Security in the OSG
The Real Lil Nas X?

Image By DiFronzo - BiznessBoi, Lil Nas X & Boyband, CC BY 2.0, 
https://commons.wikimedia.org/w/index.php?curid=78262344
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 world**: photos, SSN, driver’s license, passport, etc.
  - **Online**: usernames (1i1nasx), certificates, tokens
Trust and Identities

• Authentication: trusting identification
  – Username + password, shared secret (public key cryptography), two-factor, tokens, etc.
  – Authentication online often goes both ways
  – HTCondor authenticates both users and machines

• Authorization: levels of trust for identities
  – A description of the privilege level of an identity
  – What are you authorized to do on our submit nodes?
• Resources and pilots verify each other’s identities
• Jobs in the same VO all run under the same user!
• Containers can provide some separation between VO users (for sites that support it)
• VOs vet users; system administrators vet servers
• The OSG Security Team tracks software vulnerabilities and responds to security incidents
Is Your Data Secure?

You are using a shared computer that you don’t own so take basic precautions:

• No sensitive data
• No world-writable files
• No data or code that CANNOT be copied
So What Can You Do?

- Protect your account
  - Do not share your account
  - Use good passwords
  - Even better, use a password store like KeePass or LastPass
  - Use SSH keys wherever possible
- Trust but verify
  - Spot checking
  - Reproduce your results
Questions?

Coming next:

• 12:15 - 1:15 Lunch
• This afternoon: Working with real software