Cloud security

COSC349—Cloud Computing Architecture

David Eyers

Learning objectives

- Contrast **cloud and local security** positives & negatives
- Outline how interacting with cloud providers involves:
  - **encryption** typically being used to preserve confidentiality
  - **checksums** typically being used to preserve integrity
  - **multiple zones and regions** being used to preserve availability
- Give example security flaws affecting IaaS, PaaS, SaaS

Computer security principles

- Common to divide up principles into three areas (CIA):
  - **Confidentiality**—unauthorised parties can't read data
  - **Integrity**—unauthorised parties can't manipulate data
  - **Availability**—authorised parties can get to the data

- Cloud technology provides many attack surface areas
  - **Cloud provider**'s hardware + software + people
  - **Internet security** between cloud and user
  - **User-side** software and hardware security

Brand value of cloud providers is key

- Legally cloud providers usually **not responsible** for issues
  - However there is also little lock-in for clients using services…
  - … so negative news is avoided by providers wherever possible
- Some smaller providers have **delayed reporting** issues
  - Presumably hoping mitigation and resolution might be private
  - Now would run into problems regarding EU GDPR and similar
- Providers can **claim to be secure**, but how to quantify?
  - Typically only know—post-breach—that security has failed

Cloud security — confidentiality

- Outsourcing means **cloud provider sees your data**
  - … but there are some notable exceptions to this
  - Hybrid and private cloud models mitigate security exposure
    - … but may lead to other problems, e.g., resilience and availability
- **Encryption** applied to data at rest and in transit
  - Online attacks possible by malicious staff at cloud provider
  - Backup operators likely to only be handling encrypted data
  - TLS (e.g., HTTPS) no longer considered expensive (use always!)

Cloud versus local security

- Often assumed that outsourcing means lower security
- But how secure is the client organisation? (*e.g.*, SMEs)
  - Cloud providers' **economies of scale** for monitoring & reacting
  - Cloud providers also get **great visibility** of threats and attacks
    - *e.g.*, Google will be able to spot malware outbreaks ‘easily’
  - Playbooks for post-incident response? Audits? Pen. testing?

- **Local confidentiality** is controllable (versus availability)
  - *e.g.*, offsite backups, and keeping offline audit records

Cloud security—integrity

- Typically integrity is enforced by using checksums
  - May protect against malicious, or accidental modification

- **Malicious modifications** detected using secure hash
  - One-way function: can't fake data to cover up modifications
- **Accidental modification** can use cheaper hash algs.
  - (Although for simplicity secure hashes may be used anyway.)
  - Hard-disk controllers often store checksum information
  - Network packets and frames contain many checksums

Cloud security—availability

- Cloud providers have **vast, global presence**
  - Multiple regions; multiple availability zones—highly available
- However cloud providers are usually **one company**
  - Court-orders could potentially affect service availability
  - … although different regions may operate under different laws
  - Think of Kim Dotcom's **FBI / Megaupload** interactions…
- High availability in the face of **cloud provider failure**?
  - **1** operate in hybrid mode, with fail-over back to local
  - **2** use multiple cloud provers in parallel

Non-cloud high availability?

- Local integrity and availability can be **highly expensive**
- Need multiple datacentres lest vulnerable to disasters
  - e.g., power issues (UPSs), fire, earthquake, war, inside attacks
  - However, need to keep different office sites in sync.
  - **Private cloud approaches** are probably easiest today
    - (Past approaches for multinationals well explored.)
- High availability must be **tested frequently**
  - Yahoo! routinely takes random datacentres offline to test HA
  - … but when S3 falls over, many popular sites fall over too …

IaaS security problems for providers

- Intel CPUs' speculative execution bug, for example
  - Speculative exec. is CPU running ahead of actual program
  - Intel's Meltdown bug: CPUs ran ahead into protected memory
    - Straightforward to slowly stream out data from anywhere
- Whole cloud server fleet **potentially vulnerable at once**
  - No reported use of the vulnerabilities in the wild, though
- Providers also potentially vulnerable to **encryption bugs**
  - e.*g*., most TLS/SSL implementations have had bugs, recently

PaaS security problems from cloud API use

- S3 storage has been a frequent source of **data leaks**
  - Cases of developers **failing to lock-down** buckets' permissions
  - S3 is operating as designed… (for anonymous & private data)
- Another common problem is **leaking of API keys**
  - GitHub repositories have included private 'tokens' by mistake
  - Attackers can scan for those tokens, and incur AWS expenses
- Note lack of EC2 password support in SSH

Security within SaaS offerings

- Assume that large-scale SaaS has excellent sec. team
  - However some stunning failures have actually happened!
- Dropbox password 'problem'
  - Mid-2011 for a four-hour window, **any password worked** (!!)
  - Cloud-scale helps clean-up: all logins are recorded
    - Thus Dropbox knows all accounts that might be affected (was <1%)
- Dropbox 'Selective Sync' bug
  - Some users' **files were deleted** by the Dropbox tool
  - Those users were given one year's free premium accounts (!)

State-sponsored attacks on TLS

- Data in motion typically protected by TLS (SSL)
- Client/server **shared secret**: preloaded **root certificates**
  - Actually may use intermediate certificates
- Security of some certification authorities is questionable
- State-sponsored attacks have **hijacked HTTPS certs.**
  - e.g., allowing eavesdropping on Gmail, YouTube streaming, …
- Some enterprises install software that hijacks TLS
  - Is intended to facilitate monitoring and audit, but…
  - may introduce additional vulnerabilities into cloud interactions