A CSIRT perspective

Andrew Cormack (UKERNA)/
Gorazd Božic (ARNES)
TF-CSIRT

http://www.terena.nl/tech/task-forces/tf-csirt
Acronyms

- CSIRT – Computer Security Incident Response Team
- CERT – Computer Emergency Response Team
- IRT – Incident Response Team

All do similar things
Origins

1980s

• CSIRTs working independently
  – Mostly in universities
• Fix broken networks and computers
  – Technically skilled staff
  – Technically skilled users
Internationalisation

1987

“there’s a bug in fingerd”

- Wide-scale attacks on networks
  - CSIRTs co-operate to fix them
- International attacks on networks
  - CSIRTs co-operate across borders
Legalisation

1990s

• New users: government, business, home
• New approaches:
  “it’s not illegal – I can’t fix it”
  “identify your user”
  “stop or I sue”
• People who don’t speak TCP/IP!
Steep learning curve

- ~80% of incidents cross-network
- ~40% of incidents cross-border
- All may have legal implications
- All staff need to know the basics
- A few teams can afford “experts”
Future

- Handbook covers 15 MS in 2003
- What about 25 MS in 2004?
- Handbook is a great start, but
  - Must be maintained
  - Should be expanded
- Needs skills and co-ordination
  - CSIRTs still need help