Dynamic Intrusion Deception in a Cloud Environment

Chia-Chi Teng, Aaron Cowley, Russel Havens
Brigham Young University
Provo, USA
Cloud Computing Security

• NIST: Cloud Computing Security Reference Architecture
• ENISA: Security Framework for Governmental Cloud
• US DoD: Digital Modernization Strategy
• ...

Honeypot etc.

• HoneyNet
• HoneyFarm
• HoneyBrid
• HoneyMix
• HoneyProxy
Open-source Projects

• Dionaea
• Honeyd
• Kippo
• Glastopf

• CloudHoneyCY
Cloud Enabled Honeypot/net

• Scalability
• Performance
• Cross-platform
• Cost

• Initial Focus: SSH Brute-force Attacks
Logical Overview
Technologies

- Windows Azure
  - Resource Group Management
  - Firewall
  - Azure Service Fabric, Reverse Proxy
- Docker & Container
- Zeek (formerly Bro) Network Security Monitor
- OpenSSH
Prototype on Azure
Features

• Dynamically provision and revoke Honeypots based on level of malicious network activities.

• High-interactivity Honeypots with dynamically configured SSH service.

• Use container technology, e.g., Docker, for increased performance and scalability.

• Easily deployable in a commercial cloud platform, e.g., Microsoft Azure.
Conclusion

- Honeypot/net as an important and necessary component in Defense-in-Depth strategy
- Cloud Computing enables better, stronger, more realistic and dynamic Honeypot/net