Towards Less Insecure Administrative Networks

John Sellens

Data Processing

Information Systems and Technology

University of Waterloo

jmsellens@uwaterloo.ca

OUCC 26

May 28, 1996

“Official” Abstract

With the imminent deployment of a major UNIX-based database server, and the replacement of our legacy financial systems, we are implementing a number of security and reliability measures. These include a high-availability database server, a major offsite backup system and offsite mirroring of data, a firewall system, SecurID one-time-password tokens for sensitive areas, tightly controlled access to our primary servers, and a review of our use of campus software support. This presentation will outline what we’re doing and have done, why, and the good and bad things that we have discovered.

Where Did We Start?

- Most “critical” administrative applications on VM/CMS
- Separate administrative subnets, but no firewall or traffic controls
- Little or no control over password selection and use
- Admin UNIX servers treated the same as other campus UNIX servers
- Inconsistent backup schedules for taking tapes offsite – some data never left the machine room
- Reliance on “good luck” rather than rigorous controls

Motivation for Change

- Primary motivation for addressing security was the looming implementation of new financial systems using Oracle on UNIX servers
- A recognition that some of our practices were pretty hard to justify in the current environment of the ’net
- A desire to bring the primary responsibility for the admin servers into the Data Processing department, rather than the central campus support group
  - Subject to current looming reorganization

Presentation Overview

- The bulk of this presentation is a “grab bag” of topics
- Most of the topics are “peripheral” to the real goal of information access, recording and manipulation
- Metaphor: The different topics are all herding our bits and bytes into line from different directions?

Offsite Disks and Backups

- New database server is a Sun PDB 1000 system – a high-availabilty, two node cluster
- One very attractive feature is the fibre optic connections to the disk arrays
  - This will allow us to place a mirrored copy of all disk data offsite immediately, with no performance penalty
- A new backup server was purchased to be inside the admin firewall and also to get offsite backups, rather than continue to use the central server
  - Tapes will be “cloned” by the backup server for reliability

Access Control and Physical Security

- Most machines are in the "red room" – the main campus machine room
  - Environment and access is controlled
- Offsite disks and backup server will be located in a new mini machine room in a separate building
  - Alarm system, limited key access
  - UPS with environmental monitoring for temperature and humidity
  - An "extension" of the red room

One Time Passwords

- We're going to be using SecurID tokens on "important" servers
- Avoids problem of passwords written down in obvious places
- Avoids problem of shared or snooped passwords
- End of day collection of tokens could be used to limit access over the network
- Why SecurID?
  - Works with our existing systems/equipment
  - Least intrusive option

User Control on Production Systems

- Or, more accurately, “control of users”
- Restricted menu as login shell – no shell, mail, news . . .
- Very fussy password command to avoid bad passwords
- .rhosts files controlled with “gatekeeper” software
- No shared passwords, thanks to SecurID
- Plans for a simple password control system for change enforcement for non-SecurID systems/users

Limiting Access to Network Services

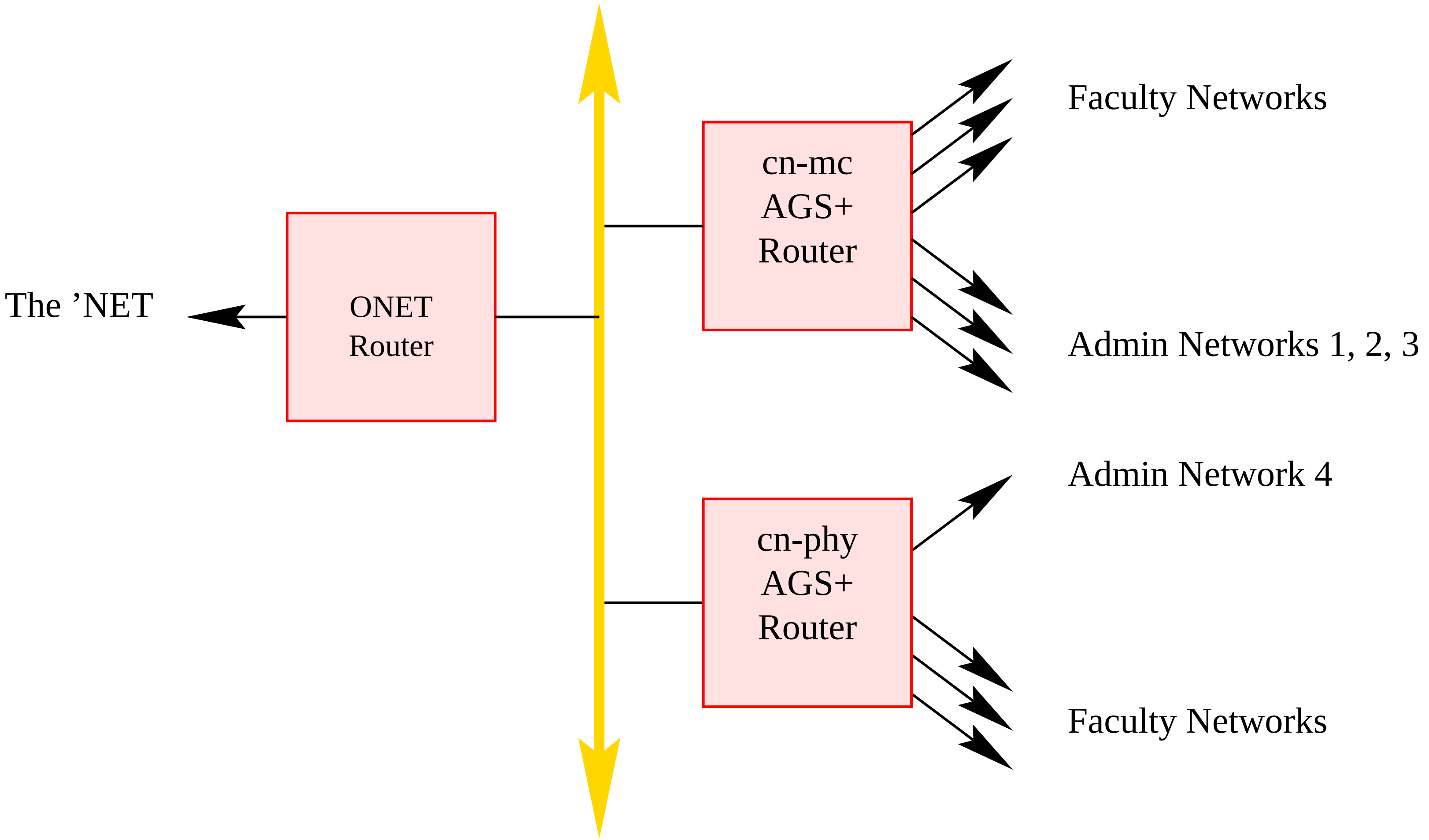
- Limiting the services available on servers (hopefully) reduces the opportunities for attack and/or uncontrolled access
- One web server on the administrative networks
  - Reduces likelihood of inadvertant publishing of secret data
- Certain services are disabled on admin servers
  - e.g. finger, ftp
- Avoid the use of NFS, NIS, RPC, etc.
- Limit/control .rhosts file use as appropriate

Network Layout, Reconfiguration, and Planning

- We are moving towards a firewall, and a switched admin networks “backbone”
- Creating a firewall after the fact is harder
- Isolate admin networks from the other networks
- Lots of special case traffic, since we need to allow access to internal machines from external users (e.g. in the faculties)

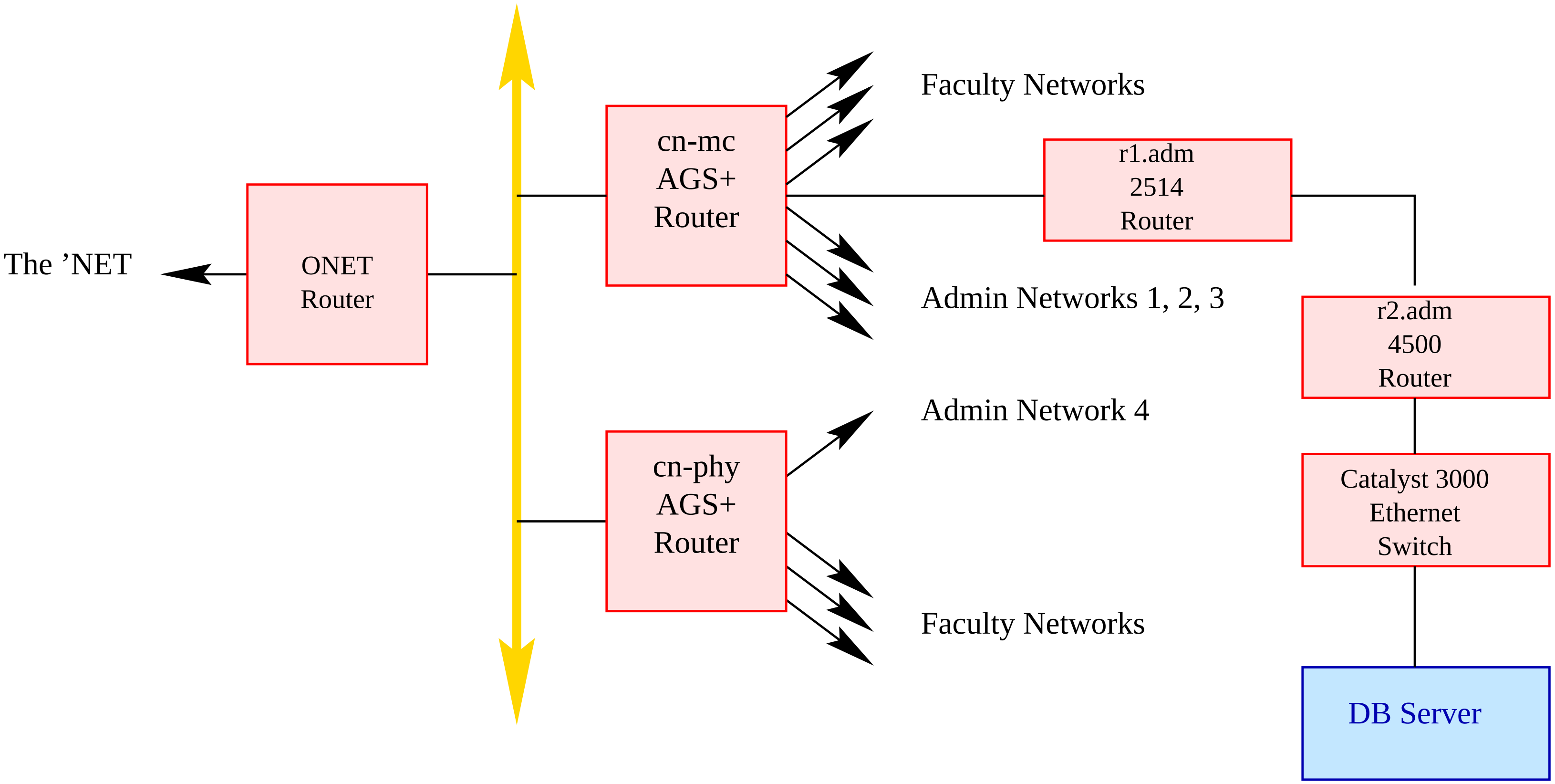
Original Network Layout

- Separate subnets on the campus network



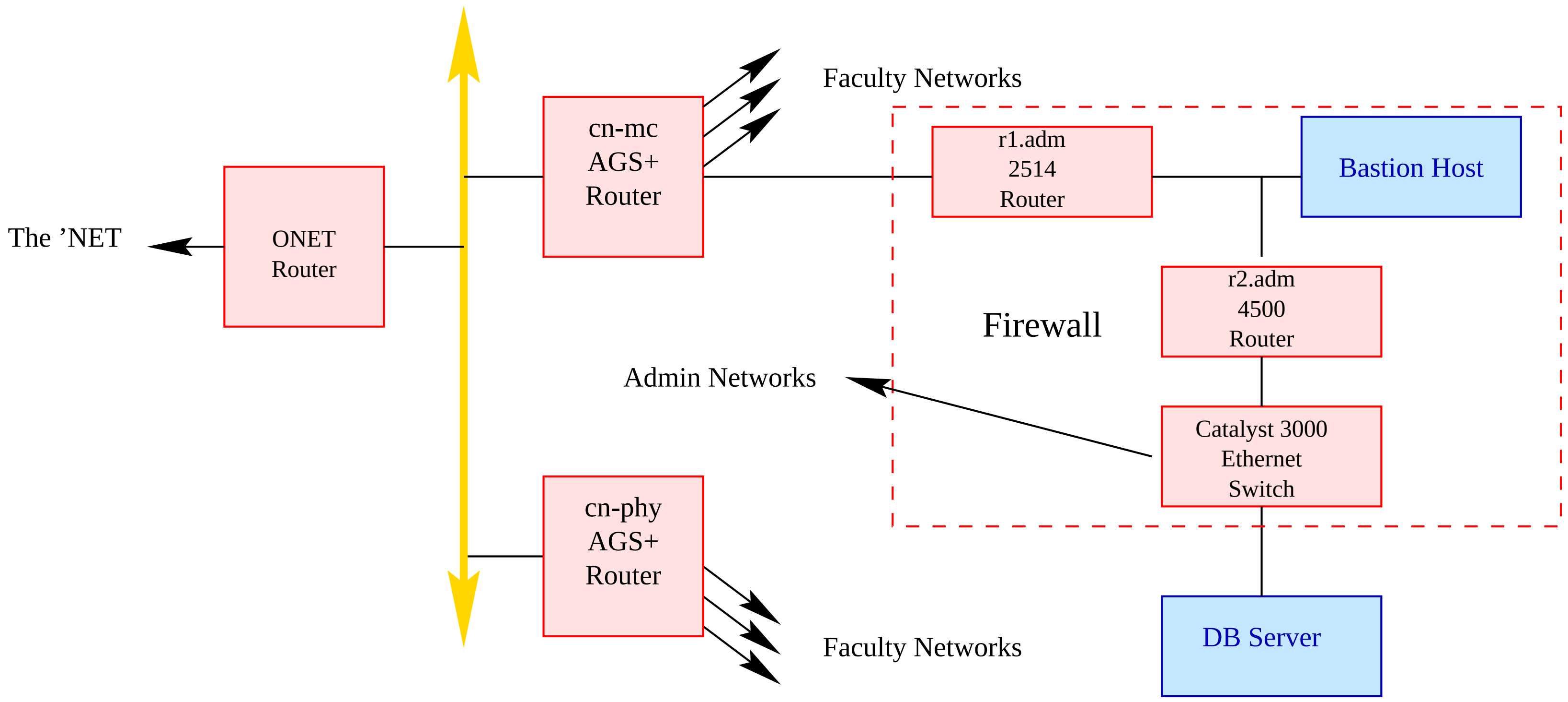
Transitional Network Layout

- Routers provide some access control



Final Network Layout

- All admin systems behind a reasonable firewall



Trusting Central Support

- Centralized UNIX software support raises the question: How can we justify trusting everyone doing central support?
- How can we control/limit the “web of trust”?
- We may be able to reduce the risks by switching to a “pull” rather than “push” model of software distribution
- Can never be 100% controlled or risk-free

What Problems Are We Ignoring/Accepting?

- Admin network snooping, outside network snooping
- Steam tunnel/conduit/wiring closet attacks
- Insecure systems on desktops
- Desktop systems not backed up
- Packet modification, session hijacking, denial of service attacks via the network
- Internal attacks from DP superusers, DBA's, and programmers

Where Are We Failing?

- Time – everything takes too long to do
- We're way behind schedule on some things
- We should have done some things differently right from the start
  - e.g. Start with a restricted 'net connection, not wide open
  - e.g. Don't mix machine uses – general purpose access vs. "production" applications
- Communication – we have not always been very good at communicating why (and how) network security is important

Where Are We Succeeding?

- Systems are running – no (detected) intrusions or significant failures (yet)
  - Famous last words
- The parts that we have implemented have gone in fairly smoothly, with little or no user disruption
  - But some of the more “disruptive” things are yet to come
- We seem to be going in the right direction

Summary and Availability

- Seem to be doing some of the “right things”
- Took (and is taking) much more time than we had hoped
- Much of the local software is freely available
  - gatekeeper, setpw, usermenu, etc.
  - Some Waterloo-isms in the code
- Copies of this presentation are available at

  http://www.adm.uwaterloo.ca/˜jmsellen/Papers/towards

  or contact jmsellens@uwaterloo.ca
- No Microsoft or Netscape software was used to create this presentation