

Grid-CERT

GridKa School 2009
August 31 - September 4, Karlsruhe

Klaus Möller
DFN-CERT Services GmbH

- DFN-CERT and (D)Grid-CERT
- Incident Response (from the viewpoint of coordinating CSIRTs)
 - Incident Response (according to NIST)
 - CSIRT Services (according to CERT/CC)
 - Case study: "Der große Grid-Vorfall" (the big Grid incident)
 - Experience so far
- Other activities
 - Verification of Grid Firewall Configurations
 - Grid-IDS

- Computer Emergency Response Team for the German Research Network (DFN)
 - Support and coordination with security incidents
 - Several 1000 incidents p/a
 - See also: "Automatische Warnmeldungen"
 - Preventive warnings about software vulnerabilities
 - Provisioning of a PKI infrastructure (DFN-PKI)
 - Annual workshop and security tutorials
- Starting 1993 as a research project at Uni HH
- Since 1999 as a private business
 - SLA with DFN-Verein for CERT & PKI services
- Basic incident response support and coordination

- Established within DGI 1
 - <http://dgi2.d-grid.de/index.php?id=342>
- Goal: Establish CERT services for Grids
 - Build on the experience of DFN-CERT
- Officially active since 12/2006
 - First as a (virtual) stand-alone service
 - Hotline 040-808077-999
 - By now fully integrated into DFN-CERT
 - Std.-Hotline 040-808077-555
- International cooperation
 - Terena TF-CSIRT – Terms of Reference
 - 1st Ad-Hoc meeting at FIRST TC 2006 in

Incident response cycle (NIST 800-61)



This analysis suggests that CSIRT activities for a Grid are not fundamentally different from those performed by a traditional CSIRT. In terms of a local security team or a coordinating CSIRT, Grids represent a new platform specialism: local teams need to be able to manage them securely, while coordinating CSIRTs need sufficient knowledge to be able to handle incidents and assess the likely impact.

A.Cormack: "CSIRTs and Grids" <http://www.terena.nl/tech/task-forces/tf-csirt/doc/CSIRTs-and-Grids-v0.5.pdf>

CSIRT Services (CERT/CC CERT Handbook)

Reactive

Alerts and Warnings

Incident Handling

- **Incident analysis**

- **Incident response on site**

- Incident response support

- **Incident response coordination**

Vulnerability Handling

Artifact Handling

Proactive

Technology Watch

Security Audits or Assessments

Configuration and Maintenance of Security Tools, Applications, and Infrastructures

Development of Security Tools

Intrusion Detection Services

Security-Related Information Dissemination

Modify / tailor CSIRT services to Grid-needs

- Alerts and warnings
 - Grid information service (i.e. Advisories)
- Incident handling
 - Help for detecting and analyzing Grid-Incidents
- Vulnerability Handling
 - Further Security Best Practices with authors / vendors of Grid software
- Security-related information dissemination
 - Development and dissemination of Security Best

“Der große Grid-Vorfall” (the big Grid-incident)

- Time frame
 - First detected in August 2008 (in DE)
 - Later found that there's been activity at least since April /May 2008
 - An ongoing case (new events this month!)
- Ongoing police investigation
- Affected: Grid sites all around the world
 - Mainly Europe and USA

“Der große Grid-Vorfall”

- Attackers modus operandi
 - Gets access to username & password or SSH-key
 - Tries login at Grid site
 - Limits himself to Linux / x86 platforms
 - Local root exploit (different kinds)
 - Collects data from `~/.ssh/*` of all users
 - Installation of a trojaned SSH-client
 - Installation of a, until then, unknown Rootkit with backdoor and keylogger

“Der große Grid-Vorfall”

- Help by coordinating CSIRTs
 - Notification of compromised sites
 - Analysis of data from “drop-sites”
 - Information dissemination via Grid-internal mailing-lists
 - “Sperrliste” (revocation list) of compromised SSH-keys
 - Guide how to find the rootkit / trojaned SSH-client / keylogger
 - Tool to scan for the rootkit in your network
 - Initial help getting police investigation started
 - We're not lawyers!

“Der große Grid-Vorfall”

- As time goes by ...
 - The attacker has continually improved his rootkit
 - New compromised sites were detected every week
 - Many sites had to be contacted multiple times
 - Almost no reports from compromised sites at their own initiative
- Most of the active work done by 3 CSIRTs (DE, USA, XX)

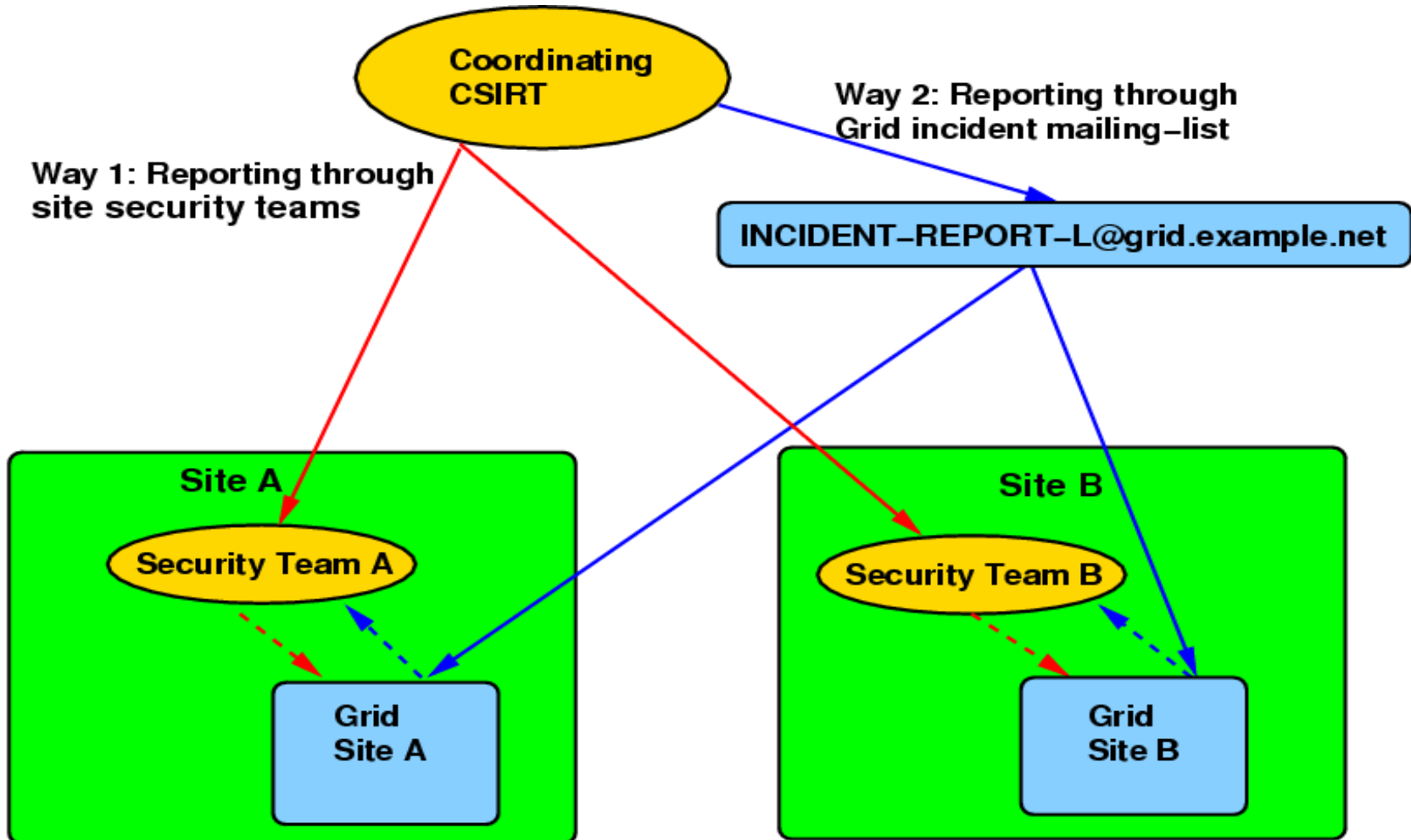
- Only very few “Real Grid Incidents”
 - Until now no exploits of vulnerabilities in Grid-SW
 - However lots of Open Source SW with known vulnerabilities
 - Most common attack: Identity Theft (passwords, certificates)
 - Sometimes other SW (i.e. NMS)
- Can't limit an incident to one Grid (VO)
- And it makes no sense anyway
 - Cluster (Grid-resourcen) used by many projects / VOs
 - Users are in more than one project at a time (Grid

Finding security contacts

- Typically, every incident “starts” with an event at an IP-Address (portscan, SPAM, etc.)
- Find the responsible person/team for this IP-address
 - Typicals: WHOIS (sometimes internal CSIRT-DB)
 - There's no database about which IP-address belongs to which Grid (and there will never be one)
 - Grid and local site security team **may or may not** be identical
- Needed: New ways to find responsible security contacts

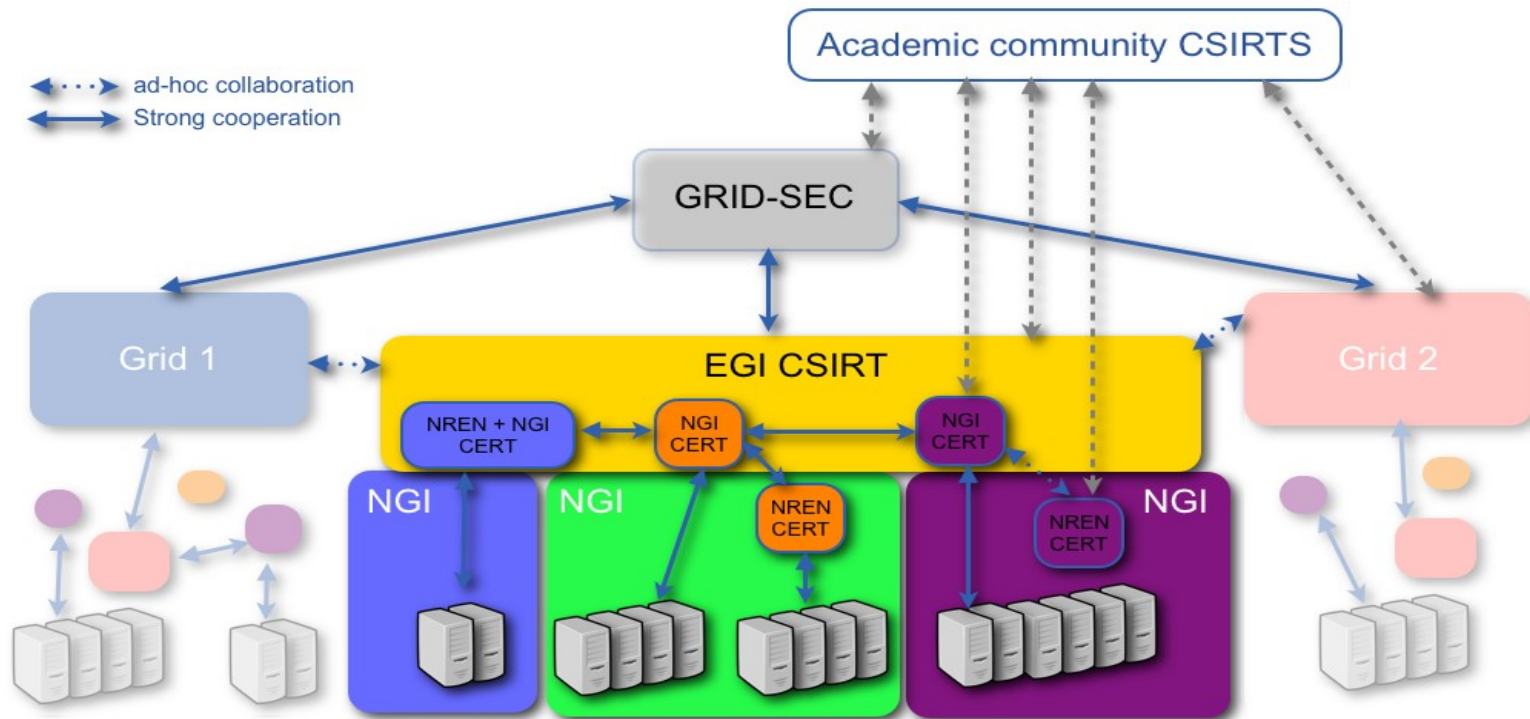
Incident reporting

(OSG proposal)



Incident reporting

(EGI proposal)



Incident reporting

- None of the proposals fulfills the needs
 - Too many points where information will be lost / filtered / delayed (see “Der große Grid-Vorfall”)
 - No acceptance for a hierarchy of coordinating CSIRTs (see EuroCERT)
 - Experience shows that feedback to coordinating CSIRTs is sporadic at best
 - Doesn't solve the problem “finding the responsible person” for CSIRTs
- What does work so far
 - Forums for sharing experience (TF-CSIRT)
 - Integration of Grid and “Network” CSIRTs

- The most Grid incidents: PlanetLab
 - Mostly false positives
 - Scan / Mapping Experiments
 - Ping / traceroute from PlanetLab hosts
 - Phishing – CoralCDN
 - Site content is hosted elsewhere – System will be reported as a Phishing Site
- Very effective system for incident reporting/handling
 - As soon as you find out its a PlanetLab system
 - Automated reporting through web interface
 - However: Local admins do not know whats running on a PlanetLab system

- The most important Grid infrastructure?
 - CRL-Server
 - Even a few minutes downtime will affect all clients and server, throughout all Grids
- What comes next?
- XSS / CSRF against Grid-Portals
 - As soon as the certificates are accessible from the browser, Grid-resources can be attacked without Identity Theft

Grid Firewall Verification Tool

- DGI 2 FG 3-3, cooperation with RRZN Hannover
- Verification of a Grid Firewall Configuration from the outside by (port)scanning
 - Start with policy / specification (Grid Firewall Profile)
 - Scan the actual configuration (nmap)
 - Results / History shown through web site
 - Integration into DFN-CERT portal planned

Grid IDS

- LRZ, RRZN, Stonesoft, DFN-CERT, (Fujitsu)
- Goal: Federated Grid Intrusion Detection System

International Cooperation

- Experience sharing between CSIRTs
 - Terenas TF-CSIRT: European CSIRT forum
 - Grid-Sec member
 - FIRST: International CSIRT forum

DFN-CERT - One CERT for all

- Long standing experience
 - With real incidents
- Established and well networked
 - Grid-Sec, FIRST, TF-CSIRT, CERT-Verbund, ...
- Our mission:
 - Avoid replication of work (compare PKI)
 - Improve and refine services