

Cloud Computing Threats (Real and Perceived)

Sotiris Ioannidis
FORTH-ICS

sotiris@ics.forth.gr

What is Cloud Computing

- Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS)
- *-as-a-Service
- Rich Internet Applications (RIAs)
- Managed Service Providers

- If you don't own some (or all) of your infrastructure, it's cloud computing!

- Concentrate on security-related threats. SLAs, hidden costs, etc. out of scope of this talk.
- Evolving technology → not all threats understood.

Cloud Computing Security

- Data security
- Backups/logs/other metadata
- Key management
- Network security
- Regulatory and Legal Compliance
- Business process safety/continuity

Data Security

- Various abstractions exist for data services
 - Raw storage
 - Database-level access
 - Other structured data (documents, images, ...)
- Physical security: is my service provider properly guarded?
- Logical security: how good is the access-control/authentication/authorization of the underlying OS?
- Cryptographic security: encrypt my data, push the problem to key management.
- Integrity: if you have a PB (10^{15} Bytes) of data, a 10^{-14} error rate is ten errors when you scan your entire dataset!

Backups, Logs, Crashdumps, other metadata

- Traditional protection against data loss: (off-site) backups
- Who backs up the cloud data?
 - Provider could offer it as a service
 - You back it up, but where? → in another cloud.
- Logs contain information about things that fail → rich target for attacks.
 - So, logs themselves are data that need protection.
 - ...
- Keep them in logically separate subclouds.

Key Management

- Keys now become extremely sensitive data
- Can't have secure storage (hardware tokens) in a cloud.
- What is the trust anchor?
 - TPM virtualization (in Xen) assumes you trust the hypervisor
 - HSMs not usable
 - Secure booting not applicable
- **We need a good solution for this!**

Network Security

- No firewalls
 - We'll finally have to take host security seriously
- Yes, services run on VLANs and VPNs, but:
 - Less work has gone into studying attacks on virtualized network resources.
 - Virtualized routers a ripe area for new attacks.
- Network resource consumption/sharing
- Increased demand for network capacity and network services

Virtualization problems

- Shared resources → side-channel attacks.
 - Cache timing attacks
 - CPU timing attacks
 - ...
 - All the OS attacks we've seen in time-shared OSes apply here
- Attacks on the hypervisor
 - Equivalent to processes attacking the kernel
 - Never know what you're going to find.
- Network virtualization
 - Cause congestion
 - Interpret traffic patterns

Regulatory and Legal Compliance

- Some businesses are regulated, by statute or by contract
 - PII protection, other data protection laws
 - PCI compliance
- If your service is composed of compliant components, is it itself compliant?
- Can you have a compliant service out of non-compliant components?
- Who is responsible for submitting to court orders?

Business issues

- “Locked in Open Systems”?
- Data formats: if your storage/cpu/whatever provider goes out of business, are there compatible providers?
 - Ad: Operation Data Freedom!
- Paradoxically: concentration of resources in huge data centers
 - A physical disaster takes out many businesses, all of which may then overload neighboring data centers.
- Captive to your providers
 - True at many levels: can't leave a social-networking site that has become oppressive; can't leave your network provider without renumbering; similar issues in clouds.

Summary

- Cloud computing is here to stay
- We need to understand what is new in:
 - The threat model
 - The trust model
 - The tools
- “[Cloud computing is] like any other [technology]; [it's] either a benefit or a hazard. If [it's] a benefit, it's not my problem.”