Security Update

Mingchao Ma
EGI Security Officer
STFC, UK

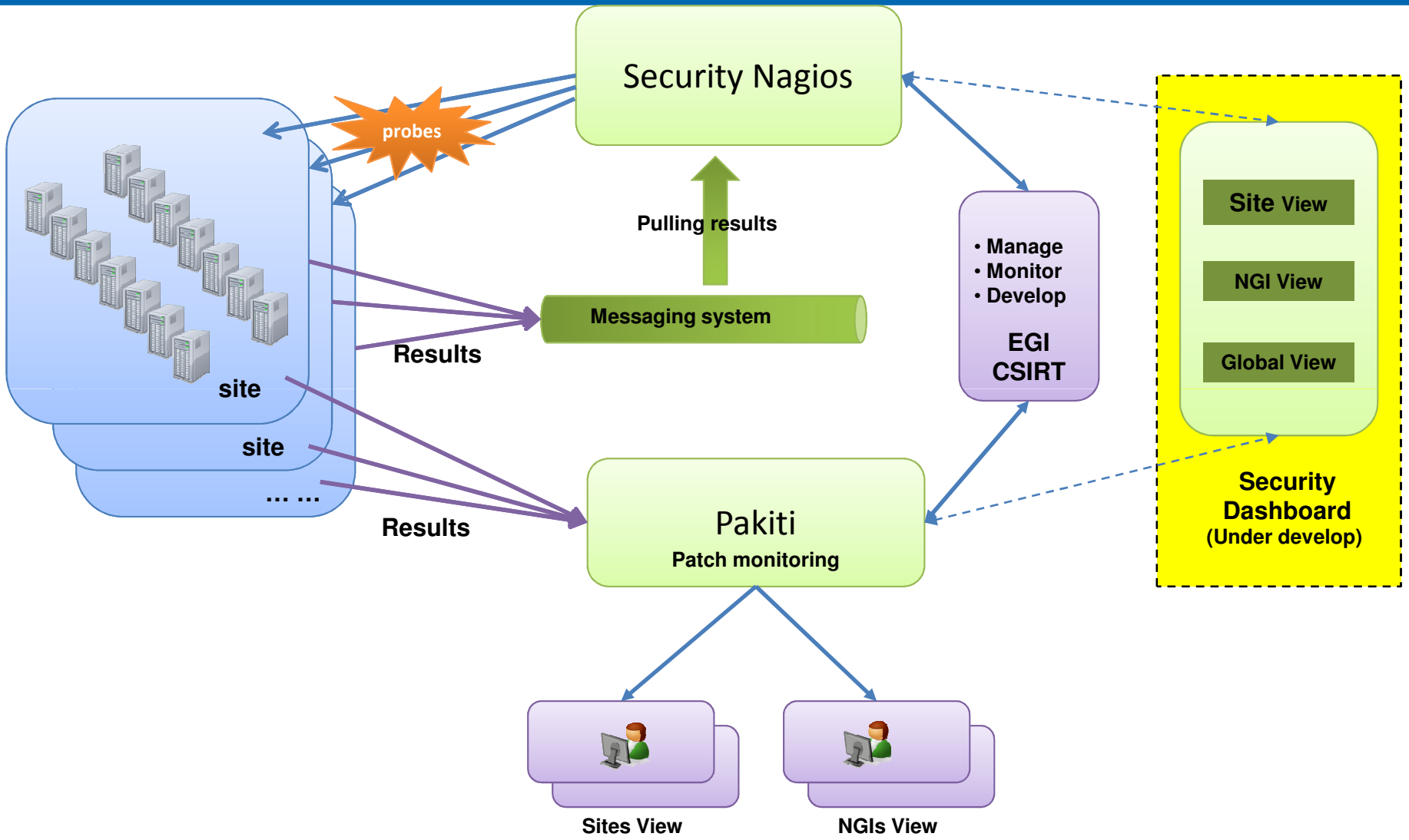
Overview

- Security Update
  - Incident response
  - Security monitoring
  - Security training
  - Security Drills
    - Security Service Challenge 5

Incident Response

- Incident Response Task Force
  - Day to day operation
  - Follow up with sites flagged by security monitoring tool
  - No incident reported in last two months
  - High risk vulnerability in Torque server, alert sent to sites on 16th June

Security Monitoring



Security Training

- Training session at EGI TF2011 planned
  - Six hours requested
  - 3 hours operational security – EGI CSIRT
  - 3 hours grid middleware security – middleware security experts and developers
  - Provisional list of training topics discussed
  - Will finalise the detail once the requested sessions are confirmed

Security Drills

- Security Service Challenge (SSC)
  - Objective: improve both EGI site security incident response capabilities and EGI CSIRT incident coordination capabilities
  - SSC 1-3 were carried out in EGEE ear
  - Continue in EGI
    - Much improved SSC framework
    - SSC4: 13 sites including all WLCG Tier1 sites were challenged last year
    - SSC5: started on 25th May 2011

SSC5

- Participants/Players
  - 40 sites in 20 countries
    - https://wiki.egi.eu/wiki/EGI_CSIRT:Security_challenges
  - ATLAS VO
  - 3 “compromised certificates” from 2 CAs
  - ATLAS Pilot framework for job submission
  - NGI security officers assisted sites investigation
  - EGI CSIRT coordinated the overall response

The Scenario

- SSC5 operator simulated a large scale cross NGIs incident by submitting “malicious jobs” to multiple sites with “compromised” certificates
- The “malicious jobs” running at multiple sites built up a “botnet”
- The “bot (malicious job)” periodically reported to C&C server
- The “bot” was controlled by C&C server

The Challenge

- Affected site
  - To identify malicious jobs/bots running at sites
  - To identify malicious job owner(s)
  - To identify malicious network traffic
  - To identify compromised DNs
  - To contain the incident
  - To find further information related to the malicious job and/or compromised DNs
  - To report findings to EGI CSIRT promptly

The key is to follow incident handling procedure

The Challenge

- NGI security officers
  - To assist site's investigation
  - To coordinate NGI wide response
- EGI CSIRT
  - To assist site and NGI security officer
  - To coordinate with sites, VO, CA and NGI security officer to contain the incident as soon as possible
  - To understand the nature of the incident and possible damage
  - To do the forensic analysis of malicious binaries
  - To manage information flow among all involved parties

Timeline

- Stage 0 - preparation
  - Improved SSC framework and SSC mornitoring
  - NGI security officers identified participating sites
  - Informed sites about SSC5
- Stage 1 - incident simulation
  - Started on Wednesday 26th May 2011 until Friday 28th May 2011
- Stage 2 – final report collection
  - Due on 22nd June
- Stage 3 – feedback collection
- Stage 4 – final result/evaluation

Some Early Observations

- Most sites were able to identify the malicious job and compromised DN(s)
- The quality of incident report from sites was various
- The template for incident report improved the quality of site's report
  - But some sites did not use it
- Some sites provided detail forensic analysis of malicious binaries
  - A member of EGI CSIRT provided very detail analysis in just a few hours

Some Early Observations

- A few sites still failed to ban the malicious DNs at the first attempt
  - Most due to mis-configuration
- Revoked VO membership could not effectively contain the incident
- However, revoked compromised certificate can contain the incident
  - But might have serious impact on VO, e.g. revoke pilot user certificate
  - Might not comply with CA's CP/CPS policy

Some Early Observations

- To spot malicious SE activities was tricky, but we did manage to discover them
- For incident coordinator, to manage information flow was challenging
  - RTIR ticket system did help to some extend
  - Too many emails (more than 500 in about 3 days), many information was duplicated
  - This will be discussed further within EGI CSIRT

Conclusion

- Still in a early stage, still processing sites reports and other information
- Final result will be made available in due course
- A detail report will be given at next EGI TF