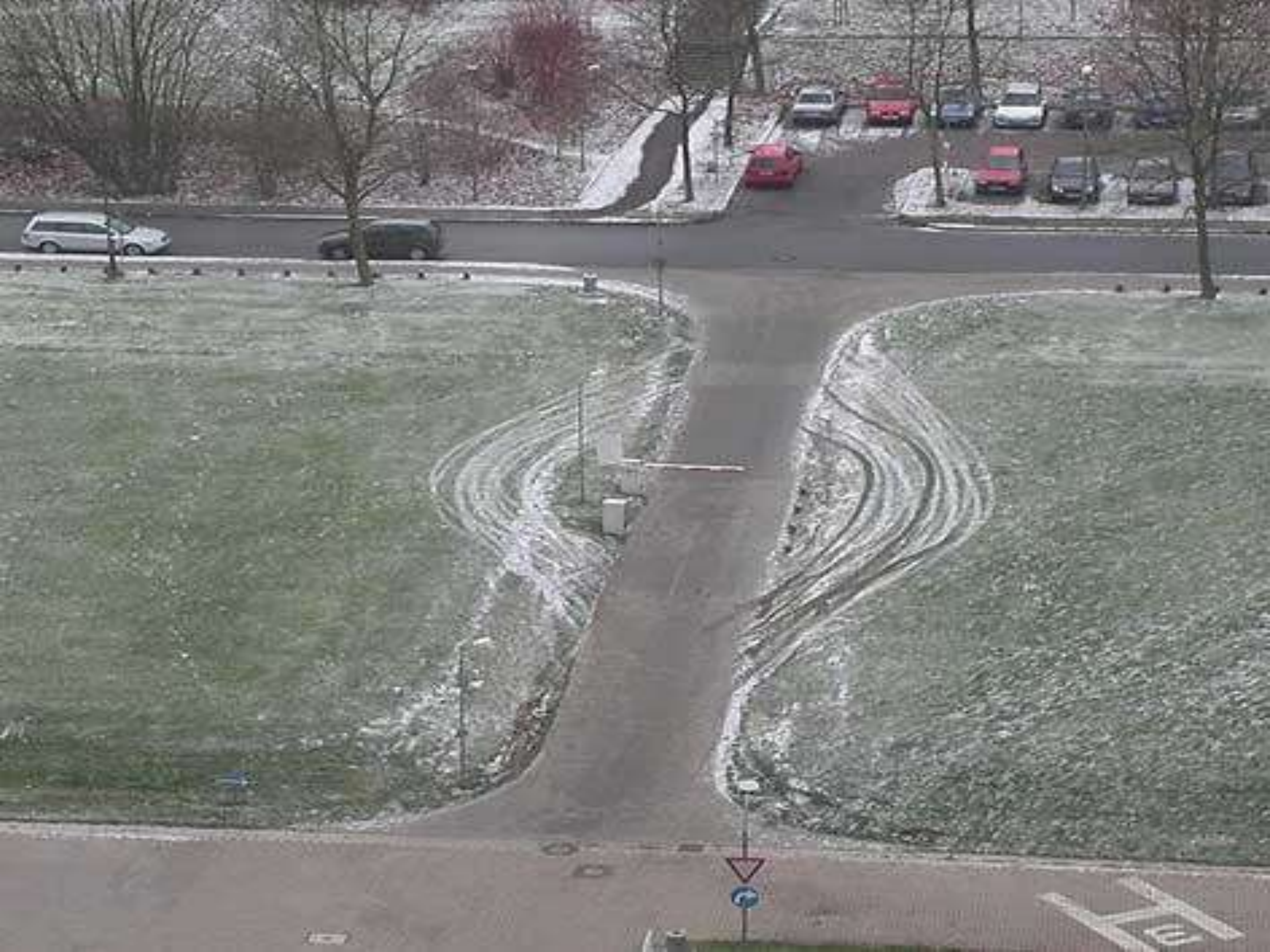
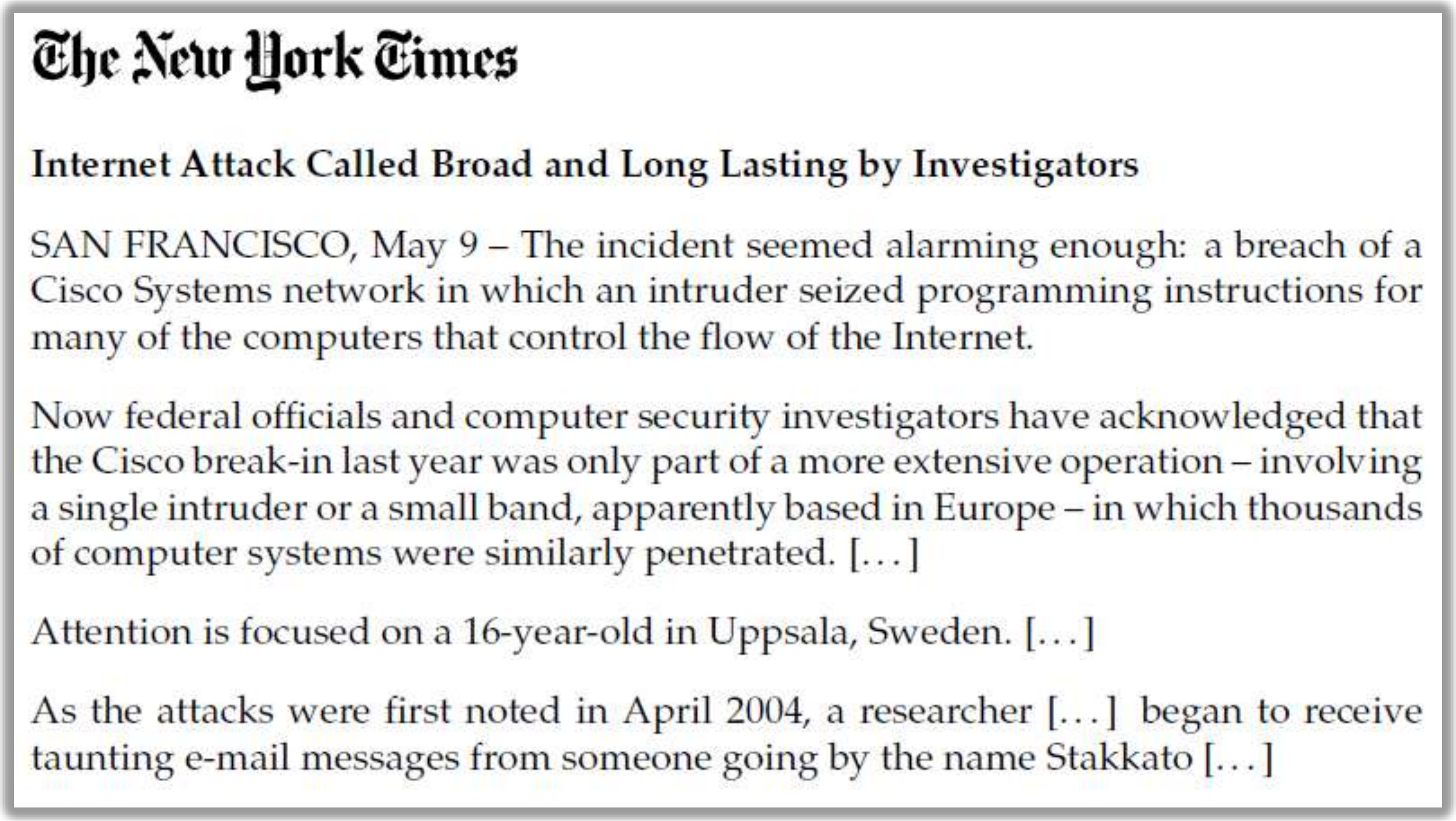


Grid Security and Authentication

David Groep

Physics Data Processing group Nikhef

Stakkato



The New York Times

Internet Attack Called Broad and Long Lasting by Investigators

SAN FRANCISCO, May 9 – The incident seemed alarming enough: a breach of a Cisco Systems network in which an intruder seized programming instructions for many of the computers that control the flow of the Internet.

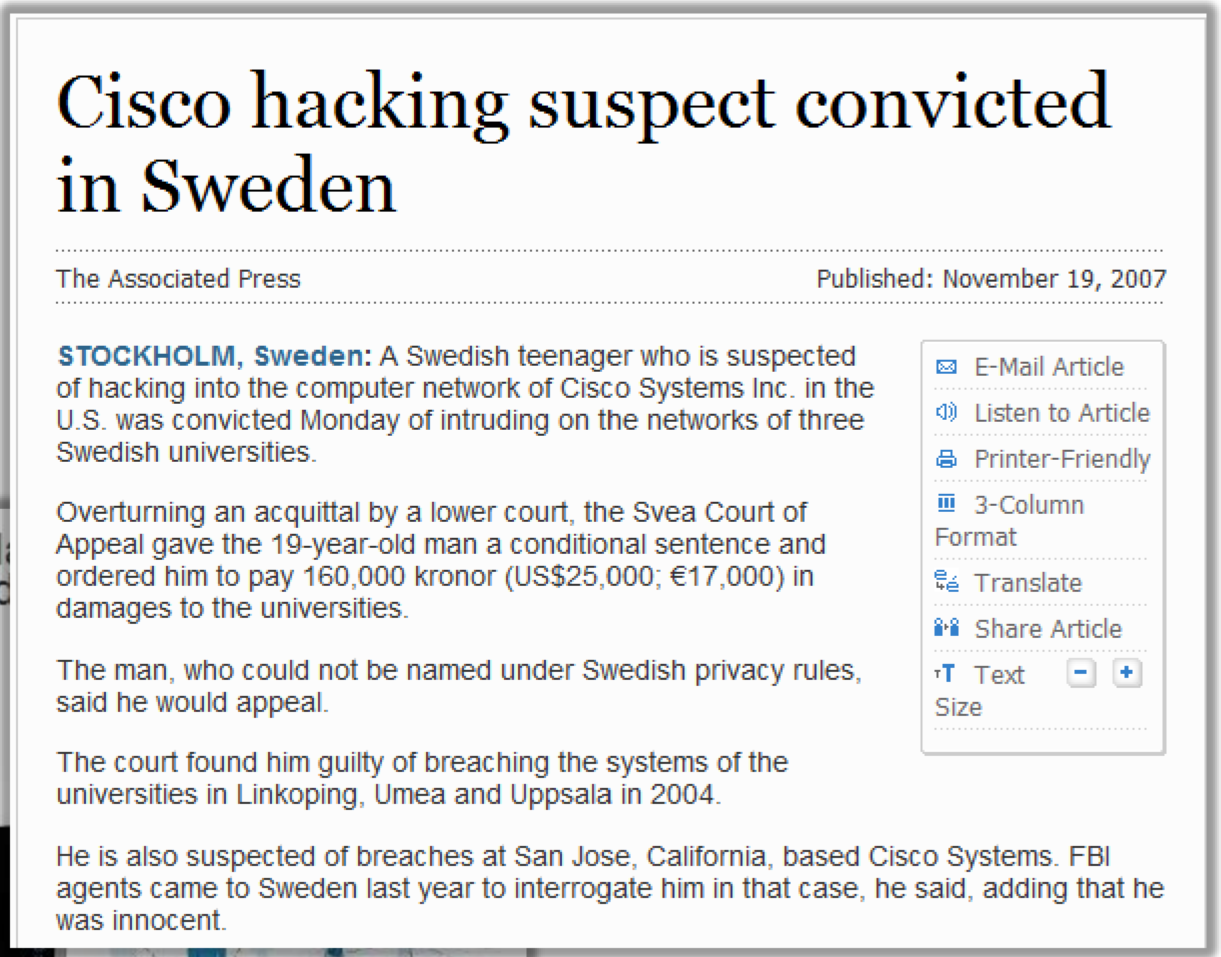
Now federal officials and computer security investigators have acknowledged that the Cisco break-in last year was only part of a more extensive operation – involving a single intruder or a small band, apparently based in Europe – in which thousands of computer systems were similarly penetrated. [. . .]

Attention is focused on a 16-year-old in Uppsala, Sweden. [. . .]

As the attacks were first noted in April 2004, a researcher [. . .] began to receive taunting e-mail messages from someone going by the name Stakkato [. . .]

Slide and info: Leif Nixon, NSC, Linköping – CCGrid06 key note “The Stakkato Intrusions”

Then, in 2007 and February …



Cisco hacking suspect convicted in Sweden

The Associated Press

Published: November 19, 2007

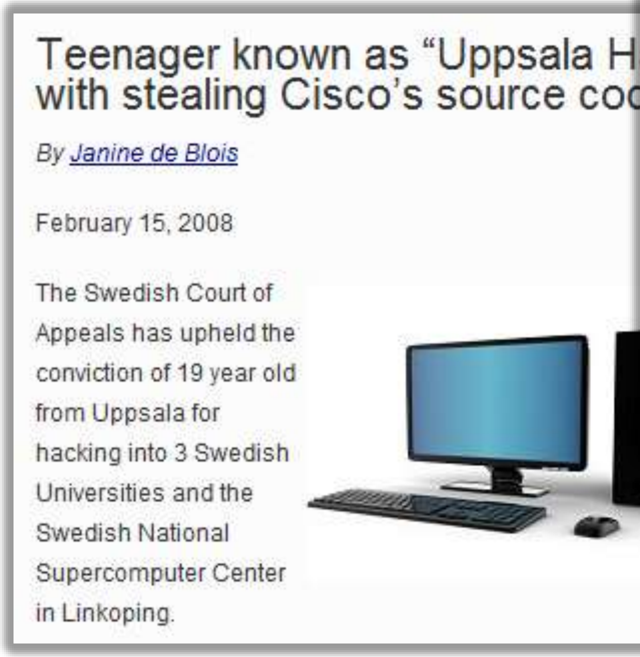
STOCKHOLM, Sweden: A Swedish teenager who is suspected of hacking into the computer network of Cisco Systems Inc. in the U.S. was convicted Monday of intruding on the networks of three Swedish universities.

Overturning an acquittal by a lower court, the Svea Court of Appeal gave the 19-year-old man a conditional sentence and ordered him to pay 160,000 kronor (US$25,000; €17,000) in damages to the universities.

The man, who could not be named under Swedish privacy rules, said he would appeal.

The court found him guilty of breaching the systems of the universities in Linkoping, Umea and Uppsala in 2004.

He is also suspected of breaches at San Jose, California, based Cisco Systems. FBI agents came to Sweden last year to interrogate him in that case, he said, adding that he was innocent.



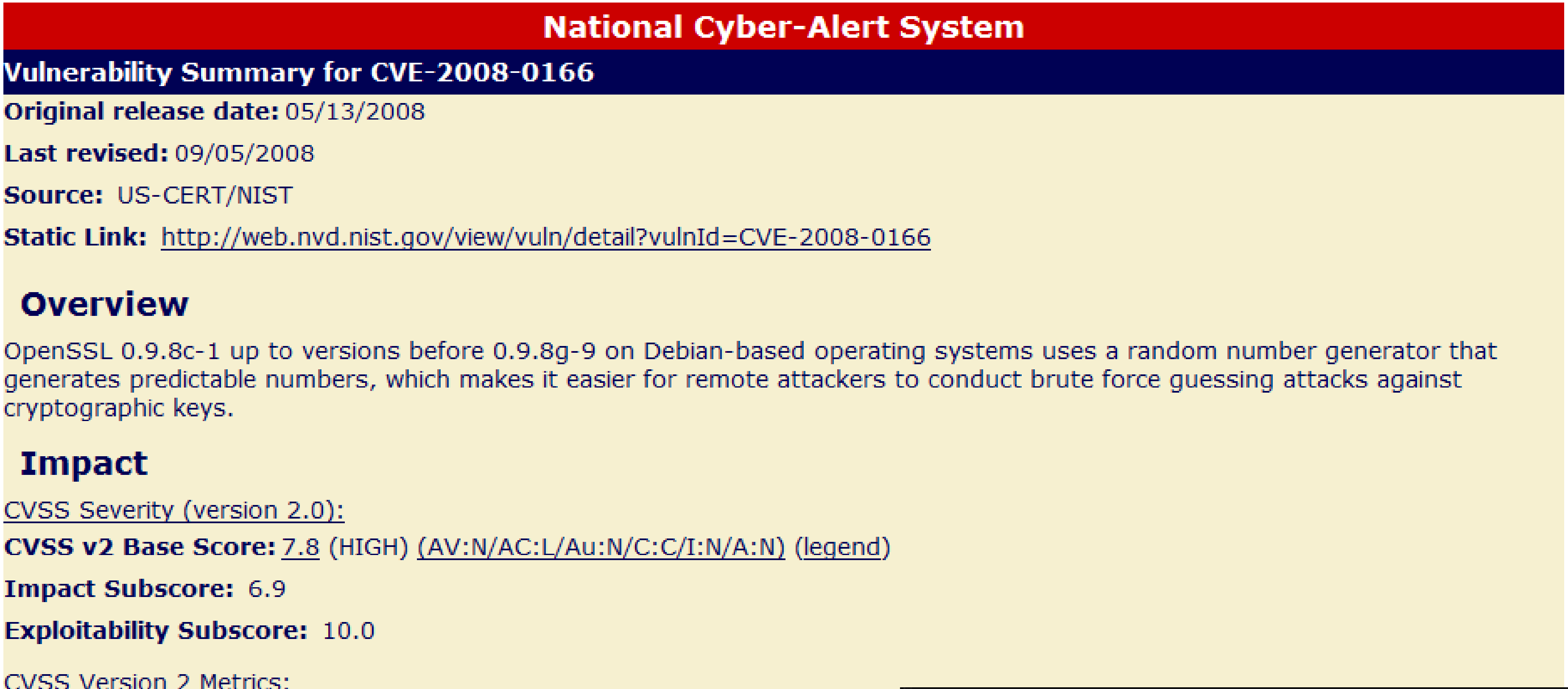
Teenager known as “Uppsala Ha with stealing Cisco’s source coc

By *Janine de Blois*

February 15, 2008

The Swedish Court of Appeals has upheld the conviction of 19 year old from Uppsala for hacking into 3 Swedish Universities and the Swedish National Supercomputer Center in Linkoping.

Is It Random: 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3



National Cyber-Alert System

Vulnerability Summary for CVE-2008-0166

Original release date: 05/13/2008

Last revised: 09/05/2008

Source: US-CERT/NIST

Static Link: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166

Overview

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.8 (HIGH) (AV:N/AC:L/Au:N/C:C/I:N/A:N) (legend)

Impact Subscore: 6.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

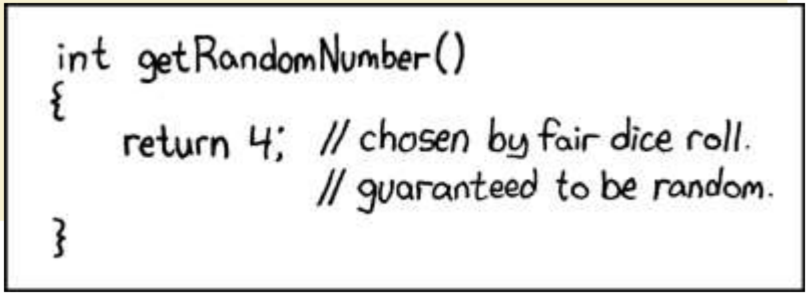
Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information

Only 163840 possible ssh keys!



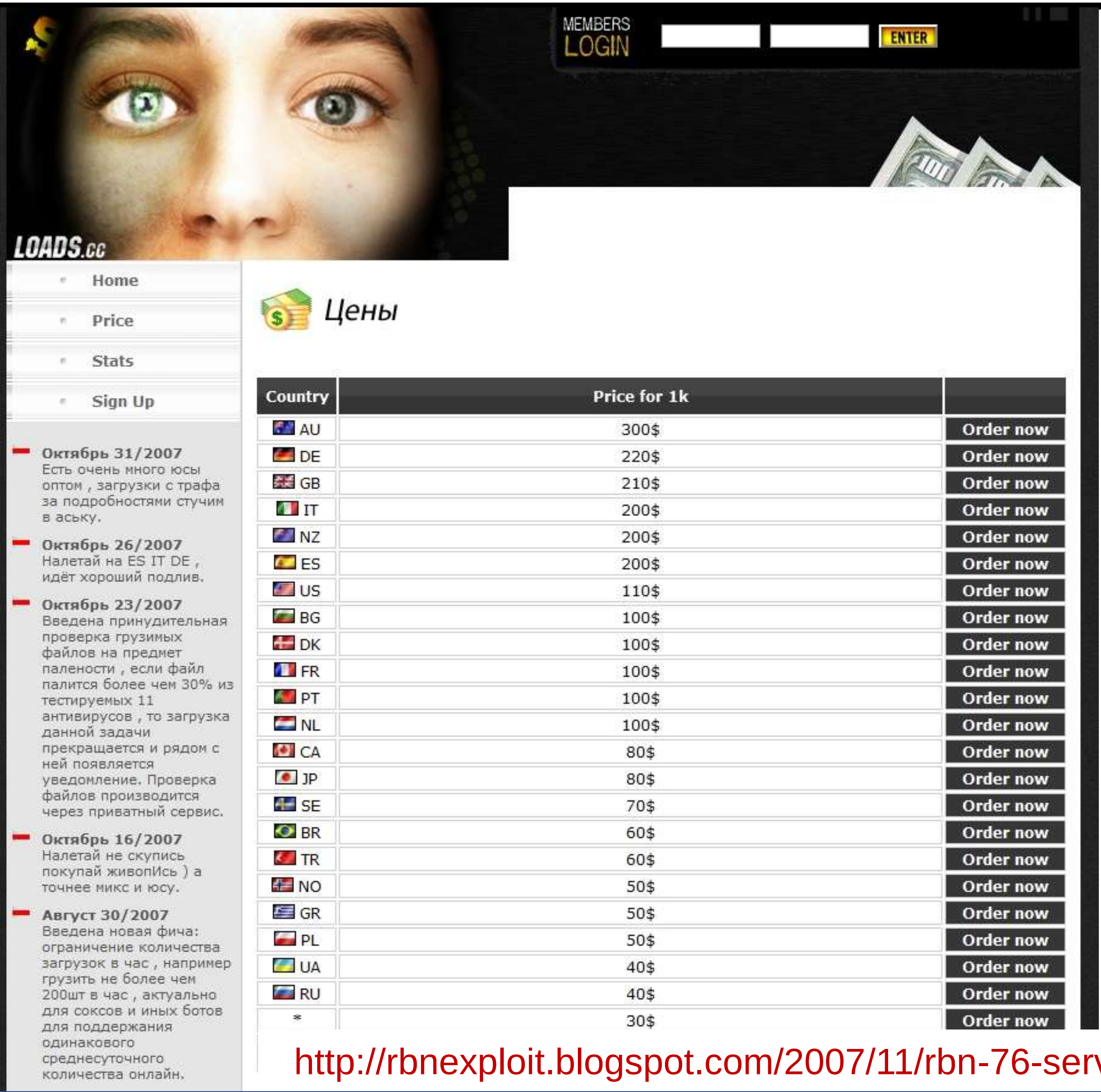
```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

http://xkcd.com/221/

More ssh

‘XXXX-CERT-20080805’

Zombies for Sale



Октябрь 31/2007
Есть очень много юсы оптом , загрузки с трафа за подробностями стучим в аську.

Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.

Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

Октябрь 16/2007
Налетай не скупись покупай живопИсь) а точнее микс и юсу.

Август 30/2007
Введена новая фича: ограничение количества загрузок в час , например грузить не более чем 200шт в час , актуально для соксов и иных ботов для поддержания одинакового среднесуточного количества онлайн.

Цены

Country	Price for 1k	
AU	300$	Order now
DE	220$	Order now
GB	210$	Order now
IT	200$	Order now
NZ	200$	Order now
ES	200$	Order now
US	110$	Order now
BG	100$	Order now
DK	100$	Order now
FR	100$	Order now
PT	100$	Order now
NL	100$	Order now
CA	80$	Order now
JP	80$	Order now
SE	70$	Order now
BR	60$	Order now
TR	60$	Order now
NO	50$	Order now
GR	50$	Order now
PL	50$	Order now
UA	40$	Order now
RU	40$	Order now
*	30$	Order now

Price for 1000 infected consumer computers:

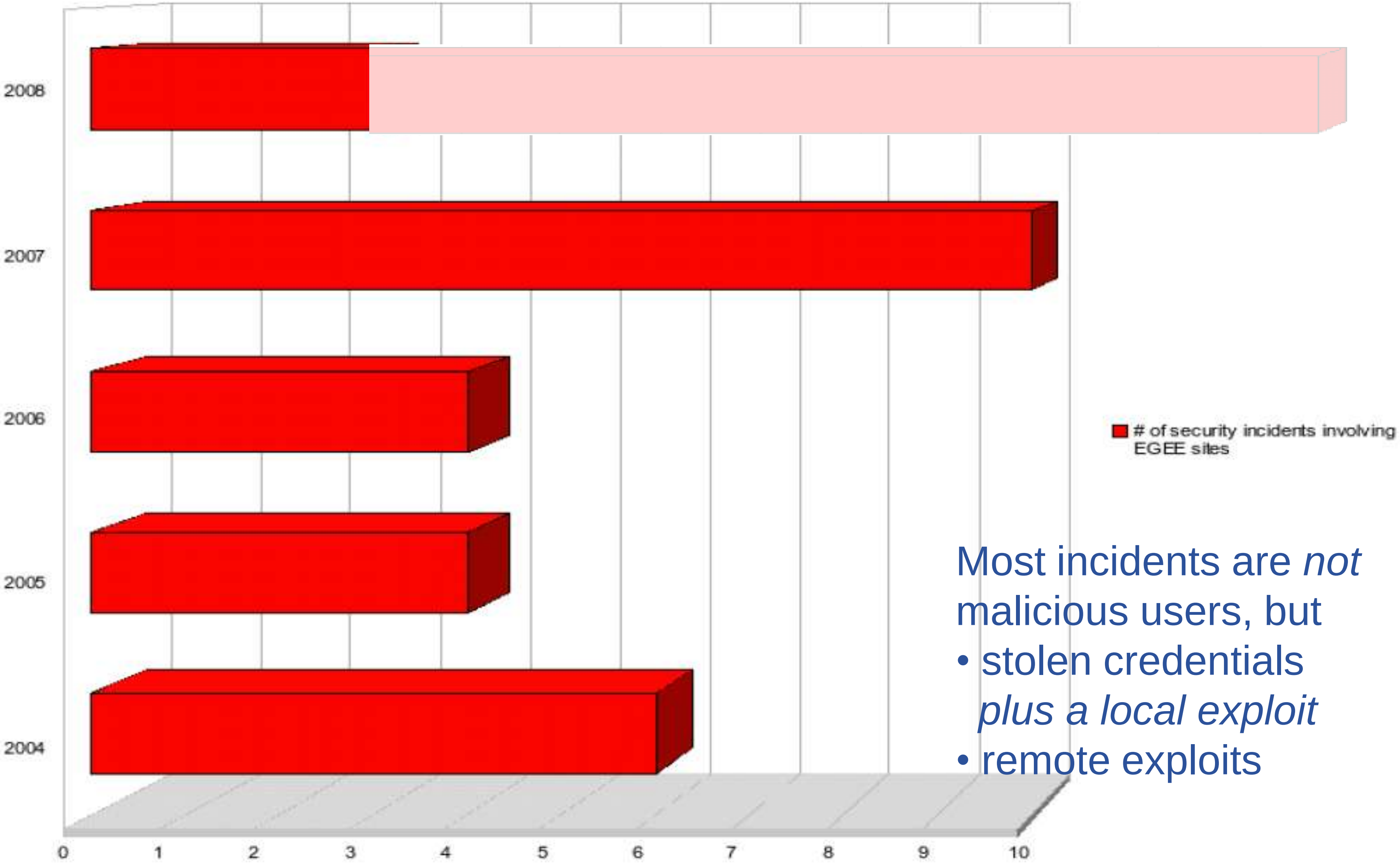
AU:	**US$ 300**
US:	**US$ 110**
NL:	**US$ 100**

And grid systems are better connected than xDSL systems, so …

http://rbnexploit.blogspot.com/2007/11/rbn-76-service-team-loads-cc-and-their.html

Incidents involving EGEE sites

(per 3/2008 and extrapolated)



Most incidents are *not* malicious users, but

- stolen credentials *plus a local exploit*
- remote exploits

Romain Wartel, CERN and OSCT; http://romain.wartel.net/talks/20080409Wartel-short.pdf

But What About Containment?

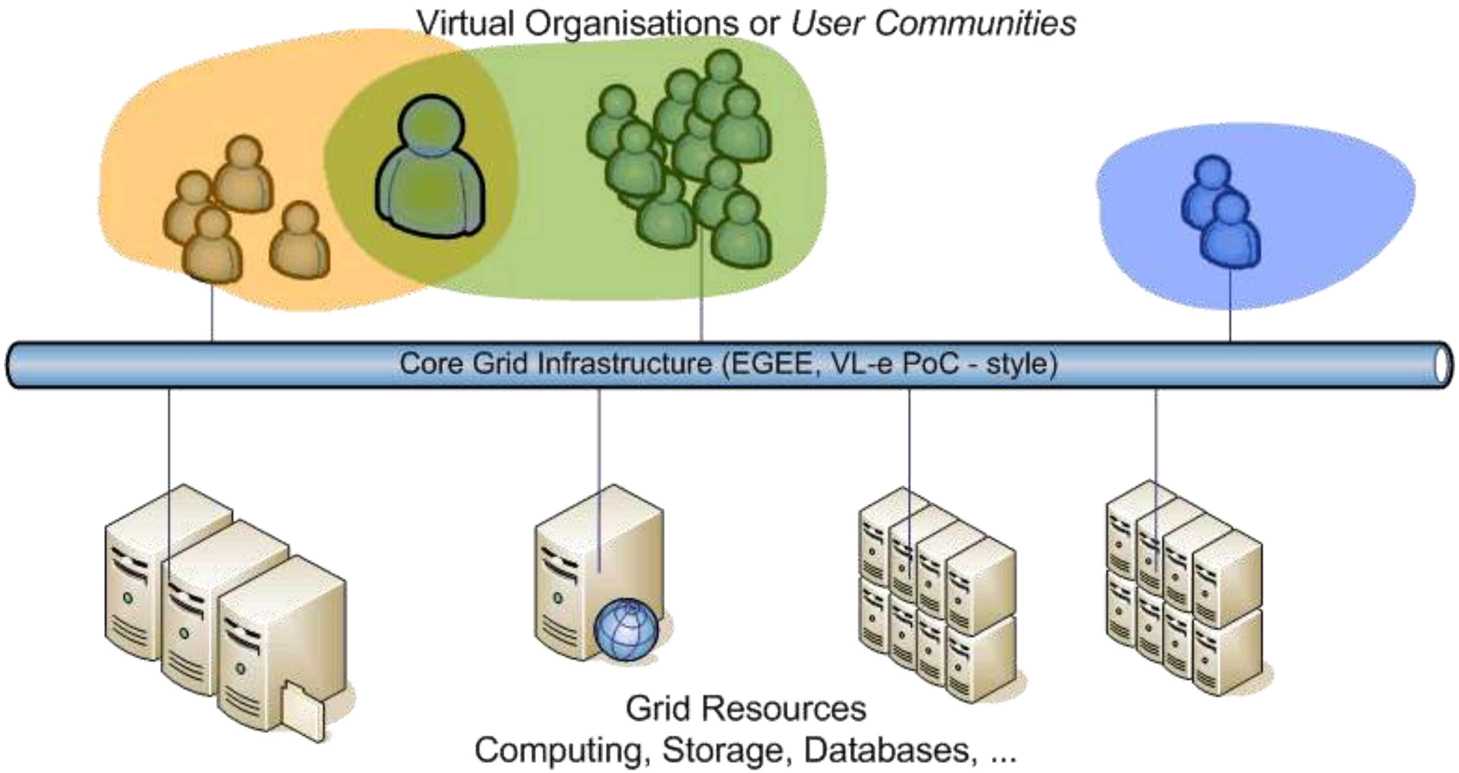
Oops … *ssh* keys

- do not expire
- cannot be revoked

Security And Availability For All Involved

Who are playing in the Grid Space, and thus: who get attacked?

- **Virtual Organisations or Communities: you and your colleagues**
- **Resource Centres and Grid Services:
  CPU, Storage, Data base and service providers
  central services and coordination**


Virtual Organisations or *User Communities*
Core Grid Infrastructure (EGEE, VL-e PoC - style)
Grid Resources
Computing, Storage, Databases, ...

Security and Availability

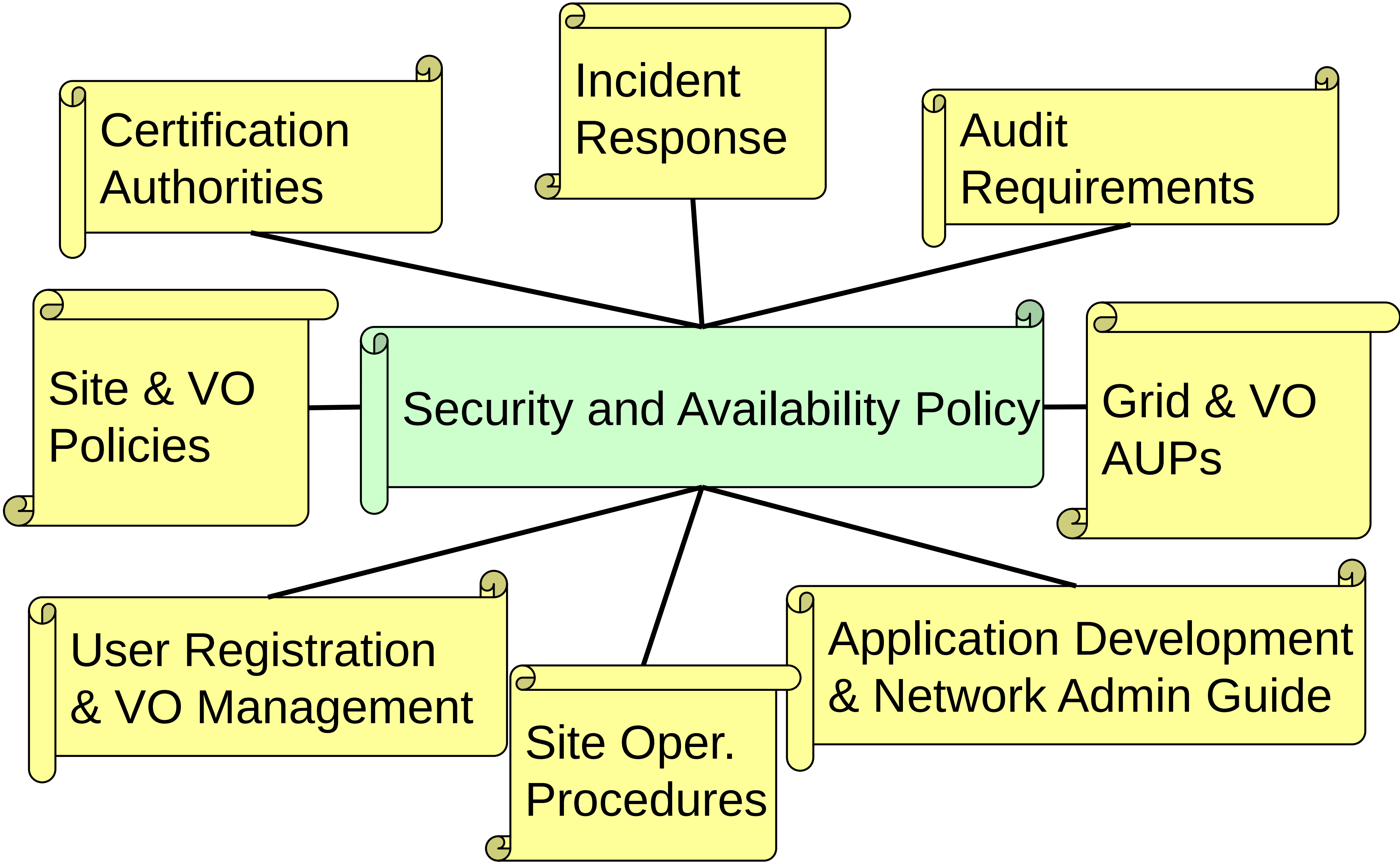
‘Security means more than merely preventing unauthorised access.

It is pro-actively concerned with maximising the availability and integrity of all the services and data that might be required by authorised users.

This Policy accordingly addresses the protection, confidentiality, integrity and availability of Resources and the Services running on them.’

From: LCG Security and Availability Policy version 4.0c

Security Policies



Certification Authorities

Incident Response

Audit Requirements

Site & VO Policies

Security and Availability Policy

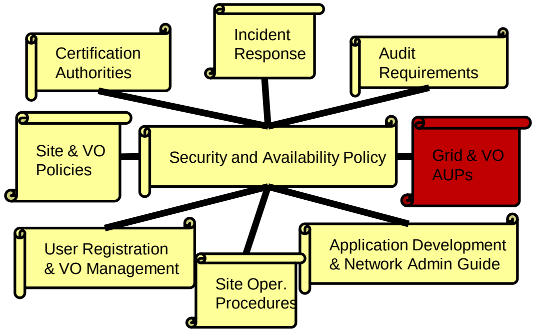
Grid & VO AUPs

User Registration & VO Management

Site Oper. Procedures

Application Development & Network Admin Guide

Grid Acceptable Use Policy


Certification Authorities
Incident Response
Audit Requirements
Site & VO Policies
Security and Availability Policy
Grid & VO AUPs
User Registration & VO Management
Site Oper. Procedures
Application Development & Network Admin Guide

Protecting the Grid and Resource Centres and tells you what you consent to:

1. Don’t do anything nasty
2. Your work stays within the scope of your VO
3. Report (potential) abuse or suspected account compromise
4. The Grid is *not* a guaranteed resource
5. Registration and logged information is used only for *administrative, operational, accounting, monitoring and security purposes*
   may be disclosed to other organizations anywhere in the world for these purposes
6. You’re liable for the consequences of violating the AUP

But Who Are You, and Why?

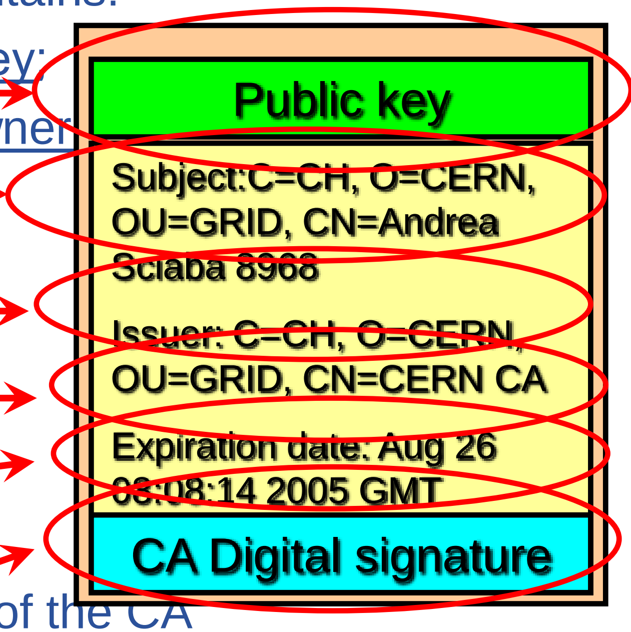
You already got a ‘digital certificate’

- A digital passport: it says who you are, not where you can go
- Technically called ‘X.509 identity certificate’
- Digitally signed by a ‘certification authority’
- Contains: your name, and a unique name in the world

You prove possession by a ‘private key’ that only you know to sign transactions

An X.509 Certificate contains:

- owner’s public key;
- identity of the owner;
- info on the CA;
- time of validity;
- Serial number;
- digital signature of the CA



Public key

Subject:C=CH, O=CERN, OU=GRID, CN=Andrea Sciaba 8968

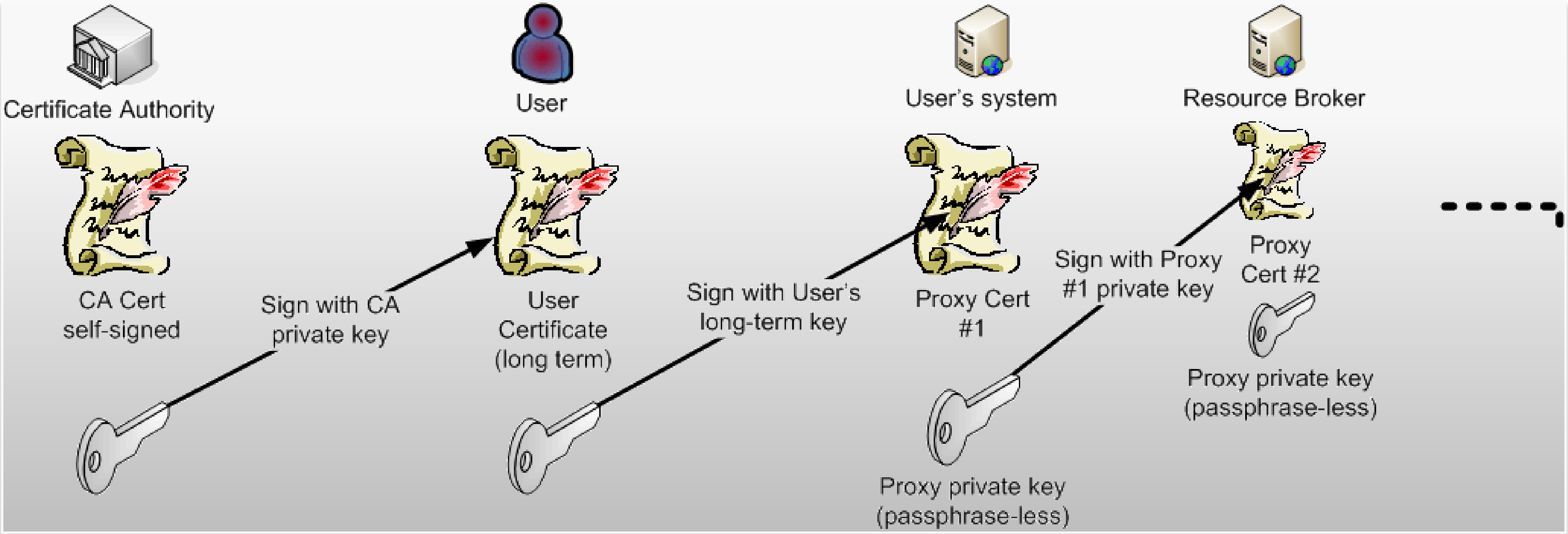
Issuer: C=CH, O=CERN, OU=GRID, CN=CERN CA

Expiration date: Aug 26 08:08:14 2005 GMT

CA Digital signature

Grid By Proxy

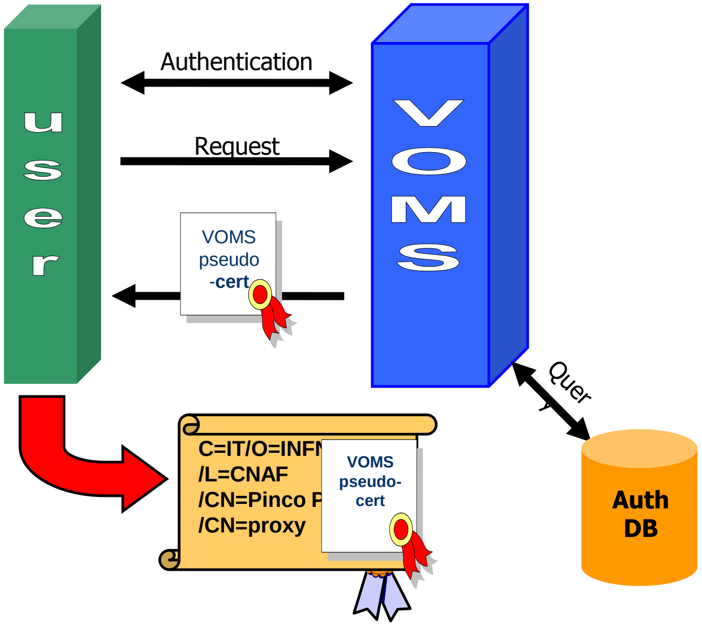
- Your private key MUST be protected by a pass phrase
  - Like ‘gRatJESolleSB&E’, or ‘o~gemds!oniE’
- But
  - You don’t want to type that every few seconds
  - The broker has to work on your behalf
  - Password-less, short-lived, proxy certificates:

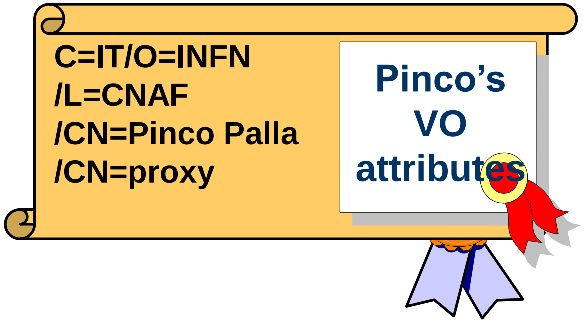


Attached to your passport are ‘Visa’

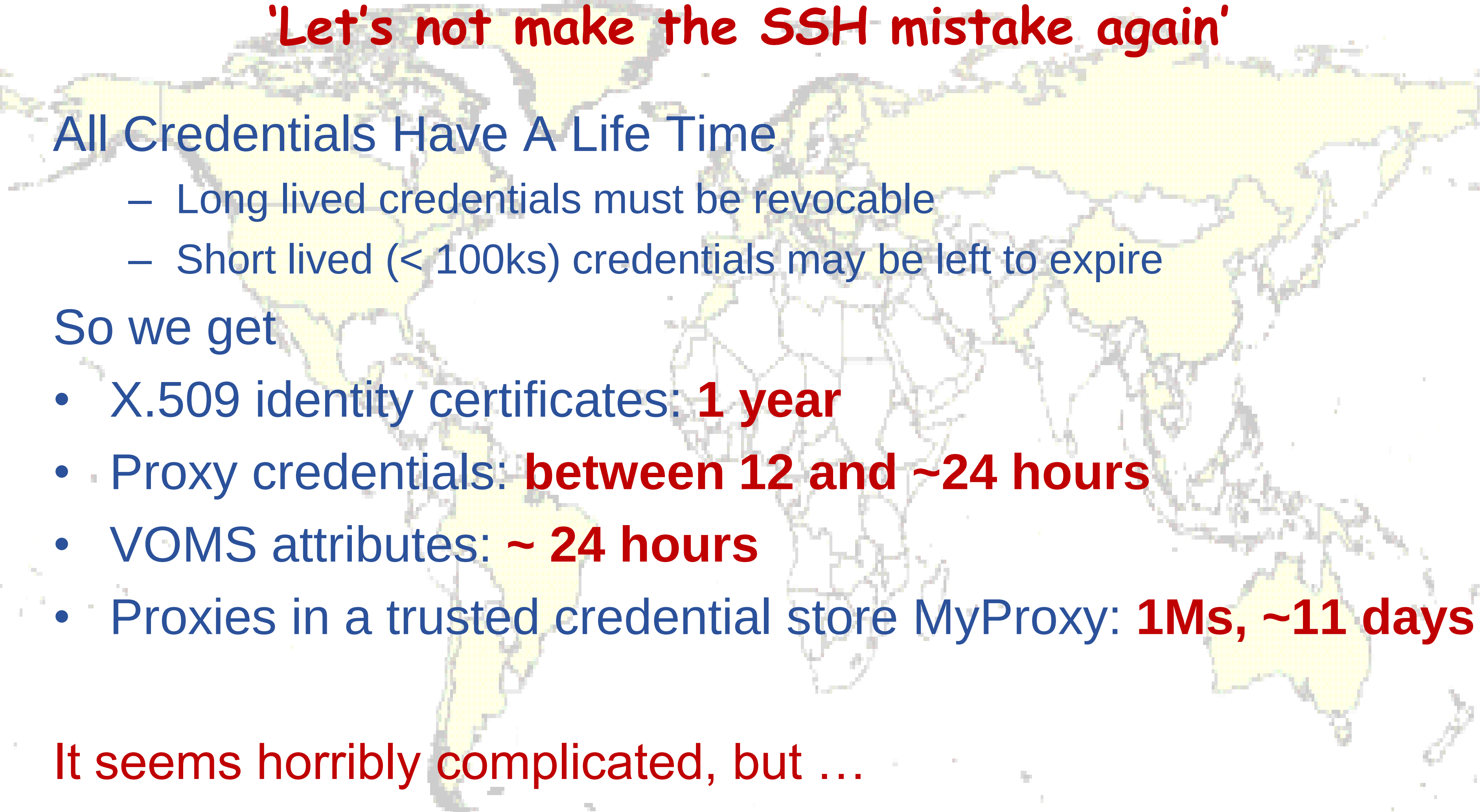
Grid ‘visa’ are issues by your community (VO)

- Technically called ‘VOMS Attribute Certificates’
- Digitally signed by the community server
- Contains: your roles and group memberships
- Bound to your passport (“X.509”) distinguished name
- Embedded in your temporary *proxy certificate*





Acceptable Credentials on the Grid



'Let's not make the SSH mistake again'

All Credentials Have A Life Time

- Long lived credentials must be revocable
- Short lived (< 100ks) credentials may be left to expire

So we get

- X.509 identity certificates: **1 year**
- Proxy credentials: **between 12 and ~24 hours**
- VOMS attributes: **~ 24 hours**
- Proxies in a trusted credential store MyProxy: **1Ms, ~11 days**

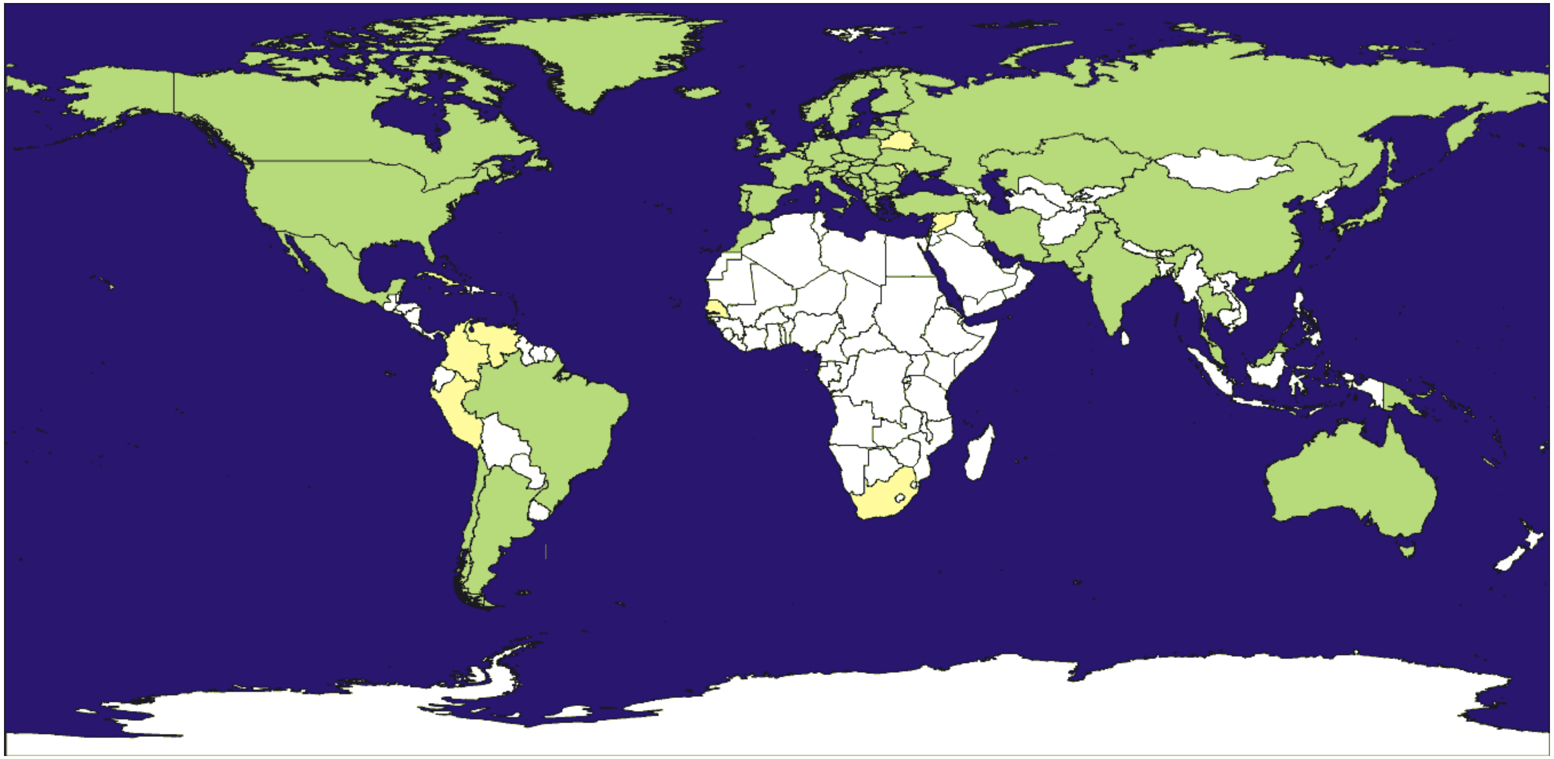
It seems horribly complicated, but …

… but you get global trust, instead of signing up at 250 sites!

How do the sites know me (and I them)?

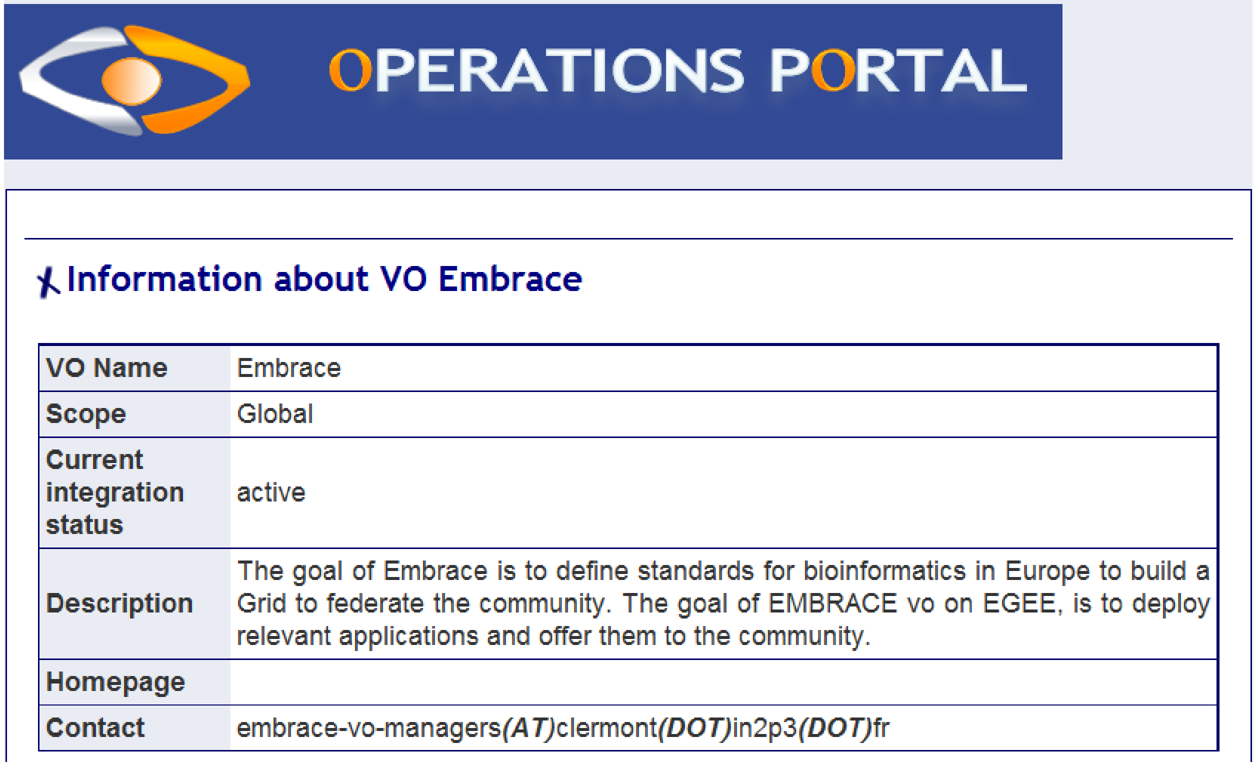
International Grid Trust Federation

- All research grid infrastructures share the same base set of trusted third parties ('CAs')
- There is typically one in each country
- The credentials they issue are comparable in quality



VOs that comply with the Policy

- Sites supporting the VO trust the ‘visa’ issued
- Trust anchor available to all sites from the trusted source
- VO *manager* is responsible for adding and removing users *subject to the VO management policy*



Information about VO Embrace

VO Name	Embrace
Scope	Global
Current integration status	active
Description	The goal of Embrace is to define standards for bioinformatics in Europe to build a Grid to federate the community. The goal of EMBRACE vo on EGEE, is to deploy relevant applications and offer them to the community.
Homepage	
Contact	embrace-vo-managers*(AT)*clermont*(DOT)*in2p3*(DOT)*fr

EGEE Operations Portal: http://cic.gridops.org/

So, where does that leave us?

Is the grid safe? You never know …

- Strong authentication of users and resources by certificates
- Exposure is time-limited and revocable
- Community membership via secured ‘visa’
- Encrypted and integrity-protected communications

- Grid and sites subject to policies, with data protection taken seriously, commensurate with the open, scientific nature of the infrastructure

- A vulnerability and risk assessment process to work on the software
- Auditing and incident response teams across Europe and the Grids

And you now know more-or-less how this works

But, as always, it remains a matter of *trust* …