An Active Security Infrastructure for Grids

Stuart Kenny*, Brian Coghlan

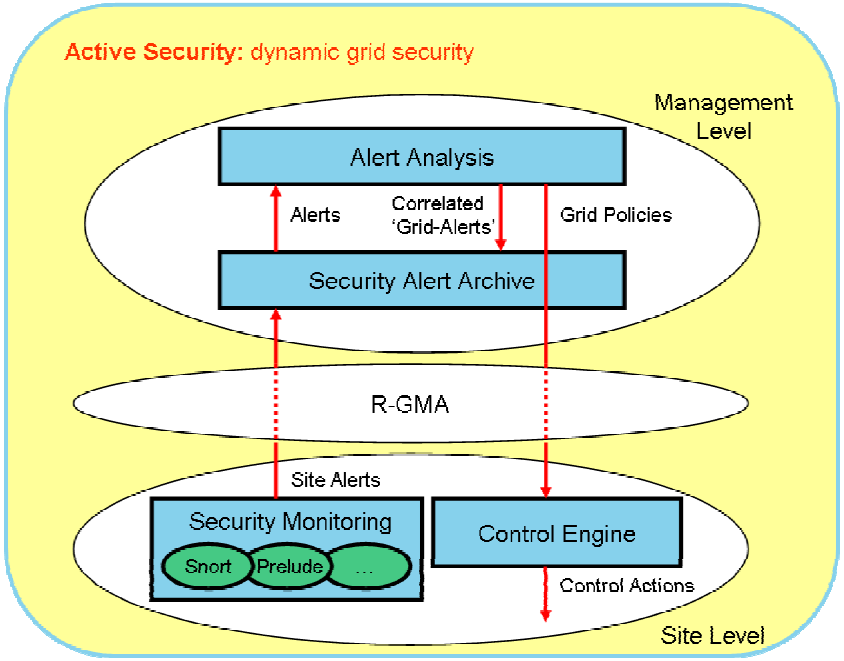
Trinity College Dublin

Overview

- Grid-Ireland security monitoring
- Infrastructure
- Analysis
- Future work

Grid-Ireland Security Monitoring

- Grid-Ireland Gateway
  - Point-of-presence at 18 institutions
  - Centrally managed by Grid Operations Centre (OpsCentre) at TCD
- Track overall state of security of infrastructure
- Existing Grid security activities focused on prevention
  - Authentication, authorization
- Active security focused on
  - Detection
  - Reaction
- Communication via Grid monitoring system:
  - R-GMA

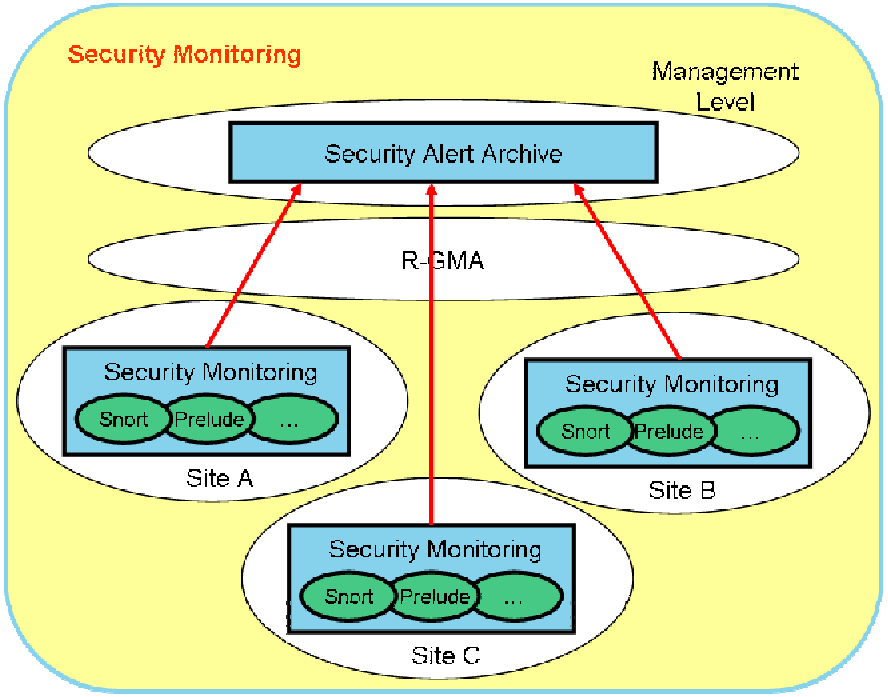


Monitoring

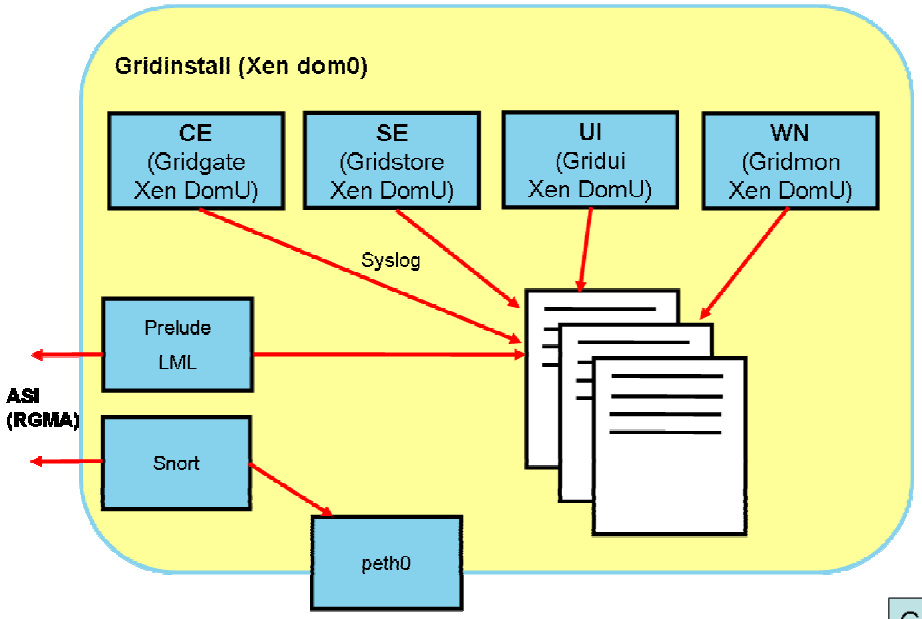
- **Why do we need detection**
  - Grid only as strong as weakest link
    - No knowledge of state of security of sites
  - Security Service Challenge level 1 debriefing report
    - Sites not responding due to
      - Security contact list not up to date
      - Security contact was overloaded
      - Security contact did not understand alert
      - Security contact had not received guidance
    - Retention period for log files not sufficiently long
    - Complexity of analysing log files
- **Active Response**
  - “5 pillars of cybersecurity” (iSGTW 09 April 2008)
    - Can never produce 100% secure general purpose computing system
    - Speed of attack and ensuing spread of system damage is more rapid than a human can manage or mitigate

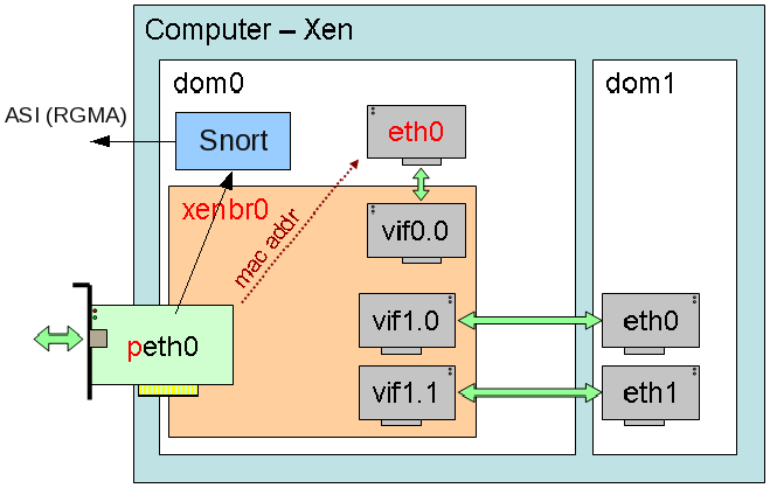
Security Monitoring (Site Level)

- Monitors state of security of a site
- Reports detected security events to security alert archive
- Monitoring performed by 'R-GMA enabled' security tools
  - Snort
  - Prelude-LML
- Extensible
  - Easy inclusion of additional tools, e.g., Tripwire
- R-GMA
  - Relational model
  - Soft state registration and discovery
  - Fault tolerance and load balancing
  - Information security



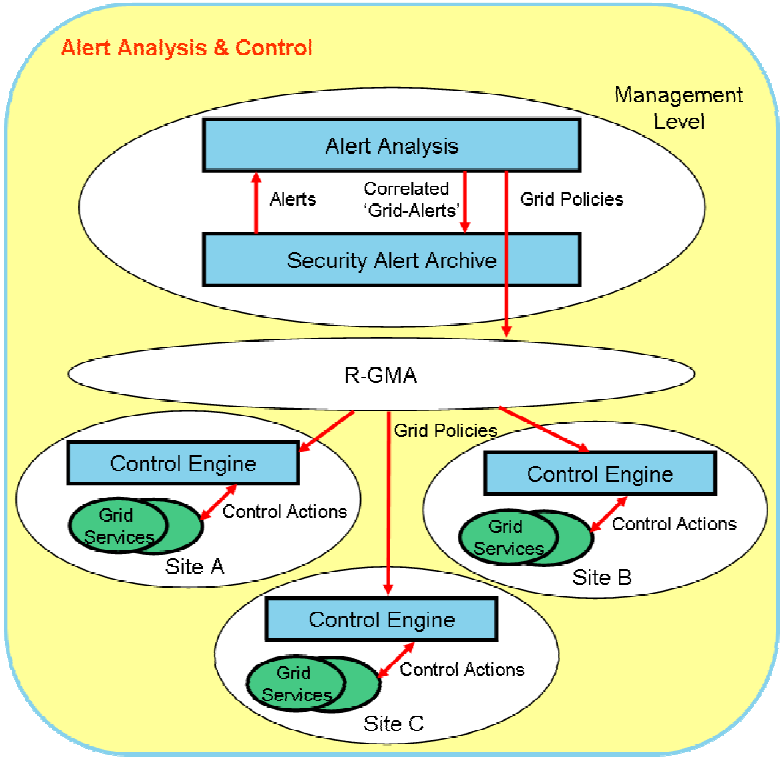
Grid-Ireland Deployment





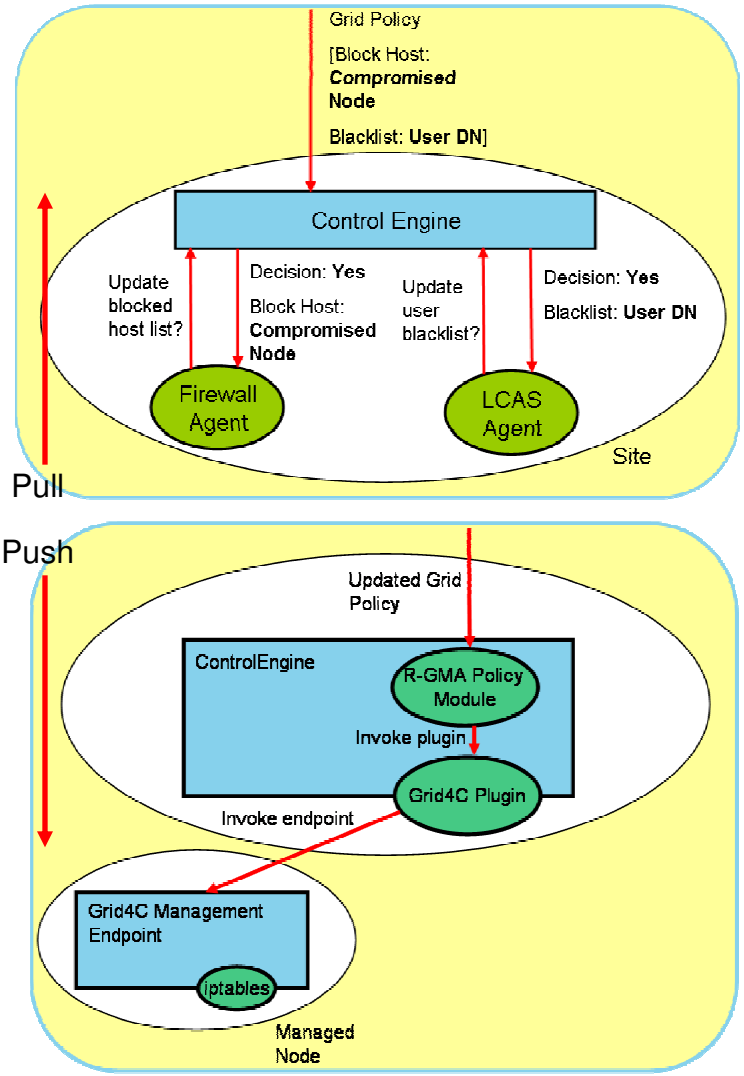
Alert Analysis (Management Level)

- Filter and analyse alerts contained in alert archive
  - Detect patterns that signify attempted attack
- Attempts to join alerts into high-level attack scenarios
- Output
  - Correlated high-priority Grid alert
  - New Grid policy
    - Define actions to be taken in response to security event
- Extensible
  - Define additional ‘attack scenarios’ and base policies

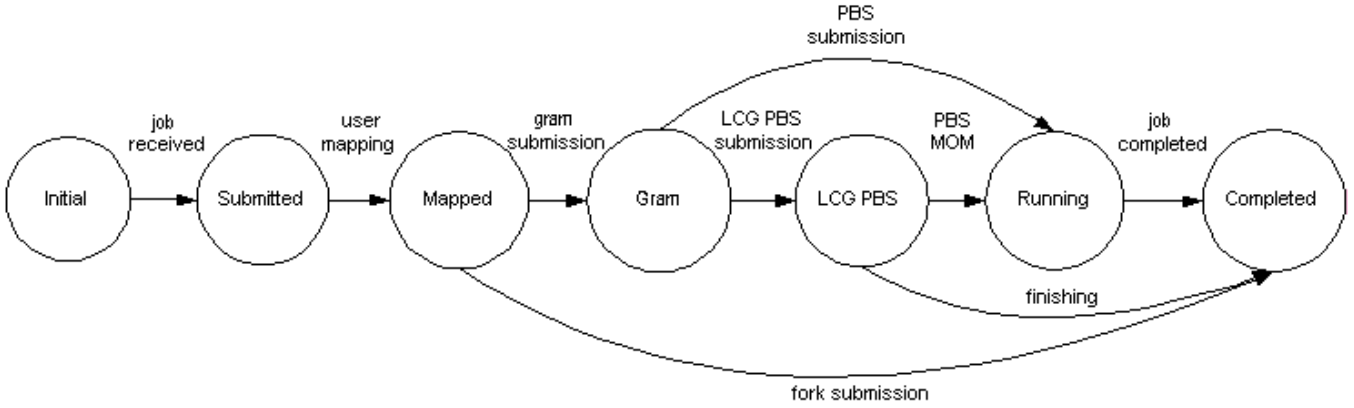


Control Engine (Site Level)

- Input:
  - Grid policies generated by analysis component
- Site Policy Decision Point
  - Evaluates requests for guidance from service agents
  - Decision based on applicable policies
- Decision contains action to be taken to mitigate risk of possible security incident
- Active Plug-in
  - Plug-ins invoked on policy update
  - User defined code handles response and enforces obligations



Analyzer Scenarios: Job Monitoring



- Scenario models attack as series of state changes
  - Models states job passes through once submitted to a site
  - State changes triggered by published alerts
    - Prelude LML and PBS scripts
  - Can be used as basis for ‘higher-level’ scenarios
    - E.g., job executing restricted command
- This is effectively Grid user tracing

Analyzer Scenarios: Job Monitoring

analyzerid	createtime	classification	transition
gridgate.cs.tcd.ie:1228919061	2008-12-10 14:25:20.929768	Job submitted to gatekeeper	initial → submitted
gridgate.cs.tcd.ie:1228919061	2008-12-10 14:25:20.931820	Local user mapping	submitted → mapped
gridgate.cs.tcd.ie:1228919061	2008-12-10 14:25:20.933663	Job Manager ID assigned GRAM Script Job ID	mapped → gram
gridgate.cs.tcd.ie:1228919061	2008-12-10 14:25:23.565347	PBS-MOM job submission	gram → running
gridgate.cs.tcd.ie:1228919061	2008-12-10 14:25:36.944744	Job completed	running → completed

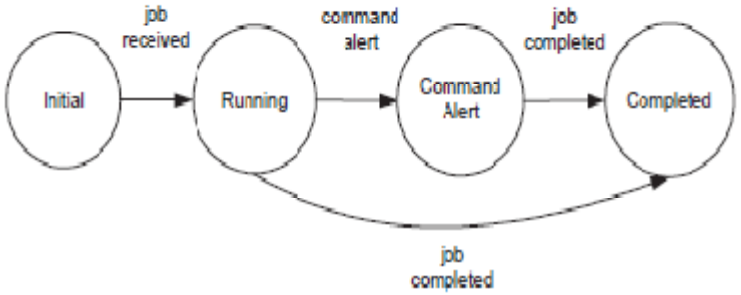
```
<AdditionalData type="string" meaning="GATEKEEPER_JM_ID">
   2008-12-10.14:25:17.0000011823.0000000000
</AdditionalData>
<AdditionalData type="string" meaning="USER_DN">
   /C=IE/O=Grid-Ireland/OU=cs.tcd.ie/L=RA-TCD/CN=Stuart P. Kenny
</AdditionalData>
<AdditionalData type="string" meaning="Log received from">
   /var/log/messages
</AdditionalData>
<AdditionalData type="string" meaning="Original Log">
   Dec 10 14:25:20 gridgate gridinfo[11835]: JMA 2008/12/10 14:25:20
   GATEKEEPER_JM_ID 2008-12-10.14:25:17.0000011823.0000000000 for
   /C=IE/O=Grid-Ireland/OU=cs.tcd.ie/L=RA-TCD/CN=Stuart P. Kenny on 134.226.53.29
</AdditionalData>
<AdditionalData type="integer" meaning="Rule ID">5001</AdditionalData>
<AdditionalData type="integer" meaning="Rule Revision">1</AdditionalData>
```

Analyzer Scenarios: Job Monitoring

analyzerid	createtime	classification
asistat:1.0	2008-12-10 14:25:27	Job execution started
asistat:1.0	2008-12-10 14:25:39	Job execution completed

```
<AdditionalData type='string' meaning='userdn'>
   /C=IE/O=Grid-Ireland/OU=cs.tcd.ie/L=RA-TCD/CN=Stuart P. Kenny
</AdditionalData>
<AdditionalData type='string' meaning='gatekeeper_jm_id'>
  2008-12-10.14:25:17.0000011823.0000000000
</AdditionalData>
<AdditionalData type='string' meaning='local_user_id'>
   gitest008
</AdditionalData>
<AdditionalData type='string' meaning='gramid'>
   77533.gridgate.cs.tcd.ie
</AdditionalData>
<AdditionalData type='string' meaning='jobname'>
   STDIN
</AdditionalData>
<AdditionalData type='string' meaning='pid'>26778</AdditionalData>
```

Analyzer Scenarios: Job Monitoring



analyzerid createtime	classification	transition	
asistat:1.0	2008-12-11 10:12:40	Job execution started	initial → running
gridgate.cs.tcd.ie:1228919061	2008-12-11 10:13:40.302965	Restricted executable (at) by user gitest008	running → commandalert
asistat:1.0	2008-12-11 10:14:45	Job execution completed	mapped → gram

analyzerid	createtime	classification
asistat:1.0	2008-12-11 10:13:42	Restricted executable detected

```
<Obligation PolicyId='LcasUserBanPolicy'
     ObligationId='UserBanList' FulfillOn='Permit'>
   <AttributeAssignment AttributeId='userdn'
        DataType='http://www.w3.org/2001/XMLSchema#string'>
            /C=IE/O=Grid-Ireland/OU=cs.tcd.ie/L=RA-TCD/CN=Stuart P. Kenny
   </AttributeAssignment>
</Obligation>
```

Future work

- Detection
  - How to detect ‘Grid-attacks’
    - Mostly compromised hosts
  - Need new sensors
- Correlation approach
  - Need to evaluate more techniques
    - Pre-requisite, consequences
    - Probabilistic
- How to define scenarios
  - Automated approach?
- Control
  - Integrate with existing control mechanisms?