Grid-CERT Services

Modification of traditional and additional new CERT Services for Grids

Presentation at the Annual FIRST Conference
Vancouver, Canada - June 26, 2008
Antonio Liu

PRESECURE®

* Outline

1. Background
2. Introduction
3. Some significant Aspects of Grids
4. Incidents and Incident Priority Lists
5. Traditional CERT Services
6. Modification of traditional CERT Services
7. New Services and a new Service Category
8. Conclusion

* 1. Background

- PRESECURE Consulting GmbH
- Established in 2000
- IT Consulting
- Focus on Incident Response, Situational Awareness and Early Warning
- Research projects for e.g. EU and BMBF
- Close working relations with various CERTs e.g. S-CERT, Siemens CERT, Telekom-CERT a.o.
- Especially DFN-CERT

* Background

- Presentation based on technical report for and operating experience of the DFN-CERT

* 2. Introduction

- Rapidly increasing number of Grids
- Grid-Security is focused on secure communication and data transfer
- First reports of incidents in Grids
- Grids are insecure and the number of incidents will increase considerably
- CERTs – a well proven security management concept can improve the operational security of Grids

* Introduction

- D-Grid initiative started 2005
- Six Community Grid projects and one Grid Integration project
- DFN-CERT was tasked to research security relevant aspects
- CERT members perspective
- Grid community perspective
- Report uses different approach

Grids

- **First descriptions of Grid concepts in 90ties**
- **Ian Foster and Carl Kesselmann: „ The Grid: Blueprint for a new Computing Infrastructure“, 1998**
- **Most concepts and techniques developed at universities and research labs**
- **Solution to:**
  - Enable complex computation and simulation
  - Better use of existing ressources
  - Connection of heterogeneous systems
  - Provide easy access to computational power and ressources „on demand“

Definition of Grid

- **Various different definitions**
- **Foster (2003) defines:**
  - *„A Grid is a system that:*
    1. *Coordinates resources that are not subject to centralized control,*
    2. *Using standard, open, general-purpose protocols and interfaces,*
    3. *To deliver nontrivial qualities of service.“*

Grids – categorized by shared Resources

- Computing Grid
- Data Grid
- Resource Grid
- Service Grid
- Knowledge Grid
- Equipment Grid

Grids – categorized by Purpose and Task

- Distributed Computing
- Large-scale Data Analysis
- Computer-in-the-Loop Instrumentation
- Collaborative Work
- Science Portals

Grid Software and Projects

- **Most established Grid implementations:**
  - Globus Toolkit
  - gLite
  - UNICORE (UNiform Interface to COmputing REsources)
- **Grid Projects and Initiatives:**
  - D-Grid
  - EGEE/EGEE2 (Enabling Grids for E-Science
  - LCG (Large Hadron Collider Grid)
  - SETI@home (Search for Extraterrestrial Intelligence at Home)

* 3. Some significant Aspects of Grids

- **Integration of resources and users from different administrative control domains, with distributed locations and varied organisational setup**
- **Collaborative use of resources**
- **Middleware**
  - Functionalities for authentication, authorisation, identification of available and free resources as well as access to resources
- **Large software packages**
  - e.g. GLOBUS Toolkit has 250 MB of binaries and config files, over 50 server processes after installation
- **Usage of other opensource software & standards**
  - e.g. Apache, OpenSSL, OpenSSH, a.o.

PRESECURE®

* Some further Aspects of Grids

- User management carried out by each participating domain – Single Sign On
- No centralized control of authentication, authorisation or data transfer – use of proxy certificates
- No centralized logging or monitoring
- Intransparency wrt where a job was processed or what was processed on a system

PRESECURE®

4. Incidents

- **No commonly accepted definition**
- **Enourmous increase of reported incidents and attacks since many years**
- **Possible explanations:**
  - Enourmous increase of hosts
  - More detection through technical advances
  - Growth of software increases number of vulnerabilities (estimated average of 2 bugs per 1000 lines of code)
  - Increasing complexity of software leads

    to increase of configuration errors

Definition for Incident

- Tilman Holst defines:
  - *„**Event**: An event is something observable.*
  - ***Incident**: One or more events, which lead to a violation of an explicit or implied policy.*
  - ***Attack**: An intentional incident.*
  - ***Accident**: An unintentional incident.“*

* Incidents – categorized by technical nature

(1) Scan

(2) Compromise

(3) Sniffer

(4) Abuse

(5) DoS

(6) Virus

(7) Trojan

(8) Spam

(9) Social engineering

(10) Warez

(11) Bot

(12) Botnet-CC

(13) Account probe

(14) Phishing site

(15) Attempt

(16) Malware hosting

(17) Defacement

(0) Other

* Incidents – categorized by threat level

- Priority 1 – Threat to life and limb
- Priority 2 – Threat to network infrastructure
- Priority 3 – Threat through automated widespread attacks
- Priority 4 – Threat through compromise on system/root level
- Priority 5 – Threat to availability of certain services
- Priority 6 – Threat through compromise on account/user level
- Priority 7 – Threat through theft of data
- Priority 8 – Threat through further attacks
- Priority 9 – Threat through other trivial attacks

* 4. Incident Priority List

Examples for incident categories

Priority	Examples
1	Life and health threatening attacks (Hospital nets etc.)
2	Attack on net infrastructure (Router, DNS-Server etc.)
	Attack on the DFN-CERT network
3	Worms (e.g. Nimda)
	Report about DDoS-Handler or DDoS-IRC-Channel
4	Sniffer-installation
	Theft of particularly secured data
	Other particularly secured data
	Root-Compromise
	Root-Compromise with logs
	Report about DDoS-Agents
	DDoS-Reports in general
5	SPAM-DoS (falsified headers “From:”)

* Incident Priority List

Priority	Examples
6	Account-Compromise (Non-Root, single case)
	Open mail relay
	DoS attack
7	Theft of data (e.g. /etc/passwd etc.)
	Phishing
8	Unsuccessful login attempts
	Port scans
9	NMAP-Scans (general port scan)
	Unsuccessful cgi-bin/phf attack
	TFTP-Attempt
	DHCP-Attempt
	SPAM (single case)
	Fake mails (single case)
	FTP-Abuse (Swap-Site)
	Virus problems

* Modified Incident Priority List

Priority	Examples
1	Life and health threatening attacks (Hospital nets etc.)
2	Attack on net infrastructure (Router, DNS-Server etc.)
	Attack on the DFN-CERT network
3	Worms (e.g. Nimda)
	Report about DDoS-Handler or DDoS-IRC-Channel
	Attack on Grid-Server/Application including DDoS-Reports
4	Sniffer-Installation
	Theft of particularly secured data
	Other particularly secured data
	User/Root-Compromise
	User/Root-Compromise with logs
	Report about DDoS-Agents
	DDoS-Reports in general
5	SPAM-DoS (falsified headers “From:”)

* Modified Incident Priority List

Priority	Examples
6	Open mail relay
	DoS attack
	Theft of data (e.g. /etc/passwd etc.)
7	Phishing
	Unsuccessful login attempts
8	Port scans
	NMAP-Scans (general Port Scan)
9	Unsuccessful cgi-bin/phf attack
	TFTP-Attempt
	DHCP-Attempt
	SPAM (single case)
	Fake Mails (single case)
	FTP-Abuse (Swap-Site)
	Virus problems

* 5. Traditional CERT Services

Reactive Services

- ✚ Alerts and Warnings
- ✚ Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- ✚ Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- ✚ Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

- ⟳ Announcements
- ⟳ Technology Watch
- ⟳ Security Audit or Assessments
- ⟳ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ⟳ Development of Security Tools
- ⟳ Intrusion Detection Services
- ⟳ Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

* 6. Modification of CERT Services

	Traditional CERT Services	Relevance in Grid Environment	Practical Applikation / Use in Grid Environment	Requirements
Reactive	Incident Handling	Fundamentally important (++)	Needs modification (0)	Some necessary preparation / preliminary work (0)
	Alerts and Warnings	Fundamentally important (++)	Needs modification (0)	Some necessary preparation / preliminary work (0)
	Vulnerability Handling	Valuable (+)	Needs minor modification (+)	Some necessary preparation / preliminary work (0)
	Artifact Handling	Limited value (0)	Needs minor modification (+)	Brief preparation / preliminary work (+)
	Forensic Analysis	Limited value (0)	Hardly feasible (-)	Extensive preparation / preliminary work (-)

* Modification of CERT Services

	Traditional CERT Services	Relevance in Grid Environment	Practical Applikation / Use in Grid Environment	Requirements
Pro-active	Announcements	Valuable (+)	Needs modification (0)	Some necessary preparation / preliminary work (0)
	Development of Security Tools	Fundamentally import (++)	Needs modification (0)	Extensive preparation / preliminary work (-)
	Configuration and Maintenance of Security Tools, Applications and Infrastructures	Valuable (+)	Needs modification (0)	Extensive preparation / preliminary work (-)
	Intrusion Detection Services	Valuable (+)	Needs modification (0)	Extensive preparation / preliminary work (-)
	Security Audits and Assessments	Limited value (0)	Needs modification (0)	Extensive preparation / preliminary work (-)
	Security-related Information Dissemination	Valuable (+)	No modification necessary (++)	None (++)
	Technology Watch	Valuable (+)	No modification necessary (++)	None (++)
	Trend and Neighbourhood Watch	Valuable (+)	Needs minor modification (+)	Some necessary preparation / preliminary work (0)

* Modification of CERT Services

	Traditional CERT Services	Relevance in Grid Environment	Practical Applikation / Use in Grid Environment	Requirements
Security Quality Manage ment Services	Awareness Building	Valuable (+)	Minor modification (+)	Some necessary preparation / preliminary work (0)
	Business Continuity and Disaster Recovery Planning	Valuable (+)	Needs modification (0)	Extensive preparation / preliminary work (-)
	Education and Training	Valuable (+)	Minor modification (+)	Some necessary preparation / preliminary work (0)
	Product Evaluation and Certification	Secondary (-)	Minor modification (+)	Extensive preparation / preliminary work (-)
	Risk Analysis	Limited value (0)	Needs modification (0)	Some necessary preparation / preliminary work (0)
	Security Consulting	Valuable (+)	Minor modification (+)	Brief preparation / preliminary work (+)

* 7. New Services and Service Category

- Preparation and Enforcement of AUPs and Security Policies
- Enforcement of certain Qualities
- Clearinghouse for Monitoring Data
- Setup and Maintenance of the Grid-PKI
- Monitoring and Verification of Certificates
- Firewall Checks

⇒Infrastructure Services

⇒Improves reliability and integrity

* 8. Conclusion

- A Grid-CERT is a valuable security management concept for Grids
- CERTs should work closely together with Grid community and developers of Grid software
- CERTs must accept and understand that Grids have different characteristics and needs than usual constituency
- Traditional CERT Services have to be modified
- Especially new Infrastructure Services would provide valuable additions

* Conclusion

- The new Infrastructures Services are also valuable for traditional CERTs
- It is recommended to establish Grid-PSIRTs
- There should be:

  One Grid-PSIRT for every Grid software and one Grid-CERT for every Grid community!

* Contact details

Antonio Tung-Wang Liu

Email: al@pre-secure.de

Tel.: +49 40 808077 888