SilverLine: Data and Network Isolation for Cloud Services

Yogesh Mundada
Anirudh Ramachandran
Nick Feamster
Cloud Computing Advantages

• Reduced operational costs
• Reduced management overhead
• Easier resources scaling
• Lowers the barrier to entry for new services

Cloud revenue for 2010 was $68 billion. Estimated revenue for 2014 is $150 billion.
Recent Cloud Data Leak Incidents

• Microsoft BPOS cloud service data breach (Dec 2010)
• Heroku cloud application platform vulnerability (Jan 2011)
• Dropbox hash-tag security flaw (May 2011)

Occurrences such as these make adoption of the cloud harder
Top Cloud Computing Threats

• Shared resources
  – Heroku

• Data loss and leakage
  – Microsoft BPOS
  – Dropbox
## SilverLine Solution: Isolation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Attack</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss</td>
<td>Service exploit, Operating environment exploit, Misconfigurations</td>
<td>SilverLine’s Information Flow Tracking and Control</td>
</tr>
<tr>
<td>Network Side-Channels</td>
<td>Gain more information about the environment through namespace, RTT and hop-count study</td>
<td>SilverLine’s obfuscation of network metrics to reduce the information entropy.</td>
</tr>
</tbody>
</table>
SilverLine Data Isolation

• Information Flow Tracking
  – Add taints or labels to data
  – Track the taints
  – System Call Hooks

• Components of the system
  – Tracker: Initialize and track taints, on end hosts
  – Enforcer: Stop unauthorized data flow, in the network
Example Setting

SilverLine Storage service
With automatically created labels for each database record
Example Setting

Alex’s records are Labeled with a taint ‘A’
Example Setting

VM instance that runs application logic

Storage Service

SilverLine Tracker in Kernel

Enforcer

Login

Declassifier

Front End Webserver
Example Setting

Custom LOGIN module & Declassifier
Example Setting

Network Level Enforcer in Dom0
Normal User's Interaction

A1. Login & "Get My Balance"

A2. Authenticate Alex to Declassifier

A3. Start Worker Process

A4. Get Alex's Balance

A5. Ans = $100, Label='A'

A6. Labeled Replies

A7. Alex's Replies pass

A8. Reply = $100

Database

<table>
<thead>
<tr>
<th>User</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>$100</td>
</tr>
<tr>
<td>Bob</td>
<td>$10</td>
</tr>
</tbody>
</table>

SilverLine Storage Service

Alex's Worker Process

VM

Application Logic

Front End Webserver

Login

Declassifier

Labels maintained by SilverLine

'A'

'B'

VM

Enforcer
An Attacker’s Interaction

B1. Login, SQL exploit to get Bob & Alex's Balance

B2. Authenticate Bob

B3. Start Worker process

B4. Get Bob & Alex's Balance

B5. Ans= ($10, $100), Label='B, A'

B6. Labeled replies

B7. Bob's Replies are blocked

Labels maintained by SilverLine 'A' 'B'

SilverLine Storage Service

SilverLine Tracker in Kernel

VM

Application Logic

Bob's Worker Process

Enforcer

Front End Webserver

Login

Declassifier

Bob: the attacker
SilverLine Configuration

• Labeling Service
  – Specify Taint Creation Policy
    
    \textbf{when} \texttt{query := “INSERT” and table := “USERS”}: \textit{Generate a new label; add it to the DB record}

• Custom \textbf{Login} module
  – Provided by each tenant
  – Authorizes legitimate users
## SilverLine Solution: Isolation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Attack</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss</td>
<td>Service exploit, Operating environment exploit, Misconfigurations</td>
<td>SilverLine’s Information Flow Tracking and Control</td>
</tr>
<tr>
<td>Network Side-Channels</td>
<td>Gain more information about the environment through namespace, RTT and hop-count study</td>
<td>SilverLine’s obfuscation of network metrics to reduce the information entropy.</td>
</tr>
</tbody>
</table>
SilverLine Network Isolation

- IP address obfuscation
  - Actual Internal IP to Pseudo IP
  - OpenFlow protocol
- Entirely in the software
- Minimal changes

<table>
<thead>
<tr>
<th>Actual IP</th>
<th>Pseudo IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.b.c.d</td>
<td>w.x.y.z</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>

Local Controller

Click Software Router with OpenFlowClick

Centralized Controller
• Normalize network metrics
  – Realistic RTTs between instances
  – Minimal threshold on hop counts
  – Modified openflow module for per packet decision
Summary

• Data Isolation: Information Flow Tracking
• Network Isolation: Reducing the entropy of the network side-channels

Future Work

• Measure the taint leakage
• Fine grained tainting in a VMM
Questions

B1. Login, SQL exploit to get Bob & Alex's Balance

B2. Authenticate Bob

B3. Start Worker process

B4. Get Bob & Alex's Balance

B5. Ans= ($10, $100)
Label='B,A'

B6. Labeled replies

B7. Bob's Replies are blocked

Labels maintained by SilverLine 'A' 'B'

Database

<table>
<thead>
<tr>
<th>User</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>$100</td>
</tr>
<tr>
<td>Bob</td>
<td>$10</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

Bob: the attacker