Security Issues

System vulnerabilities
and data protection laws

Ivan Andrian, Sincrotrone Trieste
JACoW Team Meeting, Frascati 2005

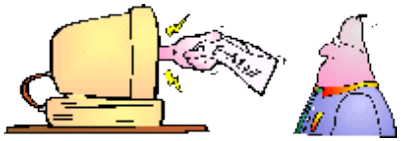
Part I: System vulnerabilities

What may be vulnerable?

"When everybody is out to get you, paranoid just seems like a good idea."

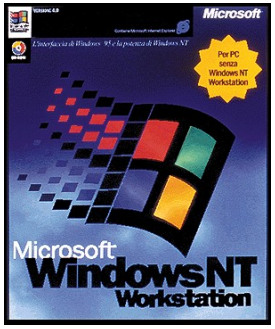
Woody Allen

- We have one or more **servers**



  - Hardware security usually guaranteed by their location (our labs...)

- We have an **operating system** on top of the hardware



  - Keep it as updated as you can
    - Windows vulnerabilities growing more and more
    - Unix vulnerabilities always possible: easier to protect
  - Use a **well configured** firewall
  - Disable anything of no use

Then comes Oracle...

"Failure is not an option, it comes bundled with the software."

anonymous

- Oracle is well known around the net...
- Default installation pretty naïve
  - No security patches applied (!)
  - "Old" Apache 1.3 installation
  - SQLnet open to the world
  - Default "CHANGEONINSTALL"-like passwords
  - Apache 1.3 with DB configuration pages (i.e., DAD) open to the world.
  - Many useless Java things here and there

Hardening Oracle

```
SELECT * FROM users WHERE clue > 0
0 rows returned
```

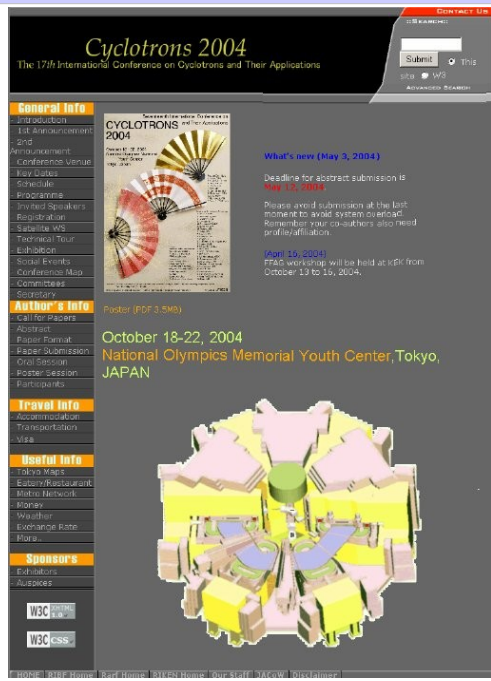
http://www.thinkgeek.com

- Apply all the **security patches** released
  - Oracle Metalink account needed
  - Keep an eye on the Oracle site
- Change passwords
- Yes, you really MUST change passwords
- Do it. Now!
- Change SQLnet parameters (TNSlistener)
- Use a firewall
- Change `httpd.conf` parameters
- Use at least simple HTTP authentication
- Use SSL (HTTPS)

Not just theory... examples! Cyclotrons 2004 (1)

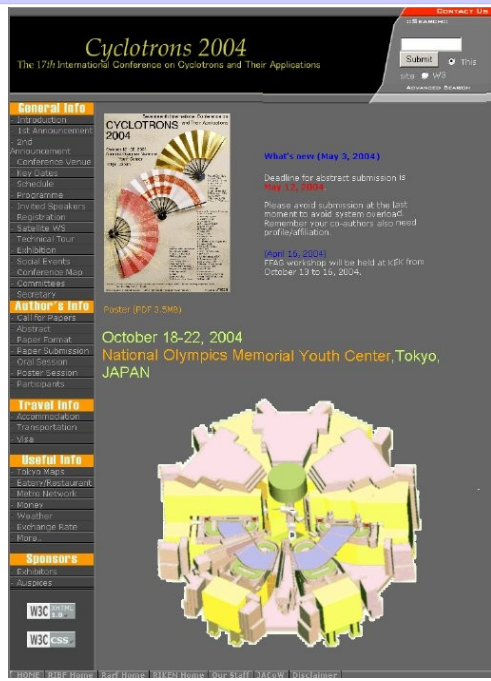
- Oracle 9.2.0.4 on Miracle Linux 2.1
  - An intrusion forced to shutdown the DB and proceed with mandatory updates
- SSL port attacked (`mod_ssl`)
  - Closed port 443
- HTTP TRACE is enabled in Apache
  - Workaround by modifying httpd.conf

```
LoadModule      mod_rewrite.so
RewriteEngine   On
RewriteCond     %{REQUEST_METHOD} ^TRACE
RewriteRule     .* -[F]
```



Cyclotrons 2004 (2)

- SOAP vulnerability
  - `Jserv` not needed: take care!
  - Disabled SOAP (renamed `soap.jar`)



- `mod_plsql` vulnerability
  - Added

    `EXCLUSION_LIST= ACCOUNT*, SYS.*, DBMS_*, OWA*`

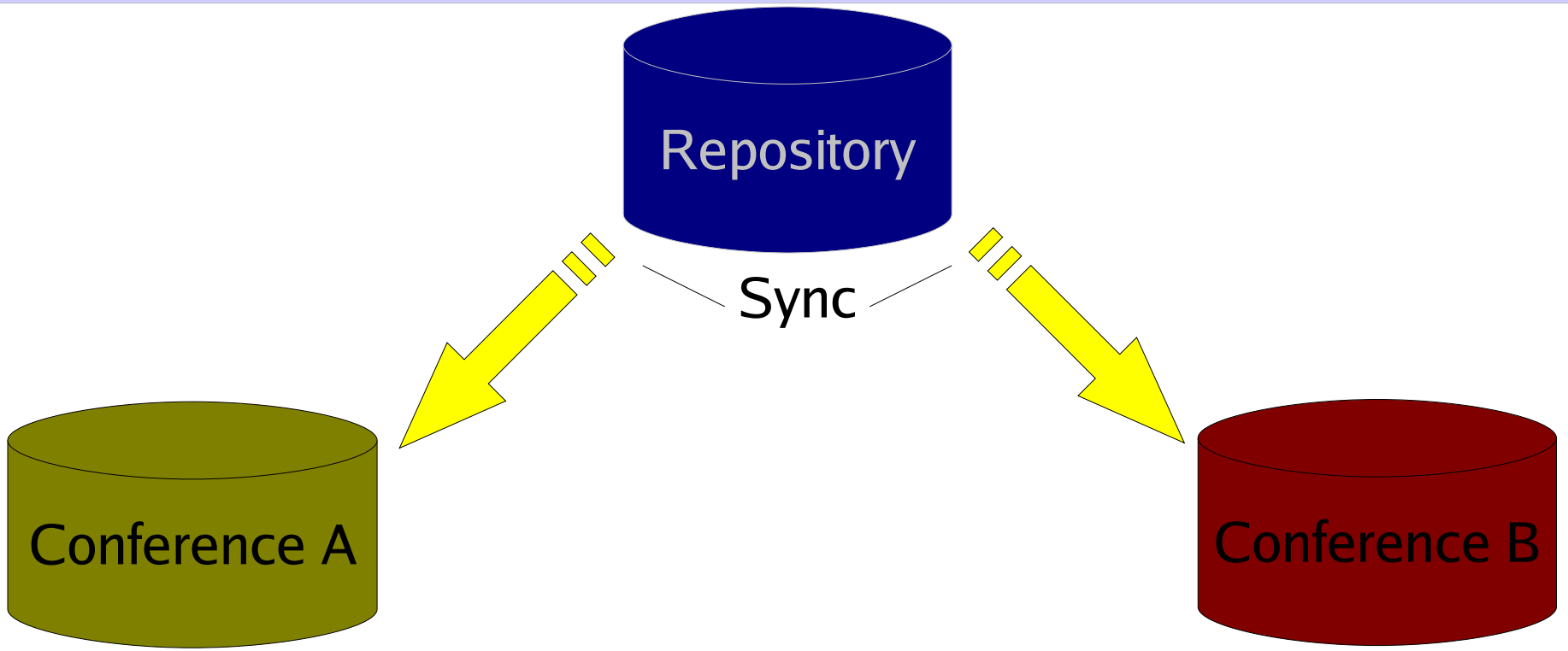
    in `wdbsvr.app`

- Oracle 9.2.0.4 on Fedora Core 1 Linux
  - Intrusion detected “by bare eyes” right after abstract submission was open
  - No problems for the SPMS but:
    IRC server installed
    - useless due to the firewall
    - EnergyMech, http://www.energymech.net
  - Oracle Security Alert #62 passed by
    - Patches 3169446 and 3210293
    - Closed unused SSL port

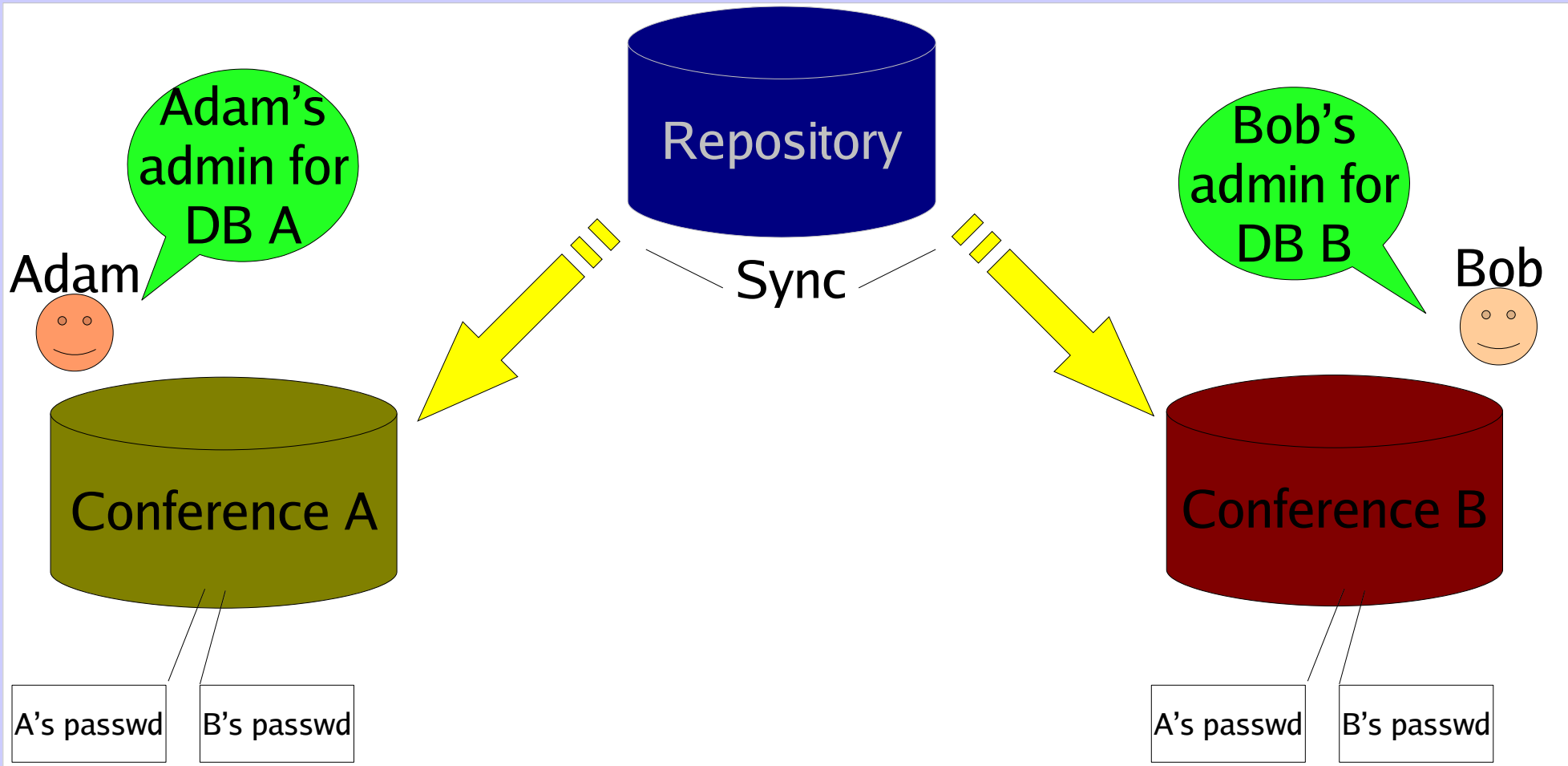
... and it's SPMS time

- Possible SPMS bugs
  - Its use during these years proved it rather secure
- Data is encrypted but password in the code (hence, in the DB)
- Account passwords are readable by admin
  - Bad feature!
  - Better being changeable but **not** readable.
  - Admin roles may change between (concurrent!) conferences

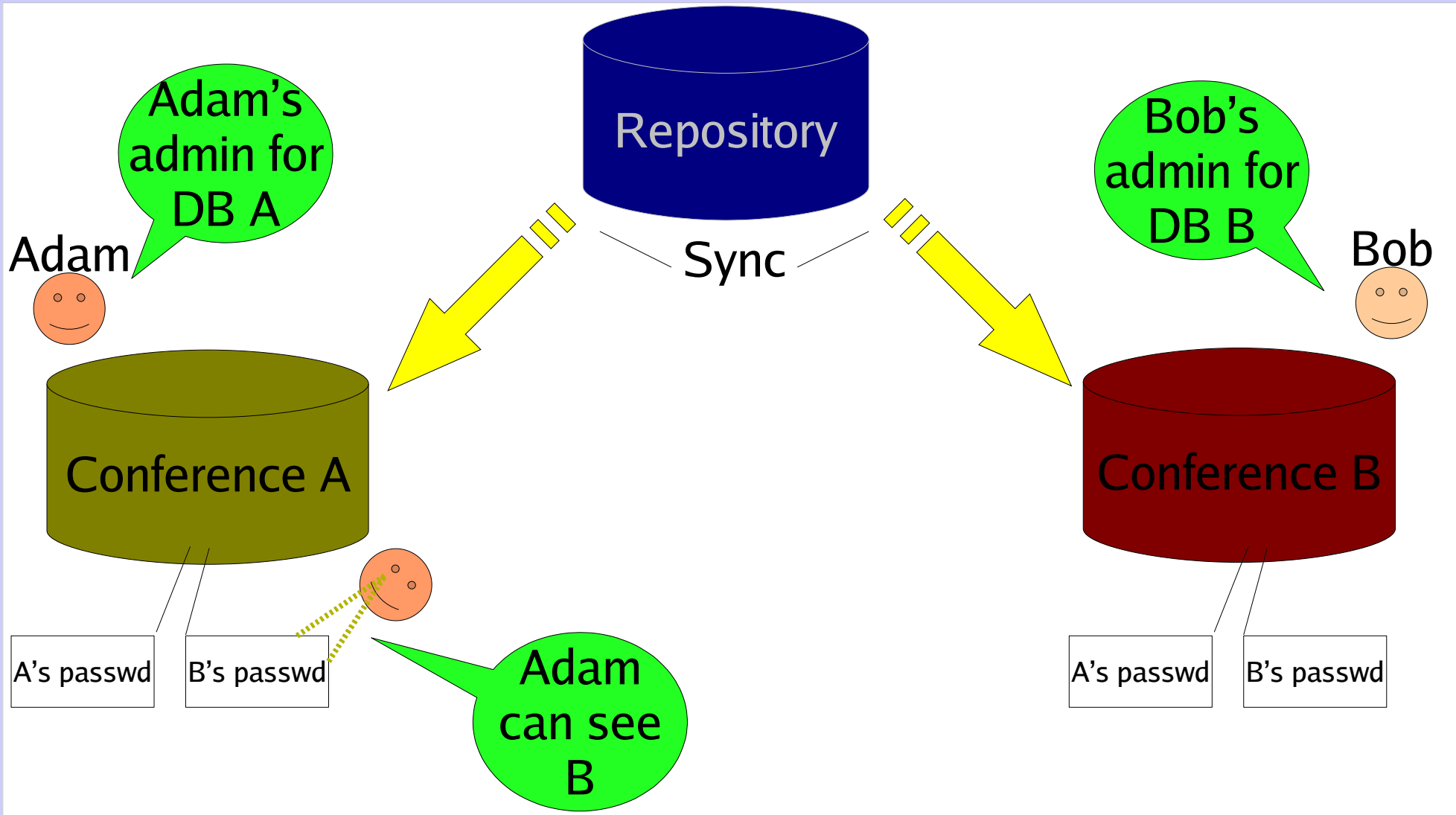
Passwords vulnerability: Simple Example



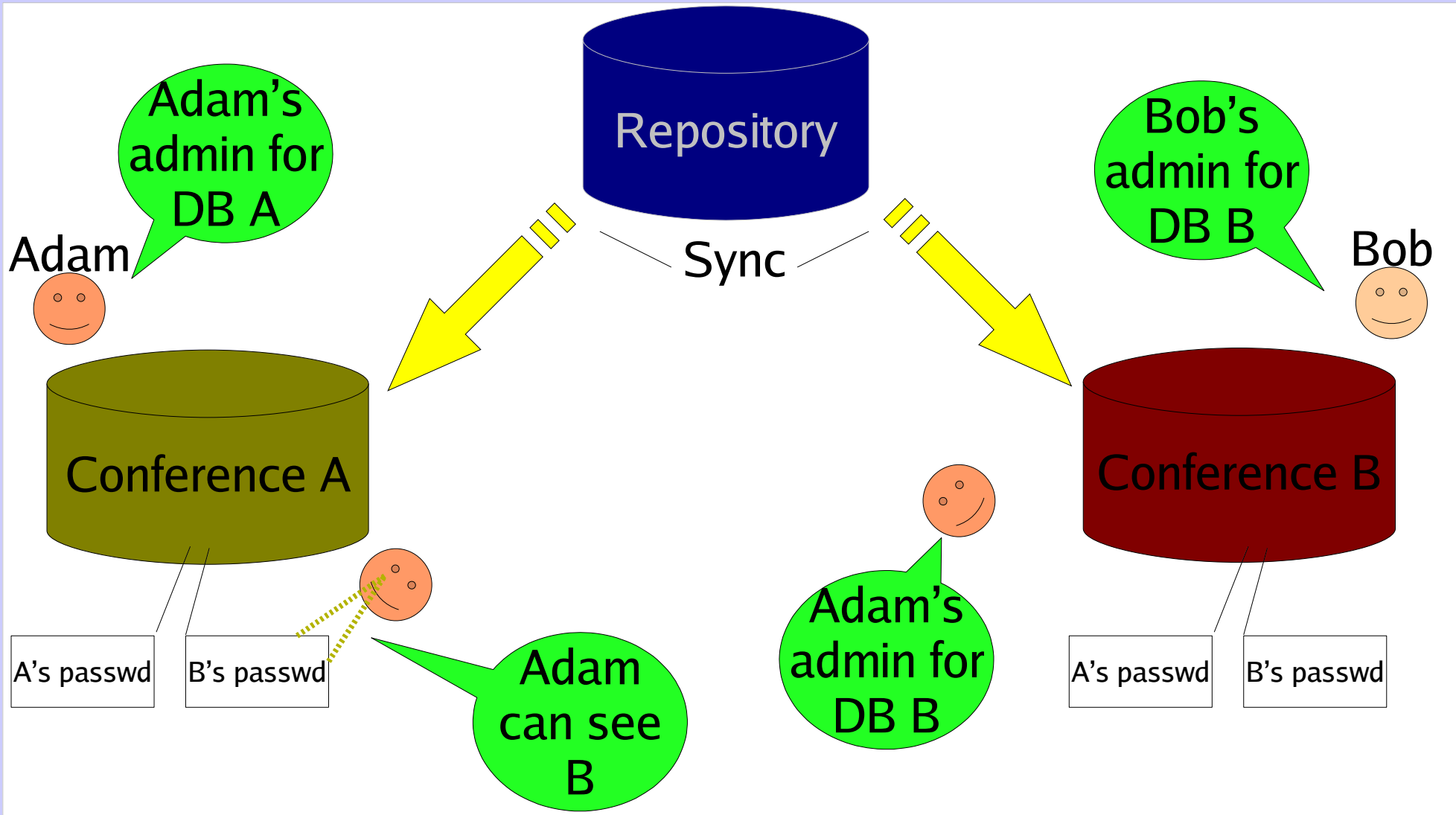
Passwords vulnerability: Simple Example



Passwords vulnerability: Simple Example



Passwords vulnerability: Simple Example



Part II: Data Protection Laws

Personal Data Protection code i.e.: Privacy! *(in EU)*

- Directive **95/46/EC** of the European Parliament and of the Council of 24 Oct. '95
  - Requested "Privacy laws" by 3 years from EU members
  - Regulates Personal Data treatment among EU states and among EU/non EU countries
  - **Personal** Data - easy
    - name, address, affiliation, phone number, bank account number, credit card, etc.
  - **Sensitive** Data – harder
    - racial or ethnic origin, religious, philosophical, political opinions, membership of parties, trade unions, as well as personal data disclosing health and sex life;

Only Personal Data, hence. How easy to handle?

- Personal Data Protection codes define
  - Rights of the owner of the data (data subject)
  - Duties for the data processor/controller
  - General terms in which data is handled
  - Regulations between countries

Data subject rights

- To know which data is possessed
- To be informed
  - of the source of the personal data
  - of the purposes and methods of the processing
  - of the logic applied to the processing, if the latter is carried out with the help of electronic means
  - of the identification data concerning data controller and data processors
  - to whom or which the personal data may be communicated

Data subject rights (2)

- To obtain updating/rectification
- To obtain deletion/blocking

- To get a detailed information about the data treatment
- To decline giving the data

- To be assured that the data is managed securely

In brief, what have we to do?

- Write a comprehensive information to give all the authors/delegates/sponsors
- Gather the consensus from them
  - MUST be of type "**OPT-IN**"
  - Must include statements that explicits who will use the data
    - JACoW conferences (general), sponsors, every already registered person and "future registered" persons
- Define & publicize who the data processors are
  - JACoW "heads"
  - Editors/Administrators for every conference
  - Include an appendix in the JACoW terms of membership

Example

fel2004 User Profiles pippo pippopo Logout

AUGUST 29 - SEPTEMBER 3 fel 2004 Trieste, Italy

Privacy statement

According to Italian law, to use this system you need to read the following notice and authorize us to register and process some data of yours.

elettra **Sincrotrone Trieste** **PRIVACY NOTICE**
Società Consortile per Azioni

1. With reference to your attendance to the XXVI International Free-Electron Laser Conference and/or the XI FEL User-Workshop from the 29th of August to the 3rd of September, and according to art. 13 of Legislative Decree 196/03, we inform you that:

   a. personal data regarding you, the members of your family and/or your collaborators directly acquired by you or by third parties, will be necessaries for:
      i. Conference and/or Workshop registration;
      ii. Managing of the scientific notes and distribution of the Conference

Do you authorize Sincrotrone Trieste S.C.p.A. to treat your data according to the statement above?
By saying "NO" your account will be immediately deleted from this system.

○ Yes ◉ No Submit

What about credit cards?

- Personal Data “only” (not sensitive)
- No more important than name, address...

well...

- not in owner’s point of view
- neither in who’s responsible for the payments

so...

- take much care!

Conclusions

- System Security
  - Keep up-to-date and well informed
  - Plan the whole thing looking for hidden vulnerabilities
  - Make passwords non-readable

- “Privacy laws”
  - It can be done
  - Write down “perfect” information for the data subject and conferences committees
    - Help from a legal department is recommended
  - OPT-IN consensus

“Make it idiot proof, and someone will make a better idiot.

http://www.thinkgeek.com