Cloud Security

Tyler Bletsch
Duke University
CLOUD

- What is it?
  - Most overused and abused buzzword of the 21st century.
Cloud

• What is it?
  • It’s when you borrow a computer over a network.
  • That’s all.

• Lots of ways to “borrow”.
• Lots of kinds of “computer”.
• Lots of kinds of “network”.

• Marketing nonsense was so bad the National Institute of Standards and Technology (NIST) produced a definition which most people go by now
What is Cloud Computing?

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, networks, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. – NIST

- Essential Cloud characteristics
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
Cloud Service Models

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)
- Storage-as-a-Service (StaaS)
- Tons of other stuff-as-a-Service (XaaS)
Infrastructure-as-a-Service

• Consumers deploy their software, including OS and application on provider’s infrastructure
  ▸ Computing resources such as processing power, memory, storage, and networking components are offered as service
  ▸ Example: Amazon Elastic Compute Cloud
• Consumers have control over the OSs and deployed applications
Platform-as-a-Service

- Consumers deploy consumer-created or acquired applications onto provider’s computing platform
  - Computing platform is offered as a service
  - Example: Google App Engine and Microsoft Windows Azure Platform
- Consumer has control over deployed applications
Software-as-a-Service

• Consumers use provider’s applications running on the cloud infrastructure
  ▸ Applications are offered as a service
  ▸ Examples: EMC Mozy and Salesforce.com
• Service providers exclusively manage computing infrastructure and software to support services
Cloud security threats

• *All the traditional threats, plus...*

• Cross-tenant data or access leakage
  ▪ What if Coke and Pepsi are running VMs on the same physical machine?
  ▪ Loss of hypervisor integrity compromises whole organizations now!
  ▪ Also: networks, storage, etc.

• Access rights issues
  ▪ There are SO MANY stories of data leaks from Amazon S3 set to world-readable
    • E.g.: [This major ISP leaked plaintext passwords, secret keys, and more](#)

• Cloud command-and-control issues
  ▪ Previous student group in Prof. Board’s cloud computing class leaked AWS credentials; attackers racked up $30,000 in service charges in a few days!

• Cloud provider has access to all your data!
  ▪ This may be a legal liability *and* a security concern
Cloud Security As A Service

- SecaaS
- Is a segment of the SaaS offering of a CP
- Defined by The Cloud Security Alliance as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers’ on-premise systems

This is bolt-on-security dumbness to appease people who want security to be easy and automatic (and we know it’s not).

Can a VM running network intrusion detection software be helpful? Yes.

Does that solve security? No.

Is it useful to call it “Sac-aaS”? No.
Cloud security practical defenses

• Do all the normal defensive techniques we’re learning

• Prevent cross-tenant data or access leakage:
  ▪ Cloud providers: keep your hypervisors up to date, ensure correct settings, apply network isolation techniques (e.g. VLANs)
  ▪ Customers: use reputable providers that do the above, ensure correct settings

• Prevent access rights issues:
  ▪ Set your access rights as restrictively as possible from the start
  ▪ Monitor access rights over time (there’s software for this)

• Prevent cloud command-and-control issues:
  ▪ Secure credentials
  ▪ Set service usage notices and pay caps

• Mitigate the fact the cloud provider has access to all your data:
  ▪ Don’t use the cloud’s storage services
  ▪ Encrypt the data before it hits the cloud (if possible)
  ▪ Don’t use cloud at all...