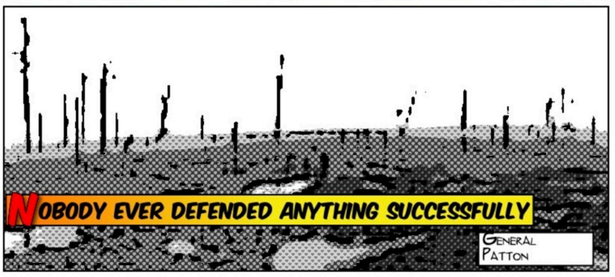


Network Based Security

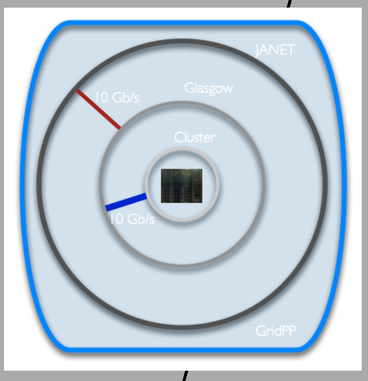
- Balance between security, speed and reliability difficult to implement out of the box

Infrastructure overlooked?

- Network infrastructure attacks less common than host based
- However, more disruptive
- Potential to cause major issues
- Network security doesn't stop at a NIC

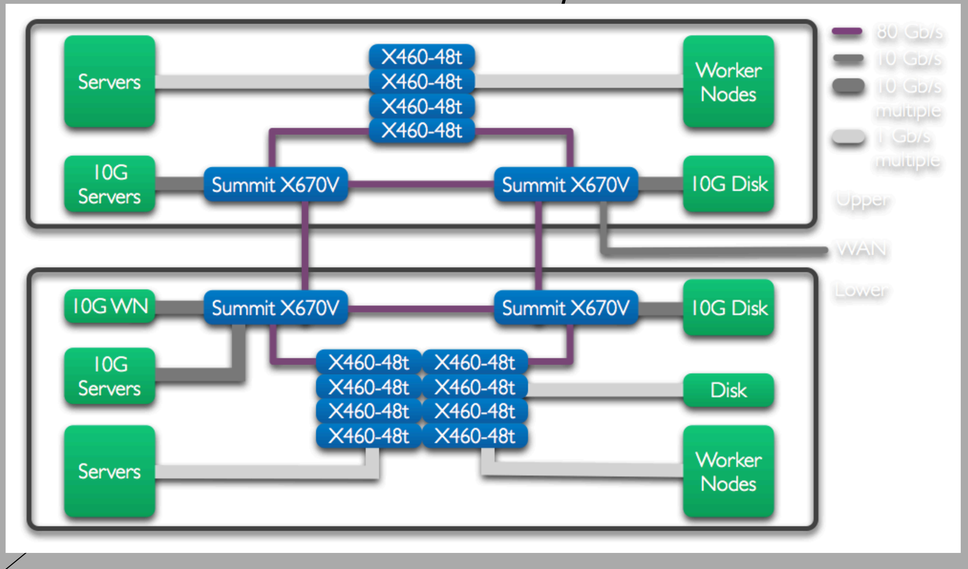
Multiple vectors

- External (Internet)
- Internal (MAN/LAN and trusted sources)
- Hardware flaws
- Software flaws
- Popularity *vs* obscurity



Scotgrid Solution

- Various Mechanisms external to the Cluster
- ACLs across multiple network devices
- Use of event triggered security using Clear Flow (experimental)
- All hosts run ossec
- Different ACLS based upon services



GridPP
UK Computing for Particle Physics

UNIVERSITY of GLASGOW