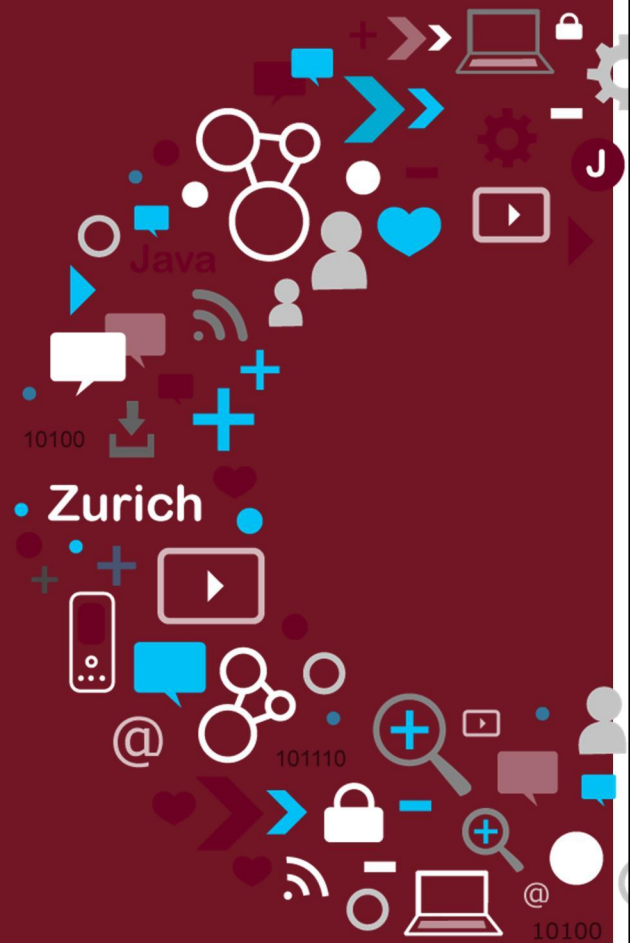
JAZOON'13

INTERNATIONAL CONFERENCE FOR THE SOFTWARE COMMUNITY

Deploying trusted developer sandboxes in Amazon's cloud

Jason Brazile, Remi Locherer, and Ronnie Brunner



This talk… potential cases for…

- cloud storage & remote dev/test
- automated read-only system images
- not-too-inconvenient encryption everywhere

Not a takeaway…

- Pre-Snowden, but complies w/ 4 of 5 Schneier's tips

http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

Background:

ESA Study: 2009-2011

potential use-cases:

- …
- Cloud for *free** data access
- Cloud for remote development
- …

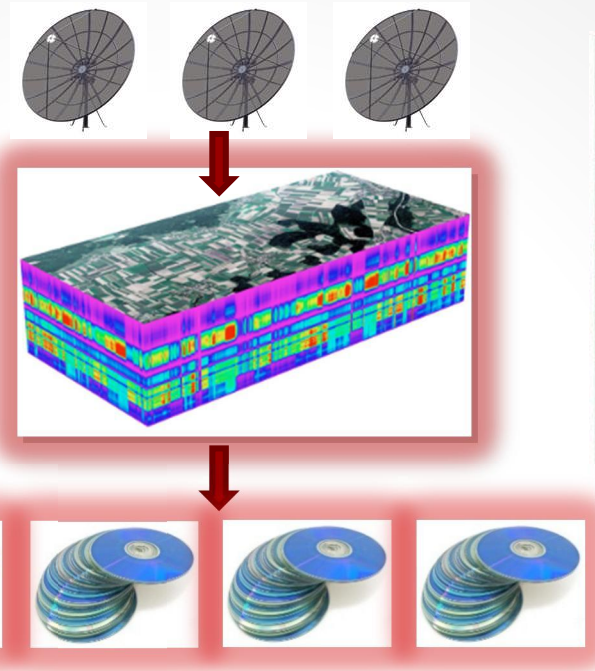
(*)https://www.google.com/?q=ESA+Earth+Observation+Data+Policy

ESRIN/Contract Nr. 227700/09/I-SB final report (245 pages)

The CIOP case

terradue 2.0 netcetera T··Systems···

- Big, free-ish, Data
- Distinct, proprietary, software devs
- Slow test data distribution to code developers
- Devs nervous about code leaking



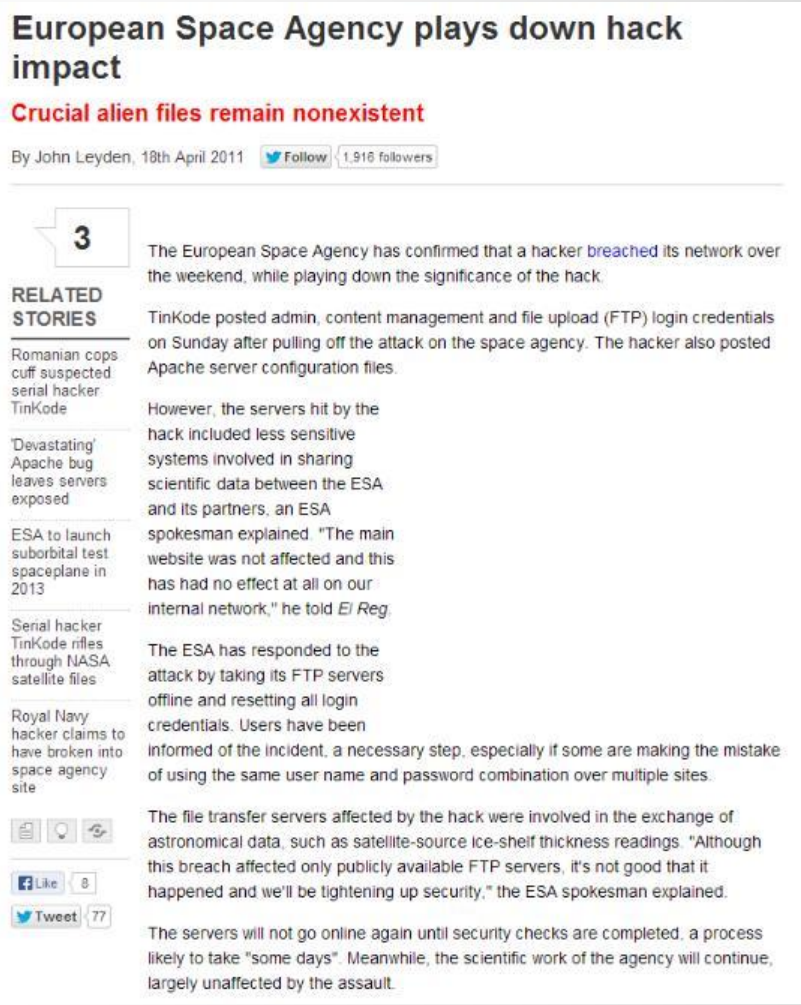
Proprietary Algorithm A dev'd by X

Proprietary Algorithm B dev'd by Y

Instead, lead the ***users*** to the ***data*** (in the cloud)

But… *Security*…

- ESA less concerned about hacking ***science data*** than ***their end–users' algorithms*** and ***brand damage***
- Data = ***not*** really sensitive
- Code = ***sensitive***
- Soln can't be ***too*** inconvenient



European Space Agency plays down hack impact

Crucial alien files remain nonexistent

By John Leyden, 18th April 2011 Follow 1,916 followers

3

RELATED STORIES

- Romanian cops cuff suspected serial hacker TinKode
- 'Devastating' Apache bug leaves servers exposed
- ESA to launch suborbital test spaceplane in 2013
- Serial hacker TinKode rifles through NASA satellite files
- Royal Navy hacker claims to have broken into space agency site

Like 8 Tweet 77

The European Space Agency has confirmed that a hacker breached its network over the weekend, while playing down the significance of the hack.

TinKode posted admin, content management and file upload (FTP) login credentials on Sunday after pulling off the attack on the space agency. The hacker also posted Apache server configuration files.

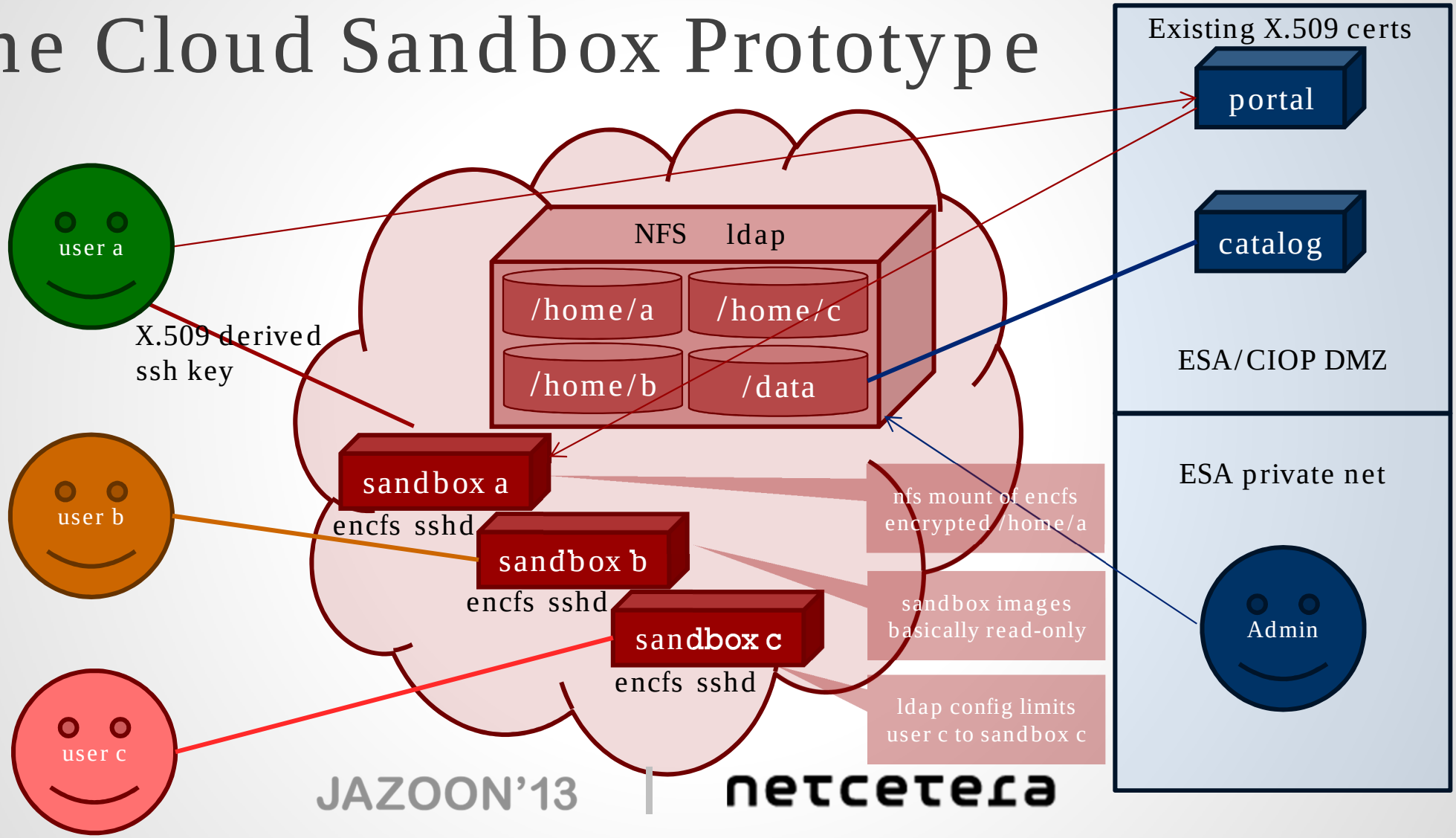
However, the servers hit by the hack included less sensitive systems involved in sharing scientific data between the ESA and its partners, an ESA spokesman explained. "The main website was not affected and this has had no effect at all on our internal network," he told *El Reg*.

The ESA has responded to the attack by taking its FTP servers offline and resetting all login credentials. Users have been informed of the incident, a necessary step, especially if some are making the mistake of using the same user name and password combination over multiple sites.

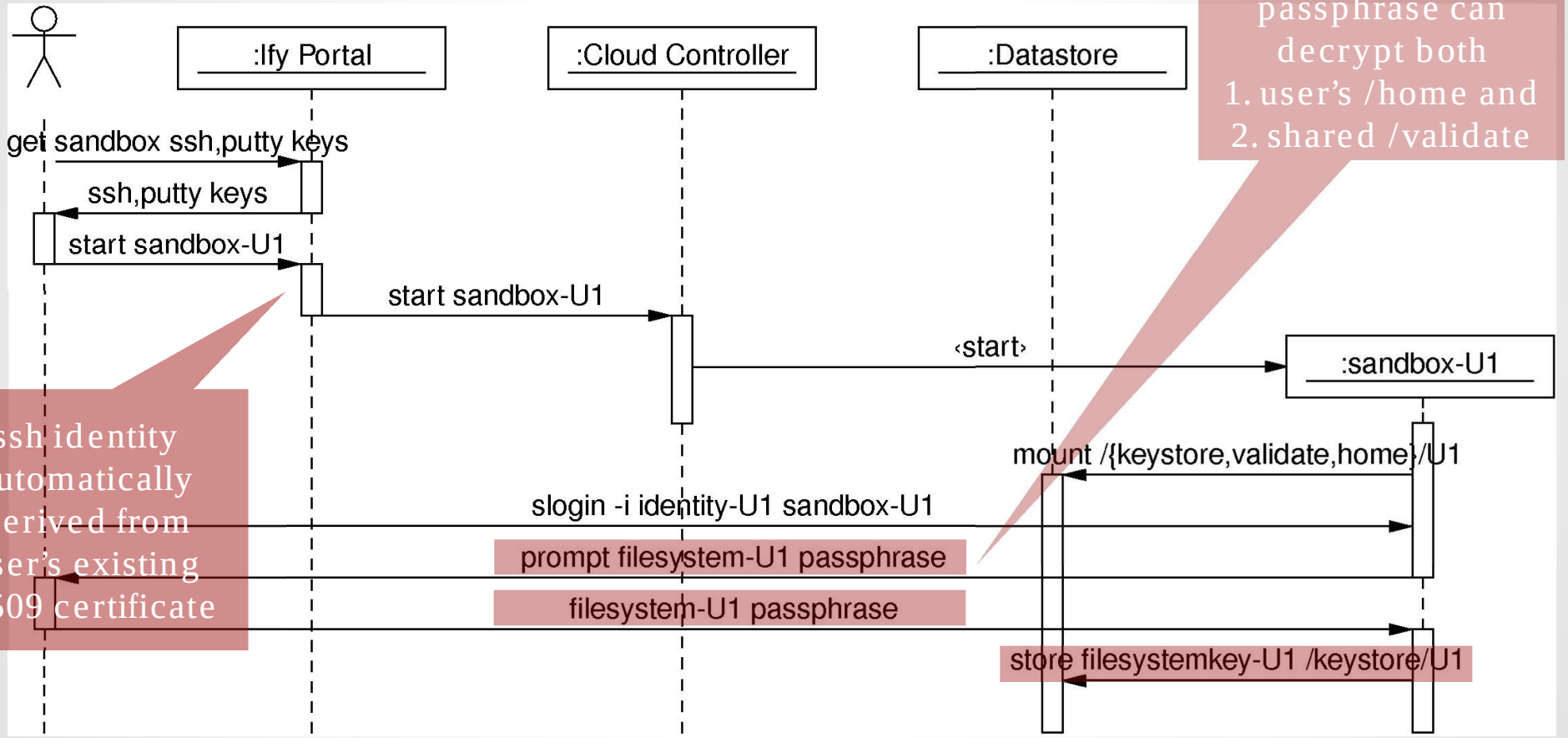
The file transfer servers affected by the hack were involved in the exchange of astronomical data, such as satellite-source ice-shelf thickness readings. "Although this breach affected only publicly available FTP servers, it's not good that it happened and we'll be tightening up security," the ESA spokesman explained.

The servers will not go online again until security checks are completed, a process likely to take "some days". Meanwhile, the scientific work of the agency will continue, largely unaffected by the assault.

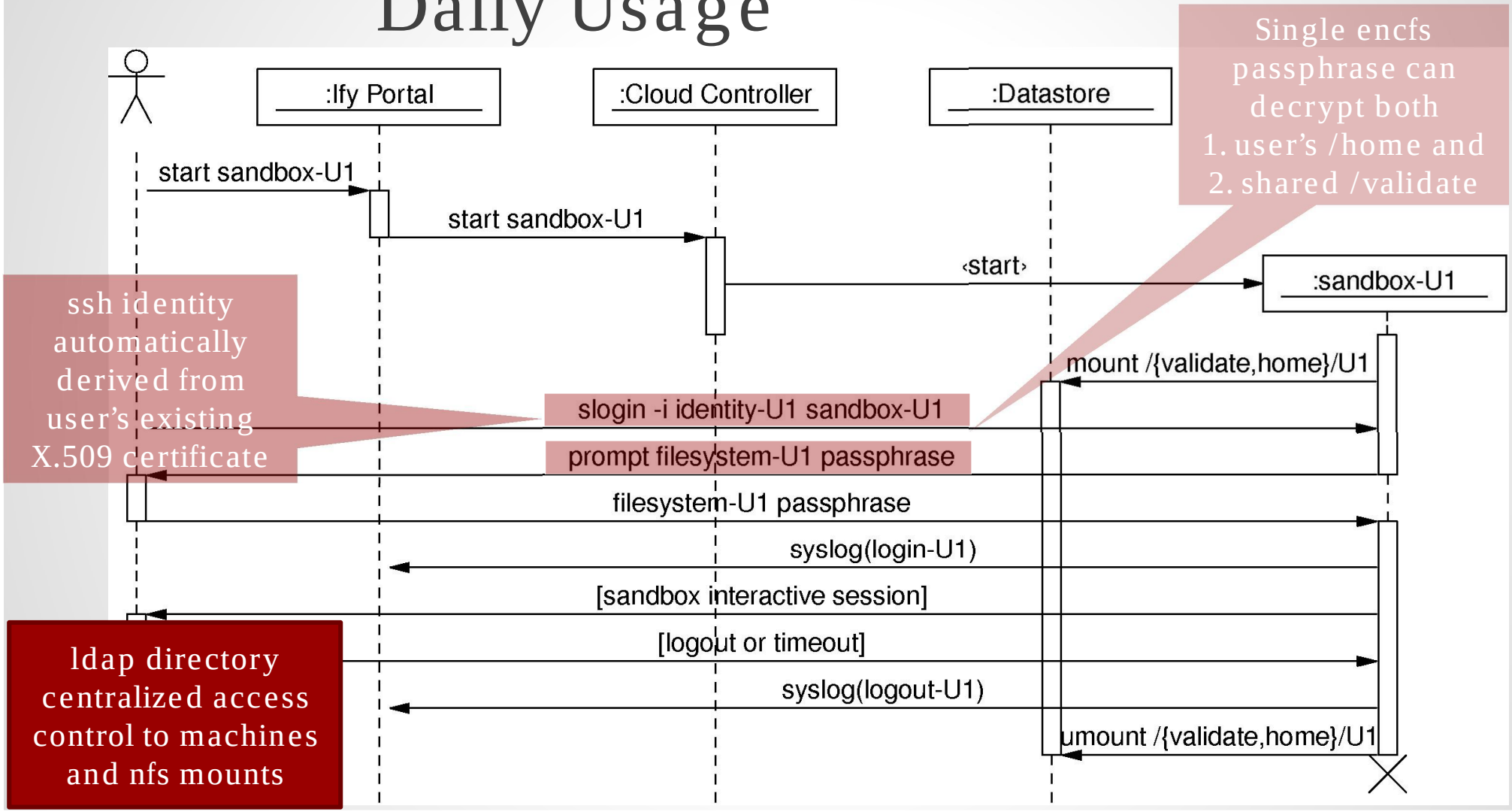
The Cloud Sandbox Prototype



First Time Usage



Daily Usage


:Ify Portal
:Cloud Controller
:Datastore
:sandbox-U1
start sandbox-U1
start sandbox-U1
‹start›
mount /{validate,home}/U1
slogin -i identity-U1 sandbox-U1
prompt filesystem-U1 passphrase
filesystem-U1 passphrase
syslog(login-U1)
[sandbox interactive session]
[logout or timeout]
syslog(logout-U1)
umount /{validate,home}/U1
Single encfs passphrase can decrypt both 1. user's /home and 2. shared /validate
ssh identity automatically derived from user's existing X.509 certificate
ldap directory centralized access control to machines and nfs mounts

Encrypted File system choices SL6

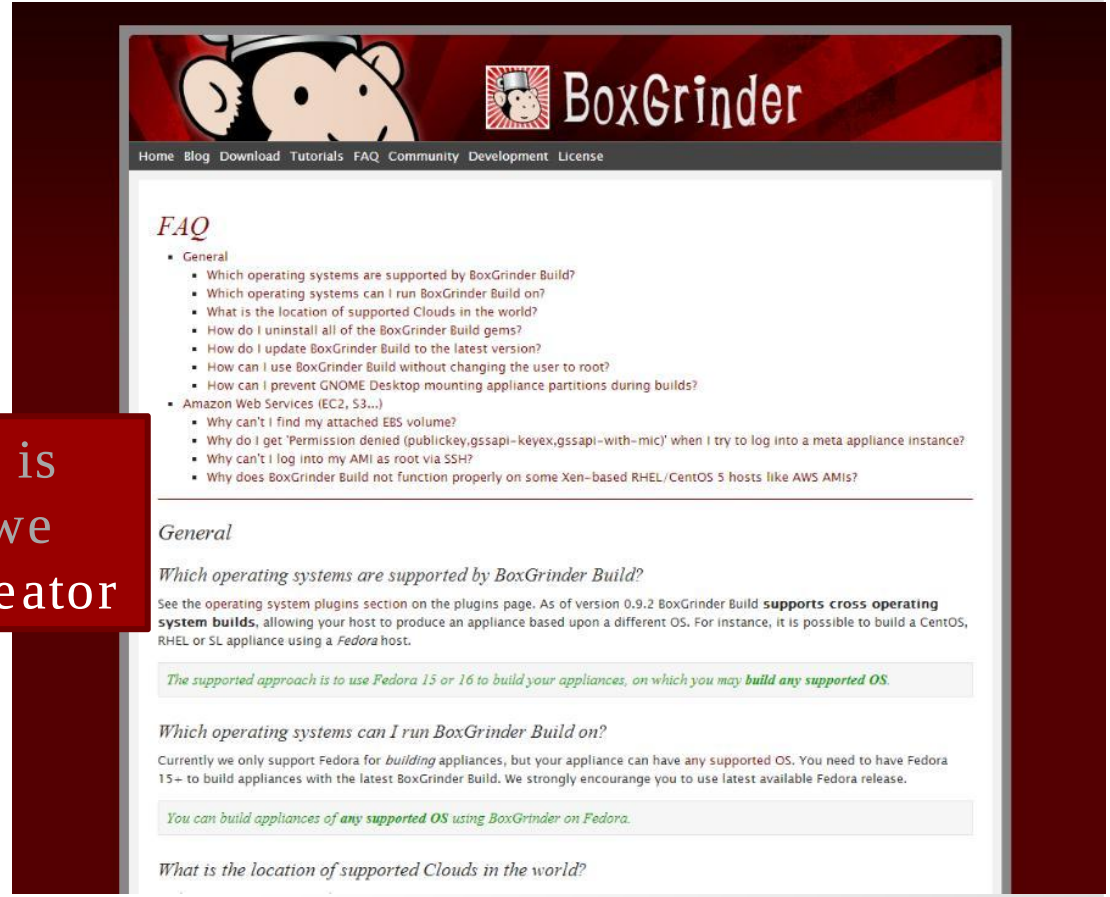
	eCryptfs over NFS	EncFS over NFS	ZFS/GELI (NFS)	dm-crypt with iSCSI/LUKS	dm-crypt with loopback mount/LUKS over NFS	S3 clone with S3 fs	ssh fs
Comments	file based, encryption done on client side	file based, encryption done on client side	no encryption officially available for SL! Encryption and decryption done on server side	block based, encryption done on client side	block based, requires additional central LDAP or similar. Encryption done on client side	mimic Amazon interface	"Just" tunnel remote file system through SSH
Expected (relative) performance							
Easy end user experience (i.e. use the already available X.509 cert)	works with same password, but not out of the box with keys	test needed (not explored yet)					
Concurrent access / mounting	Yes, but needs patch for NFS						
Block device or file level encryption	file	file	Yes on FreeBSD, but no stable release on SL	block	block	not encrypted on server	not encrypted on server
Communication to storage server encrypted							
Supports normal fs tools (copy on server for snapshot, etc.)	yes, but careful not to copy corrupt files	yes, but careful not to copy corrupt files					
Multiple keys to decrypt same content (/validate)			?	Yes, but multiple passphrases (up to 8) for a single key	Yes, but multiple passphrases (up to 8) for a single key	Multiple keys to access the same bucket possible, but it's not encrypted	Not encrypted, but multiple access keys are possible

Details: just the OS...

```
name: fedora-xfce
summary: Fedora with xfce
os:
  name: fedora
  version: 16
hardware:
  partitions:
    "/":
      size: 5
packages:
  - @base
  - @base-x
  - @fonts
  - @xfce-desktop
  - @critical-path-xfce
access_key:        yourawsaccesskey
secret_access_key: youawssecretkey
account_number:    youramazonaccountnumber
cert_file:         /root/.ec2/yourcertificate.pem
key_file:          /root/.ec2/yourprivatekey.pem
```

The only change needed:
name: sl
version: 6

Note: boxgrinder is *"sleeping"*. Now we use appliance-creator



Details: server customization (~500 lines)

```
# ldap configuration
yum install -y openldap-clients openldap-servers nss-pam-ldapd

# prepare ldap cert
cd /etc/openldap/cacerts
openssl genrsa -out cert.key 2048
…
openssl req -new -key cert.key -out cert.csr -subj \
  "/C=IT/L=Default City/O=Default Company Ltd/CN=192.168.11.10"
…
/usr/sbin/cacertdir_rehash /export/certs/

cat <<EOF> /etc/openldap/slapd.d/cn=config.ldif
…
cat <<EOF> /etc/openldap/slapd.d/cn=config/c
…
cat <<EOF> /etc/openldap/slapd.d/cn=config/c
…
cat <<EOF> /etc/openldap/slapd.d/cn=config/c
…
cat <<EOF> /etc/openldap/g-pod.ldif
…
slapadd -l /etc/openldap/g-pod.ldif
```

- Firewall
- Nfs/autofs
- Certificates
- Ldap
- Syslog

```
# local firewall rules for inbound traffic
lokkit --nostart --enabled \
  --service=ssh \
  --port=111:tcp \
  --port=111:udp \
  --port=514:tcp \
  --port=636:tcp \
  --port=662:tcp \
  --port=662:udp \
  --port=2049:tcp \
  --port=2049:udp \
  --port=32803:tcp \
  --port=32769:udp

# 111 rpc (for nfs)
# ldap-ssl (port 636)
# 514 rsyslog
# 662 statd (for nfs)
# 2049 nfs4
# 32803,32769 lockd (for nfs)
```

TODO:
rsyslog **à** TLS rsyslog

Details: sandbox customization (~250 lines)

```
# encrypt temporary filesystems
yum install -y cryptsetup-luks
# swap space
# (use "cryptsetup status /dev/mapper/swap" after reboot)
echo 'swap /dev/mapper/VolGroup-lv_swap /dev/urandom \
 cipher=aes-cbc-essiv:sha256,size=128,swap'  > /etc/crypttab
sed -i 's/.*swap.*/\/dev\/mapper\/swap swap swap defaults 0 0/' /etc/fstab
# temporary file systems
echo 'none /tmp tmpfs defaults,size=64m 0 0' >> /etc/fstab
echo 'none /var/tmp tmpfs defaults,size=128m 0 0' >> /etc/fstab

[...]

# home directory encryption
# fuse-2.8.3-1.el6 works, fuse-2.
yum install -y \
  fuse-2.8.3-1.el6 \
  fuse-encfs-1.7.4-1.el6.i686 \
  pwgen
```

- Firewall
- Nfs/autofs/fuse-encfs
- Crytpsetup-luks
- Openssh-ldap
- Syslog

```
…
chmod +x /etc/profile.d/encfs.sh


# load fuse kernel module at boot
cat <<EOF> /etc/sysconfig/modules/encfs.modules
#!/bin/bash
exec /sbin/modprobe fuse >/dev/null 2>&1
EOF
chmod +x /etc/sysconfig/modules/encfs.modules


yum install -y openssh-ldap
ho 'AuthorizedKeysCommand \
sr/libexec/openssh/ssh-ldap-wrapper' >> /etc/ssh/sshd_config


or ssh-ldap-helper
s /etc/openldap/ldap.conf /etc/ssh/ldap.conf
```

Takeaways... potential cases made for...

- cloud storage (test data) & remote dev access
- automated read-only system images (server & client)
- not-too-inconvenient encryption everywhere

github.com/netceteragroup/esa-ciop-sandbox-image-proto