

2013 DHS S&T/DoD ASD (R&E) CYBER SECURITY SBIR WORKSHOP

CloudCapsule

Security Axioms

Yeongjin Jang and Wenke Lee

July 24, 2013



Homeland
Security

Science and Technology





Company Profile



- Company founded as a spin-off from Georgia Tech
 - Based on our virtual machines and sandboxing technologies
 - Gyrus for integrity
 - Storage Capsule for confidentiality
- First year of a two-year SBIR Phase II project (funded by ARO)

Customer Need

- Secure data access in a Cloud environment



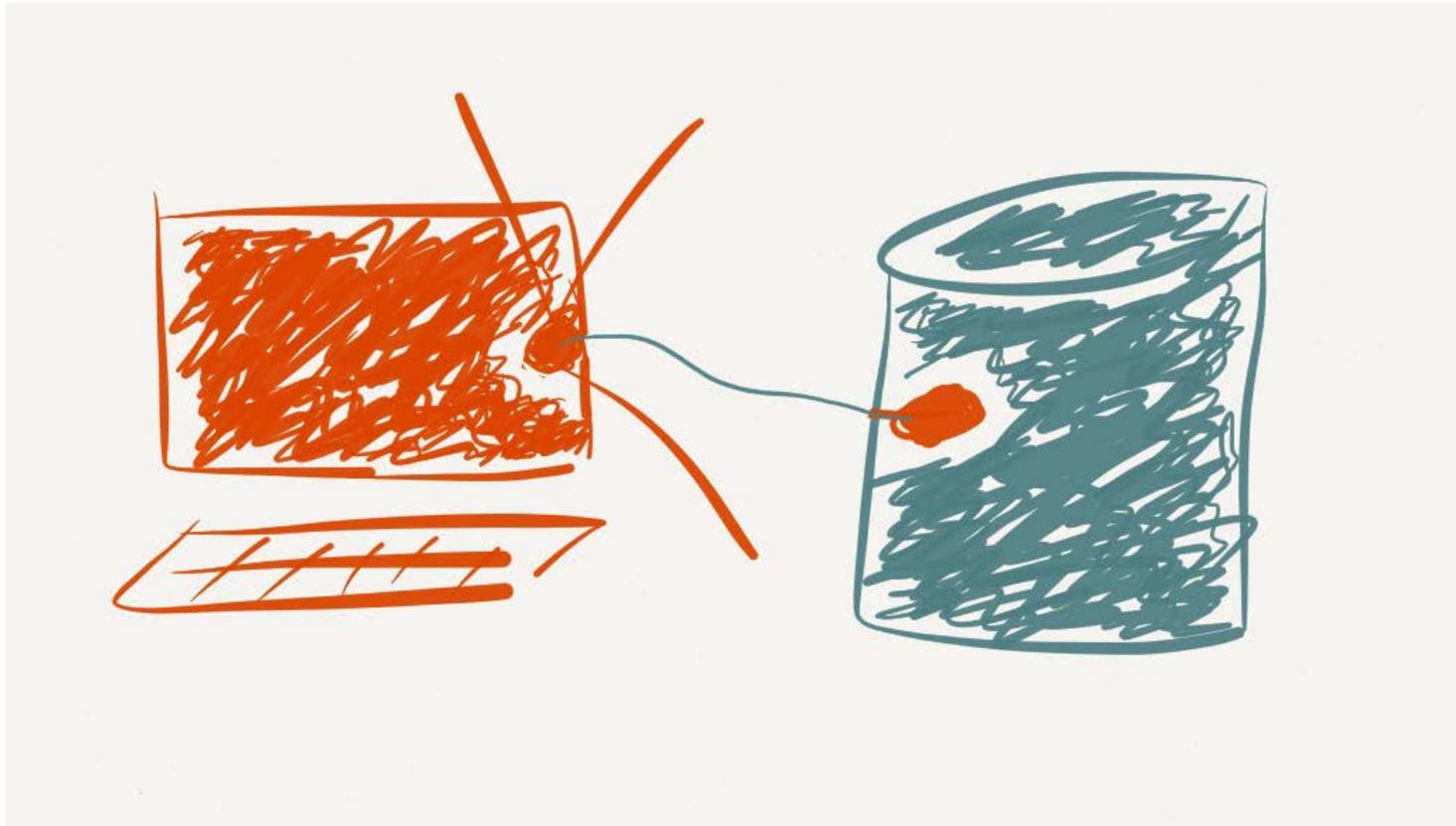
Secure Cloud/Server



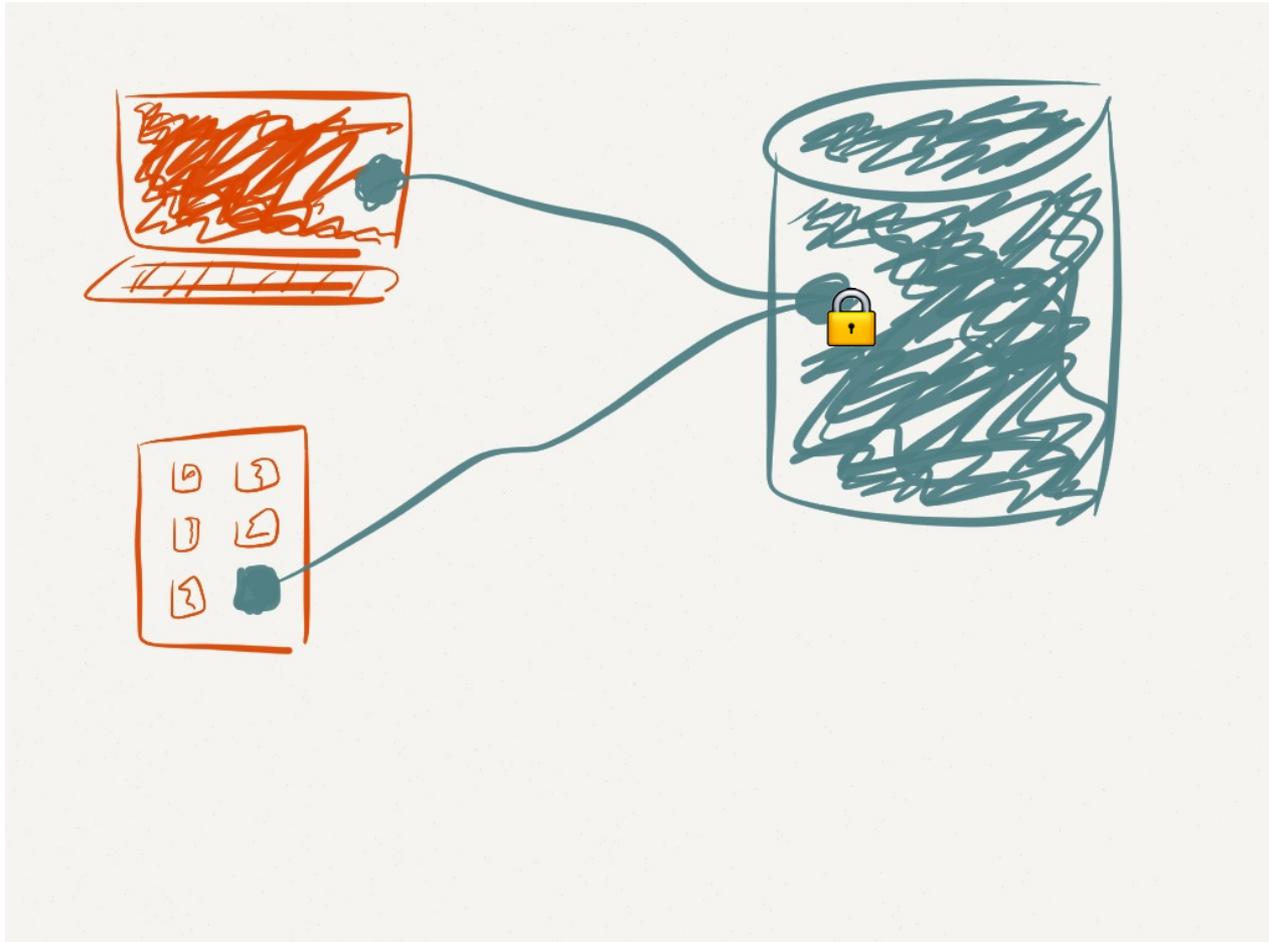
Insecure End-Devices/Clients



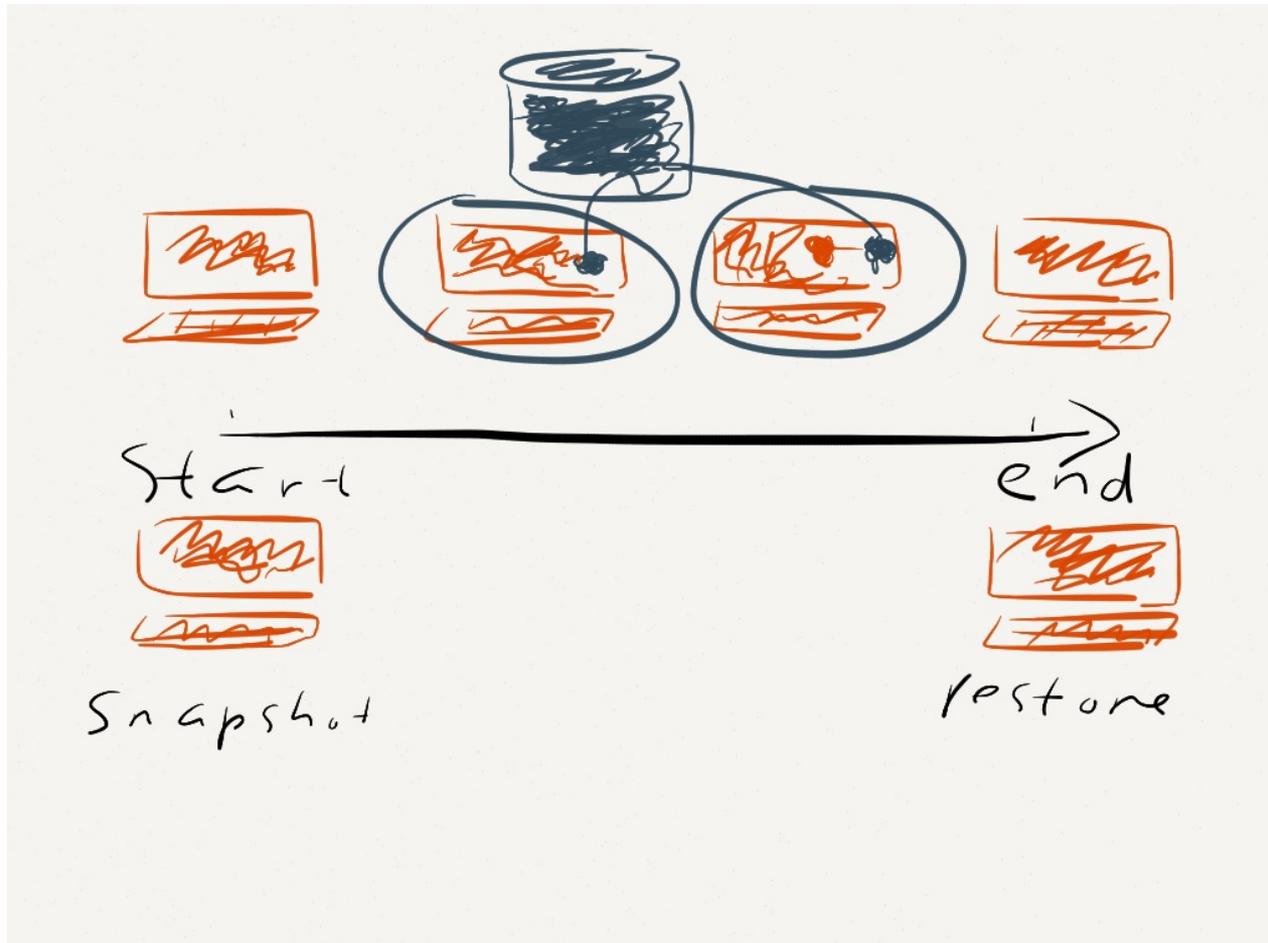
Insecure Data Access



Approach: CloudCapsule



CloudCapsule on Computers



CloudCapsule on Computers

Snapshot



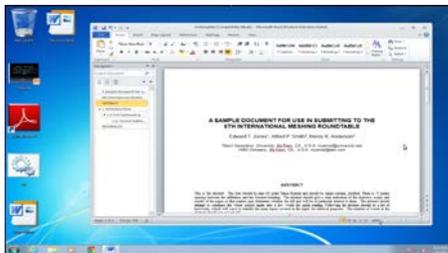
Take a VM snapshot before enters Data Access mode.

De/Encryption is handled by hypervisor, so there is no information for the key in the snapshot.



Decrypt

Data Access



Data is decrypted after snapshot is taken.

User can transparently access their data.

Data is encrypted before leaving Data Access Mode



Encrypt

Restore



Restore VM to a snapshot that is taken at start.

Any software, including Malware and OS has no knowledge for the data.



CloudCapsule on Mobile

- App Sandbox is analogous to a VM
 - Each app is running within its own sandbox
 - An app cannot touch the data of other apps

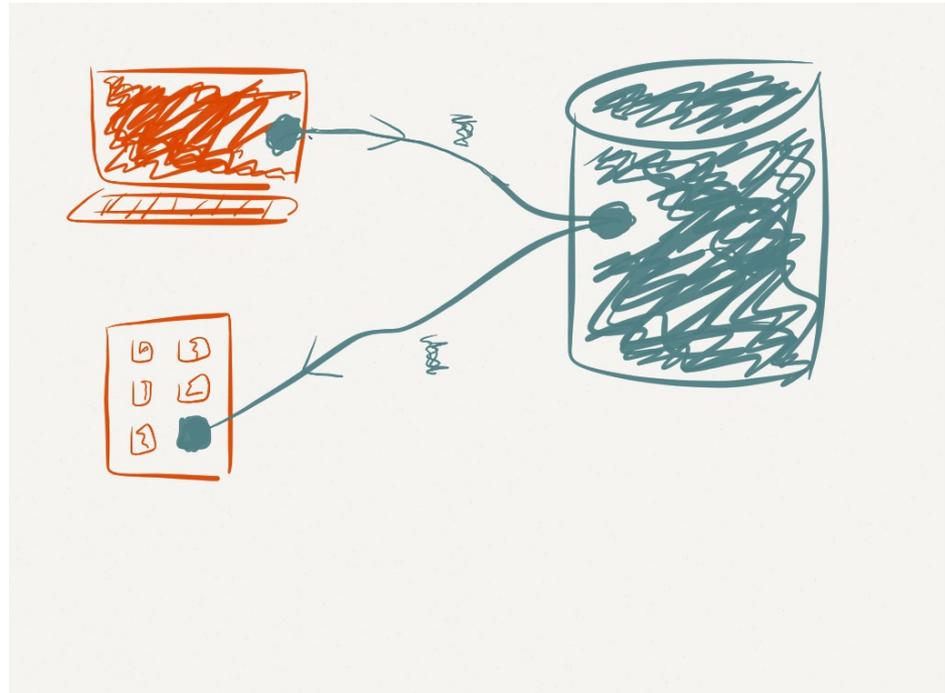


CloudCapsule on Mobile

- Keep all data and operations within CloudCapsule app
 - Only encrypted data are temporarily stored on filesystem
 - All unencrypted data use volatile memory
 - Clean-up used memory when the access is finished, and app is closed.

Integrated Solution/Workflow

- Interoperability
- Filesystem integration
- Key management
- App management



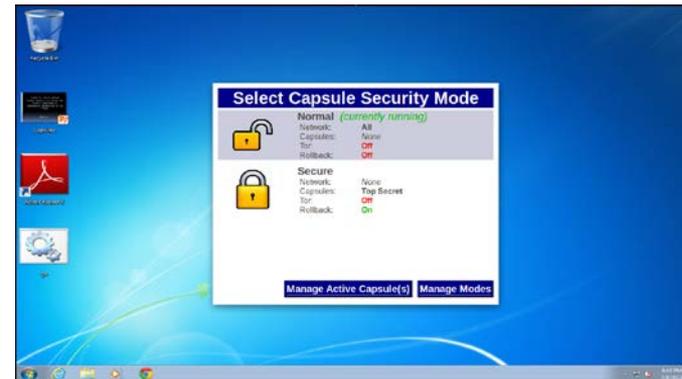
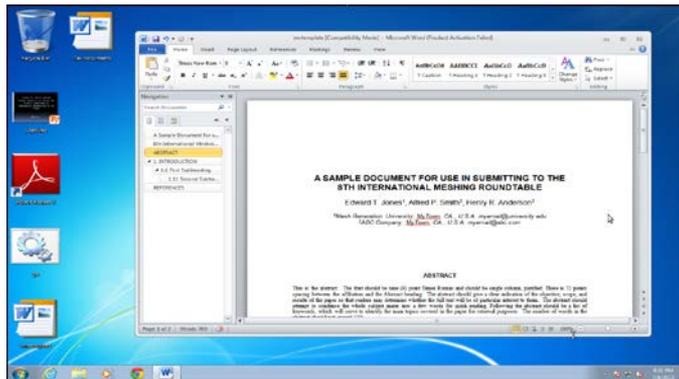
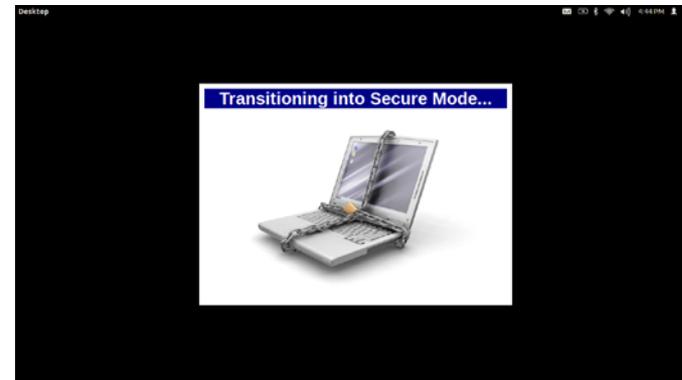
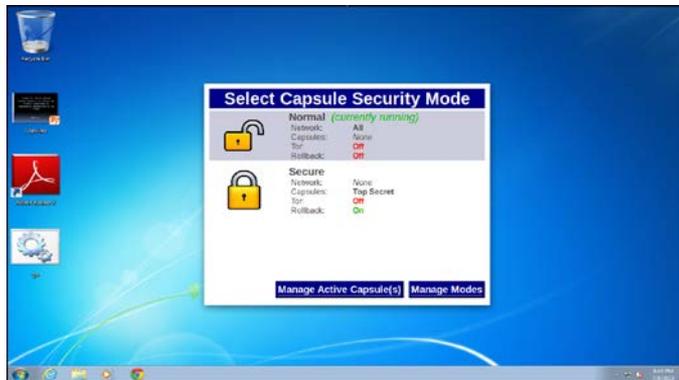


Benefits

- Stop data theft, privacy and integrity violation
 - Block malware on end-devices
 - Cloud provider cannot read user's data
 - A critical need not addressed by data encryption and server/network monitoring
- CloudCapsule runs on desktops, laptops, and mobile devices

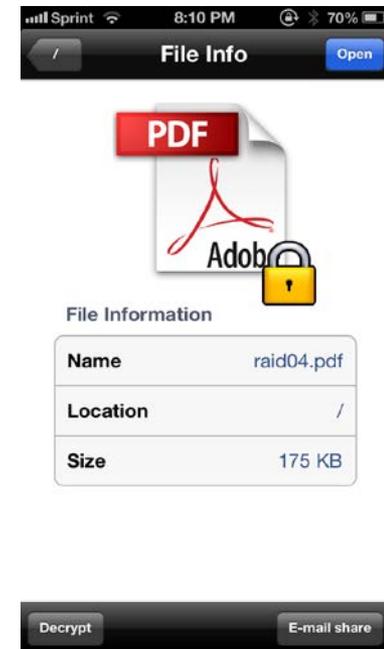
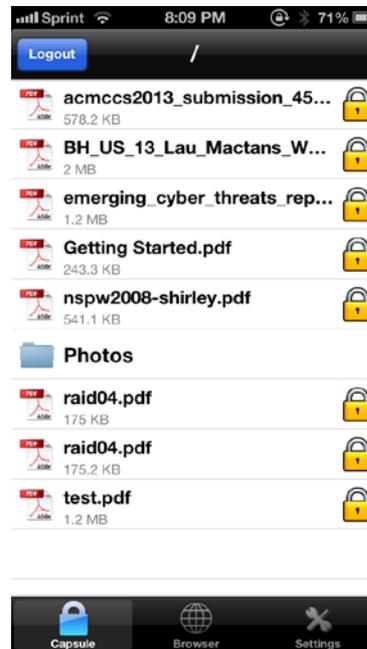
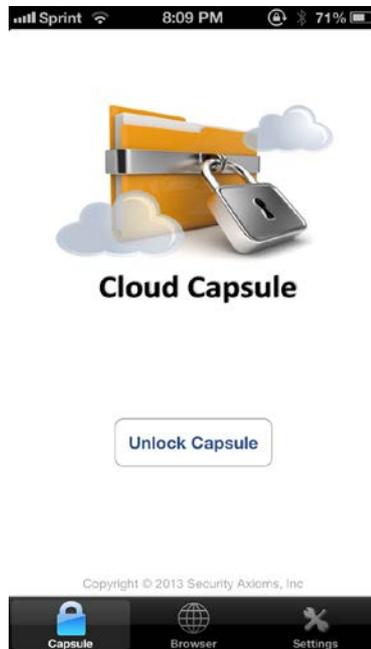
Current Status

- CloudCapsule on computers based on KVM



Current Status

- CloudCapsule app for iOS





Next Steps

- Actively exploring market opportunities
- Starting dialogs with potential partners and investors
- Looking for
 - Proof-of-concept customers
 - Business partners, both companies and individuals



Contact Information

Security Axioms, Inc.

75 Fifth Street, NW, Suite 246A

Atlanta, GA 30308

info@security-axioms.com

wenke.lee@gmail.com

yeongjinjanggrad@gmail.com