Custos
Increasing Security with Secret Storage as a Service

Andy Sayler
Dirk Grunwald

TRIOS14
10/05/14

University of Colorado Boulder
Where do we store data today?
Trust?
Secure?
How can we control and protect our data?
How can we control and protect our data? (even when storing it with third parties)
Client-Side Encryption?
Encrypt

“My Secret”

Decrypt

TXkgU2VjcmV0
But What About the Keys?
"My Secret" → Encrypt → TXkgU2VjcmV0 → Decrypt → "My Secret"
Encrypt

Decrypt

“My Secret”

TXkgU2VjcmV0
Custos
Custos

Latin for “Guard”
“Key Storage as a Service”
“Secret Storage as a Service”
"My Secret" → Encrypt → Decrypt → TXkgU2VjcmV0
Encrypt

"My Secret"

Decrypt

TXkgU2VjcmV0
Core Features
Centralized Secret Storage
Centralized Secret Storage

Flexible Access Control
Centralized Secret Storage
Flexible Access Control
Auditing and Revocation
Centralized Secret Storage
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Example: Multi-Device File Sync
Managed SSH Agent
Managed SSH Agent
Scalable SSL Processor
Managed SSH Agent
Scalable SSL Processor
Etc...
Centralized Secret Storage in Custos
Custos Server
Trust?
Do you have to trust a single provider?
Multi-Provider Sharding
Multi-Provider Sharding

Shamir Secret Sharing
Client Application
Availability
Availability

Sharding with \((k, n)\) Threshold Scheme
Centralized Secret Storage
Centralized Secret Storage

Flexible Access Control
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup

CorrectHorseBatteryStaple
Example: Autonomous Server Bootup

CorrectHorseBatteryStaple
Example: Autonomous Server Bootup

CorrectHorseBatteryStaple
Example: Autonomous Server Bootup

CorrectHorseBatteryStaple
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup
Example: Autonomous Server Bootup

1.2.3.4/24
Example: Autonomous Server Bootup

1.2.3.4/24
Example: Autonomous Server Bootup

1.2.3.4/24
Example: Autonomous Server Bootup

1.2.3.4/24
Example: Autonomous Server Bootup

1.2.3.4/24
Backup Systems
Backup Systems
Time-Limited Access
Backup Systems
Time-Limited Access
Etc...
Flexible Access Control in Custos
Custos Server

- Secret Store
- Access Control Subsystem
- Custos API

SSL

Client A
- Custos API
- Application

Client B
- Custos API
- Application

Client C
- Custos API
- Application
Custos Server

Authentication Subsystem

Secret Store

Access Control Subsystem

Custos API

SSL

Client A

Custos API
Application

Client B

Custos API
Application

Client C

Custos API
Application
Custos Server

Authentication Subsystem

Secret Store

Access Control Subsystem

Custos API

SSL

Client A

Custos API

Application

Client B

Custos API

Application

Client C

Custos API

Application
“Secret”
"Secret"

Access Control Specification (ACS)
"Secret"

Access Control Specification (ACS)

Permission A
"Secret"

Access Control Specification (ACS)

Permission A

Access Control Chain
Access Control Specification (ACS)

Permission A

Access Control Chain

Auth Attribute

Auth Attribute

Auth Attribute
“Secret”

Access Control Specification (ACS)

Read Permission

Access Control Chain

Auth Attribute

Auth Attribute

Auth Attribute
Access Control Specification (ACS)

“Secret”

Read Permission

Access Control Chain

Username

IP Address

Password
Access Control Specification (ACS)

“Secret”

Read Permission

Access Control Chain
Username
IP Address
Password

Update Perm.

Access Control Chain
Username
IP Address
...
Access Control Specification (ACS)

Read Permission
- Access Control Chain
  - Username
  - IP Address
  - Password
- Access Control Chain
  - Username
  - User Cert

Update Perm.
- Access Control Chain
  - Username
  - IP Address
  - ...
Authentication Attributes
Authentication Attributes

Plugin-Based
Explicit
  ip_src
  user_agent
  time_utc
  ...

Implicit
  user_id
  psk
  psk_sha256
  ...
  ...
Centralized Secret Storage

Flexible Access Control
Centralized Secret Storage
Flexible Access Control
Auditing and Revocation
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access
Example: Revoke Shared Access

140813: Bob Accessed
140906: Bob Accessed
141003: Bob Accessed
Example: Revoke Shared Access

140813: Bob Accessed
140906: Bob Accessed
141003: Bob Accessed
Example: Revoke Shared Access

140813: Bob Accessed
140906: Bob Accessed
141003: Bob Accessed
Auditing and Revocation in Custos
Custos Server

Authentication Subsystem

Secret Store

Access Control Subsystem

Custos API

SSL

Client A

Custos API

Application

Client B

Custos API

Application

Client C

Custos API

Application
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A

Revocation Semantics
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A

Revocation Semantics

Intrusion Detection
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A

Revocation Semantics

Intrusion Detection

Compliance Verification
Custos Prototype
Custos Prototype

EncFS: Custos-Backed Encrypted File System
Base Filesystem (ext4)

EncFS (fuse)

File (Encrypted) [On Disk]

File (Decrypted) [In Memory]

User's Computer

User

write read

write read

Enc Key

Enc Key

Custos Server

ACS

ACS

Provider
Base Filesystem (ext4)

EncFS (fuse)

User's Computer

File (Encrypted) [On Disk]

File (Decrypted) [In Memory]

User

write
read

write
read

encrypt
decrypt

User's Computer

libcustos

Custos Server

ACS

ACS

Enc Key

Enc Key

Provider
Base Filesystem (Dropbox)

EncFS (fuse)

File (Encrypted) [On Disk]

File (Decrypted) [In Memory]

User

write

read

write

read

User’s Computer

Enc Key

ACS

ACS

Custos Server

Enc Key

Provider

encrypt decrypt

libcustos
(a) `dd` Copy Throughput (MB/s)

(b) `ioping` Write Latency (ms)

(c) `bonnie++` Create IOPS
Current and Future Work
Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)
Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)

Better Management of Secret Sharing
Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)

Better Management of Secret Sharing

Audit Log Heuristics and Analysis
Custos
Key Storage as a Service
Centralized Secret Storage
Centralized Secret Storage
Flexible Access Control
Centralized Secret Storage
Flexible Access Control
Auditing and Revocation
Making Encryption More

Usable | Flexible | Applicable
Key Storage as a Service

Ecosystem
Thank You
Questions?
Extra Slides
Custos Organizational Units
Example Applications
Client-Encrypted File Locker
Multi-Device & Managed SSH Agent
Dedicated Crypto Processor
Custos Server

User

PKCS11

Web Browser

httpd

HTTPS Server

Private Key

SSaaS Provider

Custos API

Crypto

Engine

Public Key

PKCS11 Server

SSL

Custos Server

Crypto Processor

Web Server

PKCS11

httpd

Custos
Permissions
<table>
<thead>
<tr>
<th>Permission</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv.grp.create</td>
<td>create groups on a Custos server</td>
</tr>
<tr>
<td>srv.grp.list</td>
<td>list groups on a Custos server</td>
</tr>
<tr>
<td>srv.grp.override</td>
<td>escalate to any group-level permission, overriding the per-group ACS</td>
</tr>
<tr>
<td>srv.audit</td>
<td>read all server-level audit information</td>
</tr>
<tr>
<td></td>
<td>(i.e. group creation logging, group override logging, etc)</td>
</tr>
<tr>
<td>srv.clean</td>
<td>delete all server-level audit information</td>
</tr>
<tr>
<td></td>
<td>(i.e. group creation logging, group override logging, etc)</td>
</tr>
<tr>
<td>srv.acs.get</td>
<td>view the server-level ACS controlling the permissions in this list</td>
</tr>
<tr>
<td>srv.acs.set</td>
<td>update the server-level ACS controlling the permissions in this list</td>
</tr>
<tr>
<td>Permission</td>
<td>Rights</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$\text{srv.grp.create}$</td>
<td>create groups on a Custos server</td>
</tr>
<tr>
<td>$\text{srv.grp.list}$</td>
<td>list groups on a Custos server</td>
</tr>
<tr>
<td>$\text{grp.obj.create}$</td>
<td>create a key:value objects within the given group</td>
</tr>
<tr>
<td>$\text{grp.obj.list}$</td>
<td>list key:value objects within the given group</td>
</tr>
<tr>
<td>$\text{grp.obj.override}$</td>
<td>escalate to any object-level permission, overriding the per-object ACS</td>
</tr>
<tr>
<td>$\text{grp.delete}$</td>
<td>delete the given group on a Custos server</td>
</tr>
<tr>
<td>$\text{grp.audit}$</td>
<td>read all group-level audit information (i.e. object creation logging, object override logging, etc)</td>
</tr>
<tr>
<td>$\text{grp.clean}$</td>
<td>delete all group-level audit information (i.e. object creation logging, object override logging, etc)</td>
</tr>
<tr>
<td>$\text{grp.acs.get}$</td>
<td>view the group-level ACS controlling the permissions in this list</td>
</tr>
<tr>
<td>$\text{grp.acs.set}$</td>
<td>update the group-level ACS controlling the permissions in this list</td>
</tr>
<tr>
<td>Permission</td>
<td>Rights</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>srv.grp.create</td>
<td>create groups on a Custos server</td>
</tr>
<tr>
<td>srv.grp.list</td>
<td>list groups on a Custos server</td>
</tr>
<tr>
<td>srv.grp.grp_obj_create</td>
<td>create a key:value objects within the given group</td>
</tr>
<tr>
<td>srv.grp.grp_obj_list</td>
<td>list key:value objects within the given group</td>
</tr>
<tr>
<td>srv.grp.obj_delete</td>
<td>delete the given key:value object within the given group</td>
</tr>
<tr>
<td>srv.grp.obj_read</td>
<td>read the given key:value object within the given group</td>
</tr>
<tr>
<td>srv.grp.obj_update</td>
<td>create a new version of the given key:value object within the given group (the equivalent of a “write” permission for the Custos write-once system)</td>
</tr>
<tr>
<td>srv.grp.obj_audit</td>
<td>read all object-level audit information (i.e. object read logging, object update logging, etc)</td>
</tr>
<tr>
<td>srv.grp.obj_clean</td>
<td>delete all object-level audit information (i.e. object read logging, object update logging, etc)</td>
</tr>
<tr>
<td>srv.grp.obj_acs_get</td>
<td>view the object-level ACS controlling the permissions in this list</td>
</tr>
<tr>
<td>srv.grp.obj_acs_set</td>
<td>update the object-level ACS controlling the permissions in this list</td>
</tr>
</tbody>
</table>
Access Control Chain
[ 
  [ (username = 'Andy'),
    (password = '12345'),
    (src_ip = 192.168.1.0/24) ] ],
[ (username = 'Andy'),
  (password = '12345'),
  (src_ip = 75.148.118.216/29) ] ],
[ (username = 'John'),
  (password = 'Swordfish') ]
]
(username = 'Andy')

   |
   (password = '12345')

   (src_ip = 192.168.1.0/24) (src_ip = 75.148.118.216/29)

   (username = 'John')

       |
       (password = 'Swordfish')
Access Example
619a06f0-50af-11e3-8f96-0800200c9a66 ACS

```json
{
    obj_read:
    [
        [
            (ip_src = '1.2.3.4'),
            (time_utc = '1300 +/- 5')
        ],
        [
            (user_id = 'Dirk'),
            (psk = 'ImaHakzor')
        ]
    ...
    ]
...
}
```
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:
user_id = Dirk
(ip_src = '1.2.3.4')
(time_utc = '1133')
Custos Server

API

Authentication Attributes

Source IP Verification
Time Verification
User ID Verification
PSK Verification

Encryption Key Store
Access Control

API

Custos API

Encrypted File System

Dirk

Laptop
{  
  obj_read:  
    [  
      [ (ip\_src = '1.2.3.4'),  
        (time\_utc = '1300 +/- 5') ],  
      [ (user\_id = 'Dirk'),  
        (psk = 'ImaHakzor') ]  
    ...  
  ]  
}  
...
Custos Server

Encryption Key Store

Access Control

Authentication Attributes
- Source IP Verification
- Time Verification
- User ID Verification
- PSK Verification

API

Custos API

Encrypted File System

Dirk

Laptop
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:
user_id = Dirk
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)


{
  obj_read:
  [ 
    [ (ip_src = '1.2.3.4'),
      (time_utc = '1300 +/- 5') ],
    [ (user_id = 'Dirk'),
      (psk = 'ImaHakzor') ]
    ...
  ]
  ...
}
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:
user_id = 'Dirk'
psk = 'ImaHackzor'
(ip_src = '1.2.3.4')
(time_utc = '1133')
Custos Server

Access Control

Encryption Key Store

Authentication Attributes
- Source IP Verification
- Time Verification
- User ID Verification
- PSK Verification

API

Laptop

Dirk

Encrypted File System

Custos API

Laptop
Custos Server

- Encryption Key Store
- Access Control
- Authentication Attributes:
  - Source IP Verification
  - Time Verification
  - User ID Verification
  - PSK Verification

API

- Custos API
- Encrypted File System
- Dirk
- Laptop