

# OSG All hands Meeting Boston, 2011

## Security in OSG

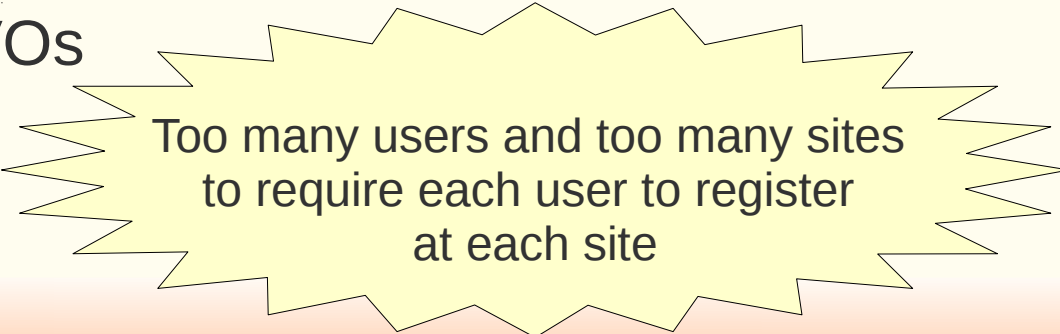
Igor Sfiligoj  
for the OSG Security team

# What is security?

- Security is both a technology and a social problem
  - We need proper technology to **prevent untrusted parties** to create damage
  - But we have a secure system only if **all the trusted participants** act responsibly
    - We strive to prevent untrusted entities to enter the system
    - **But a careless user can make almost as much damage!** (and this includes sysadmins as well)

# OSG Security model

- Multiple administrative domains
  - Each Site
    - Decides how to run its own resources
    - Decides which users to support
- Federated trust model
  - Virtual Organizations (VOs) as a middle man
    - A VO trusts its own users
    - A Site trusts a set of VOs



Too many users and too many sites  
to require each user to register  
at each site

# Authentication in OSG

(i.e. technology part of security)

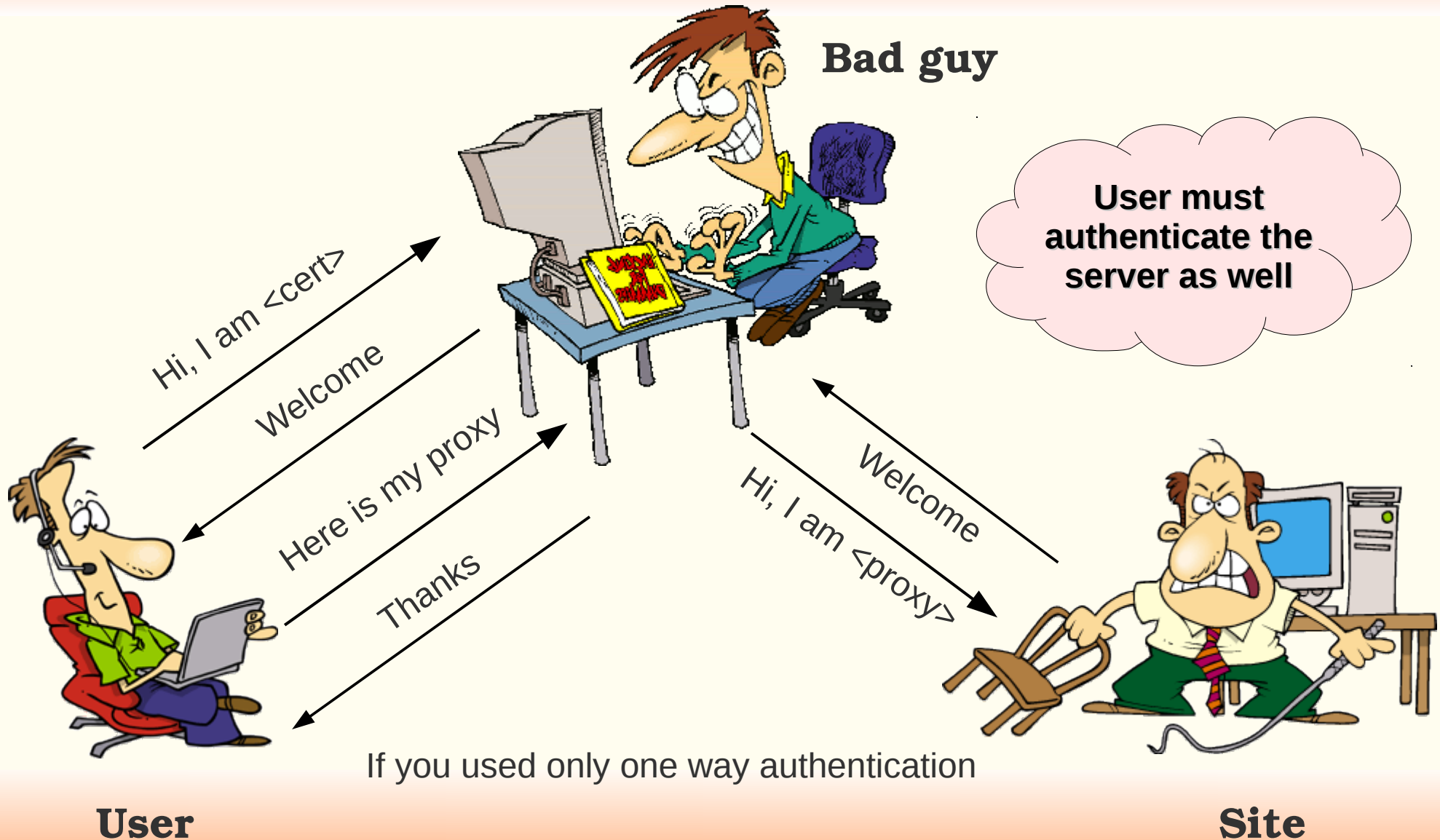
- Authentication based on x509 certs and proxies
  - A Public Key Infrastructure (PKI) technology
- Both the user and the site have a cert/proxy
  - Public part sent to the other party
  - Private key used for signing
- Signature is the authentication
  - Cannot be forged (PKI)
  - Validated through a chain mechanism rooted in a Certificate Authority (CA) certificate

# The importance of CAs

- Authentication rooted in CAs certs
  - The **trusted** CA public certs must be pre-installed locally (typically getting it through the VDT)
  - **All** user certs/proxies issued by those CAs will pass authentication, but nothing else
- Certificates can be revoked by a CA
  - Hence the Certificate Revocation List (CRL)
  - **Make sure you download the updated CRLs often!** (everything stops working if it expires)



# The importance of mutual authentication



# Authorization

- Just because someone can authenticate, does not mean a Site will authorize him/her
  - Authorization is a separate step
- The Site may also want to give different privileges to different users
  - The user must be mapped to a local security domain
  - Certificate identity -> (typically) UNIX UID
- Server authorization is instead implicit
  - Cert identity must match DNS name

# VO-based Authorization

- As mentioned in the introduction, Sites trust VOs (not users directly)
  - Each VO will keep a list of trusted user DNs
  - Through a service called **VOMS**
- OSG provides a list of trusted VOs and their VOMS servers
  - The Site needs to pick which VOs to support
  - Should always support the MIS VO (OSG operations)
- Users authenticate with a VOMS-extended proxy (voms-proxy-init -voms ...)



# User Mapping at Sites

- OSG provides **GUMS** for mapping
  - Talks to VOMS servers to get the list of user DNs
- **Site admins decide the mapping**
  - Although OSG provides a suggestion
- Two types of mapping: group and pool
  - Group mapping maps multiple certs to the same UID
    - **Potentially dangerous**  
[https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/BestPractices#Mapping\\_Grid\\_DN\\_s\\_to\\_Local\\_Accou](https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/BestPractices#Mapping_Grid_DN_s_to_Local_Accou)
  - VO should contact sites that do that if not comfortable with it

# Keeping a system secure

- Keep all the software up-to-date  
(mostly patching, but also upgrades as needed)
  - Operating system
  - System services
  - OSG/VDT provided software
- Keep security data up-to-date
  - List of trusted CAs
  - Associated CRLs
  - List of supported VOs
- Without, the risk of a compromise raises significantly

# Security notifications

- OSG security team will send security notifications through e-mail when needed
  - Please read and act upon them
  - Make sure they have a legitimate signature  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/OSGSecurityNotifications>
- **But we need to know who to contact!**
  - Sites should have a designated security contact
  - The OSG repository for such information is OIM  
<https://oim.grid.iu.edu/oim/home>
    - Important to keep information updated there

# Local security first

- While OSG will help you as much as possible, each Site should have its local security team
  - Most Campuses and Institutions already have one
  - Know and possibly be in contact with them
    - They can provide invaluable help both in preventing and fixing security incidents
- **In case on a security incident, local security team should be the first to be notified!**
  - If any Grid-related services are involved, please ALSO notify the OSG security team  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/IncidentDiscoveryReporting>

# What is a security incident?

- Any activity that is not authorized!
  - e.g. spam-bots, credential stealing, rootkits
  - Grid-wise, we are mostly worried about certs/proxies being stolen (or harvested!)
- A Grid-related security incident does not need a Grid vulnerability
  - Actually, we know of no Grid-induced compromises!
  - Usually attackers use “standard” vulnerabilities
    - Ssh, Web and OS vulnerabilities
    - Including weak passwords!

# Discovering compromises

- You need to actively look for signs of compromise
  - Well preformed compromises leave no obvious traces
- Log files can provide a lot of info  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/SearchLogFiles>
- Yes, it can take a lot of time
  - But it pays big dividends
  - A Site security incident can make the Site unusable for weeks (or worse)
  - A user machine compromise can similarly prevent a user from doing any computing for just as long



# Summary

- Security is both a social and technical problem
- Certificates are used for authentication, authorization is a separate step
- Not all the CAs are trusted, and you need to keep CRLs updated
- Keep your system software up-to-date
- Keep your contact information up-to-date in OIM
- Know how to report a security incident

# Additional reading

- OSG Certificate page  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateWhatIs>
- Wikipedia X.509 description  
<http://en.wikipedia.org/wiki/X.509>
- A talk about VOs  
<http://staff.science.uva.nl/~demch/presentations/cts2006-ydemchenko-vo-dynamic-associations01.pdf>
- OSG Security Home page  
<https://twiki.grid.iu.edu/twiki/bin/view/Security/>
- OSG Security and Certificates FAQ  
[https://twiki.grid.iu.edu/bin/view/Documentation/OsgFaq#Security\\_and\\_Certificates](https://twiki.grid.iu.edu/bin/view/Documentation/OsgFaq#Security_and_Certificates)
- OSG Certificate Request Documentation  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateGet>
- NCSA OpenSSL Cheatbook  
<http://security.ncsa.illinois.edu/research/grid-howtos/usefulopenssl.html>



# Additional reading <sup>2</sup>

- OSG Site Security Responsibilities  
<https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/SecuritySiteResponsibilities>
- OSG Security Hands On Training  
<https://twiki.grid.iu.edu/bin/view/Security/SecurityHandsOnTraining>
- Security Session at the 2009 OSG Admin Workshop  
<http://indico.fnal.gov/sessionDisplay.py?sessionId=4&slotId=0&confId=2497#2009-08-06>

# Copyright notice

- These slides contain copyrighted images by ToonADay.com
- All such images have been licensed to Igor Sfiligoi for use in presentations
- Extracting such images and use them in other context is not permitted