- Supports enterprise features

Who am I?

- Head of Cyber OPs Program @ SCE
- Evolutionary Computation researcher
- *Liberté Linux* developer, as “Maxim Kammerer”

LENTA.RU четверг, 29.06.2017, 00:06:15
издание Rambler Media Group
Интернет, Технологии

Пресс-конференция

Максим Каммерер. Фото из личного архива

Максим Каммерер, создатель дистрибутива д настоящих "анонимусов" Liberté Linux

Как обеспечить безопасность общения в интернете?
Из-за утечки SMS, отправленных абонентам "Мегафона", достоянием общественности стали лич интимные сообщения, телефонные номера адресатов и в некоторых случаях даже связки логинов электронной почты и социальных сетей. Насколько стоит доверять операторам связи и актуальн выражение "это не телефонный разговор"? Как обеспечить конфиденциальность общения и мож гарантировать абсолютную анонимность в интернете? На эти и другие вопросы читателей "Лент Максим Каммерер, создатель дистрибутива для настоящих "анонимусов" Liberté Linux.

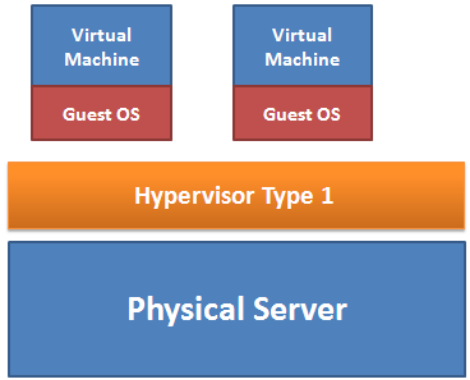
SCE
SHAMOON COLLEGE OF ENGINEERING
Cyber Operations Program

The Problem

- Users in hostile environments face a dilemma:
  - Use familiar OS / Architecture; or
  - Use specific secure OS such as TENS or Tails
- Unable to rely on familiar OS from security standpoint

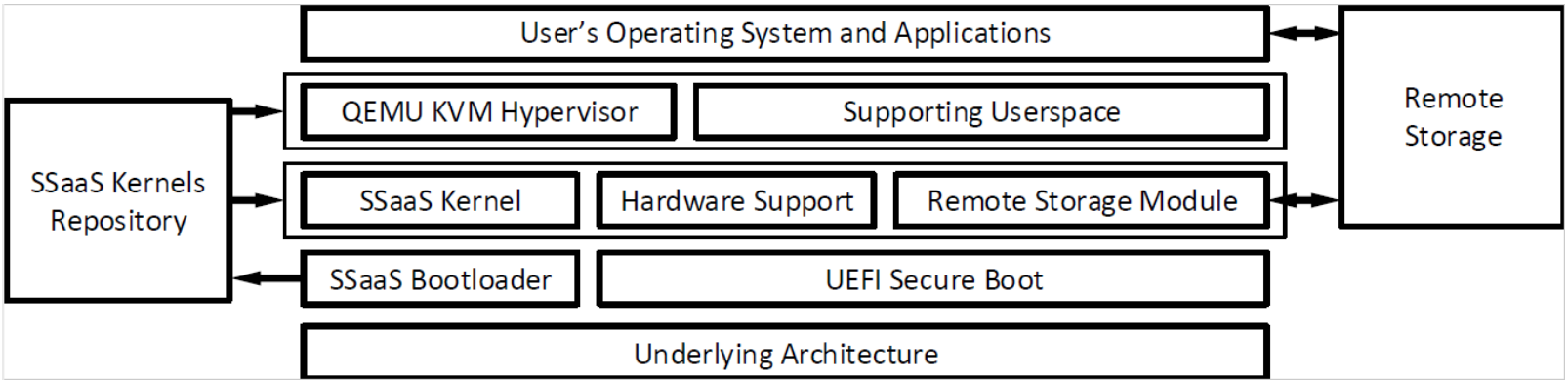
The Solution

- Wrap user's OS in a hypervisor
- Control OS network communication
  - VPN, Tor, whitelisting, …
- Control OS hardware access
- Do not rely on system integrity
  - Move all storage into cloud (including OS)



Implementation Details

- System components:



Principles of Operation

- Tiny bootloader on hard drive or disk-on-key
  - Integrity is guaranteed by trusted boot chain
- Fetches SSaaS hypervisor OS from cloud
  - Moving existing OS to cloud is also possible
- SSaaS OS initializes hardware and cloud access module
- Module is configured for accessing remote storage
- User's OS is started in a VM, subject to policies

Enterprise Features

- Third-party authorization for login
- Corporate VPN network policies
- Encrypted connections introspection via access to keys in guest OS memory
- Side-channel attacks prevention via hardware access policies

Related Work

- Ecosystem of securing computing environments
  - Hard drive encryption
  - Anti-virus solutions
  - VPNs
  - Remote storage
  - Thin clients
- All rely on a locally installed OS

- Commodity hardware and network now allows for complete decoupling

Disadvantages

- Hardware support by SSaaS OS may be lacking
  - Focused testing of client-approved hardware
- Mobile devices often lack virtualization capabilities
  - Situation is improving in ARM and Wind River
- Network access may be unreliable
  - Use local storage as transient encrypted cache
  - Regular apps rely on network anyway

Market

- POC should generate interest in privacy-conscious communities
- Must including open-sourcing security-related code
- Can develop custom solutions for enterprise
- Can sell managed-storage solutions
- Can sell enterprise support services
- …