Spyglass:
Secure Cloud System Administration

Patrick T. Cable II, Nabil Schear

29th USENIX Large Installation System Administration Conference

11 November 2015

Distribution Statement A: Approved for Public Release, Distribution is Unlimited. This work is sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.
A System Administrator’s Life

System administrators have unrestricted access to security-sensitive infrastructure
The Problem

Phishing

Internet

Cloud Controller Network

The Insider

Cloud Controller Network

Problems for all...

... big, and small.
Let’s Protect a Network

A look at how well different network devices audit and protect

Firewalling

Virtual Private Networks

Bastion Host

Limit impact of malicious clients through secure auditable bastion host
Building a Better Bastion Host

The Problem with Bastion Hosts

• Easy to implement insecurely
• Unprotected auditing
• Single point of failure
• Good for side-channel analysis

Spyglass
Threat Model

System assumptions:

• Remote attacker trying to persistently access private network

• May have compromised a valid user’s source system or credentials

• Attacker can compromise applications inside of containers that face the remote network and cannot break container isolation

• Attacker cannot compromise control process

• Proper configuration of SSH and container manager

• Valid users must use present multiple factors to authenticate
Welcome

Spyglass is an application that manages non-persistance containers that allow you to access a private network.

To get started, add a public SSH key to your profile, then start a new session using the menus above.

© 2015 Massachusetts Institute of Technology
Spyglass: Add a Key

New Key

Key Name
Desktop

SSH Key
ssh-rsa
AAAAB3NzaC1yc2EAAAADQABAAAAABAQCGgQz4EpBS/sCuJ8vM7MtfQaGz4s0rhSNnrqVXZxA9/por

Add Key

© 2015 Massachusetts Institute of Technology
Spyglass: New Session

New Session

Key Name
Desktop

Spawn Container

© 2015 Massachusetts Institute of Technology
## Spyglass: Session Details

### Sessions

<table>
<thead>
<tr>
<th>ID</th>
<th>Host</th>
<th>Port</th>
<th>Created</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Se00eb4f17da</td>
<td>labuser</td>
<td>49156</td>
<td>07Apr15 1204 EDT</td>
<td>delete</td>
</tr>
</tbody>
</table>

© 2015 Massachusetts Institute of Technology
Container Instantiation Speed

Containers are quickly available for end-admin use
Host Overhead

Containers are not a memory or CPU burden for the host
Attacks

Host Denial of Service
- Was able to fill file system on container host
- Workarounds noted, though may have impact on performance
- User namespaces will make this more difficult

Network Protection
- Proper configuration options with Docker disables container/container comms
- Further tweaking with IPTables allows for finer grained controls

Escalation & Escape
- User must escalate to root inside container
- No SELinux in demo implementation, would add another layer of complexity
- Matters to a varying degree depending on public and private networks

User Namespaces Coming Soon to Docker
Conclusion and Future Work

• Conclusion
  – Unauthorized access to control networks allow an attacker to wreak havoc on your organization
  – Spyglass provides an architecture to monitor your admins and protect your sensitive control networks

• Future Work
  – Provide container host key ID to web application
  – Make auditing collector far more resilient
  – Ignore sensitive details in audit log
  – SELinux support
  – Enterprise authentication tie-in
  – VNC session support

Relax system admins… you’re less of a liability now!

Fork & Improve Spyglass!
github.com/mitll-cyber