Cloud Terminal: Secure Access to Sensitive Applications from Untrusted Systems

Lorenzo Martignoni,* Pongsin Poosankam,*† Matei Zaharia,* Jun Han,† Stephen McCamant,* Dawn Song,* Vern Paxson,* Adrian Perrig,† Scott Shenker,* and Ion Stoica*

*UC Berkeley and †CMU

Challenge

- Goal: protect sensitive information in applications
  - Confidentiality and integrity
- Problem: client-size software stack
  - Complexity $\longrightarrow$ bugs
  - User-administered $\longrightarrow$ out of date, mis-configured
  - Malware can be present at any level

Vision

- Sample application: online banking
- Quickly switch your PC to a secure operation mode
- Application provides a normal GUI
- But, information security does not depend on primary OS or its software
  - Even if commodity OS is compromised by malware

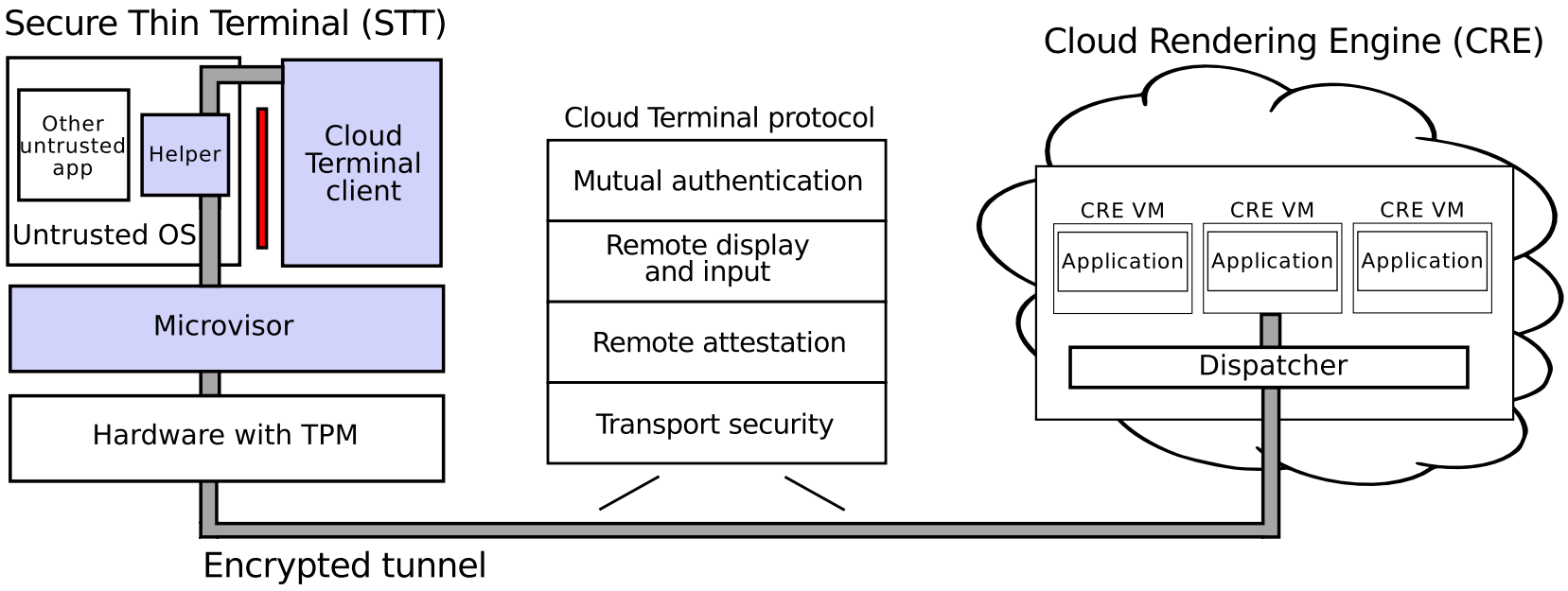
Existing Approaches

Property	Red / Green VMs	Per-app VMs	Browser OS (Chrome)	VDI & Thin Clients	Flicker
Installable w/existing OS	✘	✘	✘	✔	✔
Attestation	✘	✘	✘	✘	✔
Fine-grained isolation	✘	✔	✔	✘	✔
No trust in host OS	✔	✔	✘	✘	✔
User interface	any	any	browser	any	✘
Mgmt. effort	med.	high	low	low	low
TCB size (LOC)	>1M	>1M	>1M	>1M	250 + app logic

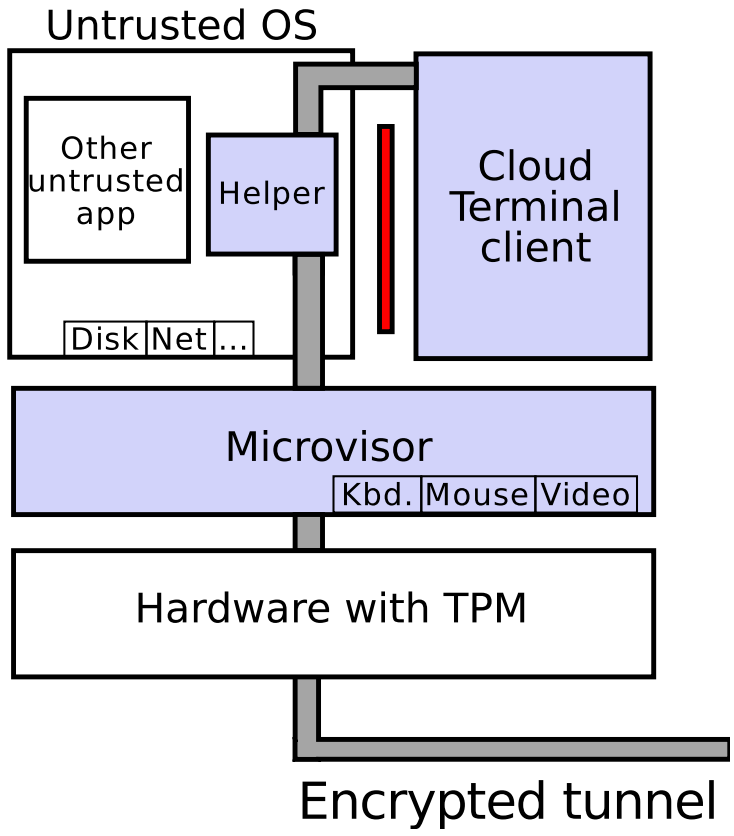
Existing Approaches

Property	Red / Green VMs	Per-app VMs	Browser OS (Chrome)	VDI & Thin Clients	Flicker	Cloud Terminal
Installable w/existing OS	✘	✘	✘	✔	✔	✔
Attestation	✘	✘	✘	✘	✔	✔
Fine-grained isolation	✘	✔	✔	✘	✔	✔
No trust in host OS	✔	✔	✘	✘	✔	✔
User interface	any	any	browser	any	✘	any
Mgmt. effort	med.	high	low	low	low	low
TCB size (LOC)	>1M	>1M	>1M	>1M	250 + app logic	22K

Architecture



Secure Thin Terminal (STT)



Microvisor

- Minimal hypervisor, does not support multiple general VMs
- Uses hardware virtualization (Intel VT)
- Intercepts PS/2 keyboard and mouse
- Redirects frame buffer when Cloud Terminal is active

Startup and attestation

- Microvisor starts from a running untrusted OS
- Intel TXT with dynamic root of trust
  - Code derived from Flicker
  - CPU atomically hashes the microvisor, stores hash in TPM
  - Generate key pair kept by microvisor (but lost on reboot)

Cloud Terminal client

- Lightweight implementation of RFB (VNC) protocol
- When active, takes complete control of mouse, keyboard, and display
- Transport security based on SSL
- Reverse password to demonstrate authenticity

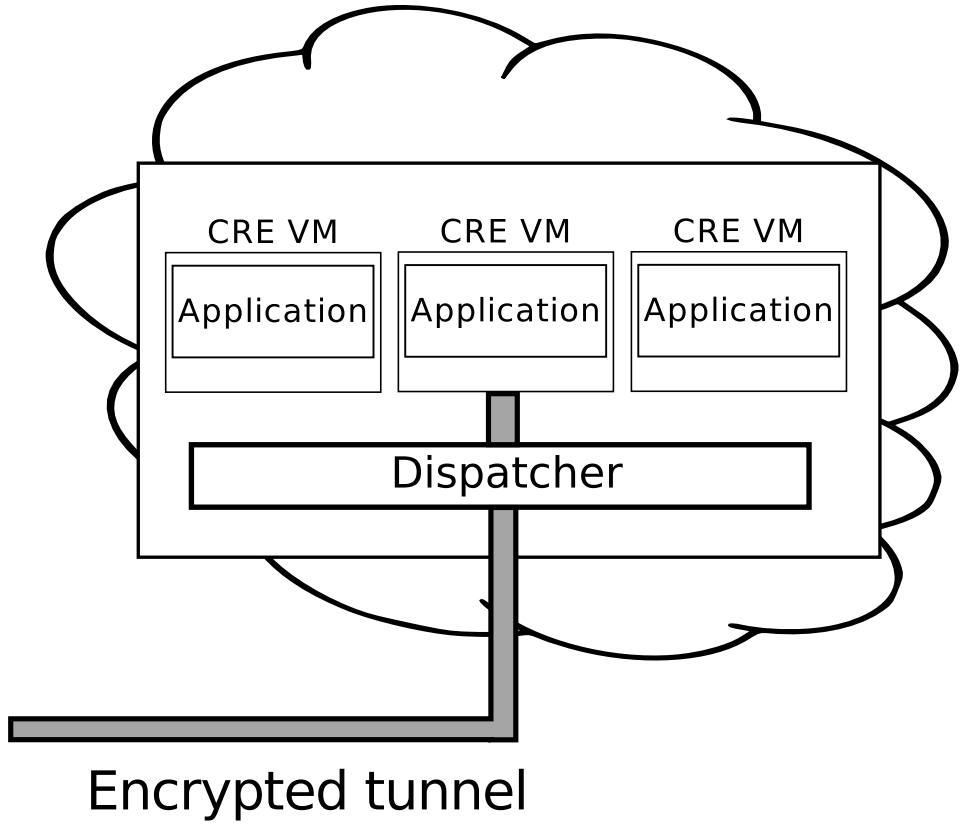
Untrusted user-space helper

- Runs as an unprivileged process inside commodity OS
  - Active when the Cloud Terminal is
  - Communicates with microvisor via hypercalls
- Relays encrypted data
  - Across network to CRE
  - To disk for persistence
- Cannot access or modify plaintext data

STT installation

- Case 1: pre-installed
  - Corporate-provided laptop
  - Out-of-the box consumer device
- Case 2: install on existing machine
  - Verification service performs remote attestation
  - User confirms a random nonce via an out-of-band (telephone) channel

Cloud Rendering Engine (CRE)



CRE approach

- In provider-administered data center
- Each user application runs in a VM with a standard VNC server
- *Dispatcher* relays connections to application VMs
- VMs run standard (e.g. Linux) applications
  - In a stripped-down environment

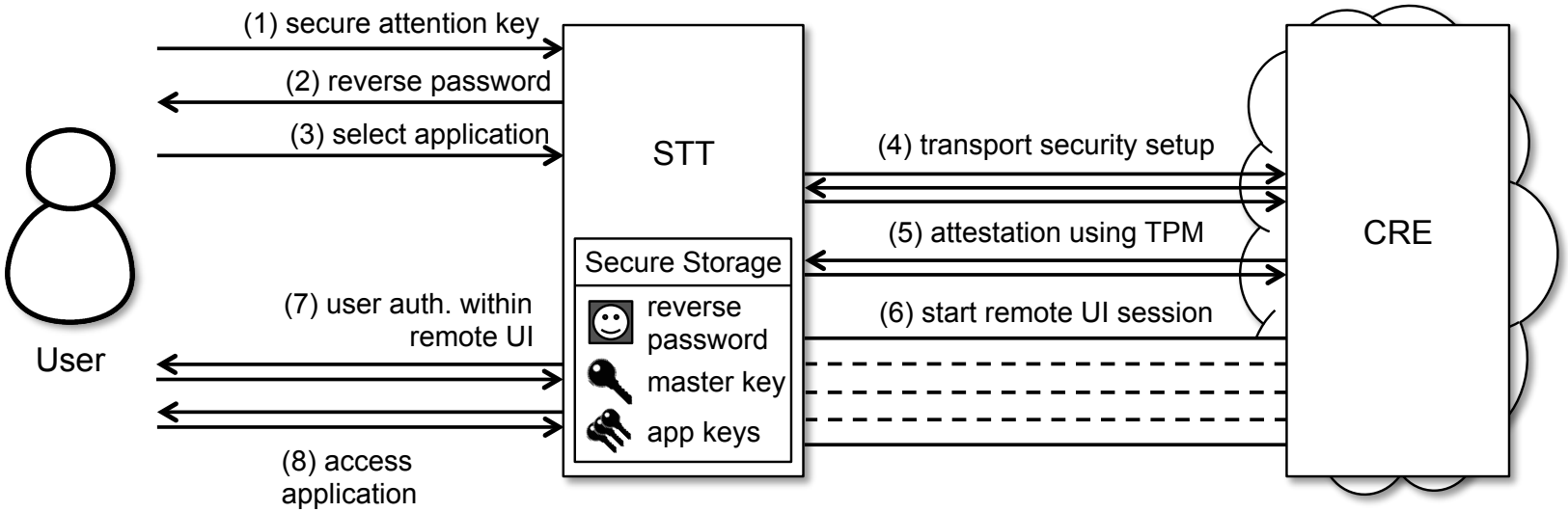
CRE scalability

- Share identical memory pages copy-on-write (up to 61% savings)
- Share base disk image
- Remove software not needed for desired application
- Disable periodic timer interrupts

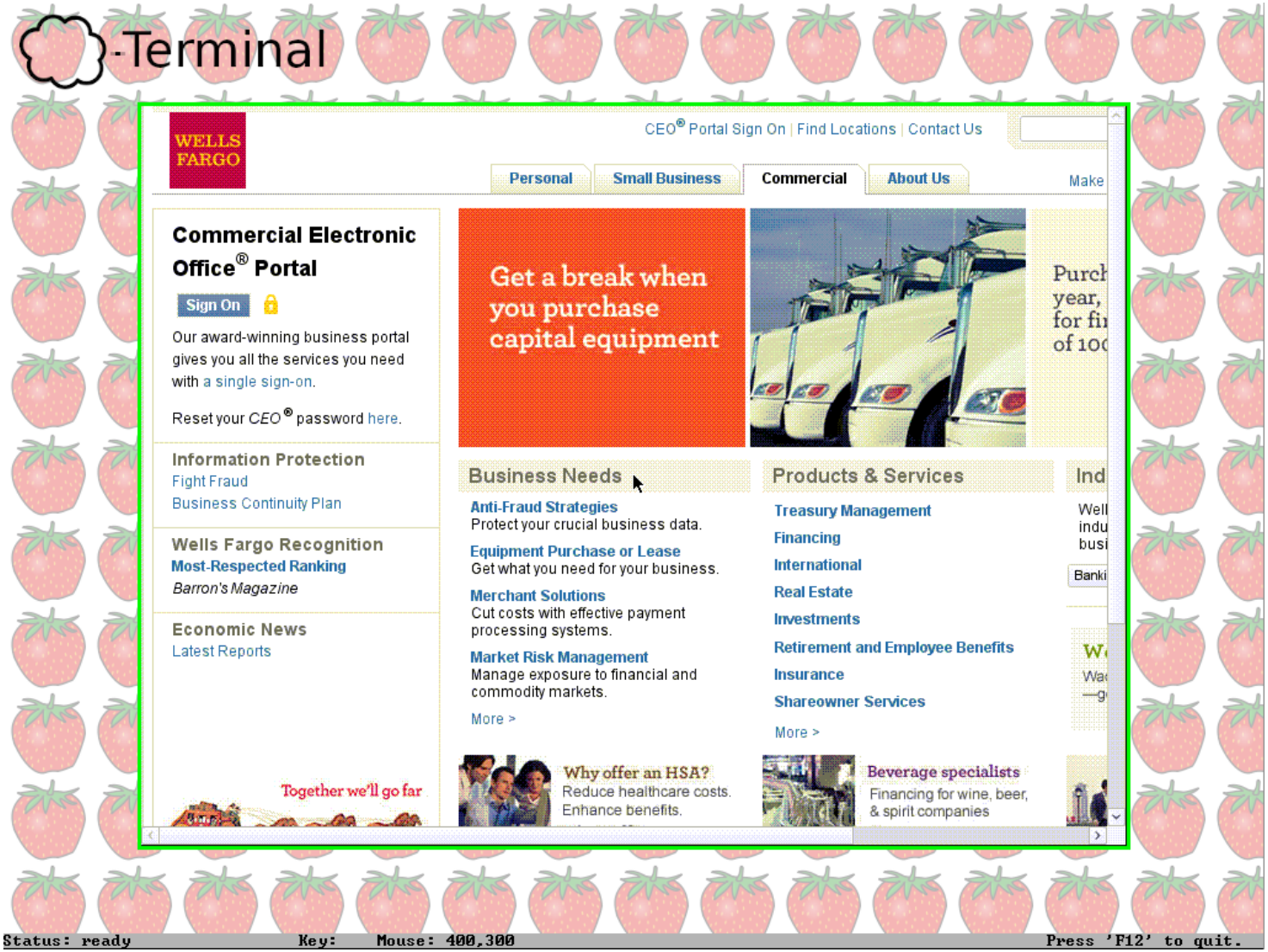
CRE security

- Each VM has its own virtual network and firewall white-list
- Resource usage is capped
- Limited user environment
  - I.e, kiosk mode
- VM has no more authority than its user

Session walk-through



User experience



Evaluation: client TCB

Component	Lines of Code
Microvisor	7.7K
Terminal client	3.0K
Crypto (PolarSSL)	5.5K
Attestation (Flicker)	5.7K
Total	21.9K

Evaluation: applications

- Document editing: AbiWord
  - MS Word `.doc` compatible
- Document viewing: Evince (PDF)
- Online banking: Firefox + Wells Fargo
- Secure email: Firefox + Gmail

Evaluation: performance

16 core, 64GB server, 670 mi from client

Simultaneous clients replay recorded usage

App.	Activity	Baseline (ms)	STT (ms) with # of clients =			Network Usage (bytes)	
			150	200	300	inbound	outbnd
Edit	Launch	2,844	2,208	2,441	2,553	487,047	3,888
	Type a key	30	53	50	54	1,607	346
	Move mouse	32	49	59	51	480	138
PDF	Launch	1,699	2,093	2,147	2,493	483,219	2,040
	Scroll	114	1,270	1,380	1,704	352,358	5,497
Bank	Launch	6,911	2,319	2,563	—	490,149	4,680
	New page	1,183	2,610	2,661		415,732	10,939
Gmail	Launch	6,936	2,254	—	—	488,367	3,954
	Display msg.	992	2,254			318,300	8,416

Qualitative usability

- Display is 800x600, 8 bit color
  - Suitable for a single application
  - Could be improved with compression
- Typing latency feels usable
  - Similar to SSH
- Scrolling feels sluggish
  - Add optimization of block moves

Cost analysis

- A suitable server costs $1010/month
- Between 1.2 and 2.5 cents per user-hour
- Online banking: 5 cents per user per month
- Corporate application: $3 per employee per month (8 hours per day)

Summary

- Cloud Terminal: new architecture for secure remote applications
- Achieves sweet spot between security, trusted code size, and generality
  - Near minimal client size for remote interaction
- Runs inexpensively using standard hardware

http://bitblaze.cs.berkeley.edu/