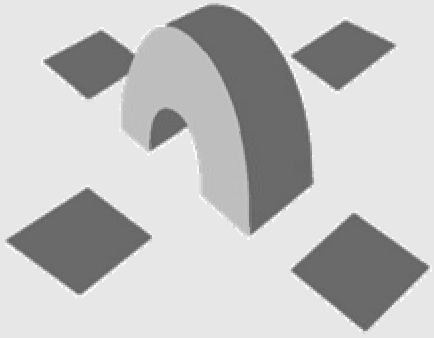
# 3rd TF-CSIRT Meeting

**Ljubljana, Slovenia. 31st May 2001**



Red IRIS

## IRIS-CERT

The Computer Emergency Response Team of the Spanish Research and Academic Network

**IRIS-CERT**
cert@rediris.es
**Chelo Malagón**
chelo.malagon@rediris.es

# Overview

- RedIRIS
- What is IRIS-CERT?
- Services provided
- Liaison with the Constituency
- Incident handling at IRIS-CERT
- Incident statistics

# RedIRIS

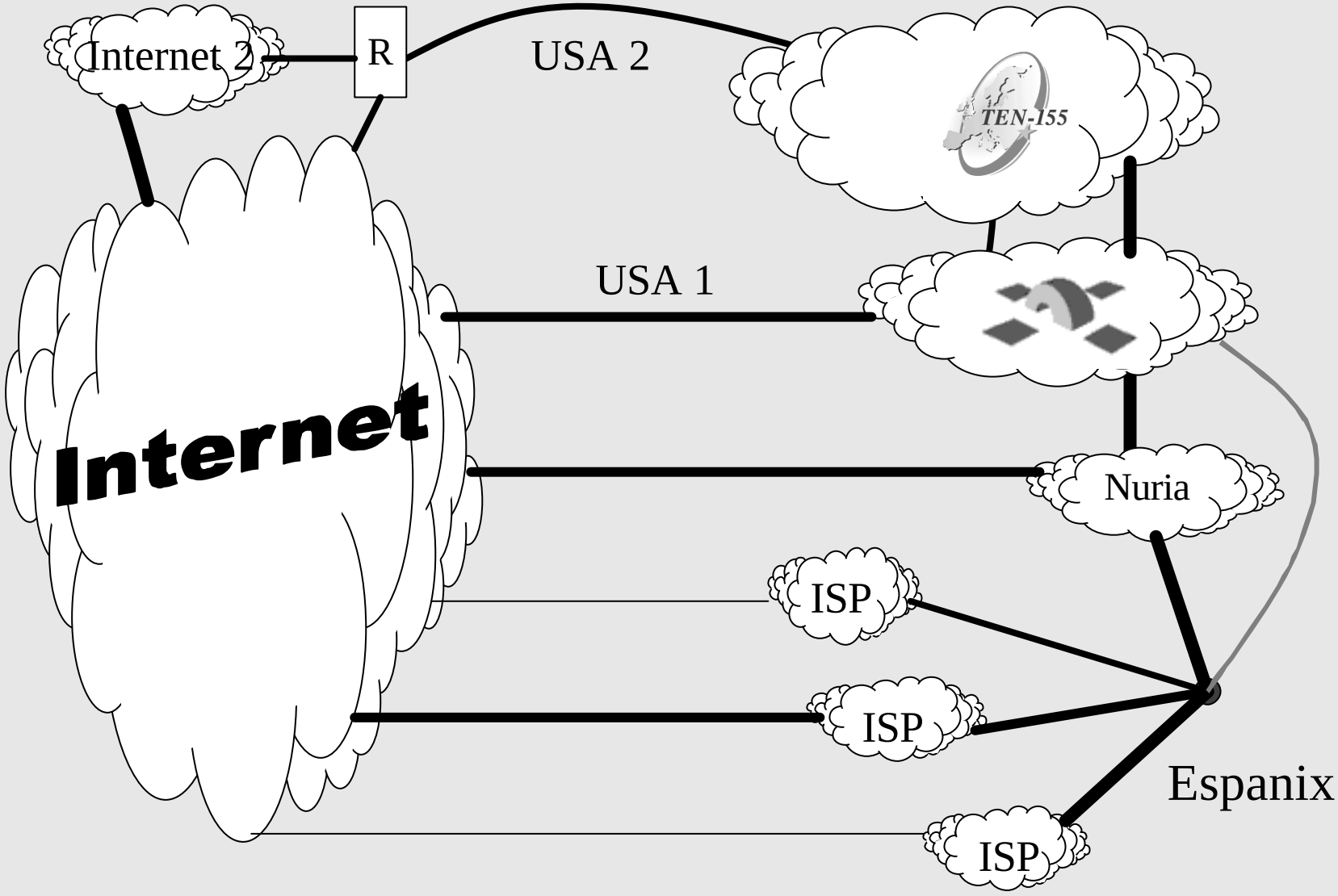
## The Spanish Research and Academic Network

- Established in 1991
- Funded by the Spanish National R&D&I Plan
- Managed by the Scientific Research Council (dependent on the Science and Technology Ministery)
- Provides network infrastructure and application services to the Spanish Research and Academic Community
- ≅ 260 institutions already connected (universities, R&D Centers, Hospitals and other public institutions)

# RedIRIS National Backbone

- 17 nodes, one in each Autonomous Region
- Star topology
- Bandwidth between 5 and 155 Mbps

# International Links



# IRIS-CERT (I)

- The CSIRT of RedIRIS
  - Established in November 1995
  - Currently 3 FTE + 1 Technical Coordinator
- Constituency

  http://www.rediris.es/cert/servicios/iris-cert/const.en.html
  - Full Service ↑ all institutions connected by RedIRIS (AS766)
  - Limited Service (IR Coordination) ↑ *.es domain
- Formal description (RFC 2350)

  http://www.rediris.es/cert/servicios/iris-cert/rfc-2350-v1.0.en.html

# IRIS-CERT (II)

- Took part in the EuroCERT/SIRCE Project
- FIRST member since 1997
- TI “level 2” Team since March 2001

- Business hours
  - Mon-Fri 09:00 - 18:00 GMT+0100/0200 DST

# Services provided

- Reactive Services
  - Critter analysis
  - Forensic analysis (without legal value)
  - IR Support
  - IR Coordination ↑ *.es domain
- Proactive Services
  - Security audit on demand
  - Maintenance of security tools and documentation
  - Maintenance of coordination security mailing list
  - Links to Security related sites, mailing lists and newsgroups
- Quality Management Services
  - Training (2 Security Coordination Groups per year)
  - Awareness building

# Other Services and Working Groups

- RedIRIS Policy Certificate Authority (IRIS-PCA)
  http://www.rediris.es/cert/proyectos/iris-pca/index.en.html
- GTI-AUP WG
  - To help institutions develop their own Security Policies
- GTI-SDIR WG
  - Forum on the use of NIDS in RedIRIS and for the development of a NIDS distributed network in the community
- Open Services
  - PGP Public Keyserver
    http://www.rediris.es/cert/servicios/keyserver/index.en.html
  - RedIRIS TimeStamp Server
    http://www.rediris.es/cert/cuco
- Forum for security incident coordination between Spanish ISPs (ISPES)
- IRIS-CERT can also acts as liaison point with the Spanish Law Enforcement Agencies although our role in any legal process would be limited to technical assessment

# Liaison with the Constituency

- Mandatory site security contact per institution connected by RedIRIS (full service)
  - Given by PER (Contact Point to RedIRIS) when joining
  - Subscribers of RedIRIS Security Coordination mailing list
    - IRIS-CERT@listserv.rediris.es
- Non mandatory site security contact for those institutions with limited service

# Incident Handling at IRIS-CERT

## Incidents Opening

- Contacting methods → e-mail/fax/phone
- Incident reporting forms available on WWW
  - External Interface → http://www.rediris.es/cert/
- At least one member on duty (2 weeks shifts)

- Incident handling according to a priority scheme → Emergency/High/Medium/Low
- Incident classification according priority/category
- E-mail sent to all parties involved
  - Within the same working day
  - Always PGP signed using the PGP Team Key

# Incident Handling at IRIS-CERT

## Incidents Closure

- Originated within RedIRIS
  - Must be solved in a certain period of time (depending on category)
  - If not ↑
    - IRIS-CERT asks the security contact point to filter the node or
    - RedIRIS NOC filters the node until the problem is solved
- Originated outside RedIRIS
  - Automatically closed if not response in a predefined period of time (depending on category)

- Incident follow-up sent every two weeks
- Report of actions taken sent to all parties involved

# Incident Handling at IRIS-CERT

## Internal Interface

- Incident Tracking and Registration Tool
  - exmh + tcl/tk scripts + perl scripts
- Repository of Incidents
  - Stored in well-protected filesystems in IRIS-CERT staff boxes
    - Access restricted to IRIS-CERT members
    - Properly monitored
- Investigation Tools
  - home-made scripts (perl)
- For statistics
  - Records in plain text file with special format (not containing sensitive information)
    - reference number, date, source, target, category, priority, comment, international/national CERT contacted
- LDAP ↑ Security Contact Points

**INTERNAL INTERFACE MUST BE IMPROVED!!!!!**

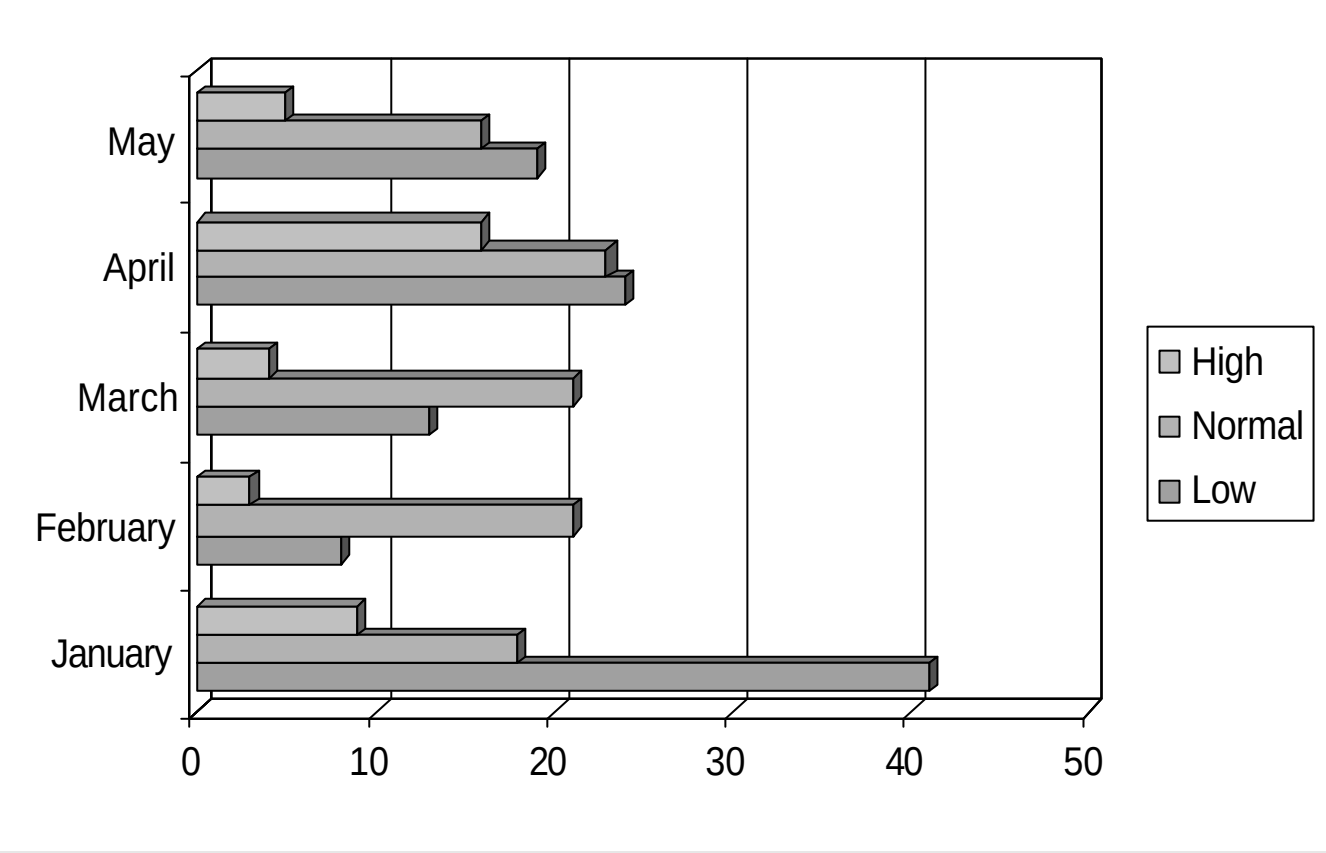
# Statistics

## January - May 2001

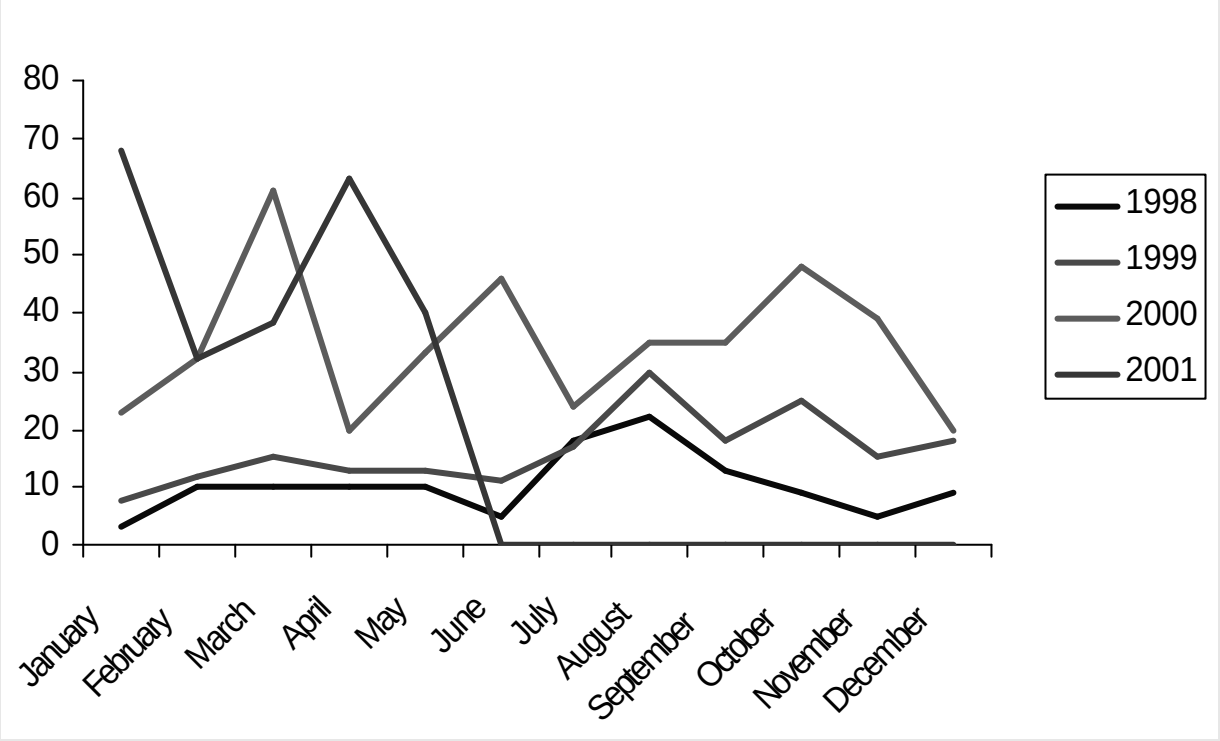
- Total number of incidents ↑ 241
- Incidents involving RedIRIS nodes ↑ 218 (90.45%)
  - 23 incidents involving Spanish nodes outside RedIRIS
- By priority
  - Low: 105 (44%)
  - Normal: 99 (41%)
  - High: 37 (15%)
  - Emergency: 0 (0%)
- Increase of incidentes in relation to the same period in the previous year ↑ 72 (142.60%)
- SPAM ↑ 33

# Incidents by priority

## January - May 2001



# Incidents handled by IRIS-CERT
## 1998-2001



# Main problems

- Great differences in effectiveness between Security Contact Points in institutions connected by RedIRIS
- ISPs lack of response and coordination

- Many systems without management and/or not duly updated

- Improvement of the internal interface
- Imperious need of new staff members to improve the service offered to our community and to afford the incident increase

# Questions?