The security implications of Ansible scared me

Mark Jenkins

```
1DEE 93CC DA25 F8A3 F9E3
57A9 A8F8 6493 AA4D B1FB
```

Q&A in hallway track

In your mind

you have capacities you know

To telepath messages

through the vast unknown..

Calling occupants of interplanetary craft

ANSIBLE

Controller

Control

Push model

Agentless

“Agentless”

Implication of the push model

- Credentials on the controller could be safe….
- But as long as pushed code can be altered...
- Bad things can happen
- To all the things

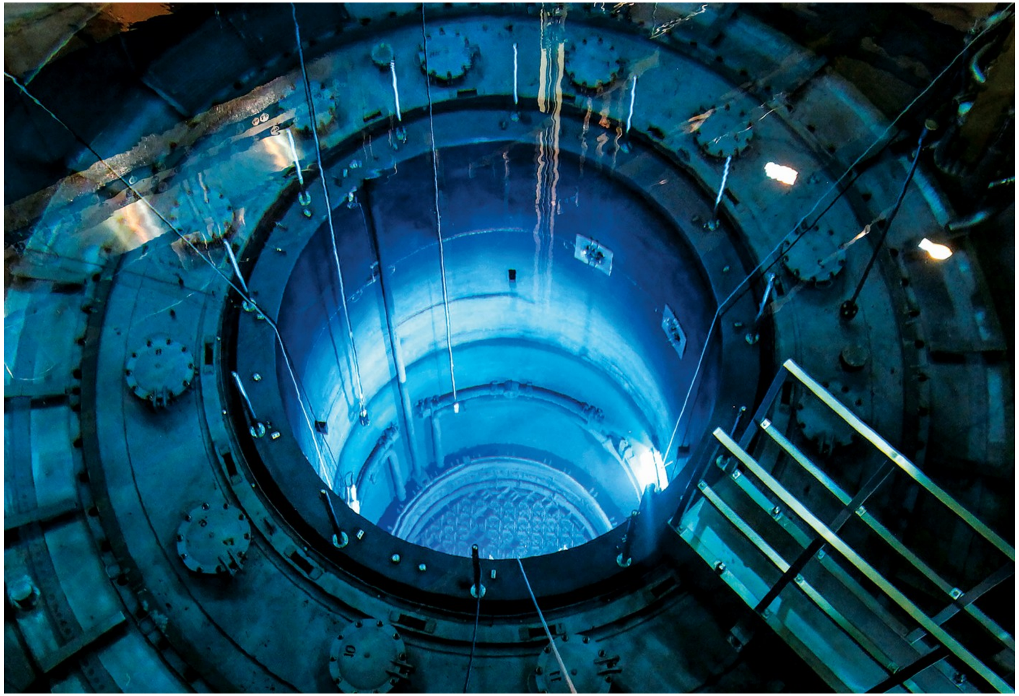
Possible points of compromise

1. Web interface

1. Web interface

2. Supply chain

Core – ansible.builtin



pip install ansible

community.general

galaxy

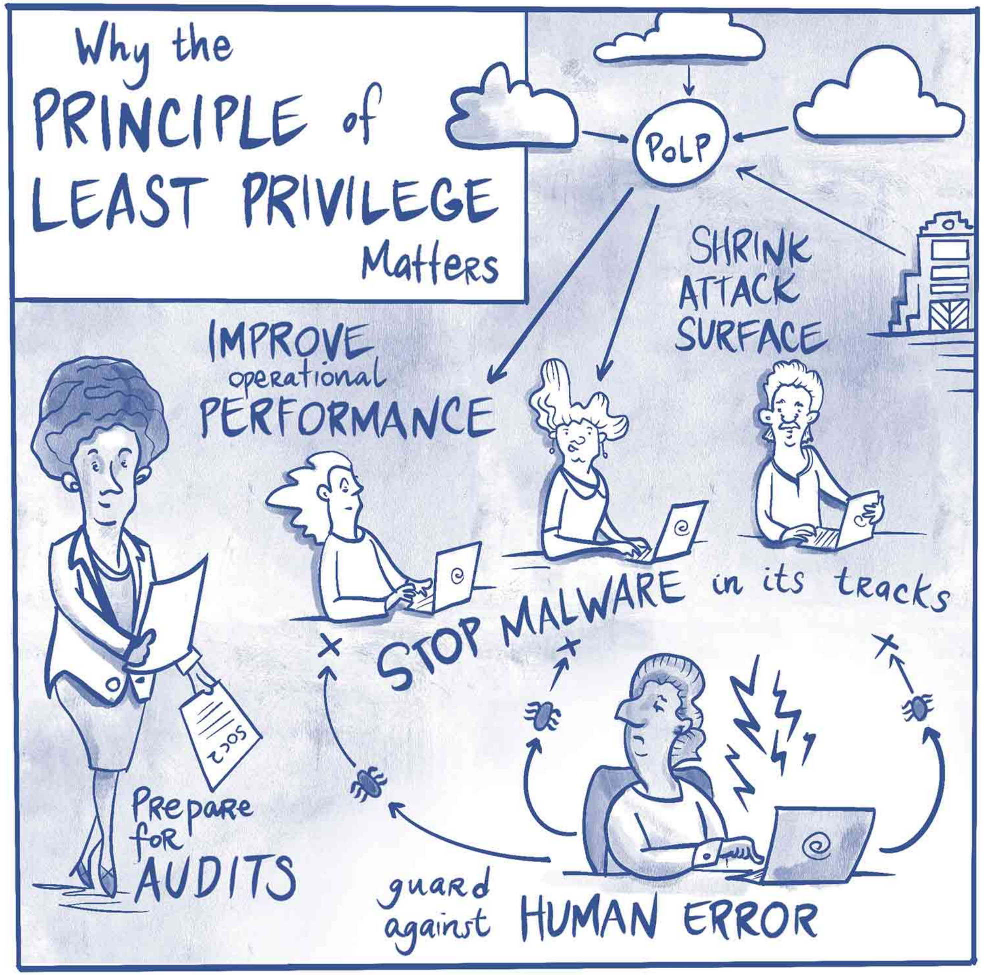
Insider attack

“Insider” attack

3. Backwards communication

4. System flaws (e.g. ssh/kernel)

Risk Mitigation


Why the PRINCIPLE of LEAST PRIVILEGE Matters
PoLP
SHRINK ATTACK SURFACE
IMPROVE operational PERFORMANCE
STOP MALWARE in its tracks
SOC2
Prepare for AUDITS
guard against HUMAN ERROR

Demo 1 – Provisioning workstation

Don’t put web interface on public internet

Demo 2 – client certificate

Certificate of Excellence

In honor of your outstanding performance and dedication
we hereby present

____

with this certificate of excellence

____

This ______ *day of* ____________ ______

____

ACHIEVEMENT · EXCELLENCE · HONOR

AUDIT

Code signing and verification

SIGN COMMITS WITH
GPG, GIT AND YUBIKEY
GnuPG
+
git
+
YubiKey
=
verified
GitHub

ansible-pull

Ansible-pull and signature verification

“agentless”

In conclusion..

With your mind you have ability to form

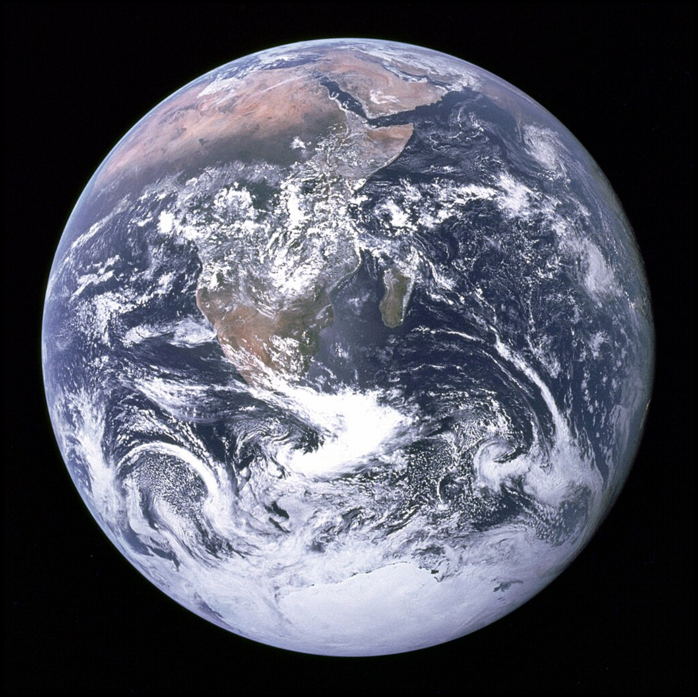
And transmit thought energy
far beyond the norm

You close your eyes,
you concentrate

Together that's the way

To send the message

We declare world contact day



Happy Hacking