Open Science Grid

# Security in the OSG

King of France, Louis XVI Restorer of French Liberty
Place d'Armes, 78000
Versailles, France

# The Real King Louis XVI?

Nope, he was a decoy because I'm not about those guillotines


# Security in the OSG

Brian Lin
OSG Software Team
University of Wisconsin - Madison

# What is Trust?


- **Trust:** reliance on the integrity or surety of a person or thing
- Obtaining trust:
  - Prior knowledge and/or experience
  - Appeal to authority
  - Chains of trust

# Identity and Identification

- **Identity:** who someone is, Willie the Cat
- **Identification:** proof of who someone is, Willie's collar
- **Real word ID:** photos, SSN, driver's license, passport, etc.
- **Internet ID:** usernames (kinglouis16), certificates

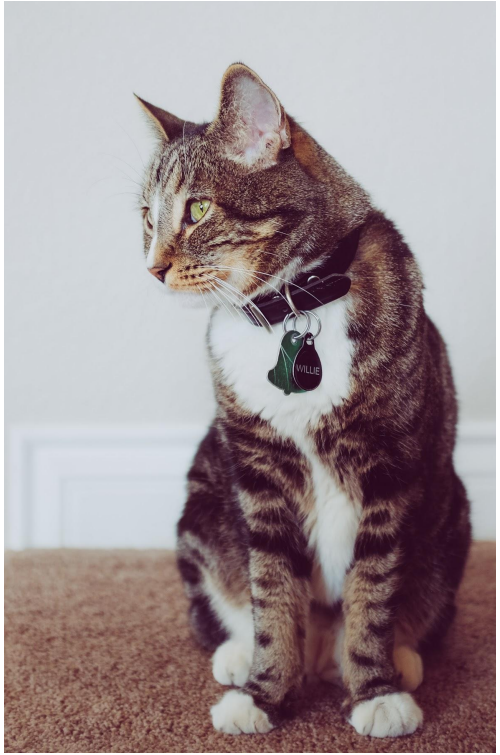


Photo by NeONBRAND on Unsplash

# Authentication (AuthN)

- Authentication: trusting identification
- Username + password, shared secret (public key cryptography), two-factor, etc.
- Authentication online often goes both ways



 

# Authorization (AuthZ)

- Authorization: trusting identities
- A description of the privilege level of an identity
- What are you authorized to do on our submit nodes?

# HTCondor AuthN and AuthZ

- Many different authentication methods (Unix file system, SSL, Kerberos, etc)
- Fine grained control over authorization levels and who belongs to each authorization level
  - Not just any server can join the pool
  - Not just any user can submit jobs
- Jobs run as your Unix user on the execute servers

# Is Your Data Secure?

- You are using a shared computer so take basic precautions (no world-writable files)!
- Save strong login credentials in a password store
- NO sensitive data (e.g. HIPAA)
- Otherwise, relatively low risk



Photo by sebastiaan stam on Unsplash

# Security in the OSG

- Certificate-based security for pilots jobs and servers
- Pilot jobs run under the same Unix user, Singularity containers provide some separation between VO users
- VOs vet users; system administrators vet servers
- The OSG Security Team tracks software vulnerabilities and responds to security incidents
- Certificate revocation of compromised machines
- Site administrators keep audit logs for traceability in case of security issues

# Questions?