Community-Based Secure Information and Resource Sharing in AWS Public Cloud

Cyber Incident Response
A Model for Information and Resource Sharing

Amy(Yun) Zhang, Farhan Patwa, Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
CIC, Oct 2015, Hangzhou, China

Presented by: Ravi Sandhu
Public Cloud

• Public cloud provides cloud services for self-service use by general public over the internet.
  • Amazon Web Service (AWS)

• Communities in public cloud
  • organizations with shared concern, such as mission, security requirements, business models, etc.
  • self-formed and self-organized.
Cyber Collaboration Initiatives

• Cyber attacks are becoming increasingly sophisticated.
  – Hard to defend by a single organization on its own.

• Collaborate to enhance situational awareness
  – Share cyber information in community
    • Malicious activities
    • Technologies, tools, procedures, analytics.

Ref: www.huffingtonpost.co.uk/2013/04/23/uk-government-faces-1000-cyber-attacks-a-day_n_3138164.html
Secure Isolated Domain (SID) Model
SID Model

Core Project (CP)

Open Project (OP)

Secure Isolated Domain (SID)

Secure Isolated Project SIP-1

Secure Isolated Project SIP-n

Org-1

Org-m

Community

Expert-1

Expert-k

Experts
Assumptions and Scope

• In a public cloud platform
• Amazon Web Service (AWS)
• Sharing amongst a set of organizations
  – Sensitive cyber information, infrastructure, tools, analytics, etc.
  – May share malicious or infected code/systems (e.g. virus, worms, etc.)
• Focus on access control model
Amazon Web Service (AWS)

• Dominant public cloud software
  – Amazon Web Services (AWS), a collection of remote computing services, also called web services, make up a cloud-computing platform offered by Amazon.com.

Ref: https://en.wikipedia.org/wiki/Amazon_Web_Services
AWS Access Control Model

- AWS Access Control within a Single Account
AWS Access Control Model

- **AWS Access Control Across Accounts** [Users in account A access services and resources in account B]
SID Model

Secure Isolated Domain (SID)

Core Project (CP)
Open Project (OP)
Secure Isolated Project SIP-1
Secure Isolated Project SIP-n

Org-1 Org-m
Community

Expert-1 Expert-k
Experts

UTSA
AWSAC-SID Administrative Model

- **SipCreate(subuSet, sip)**
  /* A subset of organization security admin users together create a sip */

- **SipDelete(subuSet, sip)**
  /* The same subset of security admin users together delete a sip */

- **CpUserAdd(adminu, u)**
  /* CP admin add a user from his home account to CP */

- **CpUserRemove(adminu, u)**
  /* CP admin remove a user from CP */

- **SIPUserAdd(adminu, u, r, sip)**
  /* Sip admin add a user from his home account to SIP */

- **SIPUserRemove(adminu, u, r, sip)**
  /* Sip admin remove a user from SIP */

- **OpenUserAdd(u)**
  /* Users add themselves to OP */

- **OpenUserRemove(u)**
  /* Users remove themselves from OP */
AWSAC-SID Administrative Model

• CpEUserAdd(adminu, eu)
  /* CP admin add an expert user to CP */

• CpEUserRemove(adminu, eu)
  /* CP admin remove an expert user from CP */

• SipEUserAdd(adminu, eu, r, sip)
  /* SIP admin add an expert user to SIP */

• SipEUserRemove(adminu, eu, r, sip)
  /* SIP admin remove an expert user from SIP */

• CpCopyObject(u, o1, o2)
  /* Users copy object from organization accounts to CP */

• CpExportObject(adminu, o1, o2)
  /* Admin users export object from CP to organizations accounts */

• SipCopyObject(u, r, o1, o2, sip)
  /* Users copy object from organization accounts to a SIP */

• SipExportObject(adminu, o1, o2, sip)
  /* Admin users export object from SIP to organization accounts */
Enforcement

• SID Service Setting-up
Enforcement

• Setting up SID service
  – Create two roles in the Core Project account: $CPadmin$ and $CPmember$
    – $CPadmin$ allows the user have limited administrative power to use the role $CPmember$ and specify policies for users from his organization.
  – Create one role in the Open Project account: $OPmember$
    – $CPadmin$ allows all users from the community to access the Open Project account.
  – SID manager maintains a list of security administrative users ($uSet$) from organizations.
Enforcement

• SIP User Assignment
Enforcement

• SIP request handling
  – Users from *uSet* send a SIP request to SID manager
  – SID manager creates a SIP
  – SID manager associates the group of organizations to the SIP
  – Two roles are created in the SIP account: *SIPadmin* and *SIPmember*
    – *SIPadmin* allows the user have limited administrative power to use the role *SIPmember* and specify policies for users from organizations to join the SIP
  – SID manager returns an SIP account number with the name of the *SIPadmin* role to each user from *uSet*. 
Conclusion and future work

• Suggested AWSAC and AWSAC-SID models to AWS public cloud
  – Allow cyber collaboration across organizations
    • cyber incident response
    • Self-service

• Future work
  – Explore other model options.
  – Explore local roles in the model.
  – Explore models in other dominant cloud platforms.
Thanks!