Durham Shared Fail2Ban

“An experiment that could lock us out of everything!”

Presented by Paul Clark

2nd May 2018

Durham University

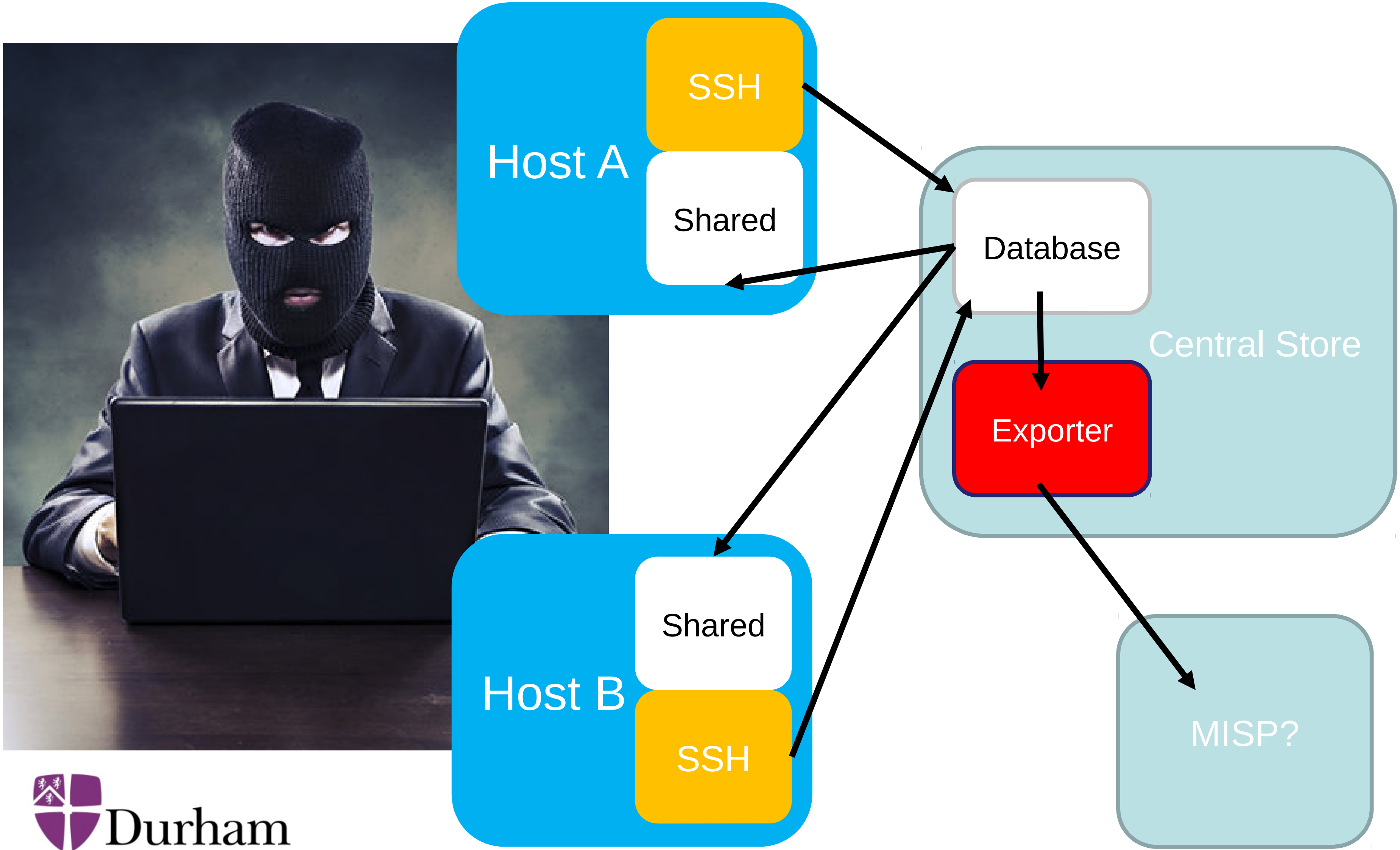
IP3

ScotGrid
Scottish Grid Service

GridPP
UK Computing for Particle Physics

View of Durham Cathedral from Owengate

Jail Flow


Host A
SSH
Shared
Database
Central Store
Exporter
Host B
Shared
SSH
MISP?

More Time for the Crime

- SSH Jail
  - 5 or 6 attempts
  - 15 minute ban time
  - Instant* share and ban site-wide

- Long Term
  - 8? SSH Bans over the site
  - 5 day ban

- Can analyse for more strict bans
- Integrate with HoneyPots?

Durham
University

Shared Threats

- Stored in database
- Can share to local IT
- Can share into MISP

- Etc etc

Durham University

Demo Time

Durham Shared Fail2Ban

“An experiment that could lock us out of everything!”

Presented by Paul Clark

2nd May 2018

Durham University

IP3

ScotGrid
Scottish Grid Service

GridPP
UK Computing for Particle Physics