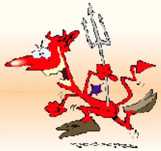
Open Science Grid

OSG School in São Paulo

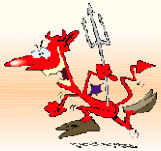
Security in the Grid world

by Igor Sfiligoi
for the OSG Security team



Overview

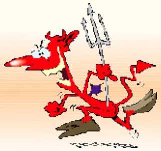
- Why we need security?
- How does it work?
- What is your role?
- How to handle emergencies



Why we need security?

- Are we not an open community?
- We have nothing to hide!

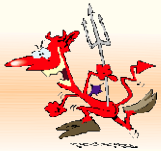
Heard many times from scientists



Why we need security?

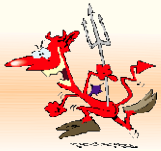
- Are we not an open community?
  - **We are**
  - But we still have limited resources;
    whatever a stranger uses cannot be used by you
  - Some people are just malicious
    - SpamBots, Denial of Service, Rootkits, etc.

    Need a way to keep them away
- We have nothing to hide!



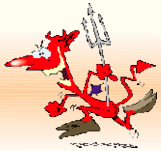
Why we need security?

- Are we not an open community?
- We have nothing to hide!
  - **Maybe**
    You may not like someone stealing
    your publication result
  - And it is not just about who can run/read
    - It is also who can re-write/modify data/files
  - You own data
    You don't want someone to tamper with it, do you?



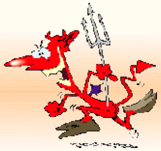
How does it work?

- OSG security based on
  - People
  - Trust relationships
  - Technical measures
- OSG technical security based on
  1) Public Key Cryptography (PKI)
  2) Virtual Organization (VO) attributes



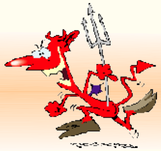
People are key!

- People are the most important element in any security scheme
  - And this includes you and me
- Any system is only as secure as the people it serves
  - No technical measure will prevent a trusted user to do something really dangerous (password sharing anyone?)
- So please take security seriously



Trust relationships

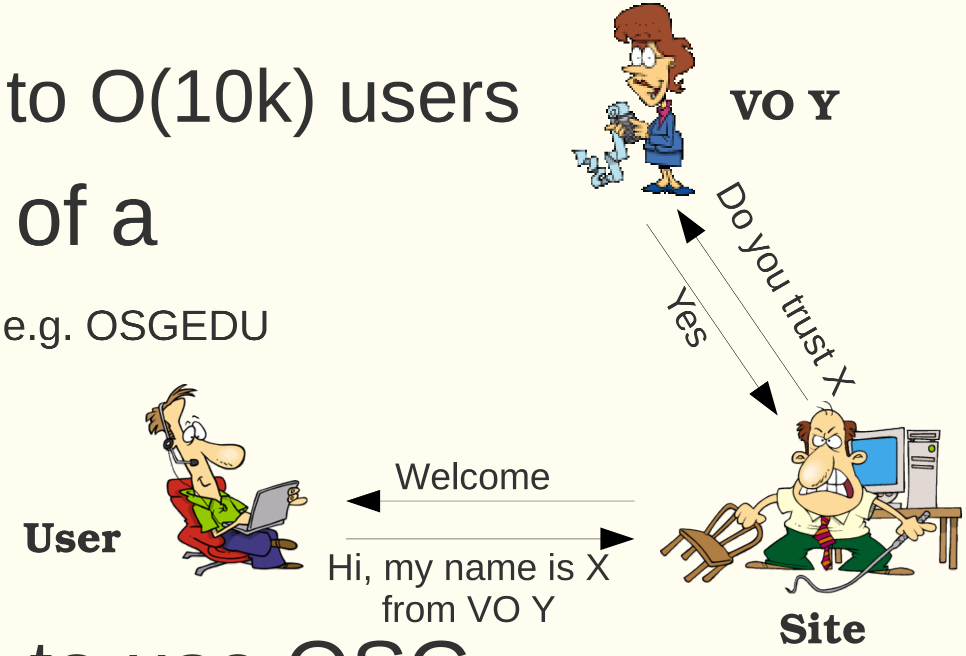
- Why should anyone
  - let you run on their CPU cluster?
  - let you write to their disks?
  - let you read/modify files created by someone else?
- It is all a matter of trust
  - They trust you to behave responsibly
    - That you will not do “bad things”
  - If you betray that trust, you may/will be banned
    - Doing too many stupid things may qualify



Trust relationships

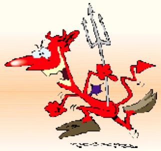
- The trust is ultimately between the service provider (site) and the user
- But there are too many for 1-to-1 channels
  - No way each site will talk to O(10k) users
- OSG thus has a concept of a Virtual Organization(VO) e.g. OSGEDU
  - The site trusts the VO
  - The VO trusts its users

So you have to join a VO to use OSG



Trust relationships

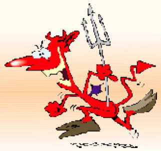
- But trust must be bi-directional
- You should trust the service provider before giving out any sensitive data
  - Ever heard of phishing?
    No known phishing in the Grid world yet, but we may get there
- The list of sites you should trust comes from the VO
  - OSG has a trusted information system, but VOs usually have more info



Technical measures

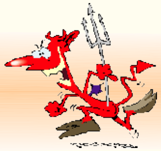
- Two layers
  - Authentication
  - Authorization
- You really only ever see the authentication part
- Authorization is handled internally by Grid sites
  - Black box for you

(Of course, selecting a trusted site
is authorization, although a manual one)



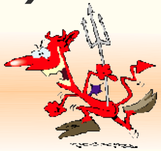
Technical measures

- Authentication handled in two layers
  - PKI, i.e. X509 Grid certificates
    to identify the user
  - VOMS attributes
    to identify the VO it is associated with
    (alongside any VO groups and roles)



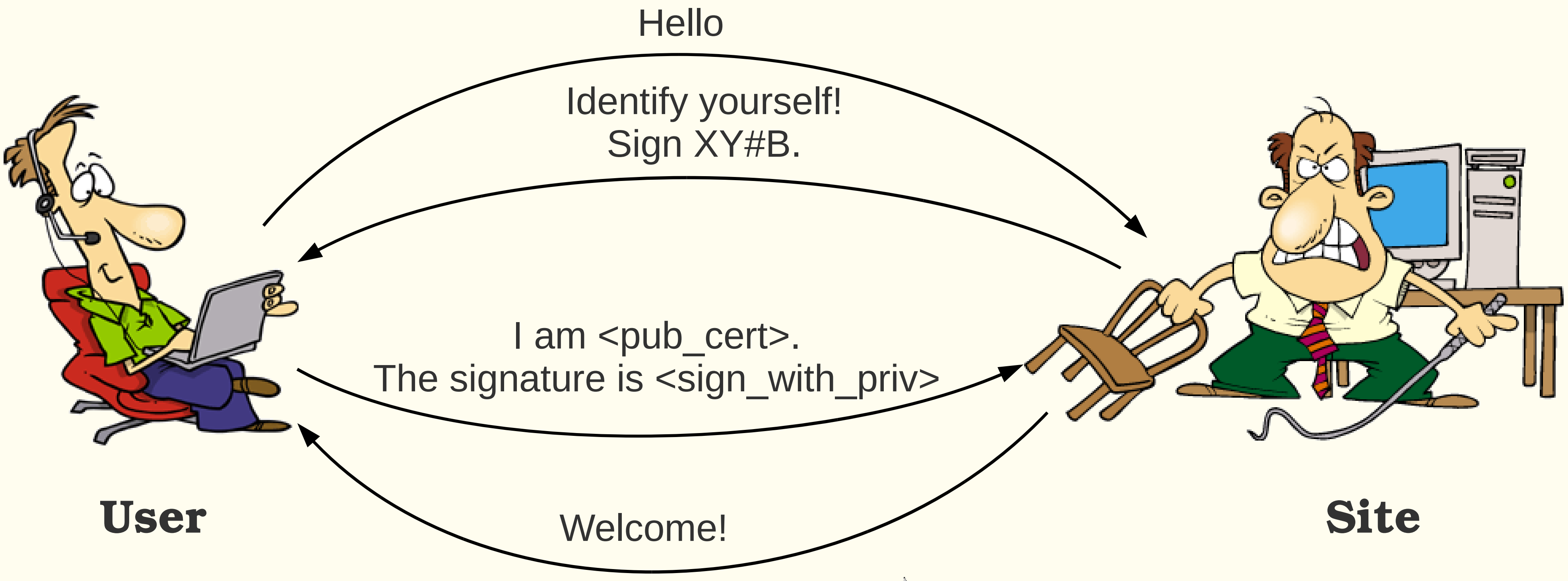
Public Key Infrastructure

- You were given a X509 certificate (Grid cert)
- Composed of 2 parts:
  - A public part, containing
    - **The user name** (also known as the **DN**)
    - Validity period (more on this later)
    - The public key
    - The signing chain (more on this later)
  - A private part (containing the private key)
- **The private part MUST be kept private**
  - The public part can (and will) be sent around



PKI – How it works?

- User proves who he is
  by signing using the private key
  - The public key in the pub_cert allows for verification



Hello

Identify yourself!
Sign XY#B.

I am <pub_cert>.
The signature is <sign_with_priv>

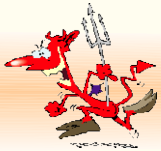
Welcome!

User

Site

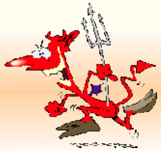
PKI – What is a signature?

- A digital signature proves who you are
  - Because **only you own the private key**
- It is strongly correlated to the public key
  - The Site uses the public key sent by the user to validate the signature
  - Not enough time to go into technical details here, consult wikipedia if interested: http://en.wikipedia.org/wiki/Digital_signature



PKI – Trust model

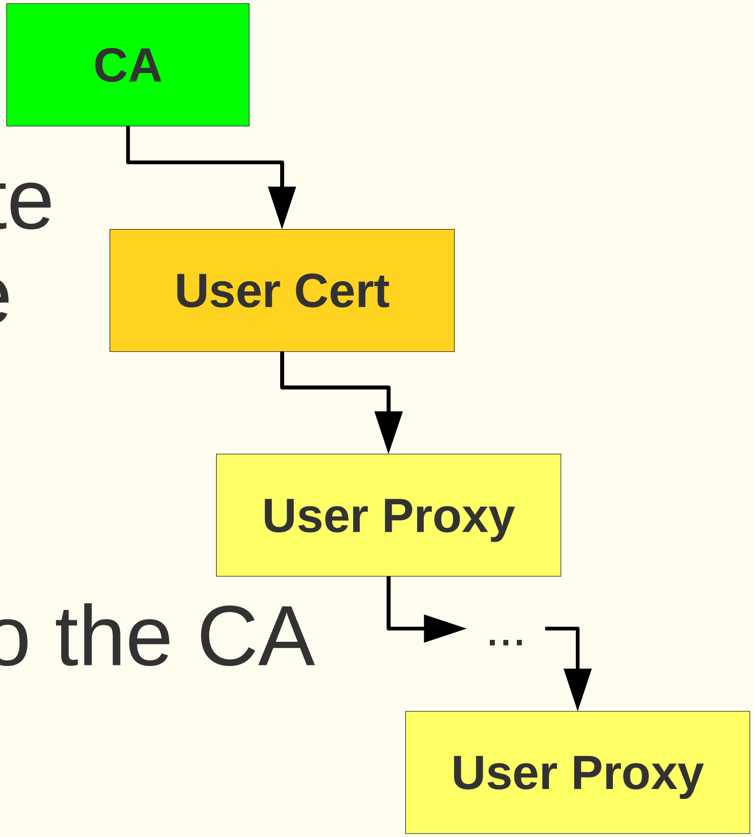
- Why should a site trust the public key sent?
  - The public key itself is signed (in the signing chain) by a trusted Certification Authority (CA)
- The CA is who you obtained the Grid cert from
  - For example the DOEGrids CA
- There are only a small number of trusted CAs
  - Sites pre-install the trusted CA public keys from a OSG repository
  - You cannot use a cert from a home-made CA



Proxies

- Now the fun/scary part – Proxies
- You have used them in your exercises
  - What are they?
- A proxy is just a new certificate derived from a user certificate
  - Possibly many times!
- The signing chain contains the info to safely climb back to the CA

http://tools.ietf.org/html/rfc3820



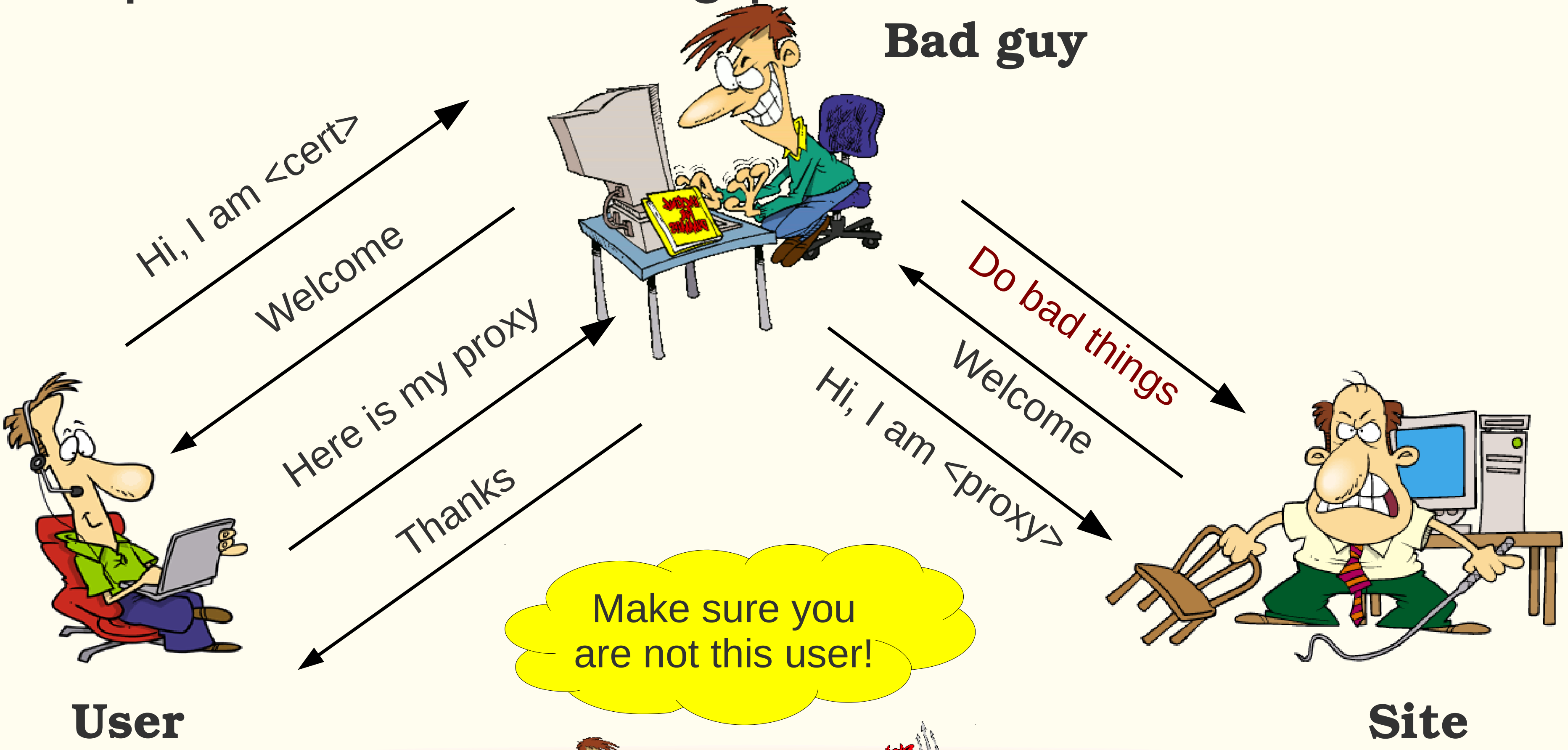
Proxies

- Why do we need a proxy?
  - The user jobs may need to talk to a remote service when running on the worker nodes (e.g. a storage element)
  - But cannot access the user cert's private key!
- A proxy is thus sent (delegated) with the job to the WN
  - **And the proxy contains a private key!**
  - So the job can impersonate the user
- Of course, delegating a private key is dangerous
  - A “bad site” can do “bad things” in your name
  - Can be mitigated by keeping the proxy lifetime short (e.g. 1 day)

Scary!

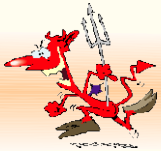
Mutual authentication

- Mutual authentication and trust particularly important when using proxies



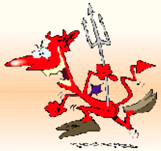
VO-based Authorization

- As said before, Sites don't trust you directly
  - They do want to see your personal proxy
  - But want the blessing of a VO before let you in
- Thus you will need VOMS attributes
  - VOMS is a service run by your VO
- Attributes get embedded in your proxy
  - When you run `voms-proxy-init`
  - Signed with VOMS private key
    - This signature is what a Site uses to trust you



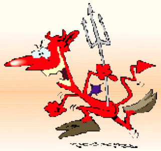
Your part

- Now you know the why and the how
  - At least to some degree
- **What is your part in it?**



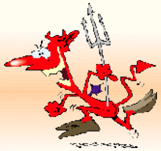
Become a Grid user

- Obtain a certificate
  - From a widely trusted CA
- Join a VO
  - Maybe even more than one
- Start using the Grid!



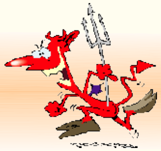
Be a trusted Grid user

- You will be allowed to use the Grid only as long as you behave well!
- Don't do anything malicious, e.g.
  - Trying to root the worker nodes
  - DDoS the Web site of a party you disagree with
- Don't do anything inappropriate, e.g.
  - Running a Web server for your business
  - Host pornography
- Don't do anything stupid, e.g.
  - Post the private key of your cert on a public Web page



Be a safe Grid user

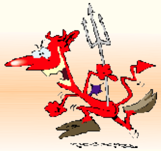
- If anyone can get your cert or proxy, you are in trouble
- Keep you client safe (avoid rootkits and spyware)
  - Patch your system software, including the OS, Web browser, Flash, PDF reader, …
    - Patch your Grid distribution, too
  - Restrict who can use your hardware (be careful if you allow password-based login from the net)
- Avoid using other's nodes for Grid activities
  - Especially public ones, like internet caffees



Be a safe Grid user

- Create only short-lived proxies
  - Like 1 day long
- Yes, it is a pain to have to renew them every day
  - But if a site gets compromised, the damage is over the next day
  - Else, you would have to apply for a new certificate

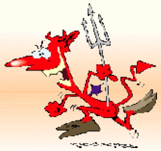
- You can automate the renewal with MyProxy
  - A service you entrust with your long-lived certificate
  - Will give a new short-lived proxy to anyone owning a valid proxy
- Easy to disable access at first sign of trouble



Know who you trust

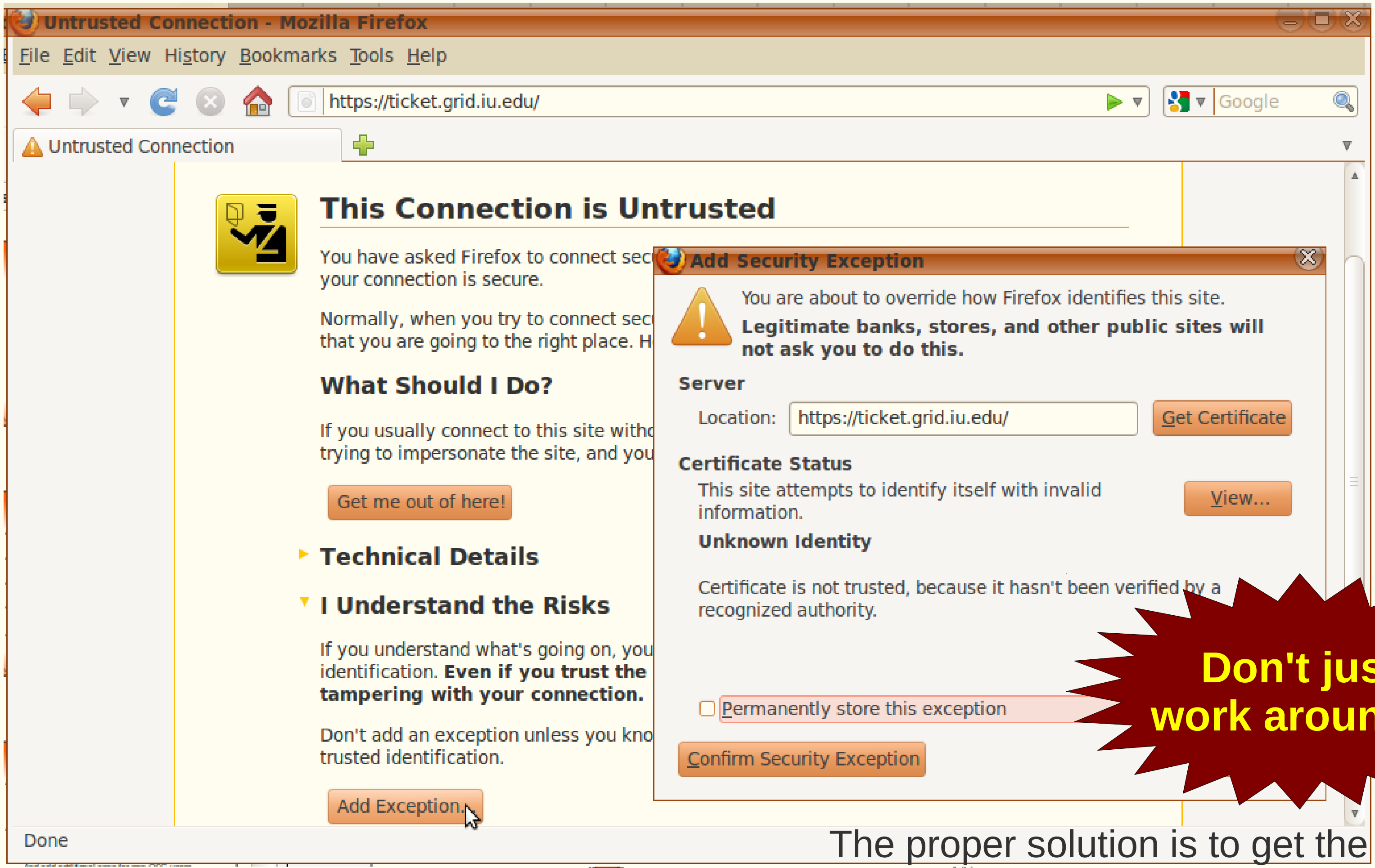
- Don't trust just any Grid service
  - Most of the time you will be delegating your proxy!
- Get the list of trusted services from your VO
  - And stick to it!

- Don't disable security checks
  - Many tools allow that for debugging purposes
- If a tool tells you something is not right, find a safe fix
  - Don't just work around it!



Example of broken security

- HTTPS server certificate problem (x509 based)



Untrusted Connection - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://ticket.grid.iu.edu/

Google

Untrusted Connection

This Connection is Untrusted

You have asked Firefox to connect sec
your connection is secure.

Normally, when you try to connect sec
that you are going to the right place. H

What Should I Do?

If you usually connect to this site witho
trying to impersonate the site, and you

Get me out of here!

▸ Technical Details

▾ I Understand the Risks

If you understand what's going on, you
identification. **Even if you trust the**
tampering with your connection.

Don't add an exception unless you kno
trusted identification.

Add Exception...

Done

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://ticket.grid.iu.edu/ Get Certificate

Certificate Status

This site attempts to identify itself with invalid information. View...

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

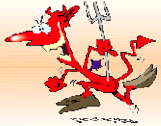
☐ Permanently store this exception

Confirm Security Exception

Not really a
Grid problem,
but easy
to visualize

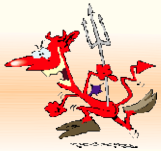
Don't just
work around it

The proper solution is to get the right CA key from
https://www.tacar.org/repos/



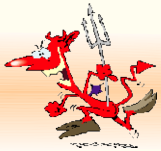
Emergencies

- Sometime things just go wrong
- So your proxy was compromised
  - Now what?
- Contact ASAP either:
  - Your VO security representative
  - The OSG Security helpline
    email: security@opensciencegrid.org
    phone: +1 317-278-9699
    https://twiki.grid.iu.edu/bin/viewauth/ReleaseDocumentation/IncidentDiscoveryReporting



Summary

- Security is more than just technology
  - It is mostly a social issue
- A certificate/proxy impersonates you
  - Whoever gets it, becomes you
  - Keep it safe, delegate only to trusted parties
  - Delegate only short-lived proxies
- Keep your Grid client secure
- Know who to contact in case of a security problem



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 any other context is not permitted