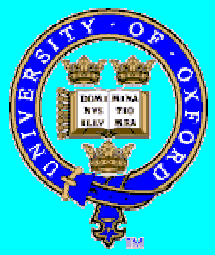
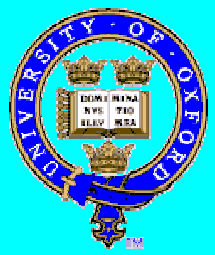


# Securing your Assets?

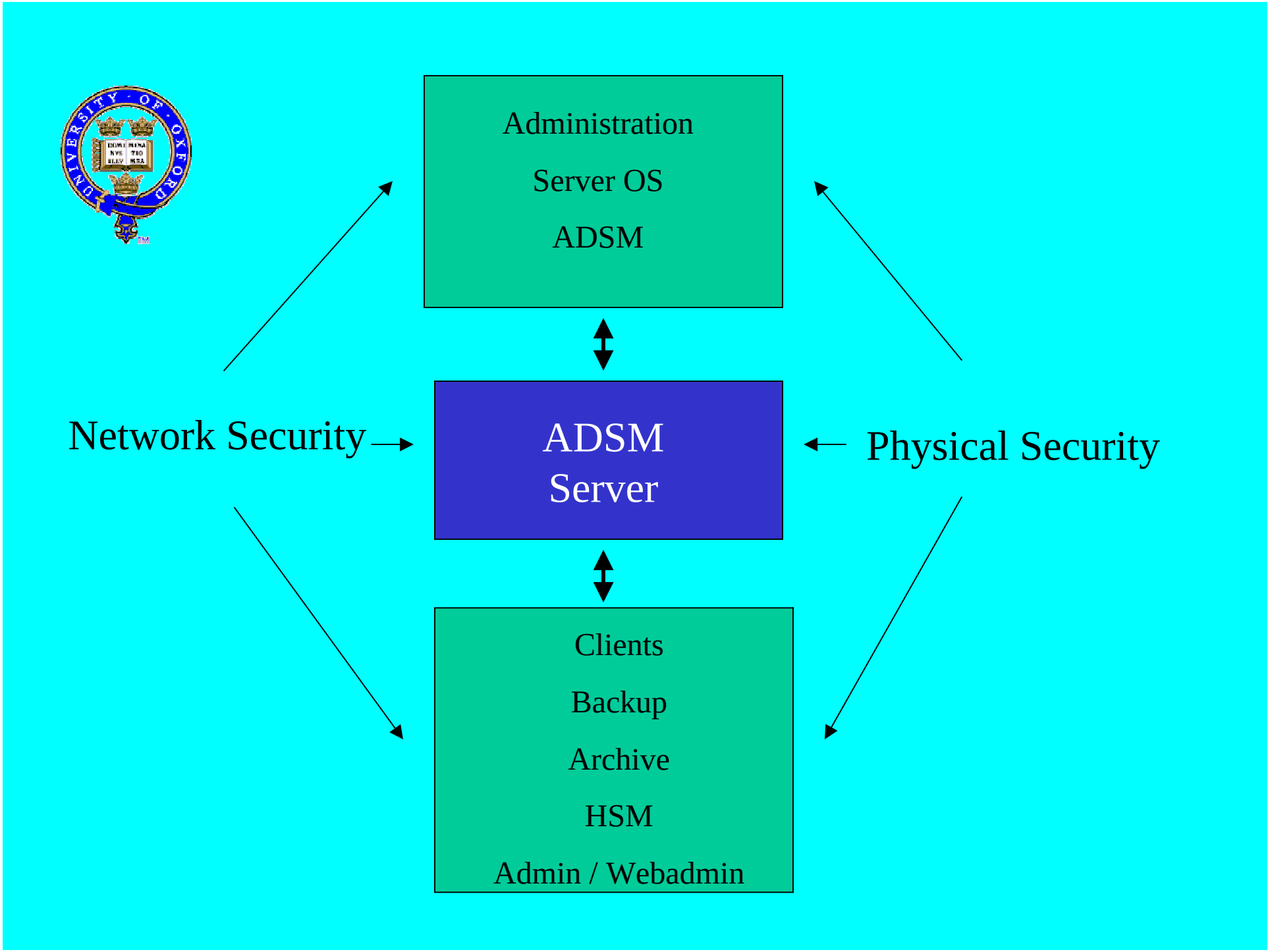
Neil J Long

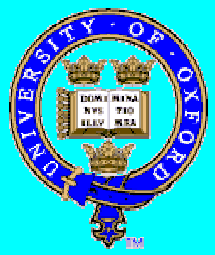
Oxford University Computing Services




# Introduction

- Security is a very big subject
- A lot of eggs in one BIG basket
- Try to break it down in to different contexts
- Review individual aspects
- How they inter-relate
- Identify critical weaknesses
- Be lucky!!

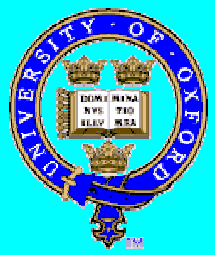

Administration
Server OS
ADSM
Network Security
ADSM
Server
Physical Security
Clients
Backup
Archive
HSM
Admin / Webadmin



# The clients

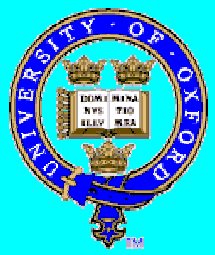
- Authenticate to server
- Trust server to safeguard the data
- May have no other copies of data
- Trust commands **from** server

- Server requires authentication
- Trusts “name”
- Trusts authentication
- Server controls policy
- Buffer Overflows



# The Server

- Trusts the Admins
- Admins trust their workstations?
- Trusts the OS
- Trusts the network?
- Physical access
- Network access
- OS patches
- Availability



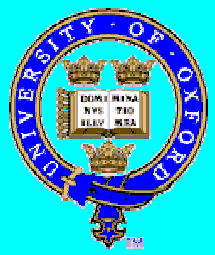

# Threats

- Accidental
- Bugs
- Tape drive micro-code
- Mechanical failure
- Tape labelling

- Deliberate
- Insider
- External
- Tape labelling
- Social engineering

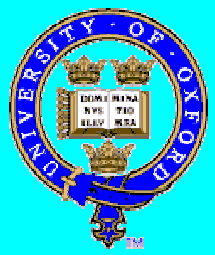
Denial of Service

Break-in - modification or access



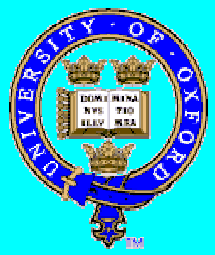

# Remote Hacker

- Network access - firewall
- Gain access by bouncing off ‘local’ net
- Denial of service attacks
- Non-privileged access
- Administrator access
- ‘Legitimate user’ access



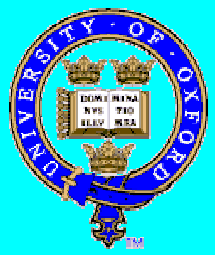

# Hacker methodology

- Reconnaissance
- Probes & tests
- Attack
- Securing access
- Making (ab)use of the system



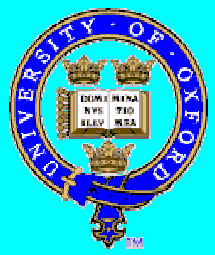

# Countering Attacks

- Firewalls - control access
- Review OS, patches, services
- Bugtraq vs. Vendor Advisories
- Intrusion Detection Systems
- Plan and test recovery from compromise



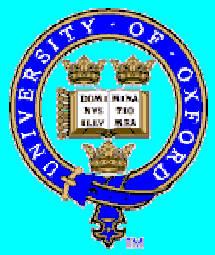

# Current Exploits

- RPC services - statd, cmsd, ToolTalk, automountd, CDE
- Anon-Ftpd servers - wu-ftpd, Bero-ftpd, Pro-ftpd




# Old Vulnerabilities

- IMAPd
- POPd
- NFSd/mountd (Linux)
- statd
- BIND
- May be old but someone probably still hasn’t applied the patches!

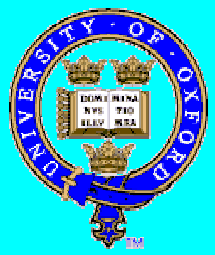



# Resources

- Mailing lists
- Advisories - CERT, CIAC, AUSCERT
- Consultants
- Other OS problems

# Summary

- Huge subject area - too many issues to handle all of them
- Identify key problems and prioritise
- Information - advance warning
- Seek help




# Conclusions

- Very complex interaction
- Need for risk evaluation
- Minimise risks from external sources
- Keep (or be kept) up to date with security issues