

GRID Security



SWITCH

Serving Swiss Universities

Dr. Serge Droz, SWITCH-CERT

Torsten Voss, DFN-CERT

Tallinn, 24. September 2009

Issues

Grid-Sec

A NREN-CERTs role in Grid-Security

Grid-Sec

A closed nsp-sec type list for grid incidents

<http://grid-sec.web.cern.ch>

Members:

- Two reps of each Grid
(EGEE, Tera-Grid, Nordu-Grid, ...)
- Two Reps from TF-CSIRT
(Currently Torsten Voss, DFN-CERT, Me)
- Other special interest Members

Activities

- So far two large grid incidents
- No Grid specific exploits
- Coordination between Continents seems working
- If necessary, Torsten or myself can provide links into NREN-CERT World
(Problematic: Only two named individuals)
- Collaboration with LEO seems good
- If affected by a one of the incidents, please get in touch with us
- Don't poke the dropservers

NREN-CERT ⇔ Grid-Security

The GRID is different

Addresses ↔ Identity

Classic

IP-Address

IP-Range

Blocking

OS-Forensics

Partner-CERT

Grid

User Identity

Grid-Initiative

Disable User

OS/Toolkit-Forensics

GRID-CERT

IP-Address ↔ User Identity

- Every Grid Job runs under a user ID. Once this ID is compromised all Grid-Nodes that allow access to this ID must be considered compromised.
- No Point in blocking IPs

Block IDs instead

IP-Range ↔ Grid-Initiative

- It's the Grid initiative that counts, not the host organisation.
- More fine grained it's the Virtual Organisation (VO) that is responsible for the given ID
- Most grids have a fairly formalized Incident Handling Procedure

Contact the VO-Manager rspt GRID-CERT
Stick to the IH-Procedures

A note on Forensics

- Forensics is complicated by the fact, that a user ID on a physical grid component is mapped on a user on that system. That mapping is dynamic.
- Grid-Jobs typically use a Toolkit. This is an additional, not always transparent layer.

Talk to your local Griddy for up-to-date tech-info

Conclusion

We have to become more fluent in the GRID language
Accept, that GRIDs are different