Secure Cyber Incident Information Sharing

UTSA Team Leads
Dr. Ram Krishnan, Assistant Professor, ECE
Dr. Ravi Sandhu, Professor (CS) and Executive Director (ICS)

April 09, 2014
LMI Research Institute (LRI): Academic Partnership Program

- Through formal working relationships with universities across the country, LMI bridges the gap between academia and industry to create innovative solutions and explore new research topics.
- The partnership program exposes students to real-world challenges faced by the federal government through structured, funded research projects.
Cyber Incident Response

• Secure information sharing amongst a set of entities/organizations
  – Often ad hoc

• What are the effective ways to facilitate information sharing in such circumstances?
  – Information sharing models
  – Infrastructure, technologies, platforms
Agile Incident Response

Long-Term Members

Org A
Org B
Org C
Org D

Personnel Join/Leave

Personnel+ Resources

Resources Add/Remove

Team 1

Team 2

County Threat Emergency Response
Local Police

Within a team:
- Controlled access
- Flexible and fine-grained access control
- Team should function unaffected by membership dynamics

UTSA Engineering
The Institute for Cyber Security
Cyber Incident Information Sharing Scenarios

• High-assurance scenarios
  – Closed network
  – Data exfiltration

• Medium-assurance scenarios
  – Community
  – Electric grid
Key Requirements

• Cyber infrastructure sharing to support data and compute
• Light-weight and agile
• Rapid deployment and configuration
• Secure environment
Cloud Infrastructure as a Service

• Virtualized IT infrastructure (servers, storage, networks, OS, etc.)
  – Delivered as a service over a network, on demand, dynamic scaling, etc.

• Prominent examples
  – Amazon AWS
  – OpenStack
Information Sharing in a High-Assurance Scenario

- Physically secure meeting room
- Air-gapped network
- Cloud-in-a-box
Enforcement in Cloud IaaS

Air-Gapped Meeting Room

Cloud-in-a-Box

Secure Isolated Domain (SID)

Participant A

Add/Remove Data
Join/Leave Users

Participant B

Add/Remove Data
Join/Leave Users

Participant C

Add/Remove Data
Join/Leave Users

View #1: OrgA
View #2: SID

View #1: OrgB
View #2: SID

View #1: OrgC
View #2: SID
Next Steps

- UTSA to incorporate 24 AF input
- Develop prototype in OpenStack
- Share research results with 24 AF
  - August/September
Thanks

• Comments, Q&A
Backup
OpenStack

- OpenStack
  - Dominant open source cloud IaaS platform

- >200 companies
- ~14000 developers
- >130 countries
Project Goal

Tasks:
1. Manage Virtual Infrastructure
2. Create and Manage Tenants (e.g. create tenant super-user)

Tenant #1
IT Super-Users (Architects)

Tasks:
1. Architect Attributes of Org’s Users + Cloud Resources
2. Create and Manage Admin Users
3. Manage Attributes of Admin Users

Tasks:
1. Create and Manage Org’s Regular Users
2. Manage Attributes of Regular Users
3. Manage Attributes of Org’s Resources

Tenant #1
Administrative IT Users

Tasks:
1. Day-to-Day Operations
2. Add/Remove Capacity
3. Manage N/W
4. Backup, Snapshot, etc.

Tenant #2
Regular IT Users

Tenant #3

Inter-Tenant Sharing

Utilize

ABAC Administrative Models

CSP’s OpenStack

Servers

Storage

Network

CSP Personnel

Utilize

ABAC Operational Models

The Institute for Cyber Security