Cloud Security Through Threat Modeling

Robert M. Zigweid
Director of Services for IOActive
Key Points

• Introduction
• Threat Model Primer
• Assessing Threats
• Mitigating Threats
• Sample Threat Model Exercise
• Conclusions and Questions
INTRODUCTION
Everything as a Service

FLEXIBLE AUTHENTICATION METHODS

MANAGED APP INTEGRATIONS
Service Providers (SPs)

HOSTED/CLOUD SERVICE
Cloud Service Providers (CSPs)

Enterprise VPC

Organization Management

Authentication Authorization

User Management

Third Party Cloud Apps

Third Party On-Premises Apps

First Party Apps

Individuals

Sign In

Username

Password

Third Party Identity Sources

LinkedIn

Google

Social ID / OpenID

Windows Server

Active Directory

LDAP

Third Party Identity Stores

Enterprise Identity Providers

LDAP

Oracle

IBM

How can security weigh-in with real risks?
Cloud Security Wisdom

This wisdom is captured best here:
Cloud Security Wisdom
What Is It?
Modeling Risks Programmatically

Microsoft SDL Process

Developing Threat Models
- Structured approach
- Repeatable way to identify attack surfaces (i.e. risk)
- Develop mitigations and acceptance criteria
- Can be applied to anything—even Cloud environments
Threat Modeling
Cloud Environments

Threat analysis guidance provided in this domain

10.6.2 Risk Analysis Recommendations

- Risk analysis of the applications for security and privacy (confidentiality, integrity and availability) are undertaken, and threat models should be built and maintained.
- Risks from the perspective of development and deployment in the cloud should be analyzed and related threat models maintained.

...good thinking, now let's talk about how to create threat models
THREAT MODEL PRIMER
Why Threat Model?

- Threat modeling is not just for code
  - Anything can be Threat Modeled
  - Output will drive risk analysis and business decisions
- Implementing in the Cloud is still code
  - Deploying and managing servers is all software
  - It has driven the rise of Dev-Ops personnel
When to Threat Model

• Not a one time event
• Adding or removing assets/components
  • It is never too late!
• What you need to know before you start
  • What are you building?
  • What needs to be protected?
• You can be too early, especially on new projects
Threat Modeling Tools

• The tool used is less important than the data recorded
• Using a tool already? Keep doing so!
• Whiteboards are a favorite
  • Do not forget longer term retention
• Data Flow Diagrams
Assessment and Identifying Threats

• Identify Data Assets
  • Determine Each Assets Relative Value
• Identify Actors and Data Asset Visibility
  • Internal Personnel
  • CSP Personnel
  • Government?
Assessment and Identifying Threats

• Data Flow Diagram
• Identify Points of Trust Boundaries
  • Points at which control changes
• Identify Points of Vulnerability
• Know Where Your Data Is
  • To the best of your visibility
ASSESSING THREATS
CSP Responsibilities–IaaS

• Hardware Layer
• Network Layer (IDS, DDoS, Guest Instances)
• Instance Access Control Rules
CSP Responsibilities–PaaS

• Hardware Layer
• Operating System Layer
• Network Layer
  • May not be inherited from IaaS
• Access Control Rules
CSP Responsibilities–SaaS

• All asset integrity and visibility is dependent upon the CSP regardless of service
CSP Threats–IaaS

• Data Visibility
  • Government requests
  • May be able to be mitigated

• Network Traffic Shaping and Manipulation

• Hypervisor Trust
CSP Threats—PaaS

• IaaS threats included
• Like a Managed Service Provider
  • Shared Root/Admin
• Less control over data
  • Depends on nature of PaaS
• Data Storage vs. Application Hosting
• Depends on how the data is used
CSP Threats—SaaS

• IaaS and PaaS threats included
• No guaranteed control over data
  • CSP must be completely trusted
MITIGATING THREATS
Mitigating CSP Threats–IaaS

- **Data Storage**
  - Storage location
  - Encryption and key management control
  - Avoid using ephemeral disks

- **Authentication and Authorization**
  - Use your own system whenever possible
Mitigating CSP Threats–IaaS

• Data transit
  • Encryption with your own certificates if possible
  • Pass through load balancers instead of terminating connections there
  • Includes administration

• Network segmentation and firewalls, if available
Mitigating CSP Threats—PaaS

• Monitor all access, regardless of who
  • It might not be a critical event—but then again, it might
• Use encrypted transit with your certificates/keys
  • Be careful where you store the private keys
• Encrypt before storing
• Log where possible
Mitigating CSP Threats–SaaS

• There is no control
• Deleted vs. non-visible
• Legal might help
The Fun Part: Multiple Services

• Most Cloud implementations use multiple services
• Data Flow Diagrams show their worth
• It is necessary to break the components down
  • Take each service on its own merit
  • They might not be from the same CSP
    • Could be a good thing
SAMPLE THREAT MODEL EXERCISE
Exercise: CSP Service Definition

<table>
<thead>
<tr>
<th></th>
<th>ACME Cloud Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Web UI supplied to customers to manage users and access</td>
</tr>
<tr>
<td>2.</td>
<td>RESTful API service to post and retrieve data in custom XML protocol</td>
</tr>
<tr>
<td>3.</td>
<td>Underlying data storage architecture undisclosed to customers</td>
</tr>
</tbody>
</table>
Exercise: Data Flow Diagram

CSP Customers

Firewall

API Service

IAM Service

Storage

CSP Employees

CSP Admins
### Exercise: Identifying Assets

<table>
<thead>
<tr>
<th>Asset</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Company Public</td>
</tr>
<tr>
<td>User Name</td>
<td>Company Confidential</td>
</tr>
<tr>
<td>User Account #</td>
<td>Company Public</td>
</tr>
<tr>
<td>User CC #</td>
<td>Secret Confidential</td>
</tr>
<tr>
<td>Account Rep ID</td>
<td>Company Confidential</td>
</tr>
</tbody>
</table>
Exercise: Identifying Actors

**Actors**
- Anonymous
- Account Rep
- Account Manager
- Account Administrator
- CSP Personnel
- CSP Customers

**Classification**
- Anyone not authenticated
- Authenticated account representative
- Account representative managers
- Controls account rep & managers access
- CSP employees and administrators
- Other customers using similar interfaces
Exercise: Identifying Threats

**Threat**
- Data accessed or modified without authorization
- Account credentials exposed or modified
- Service not available
- Operating System Access

**Potential Actors**
- Anonymous, CSP employees, CSP administrators, other CSP customers, other account representatives
- All potential users—not credential owner
- All users
- Anonymous, CSP administrators
Exercise: Identifying the Attack Surface

**Threat**
- Data accessed or modified without authorization
- Account credentials exposed or modified
- Service not available
- Operating System access

**Attack Surface**
- Web Application/Service Flaw (XSS, CSRF, SQLi), Malware on System, Hypervisor Compromised, Command Injection
- Web Application/Service Flaw (SQLi), Malware on System, Hypervisor Compromised, Command Injection
- Required Systems offline, Firewall/Router misconfiguration, DDOS, IPS, WAF
- Malicious CSP Admin, Hypervisor Compromised, Web Application Flaw (Command Injection, SQLi)
Exercise: Mitigate or Accept

**Threat**
- Data accessed or modified without authorization
- Account credentials exposed or modified

**Potential Mitigation**
- Encrypt data at rest
- Improve access groups
- Find new CSP
- Accept threat
- Enforce use of HTTPS
- Contract CSP to improve service
- Find new CSP
- Enforce use of IAM layer or service provider
Exercise: Mitigate or Accept

**Threat**
- Service is not available
- Operating System access

**Potential Mitigation**
- Onsite backup
- Caching
- Separate DR compute region
- Multiple AZs or CSPs
- Patching
- Consistent Access Control
- Enforcement
- Change CSPs
- Operating System Hardening
CONCLUSIONS AND QUESTIONS
Conclusions

• Risk vs. Reward
  • Identify risk to minimize it
  • Increase reward—leverage CSPs that work

• Cloud Projects will involve discrete backend services
  • Lots of API interaction at SaaS, PaaS, and IaaS levels
  • Focus on permissions, authentication, and authorizations

• Leverage legal contracts and compliance assurances
Questions
Thank You!

Robert M. Zigweid
rzigweid@ioactive.com