Risk assessments – introduction and PRACE practices

Jules Wolfrat, SURFsara

EGI-EUDAT-PRACE security workshop, Linkoping, Sweden, 9 October 2013

CAPACITIES

e-infrastructure

Introduction

- The EGI Software Vulnerability Group (SVG) defines a vulnerability as “a problem where a principal (e.g. a user) can gain access to or influence a system beyond their intended rights” [1]
- Vulnerability assessment is “the proactive examination of software in order to find vulnerabilities that may exist “ [1]
  - Also “handling reported potential vulnerability problems”

[1] https://wiki.egi.eu/wiki/SVG:SVG

Vulnerability assessment

- First Principles Vulnerability Assessment: http://research.cs.wisc.edu/mist/papers/VA.pdf
  - Code review

See http://research.cs.wisc.edu/mist/

PRACE Practice

- Risk reviews: analysis of the impact that a vulnerability can have
  - No code review
- Risk review procedure based on guidelines from the German BSI (Federal Office for Information Security), BSI-Standard 100-2:
  - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile.
- Using the IT-Grundschutz Catalogues for threats and safeguards:
  - https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html
  - Specifically the “threats catalogue deliberate acts”

Risk assessment procedure

- First determine the information domain and the components involved.
  - Globus Online example:
    - Domain: data management facilities
    - Components:
      - Prace GridFTP servers
      - GO (Globus Online) servers
      - External client/server systems
      - Network (switches, routers, cabling, software)

Risk assessment procedure (2)

- Then determine the protection requirements for the application, based on the categories as defined in BSI 100-2:
  - "Normal" The impact of any loss or damage is limited and calculable.
  - "High" The impact of any loss or damage may be considerable.
  - "Very High" The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organisation.

Risk assessment procedure (3)

- Based on the following damage scenarios:
  - Violations of laws, regulations, or contracts
  - Impairment of the right to informational self-determination
  - Physical injury
  - Impaired ability to perform the tasks at hand
  - Negative internal or external effects
  - Financial consequences

(should be refined?)

Risk assessment procedure (4)

- Threat analysis based on lists of possible threats
  - Determine likelihood and impact
- Determine safeguards against threats
- Based on the list of threats and safeguards determine if the service is acceptable

Threats analysis

https://prace-wiki.fz-juelich.de/bin/view/PRACE/Operations/GlobusOnlineRiskReview#Threats_analysis

- T 5.1 Manipulation or destruction of IT equipment or accessories
- **T 5.2** Manipulation of data or software
- T 5.3 Unauthorised entry into a building
- T 5.4 Theft
- T 5.5 Vandalism
- **T 5.6** Attack
- **T 5.7** Line tapping
- T 5.8 Manipulation of lines
- **T 5.9** Unauthorised use of IT systems
- T 5.10 Abuse of remote maintenance ports
- T 5.11 Loss of confidentiality of data stored in PBX installations
- T 5.12 Interception of telephone calls and data transmissions
- T 5.13 Eavesdropping of rooms
- T 5.14 Call charges fraud
- **T 5.15** "Inquisitive" staff members

Threats analysis (2)

- T 5.16 Threat posed by internal staff during maintenance/administration work
- **T 5.17** Threat posed by external staff during maintenance work
- **T 5.18** Systematic trying-out of passwords
- **T 5.19** Abuse of user rights
- **T 5.20** Abuse of administrator rights
- **T 5.21** Trojan horses
- T 5.22 Theft of a mobile IT system
- **T 5.23** Computer viruses
- **T 5.24** Replay of messages
- **T 5.25** Masquerading
- **T 5.26** Analysis of the message flow
- **T 5.27** Repudiation of a message
- **T 5.28** Denial of services
- **T 5.29** Unauthorised copying of data media

Threats analysis example

This is explained by means of a table. When possible, and as an example, the threat has been mapped to the list provided by the IT-Grundschutz Catalogues [5].

No.	Threat	Classification	Likelihood	Impact	Remarks
1	UNICORE UFTP is based on Java, but Java has security issues	T2.5, T5.2, T5.20, T5.85, T5.86, T5.88	Low	High	
2	The firewall protecting the machine running the *uftpd* daemon is misconfigured	T2.3, T5.48	Low	Medium	This takes into account: old firewalls not able to inspect FTP control channel connections and dynamically open the port negotiated for the data transfer; control channel port not opened; unnecessary ports opened for the data transfer.
3	Damaged packets can affect a UNICORE UFTP communication	T5.28	Very Low	Very Low	
4	The "secret" string sent over the command channel is eavesdropped	T5.6, T5.7, T5.8	Low	Low	The role of the "secret" string is discussed here.
5	The UNICORE UFTP ACL is not properly configured	T5.20, T5.84	Low	Medium	The effect of the possible misconfiguration of the *uftpd* ACL.
6	The UNICORE UFTP is not properly installed	T2.2, T2.5, T3.9, T5.60	Low	Medium	This is related to the deployment of the service and the various components involved.
7	Privilege escalation without SSL enabled on the control channel	T3.9	Low	High	

Safeguards example

Safeguards

The following table offers safeguard for the threats listed in the previous subsection. Only the threat number is reported and a mapping to the IT-Grundschutz Catalogues [5] is proposed, where applicable and as an exercise.

No.	Classification	Safeguard
1	S2.83, S4.65	Code can be checked and developers are trusted. The possibility of code injection is very low since sites are trusted.
2	S2.73, S4.97	The firewall has to be "FTP aware", that is it should be able to inspect the FTP connection request and understand when and which port(s) to open for the actual transfer. Only the control channel port should be statically opened and known to the user. For safety reasons it is advisable not to employ the standard one (21). If the firewall can not handle FTP protocol in a dynamic way then *uftpd* cannot work properly: a different transfer protocol should be employed. No additional ports need to be statically opened (see GridFTP). If this is done by mistake, then this issue can not be addressed by UNICORE UFTP. UNICORE UFTP supports parallel streams. Multiple ports are allocated but this is not a problem for the firewall, since the connections are started from the inside (outgoing connections are usually allowed). It would be interesting also to check that *uftpd* works with a proxy.
3	S5.39	UNICORE UFTP is based on TCP and not UDP.
4	S5.66	The "secret" string identifies the client. It is encrypted (in production) and even if it is wiretapped, no harm will occur. The secret is a one time password, tt is sent to the UNICORE/X encrypted and repeated by the client to check the identity. An attempt of anonymous login on the FTP control channel can be noticed, but this cannot not be used for any purpose because only commands for the specific file transfer are accepted.
5	S4.78	The UNICORE UFTP ACL is the list of the server DNs the UNICORE UFTP instance is allowed to communicate with. The service administrator should include only needed machines, at least UNICORE/X.
6	S4.78	Different configurations are envisaged: i.e. *uftpd* deployed on the login node(s) of the supercomputer on a stand alone machine. The only requirement is that *uftpd* should have access to the target (i.e. supercomputer) filesystem. It should be clear that *uftpd* does not rely on the TSI, it however interacts with the UNICORE/X since the control channel establishment goes through this component. Deployment on the login node allows to exchange data between supercomputers, but this configuration is not mandatory.