10. Cloud Forensics

Digital Forensics and Cybercrime course

Prof. Zanero

Enter the cloud problem

- Cloud computing is a computing-as-a-service paradigm
    - Different declinations: IaaS, PaaS, SaaS
- We will deal mainly with the concept of *public clouds* as private clouds offer significantly less challenges
- Issues with acquisition and access to evidence
- Analysis issues
- Issues with attribution (multi-tenancy systems and networks)
- Issues of legal status

I HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO CLOUD COMPUTING.
Dilbert.com DilbertCartoonist@gmail.com
BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD.
©2011 Scott Adams, Inc./Dist. by UFS, Inc.
1-7-11
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLAH BLAH PLATFORM.

Acquisition issues

- In general, even in IaaS scenarios, *no control* is given to user on hardware and storage space
  - Investigators cannot really access the metal
  - This makes traditional acquisition procedures unfeasible *for the host* (http://www.dfrws.org/2012/proceedings/DFRWS2012-10.pdf demonstrates feasibility for guests)
- Levels of access vary:
  - SaaS: cloud service provider only one who has logs/data
  - PaaS: customer may have application log, network log, database log, or operating system depend on the CSP
  - IaaS: logs until OS level accessible to customers; network/ process logs at provider level (e.g. load balancer logs)

The real cloud issue

- Data in flux
  - Some data only exists as result of transaction
  - E.g. case of reconstructing page of Youtube video
  - “There is no data”

Acquisition issues (even on simple cases)

- Acquisition of a simple web page
  - What could **possibly** go wrong?
- Dynamic content on page
  - How to capture?
  - How to reproduce in court?
  - If imported from external sites, what is its legal status?
- **Visualization is different from data**
- Attribution
  - Whois data
  - DNS resolution (proving it from multiple points)
  - Connectivity and provider identification
  - Geolocation of hoster

Analysis issues

- Main expectation of forensics: retrieval of deleted data/fragments of data
  - Basically ***impossible*** in a cloud environment
- Metadata will disappear easily
  - Snapshots and restores
- Investigation of hypervisor-level compromises
  - Lack of tools and research

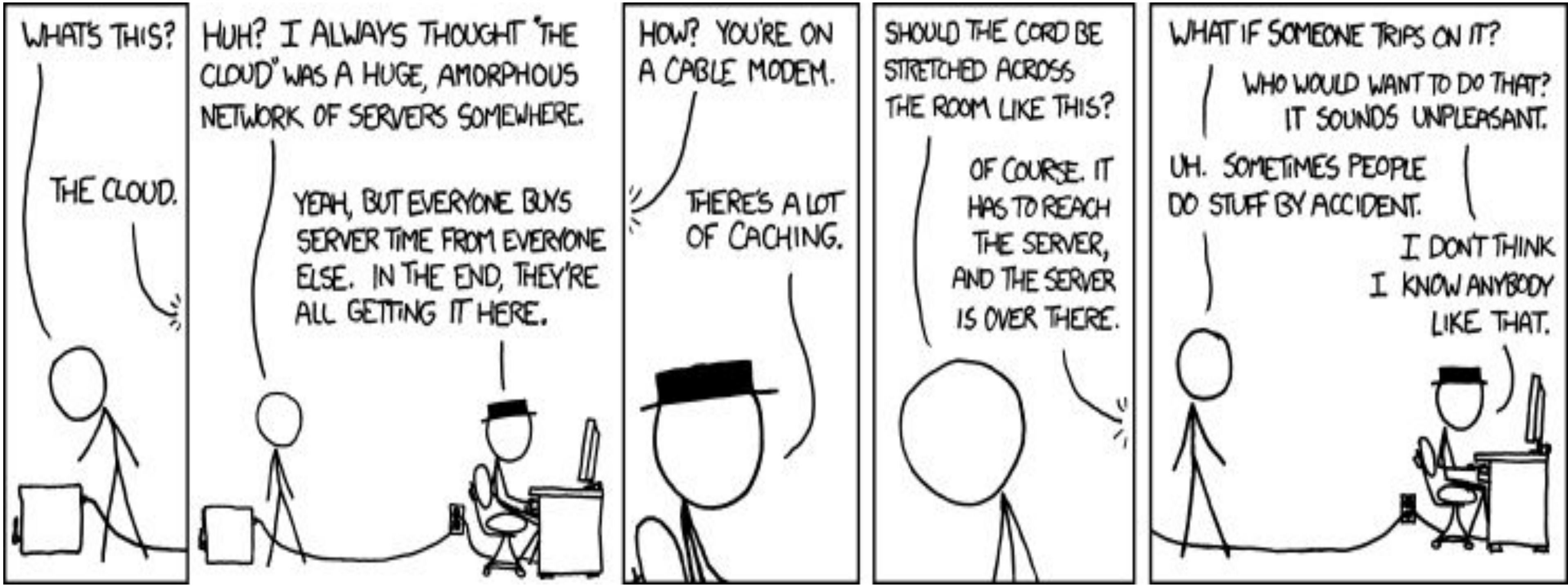
Attribution issues

- In cyberspace, attribution is hard already
  - Spoofing at IP level
  - Usage of stepping stones (i.e. attribution to technical source is not attribution to agent)
- Cloud infrastructures add an additional layer of indirection in attribution
  - Identity?
  - Actor?
  - Location?

Legal issues

- Geographic location
  - Some judiciary acts require a physical location
  - Criminal investigation/prosecution based on physical locations
  - Applicable law depends on physical location
- Electronic data is unique as it may actually span multiple physical locations!
  - No other artifact has, or ever had, this property
- Under “Budapest convention” support for the concept of “Electronic Search and Seizure”
  - Cross border?
  - Removal of obstacles (i.e. legal forceful access to systems) cannot be ordered across countries
- Contract and SLA issues with CSP

Legal issues: clouds of clouds of clouds...


WHAT'S THIS?
THE CLOUD.
HUH? I ALWAYS THOUGHT "THE CLOUD" WAS A HUGE, AMORPHOUS NETWORK OF SERVERS SOMEWHERE.
YEAH, BUT EVERYONE BUYS SERVER TIME FROM EVERYONE ELSE. IN THE END, THEY'RE ALL GETTING IT HERE.
HOW? YOU'RE ON A CABLE MODEM.
THERE'S A LOT OF CACHING.
SHOULD THE CORD BE STRETCHED ACROSS THE ROOM LIKE THIS?
OF COURSE. IT HAS TO REACH THE SERVER, AND THE SERVER IS OVER THERE.
WHAT IF SOMEONE TRIPS ON IT?
WHO WOULD WANT TO DO THAT? IT SOUNDS UNPLEASANT.
UH. SOMETIMES PEOPLE DO STUFF BY ACCIDENT.
I DON'T THINK I KNOW ANYBODY LIKE THAT.

Forensically-enabled clouds

- Drivers (why should a CSP care?)
  - SOX requires auditable storage for storage of financial and accounting data
  - HIPAA requires forensic capabilities for storage of healthcare data
- Requirements for a CSP to offer “forensic friendly” services
  - Make an effort to store (snapshots of) volatile VM data in their infrastructure
  - Make an effort to provide proof of past data possession
  - Data location (?)
  - Identity Management
  - Encryption and Key Management
  - Legal provision and SLAs

Dual considerations: cloud enabled forensics

- Drivers (why should we care?)
  - Data storage size constantly increasing
  - Analysis of large amount of data takes months or years on standard computing hardware
  - “Needle in haystack” issue
- What would be the benefits?
  - Large scale data storage
  - Large scale computing infrastructure
  - Reuse of computing concepts (e.g. map-reduce, etc.)
- What are the challenges?
  - Loss of control on evidence (privacy issues)
  - Chain of custody (same challenges as for acquisition)
  - Transnational operations are challenging from legal perspective