Managing SSH Access Without Managing SSH Keys

Niall Sheridan
niall@intercom.com
Intercom Production Systems
"Many organizations don't even know how many SSH keys they have configured to grant access to their information systems or who has copies of those keys"

- NIST IR 7966 Security of Interactive and Automated Access Management Using Secure Shell (SSH)
Hackers break into FreeBSD with stolen SSH key

A Multi-billion Dollar Defense Firm Fails to Protect Private SSH Keys

Chris Vickery, a cyber risk analyst from UpGuard, successfully retrieved a cache of 60,000 documents related to a United States military project for the National Geospatial-Intelligence Agency (NGA). The sensitive files (close to 28 GB) linked to the U.S. intelligence agency were left unsecured (without a password) on a public Amazon server for anyone to access. Some of these files included the private SSH keys of a Booz Allen – one of country’s top defense contractors – employee, and various plain text passwords belonging to contractors with Top Secret Facility clearance.

CIA Malware Can Steal SSH Credentials, Session Traffic
HOPE IS NOT A STRATEGY
SSH Certificates

- Composed of: ssh key + signature + signing key + metadata
- Only need to distribute 1 public key to machines - the signing key
- Metadata allows for some nice properties to be set
Type: ssh-ed25519-cert-v01@openssh.com user certificate

Public key: ED25519-CERT SHA256:WHATEVER

Signing CA: ED25519 SHA256:WHATEVER

Key ID: "some identity string"

Serial: 0

Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36

Principals:

    prod-user

Critical Options:

    force-command /bin/date
    source-address 12.34.56.78/29

Extensions:

    permit-pty
    permit-port-forwarding
    permit-x11-forwarding
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
    prod-user
Critical Options:
    force-command /bin/date
    source-address 12.34.56.78/29
Extensions:
    permit-pty
    permit-port-forwarding
    permit-x11-forwarding
Type: ssh-ed25519-cert-v01@openssh.com user certificate

Public key: ED25519-CERT SHA256:WHATEVER

Signing CA: ED25519 SHA256:WHATEVER

Key ID: "some identity string"

Serial: 0

Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36

Principals:

prod-user

Critical Options:

force-command /bin/date

source-address 12.34.56.78/29

Extensions:

permit-pty

permit-port-forwarding

permit-x11-forwarding
Type: ssh-ed25519-cert-v01@openssh.com user certificate

Public key: ED25519-CERT SHA256:WHATEVER

Signing CA: ED25519 SHA256:WHATEVER

Key ID: "some identity string"

Serial: 0

Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36

Principals:
  prod-user

Critical Options:
  force-command /bin/date
  source-address 12.34.56.78/29

Extensions:
  permit-pty
  permit-port-forwarding
  permit-x11-forwarding
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
  prod-user
Critical Options:
  force-command /bin/date
  source-address 12.34.56.78/29
Extensions:
  permit-pty
  permit-port-forwarding
  permit-x11-forwarding
Username(s)
Type: ssh-ed25519-cert-v01@openssh.com user certificate

Public key: ED25519-CERT SHA256:WHATEVER

Signing CA: ED25519 SHA256:WHATEVER

Key ID: "some identity string"

Serial: 0

Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36

Principals:

    prod-user

Critical Options:

    force-command /bin/date
    source-address 12.34.56.78/29

Extensions:

    permit-pty
    permit-port-forwarding
    permit-x11-forwarding
/etc/ssh/sshd_config:
TrustedUserCAKeys /etc/ssh/ca.pub

/etc/ssh/ca.pub:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDAYZL32Emt4Ap......
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDGmvJaFt37ZTz......
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDWmdffJK0YR8z......
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIOBL2PHBRyIa7ok......
% cashier
Your browser has been opened to visit
Generating new key pair
Enter token: _
Your browser has been opened to visit
Generating new key pair
Enter token:

Credentials added.

% ssh-add -l
256 SHA256:CIxATG78JkHH1AF+bk6vumRtP3z22wpRP+Y6hoMK9v4 niall_1503934975 [Expires 2017-09-04 16:42:54 +0100 IST] (ED25519-CERT)
256 SHA256:CIxATG78JkHH1AF+bk6vumRtP3z22wpRP+Y6hoMK9v4 niall_1503934975 [Expires 2017-09-04 16:42:54 +0100 IST] (ED25519)
%
## Issued SSH Certificates

<table>
<thead>
<tr>
<th>ID</th>
<th>Created</th>
<th>Expires</th>
<th>Principals</th>
<th>Revoked</th>
<th>Revoke</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>niall_1503934975</td>
<td>2017-08-28 15:37:55 +0000</td>
<td>2017-09-04 15:42:54 +0000</td>
<td>niall,prod-user</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SSH Key:

SSH Certificate:
Questions?

https://github.com/nsheridan/cashier

Niall Sheridan
niall@intercom.com