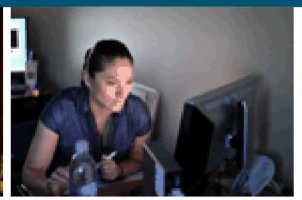
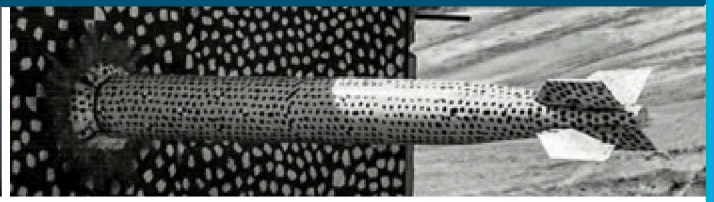
SAND2018-4791C

Securing Cloud Computing





NLIT Summit, May 2018

PRESENTED BY

Jeffrey E. Forster – jeforst@sandia.gov

Lucille Forster – lforste@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Introduction & Agenda

Todays **Agenda**

- Who Are We?
- Cloud Computing Definitions
- Benefits, Risks & Threat Model
- Notorious Nine Threats to Cloud Security
- Defense Strategies
- Conclusion & References
- Q&A: Closing Discussion

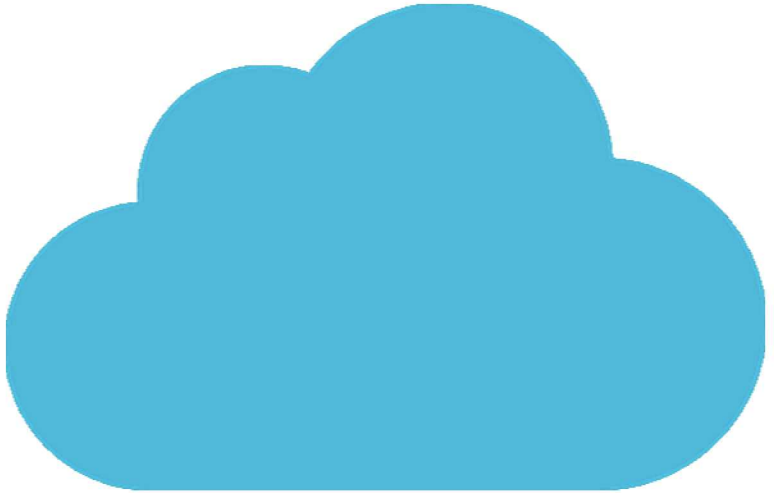
Who are **We?**

- Jeffrey Forster & Lucille Forster
  - Role
  - Background
  - Experience

Cloud Computing Definitions

What is **The Cloud?**

- **Virtualization**: a technique used to split a single physical machine into several isolated virtual machines (VMs) each with their own operating system (OS) and applications
- **Cloud Network**: a network of virtualized servers able to run a large number of VMs each with the appearance that they are running on their own physical machine
- **Cloud Computing**: multiple groups/clients making use of a cloud network's resources to perform computations and store data



Cloud Computing Service Models

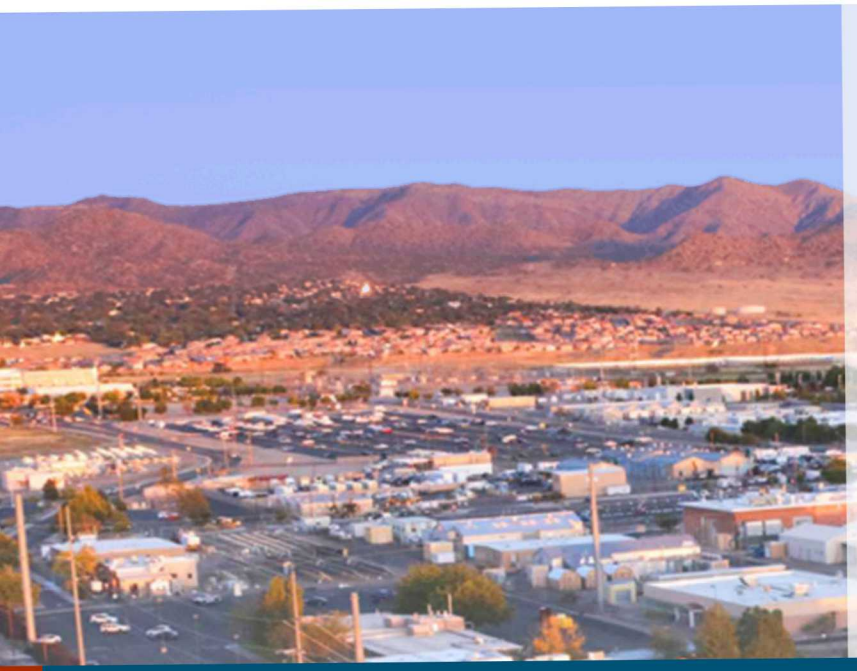
- **Infrastructure-as-a-Service (IaaS):** a business model providing a scalable infrastructure that can be used to run any system that a user needs to run
  - Examples: Amazon EC2, Microsoft Azure, Google Compute Engine
- **Platform-as-a-Service (PaaS):** a model that allows customers to use software tools to build their own programs and then host them on the server
  - Examples: Amazon Web Services (AWS) Elastic Beanstalk, Google App Engine
- **Software-as-a-Service (SaaS)**: a model allowing for applications to run in a cloud network
  - Examples: Microsoft Office 365, Google Applications

Cloud **Types**

1. **Public Clouds**: any individual with internet can pay for a use of some of a providers resources while maintaining isolation from other users
2. **Private Clouds**: a full cloud infrastructure that is only accessible by a single organization
3. **Hybrid Clouds**: a cloud network that uses a combination of private and public clouds
4. **Community Clouds**: similar to a private cloud except the ownership is shared between two or more organizations

Jungle of **Acronyms**

- **OS**: Operating System
- **VM**: Virtual Machine
- **VMM**: Virtual Machine Manager (Hypervisor)
- **IaaS**: Infrastructure as a Service
- **PaaS**: Platform as a Service
- **SaaS**: Software as a Service
- **CSA**: Cloud Security Alliance
- **CSRF**: Cross-Site Request Forgery
- **XSS**: Cross-Site Scripting
- **TEE**: Trusted Execution Environment (Enclave)

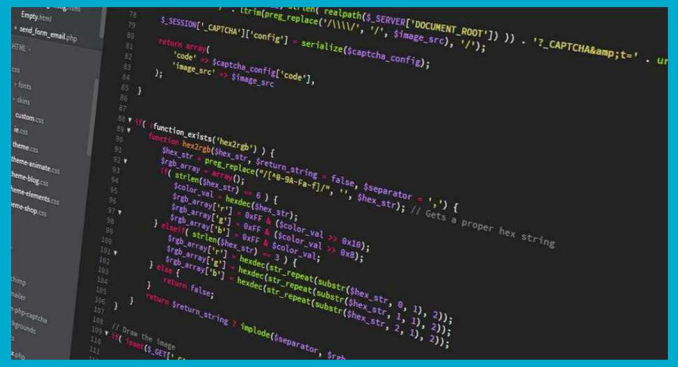


Benefits, Risks & Threat Model

for Cloud Computing

Cloud Computing **Benefits**

- Benefits for Providers:
  - Income from clients
  - Allows for heavy investment in security for the network
- Benefits for Clients:
  - Greatly reduces the costs of hardware
  - Eliminates the need to build and maintain a local data center
  - Resources are scalable
  - Limits exposure
  - Automated infrastructure deployment & configuration (Examples: Puppet, Chef, Ansible, SaltStack)



Cloud Security **Problems & Motivation**

- VMs have all the same security risks associated with physical machines as well as others because they do not run on isolated hardware
- If cloud security is compromised, both the provider and clients can all be affected
- Customers need to trust that the cloud service provider has sufficient security practices to protect their systems and data

Comparing Public & Private Clouds

Private Cloud

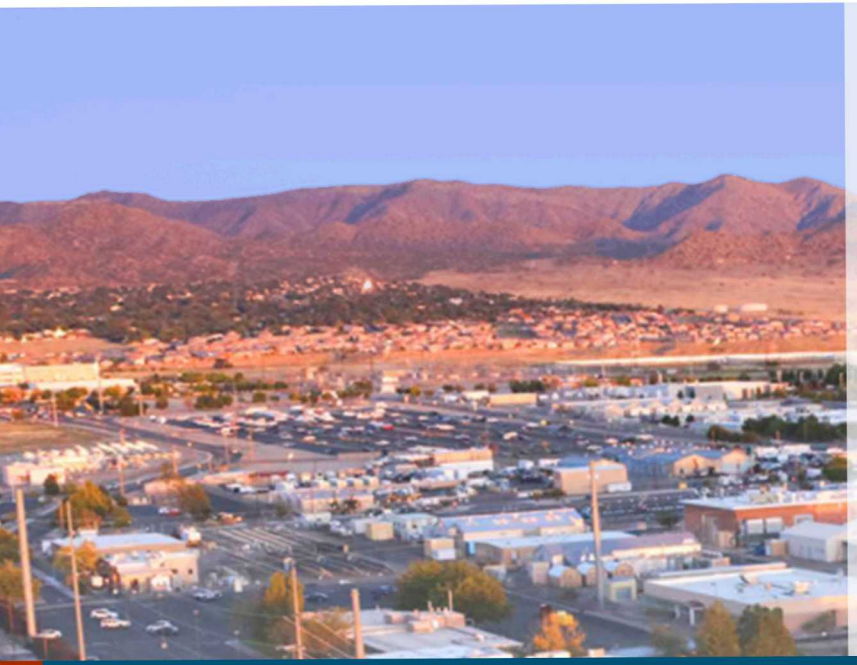
- Pros
  - More flexibility
  - More security controls
- Cons
  - Start up costs
  - Operating expenses
  - More access restrictions

Public Clouds

- Pros
  - Lower costs
  - Low to no maintenance
  - High reliability
  - Near unlimited resources
  - No wasted resources
- Cons
  - Security concerns
    - Meltdown
    - Spectre
  - Customization of resources and services may be more challenging

Security **Threat Model**

- Internal Threat
  - We consider a powerful adversary who has elevated rights to the entire software stack on the server including the hypervisor and operating system
  - Able to watch and modify any network packets as well as any data stored in the cloud providers stack
- External Threat
  - We consider an adversary who is able to exploit some vulnerability in the cloud providers infrastructure (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege)
- All attacks on the applications directly are considered out of scope since they can be applied on traditional client server and cloud based systems



The Notorious Nine

From the Cloud Security Alliance (CSA)

The Notorious Nine

1. Data breaches
2. Data loss
3. Account hijacking
4. Insecure interfaces
5. Denial of service attacks
6. Malicious insiders
7. Abuse of services
8. Insufficient due diligence
9. Shared vulnerabilities

Threat 1 **Data Breaches**

- When storing data in the cloud, data for all customers may be stored in the same location. It may therefore be possible for a secure system to be compromised if an attacker is able to successfully gain access from another secure system.
- Cloud provider insiders also pose a risk of data breaches. For example, a malicious cloud provider employee may choose to use his or her access to steal data from cloud clients.

Threat 2 Data Loss

- Even when data can't be accessed or stolen by an attacker, a vulnerability can lead to data being deleted or modified
- Even a small loss of data can be catastrophic for companies that are storing their most valuable data in the cloud
- Data loss can be caused by malicious users or by operator error

Threat 3 **Account Hijacking**

- Account hijacking is the act of exploiting vulnerabilities in an application to obtain a users private credentials
- Can be accomplished through several exploits:
  - Cross-site request forgery (CSRF) which allows an attacker to send malicious requests by exploiting a target's session with a web server
  - Cross-site scripting (XSS) which allows attackers to inject client side scripts into pages

Threat 4 **Insecure Interfaces**

- In order to interact with, communicate with, and control the cloud, Application Programming Interfaces (APIs) are often used as the intermediary interface for higher level systems
- If these interfaces are weak or do not contain an adequate amount of security features in order to prevent exploits, the cloud as a whole may become susceptible to malicious activity

Threat 5 **Denial of Service Attacks**

- Denial of Services (DoS) attacks may be the simplest attacks to implement on a cloud computing device. A DoS attack consists of flooding an Internet connected device with requests
- This overabundance of requests is harmful to the VM receiving them because the VM becomes overwhelmed with requests and therefore becomes unable to handle its standard request load
- DoS attacks are very common and can bring even large systems down for extended periods

Threat 6 Malicious Insiders

- An individual within an organization who has insider information about the organization's security practices, data or systems that uses that information to cause harm is known as a malicious insider
- Insiders are able to cause physical and financial damage to the businesses and institutions because they have elevated permissions that are legitimately needed to perform their jobs
- Malicious insiders pose many security threats because they can perform fraud, theft and sabotage on computing systems.

Threat 7 **Abuse of Services**

- One of the main advantages of cloud computing is that it is virtually computationally limitless
- Cloud users have the illusion of having infinite computing resources available on demand
- Attackers can utilize these extensive computing resources to crack encryption keys, perform DoS attacks or perform other malicious attacks that would not be possible on limited hardware
- Abuse of services can also be used to mine crypto currency

Threat 8 **Insufficient Due Diligence**

- Many organization rush to move to the cloud for all the benefits without considering all the potential problems and threats
- Even if a cloud provider has good protections from threats, there is a risk an organization's data could be compromised during the migration process
- Clients that rush to migrate to the cloud may also have misunderstanding about what the cloud provider will and will not do to protect them
- These terms of service are specified in a provider's service level agreement (SLA), and users often fail to understand the full scope of this contract

Threat 9 **Shared Vulnerabilities**

- When handling, allocating, and managing a large set of virtual machines in the cloud, it is common to have multi-tenancy situations in which multiple machines share hardware resources
- When VMs are co-located on the same system, a breach on one machine is capable of spreading to the other virtualized systems

Defense Strategies

Techniques & Tools for Securing Cloud Computing

Strategy I Service Level Agreements

- The Service Level Agreement (SLA) lists responsibilities and obligations for both providers and users
- Provides legal protection

Defends Against Threats

- Data breaches
- Data loss
- Malicious insiders
- Insufficient due diligence
- Shared vulnerabilities

Strategy 2 **Snapshots & Backups**

- Snapshots are backups of both VMs data and state
- Using snapshots allows for providers to create complete backups that can be restored at any time
- These backup restore points reduce the amount of data that is lost in the event of a failure

Defends Against Threats

- Data breaches
- Data loss

Strategy 3 Machine Separation

- Machine separation is the idea of moving data, VMs, and snapshots into different physical machines or even different data centers
- Handled by the infrastructure team
- Separating different components of one users system can reduce the risk of total failure when a machine goes down

Defends Against Threats

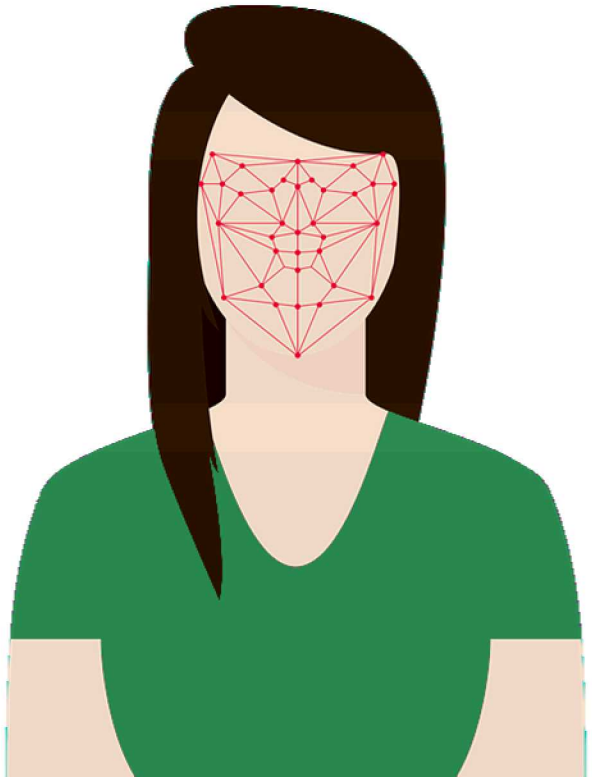
- Data loss
- Denial of service attacks
- Malicious insiders
- Shared vulnerabilities

Strategy 4 **Access Control Systems**

- Handle authentication for different accesses and limit what different users can do
- Limit each individual's power and responsibilities
- Sophisticated authentication mechanisms including two-factor

Defends Against Threats

- Data breaches
- Data loss
- Malicious insiders
- Insufficient due diligence
- Shared vulnerabilities



Strategy 5 Encryption

- Strong Encryption is very important when moving information to and from a cloud network
- Encryption can protect data from being stolen or modified

Defends Against Threats

- Data breaches
- Insecure interfaces
- Malicious insiders
- Insufficient due diligence
- Shared vulnerabilities

Strategy 6 **Trusted Hardware**

- Trusted Execution Environments (TEEs) or Enclaves enable additional security at the hardware level.
- Storage areas are built and maintained by customer, achieving protection from providers.
- One of the most popular trusted hardware implementations is Intel's Software Guard Extensions (SGX).

Defends Against Threats

- Data breaches
- Data loss
- Insecure interfaces
- Malicious insiders
- Abuse of services
- Insufficient due diligence
- Shared vulnerabilities

Strategy 7 Virtual Machine Introspection (VMI)

- VMI is a method that cloud providers can use to monitor running VMs to collect information on resource usage, network traffic, memory, etc.
- Cloud providers can use this information to determine if a VM is malicious or has been compromised
- VMI can also be used on VM snapshots

Defends Against Threats

- Account hijacking
- Denial of service attacks
- Abuse of services
- Insufficient due diligence
- Shared vulnerabilities

Conclusion & References

Conclusion

- Public and private clouds have many benefits; they also have some risks
- The Cloud Security Alliance has outlined the "Notorious Nine" which are the biggest risks
- Many of these threats are not specific to the cloud
- There is an ever growing set of techniques and tools for combating these risks

References

1. J. Forster "Using Intel® SGX Technologies to Secure Large Scale Systems in Public Cloud Environments," Master's thesis, Georgia Institute of Technology, 2018.
2. R. Los, D. Shackleford, and B. Sullivan, "The Notorious Nine Cloud Computing Top Threats in 2013," *Cloud Security Alliance*, 2013.
3. R. Kalaiprasath, R. Elankavi, R. Udayakumar, et al., "Cloud. Security and Compliance-A Semantic Approach in End to End Security," *International Journal Of Mechanical Engineering and Technology (IJMET)*, vol. 8, no. 5, 2017.
4. C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A Survey on Security Challenges in Cloud Computing," *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 47–54, 2013.
5. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2013.
6. K. Dahbur, B. Mohammad, and A. B. Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing," in *Proceedings of the 2011 International Conference on Intelligent Semantic Web-services and Applications,* ACM, 2011.

Closing Discussion, Q&A

- Discussion
  - What lessons can you share?
  - What tools and practices work for you?
  - What are your issues?
- Questions?