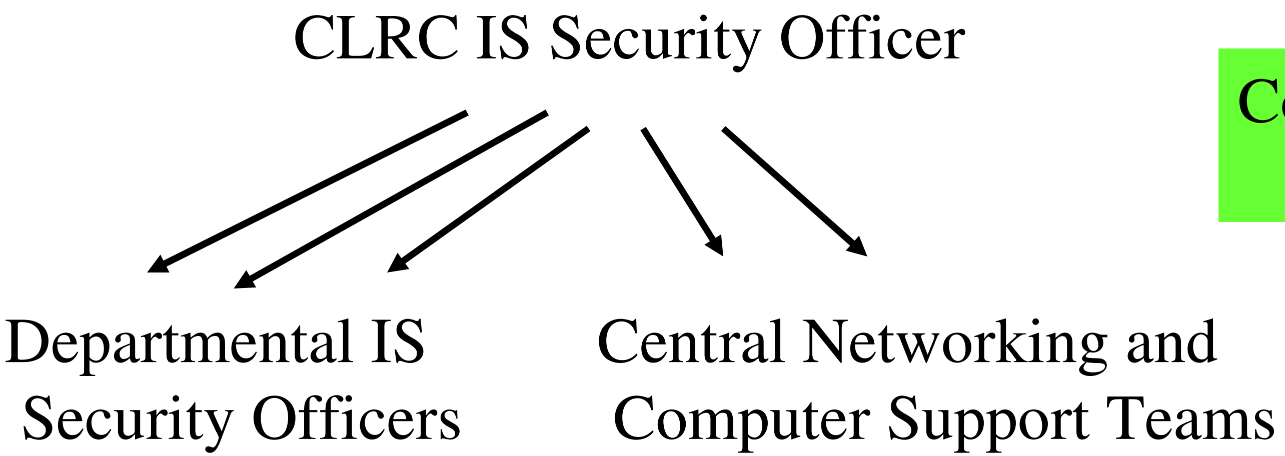
The Approach to Security in CLRC

Gareth Smith

With acknowledgements to all the members of

the CLRC Computer Network and Security Group, especially Trevor Daniels and Chris Seelig.

Organisational Structure



CLRC IS Security Officer

Departmental IS Security Officers

Central Networking and Computer Support Teams

Computer & Network Security Group.

History

- CNSG created in 1998 – result of audit recommendations.
  - Before security matters handled in separate interest groups (e.g Windows NT).
  - Manual checking of logs for scans and application of network blocks in router.
  - Creation of e-mail list for security matters.

1999 – Firewall Set-up

- Early:
  - Drafting security policy.
  - Some protocols filtered.
- Mid:
  - Move server systems into given range of IP addresses and block incoming TCP connections to all others. Implemented in routers
  - Tighten (and check) NT passwords.
- End:
  - Start to put protocol filtering in for ‘servers’.
  - Draft ‘incident recovery procedures’

2000

- As result of audit:
  - Define systems of ‘High Business Impact”
  - Modem registry
- Lovebug Virus – Approx 100 systems infected.
  - Filters put in Exchange and use of Outlook Security Patch.

2001

- Concerns over security of home PCs with ‘always on’ connections.
  - Guidelines requiring anti-virus and personal firewall on laptops & systems dialling in.
- Start internal audits of departments.
- Define rules for use of wireless LANs
- Concerns over IIS security – aim to reduce numbers of web servers.
- Use e-mail blacklist to filter spam mail.
- Nimda worm/virus. About 6 systems infected.
  - Force use of web cache.

2001 – Firewall Upgrade

- Upgrades to networking (within and off-site)
- Gnatbox
  - http://www.gnatbox.com/
  - PC based system.
- Some 300 – 400 rules.

2002

- Bad start to year with rise in number of incidents.
- Roll out of latest Internet Explorer Security Patch within a week.
- *Who knows what is next ……*

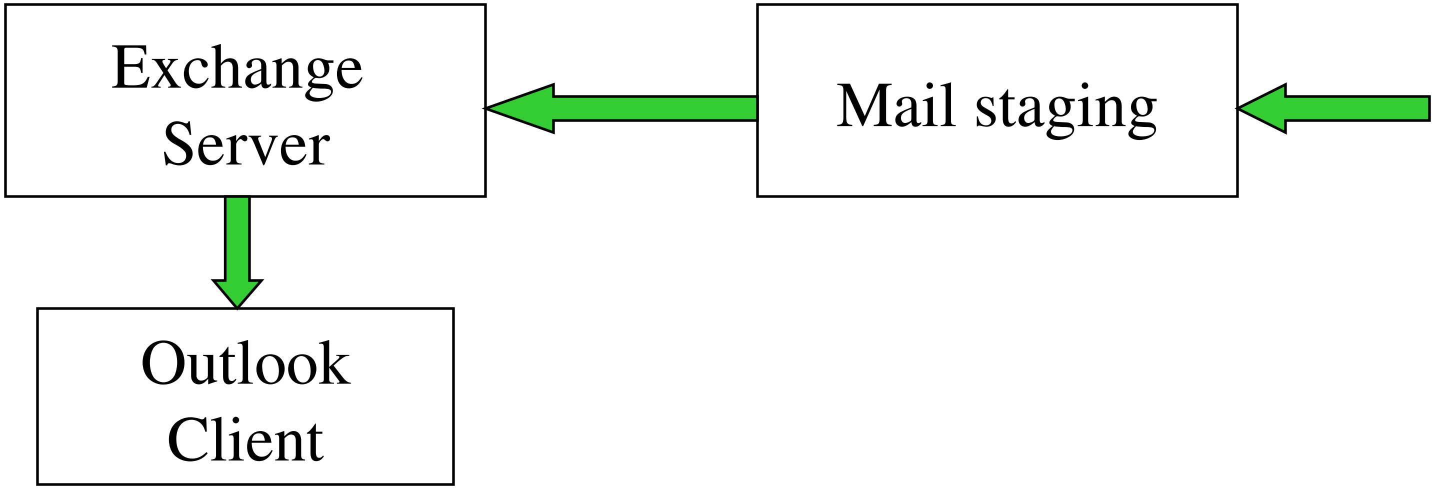
Nimda Virus / Worm

- 4 methods of infection:
  - E-mail
  - Web browsing
  - Network shares
  - ‘Code Red’ worm.

E-mail protection

Anti Virus Scan (2)
Some attachments removed.

Anti Virus Scan (1)



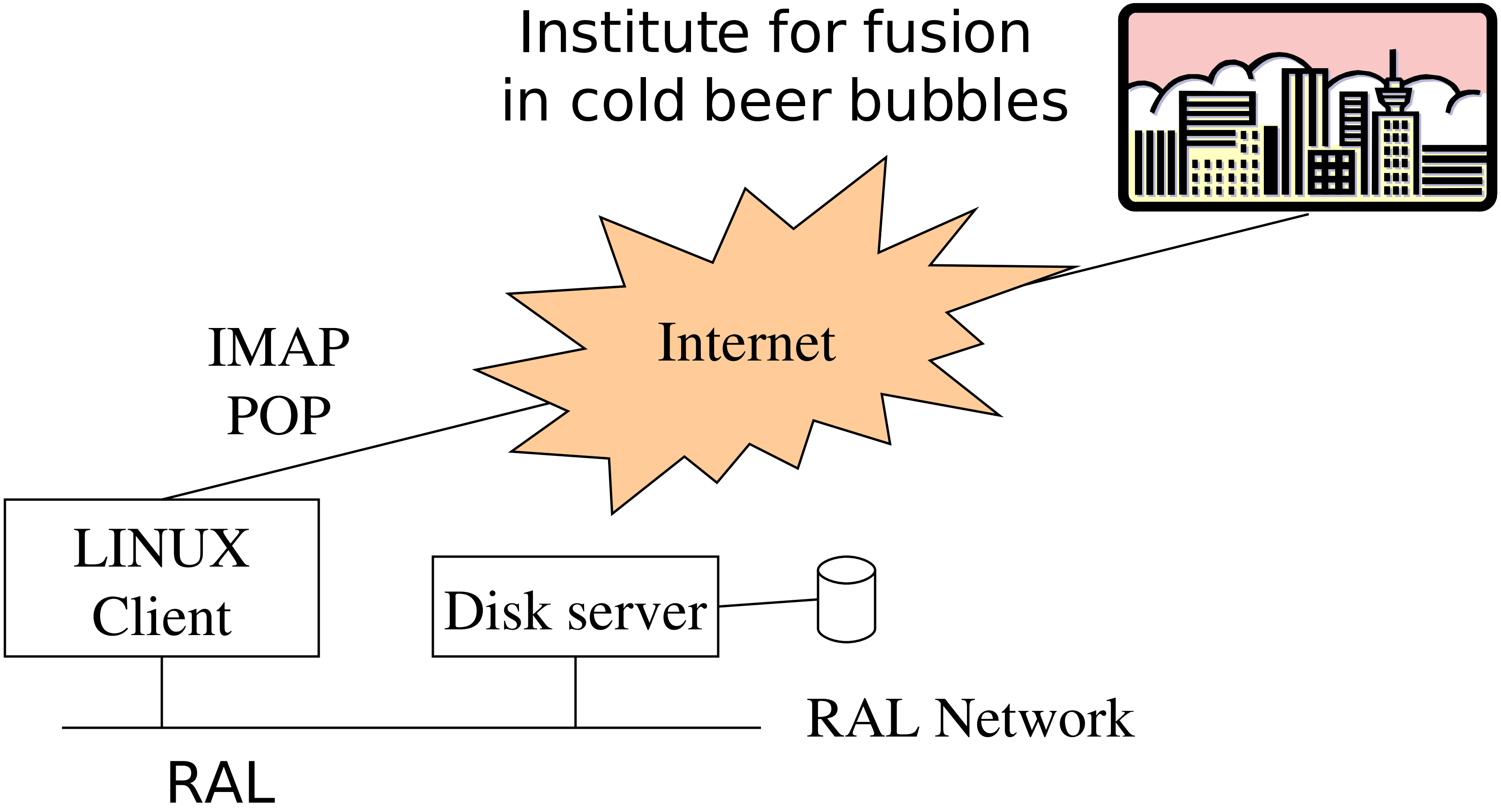
Exchange Server

Mail staging

Outlook Client

Anti-Virus Scan (3)
Some attachments removed.

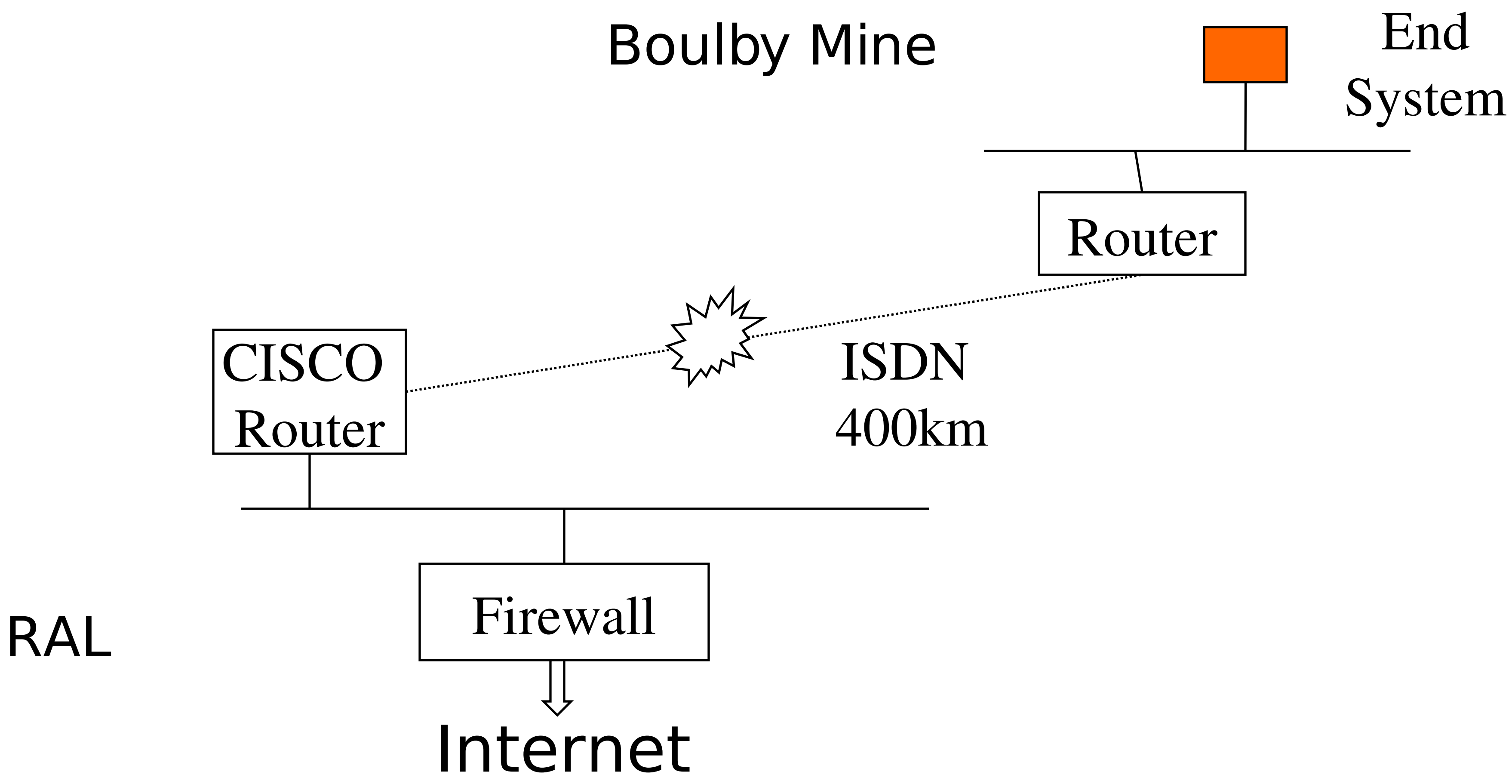
Lack of e-mail protection


Institute for fusion in cold beer bubbles

How have we been hacked (1)

- Anonymous ftp left open on web server.
  - Found by anti-virus software.
  - System being used as a repository.
  - Analysis of logs was confusing
  - Server had to be completely re-installed.

How have we been hacked (2)



Concerns / Aims

- Concerns
  - Rapidly spreading virus/worm.
    - Need to subdivide network to contain any infection.
  - Risks of web browsing
    - Need to keep patching.
- Aims
  - More than one line of defence in all cases.