

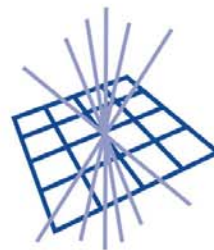
# Grid Security: Expecting the Unexpected

Mingchao Ma

STFC - Rutherford Appleton  
Laboratory, UK



Science & Technology  
Facilities Council



**GridPP**  
UK Computing for Particle Physics

# Overview

- Security Service Challenges (SSC) Review
- Grid Security Incident - What had happened?
- Risk - expected and unexpected
- Lessons learned

## SSC - What is it?

*"The goal of the LCG/EGEE Security Service Challenge, is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available"*

Like a fire drill!



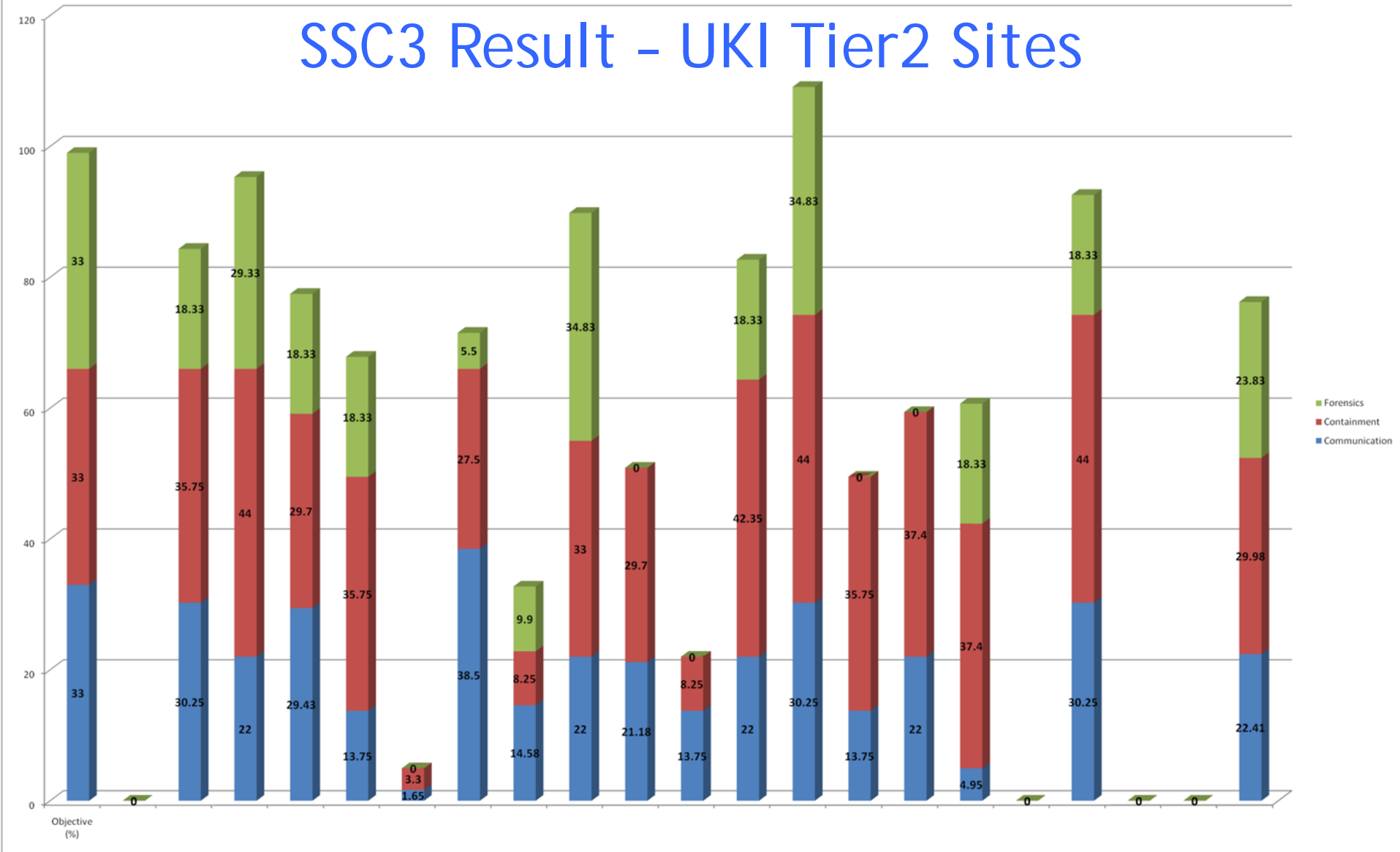
# Security Service Challenges

- SSC 1: challenges the Workload Management System (WMS) on the Grid: Resource Broker (RB) and Compute Element (CE) (2005)
- SSC 2: challenges the Storage Elements on the Grid (2007/2008)
- SSC 3: challenges the Operational Diligence of the LCG/EGEE Grid Sites (Dec 2008)

<http://www.gridpp.ac.uk/security/ssc/>

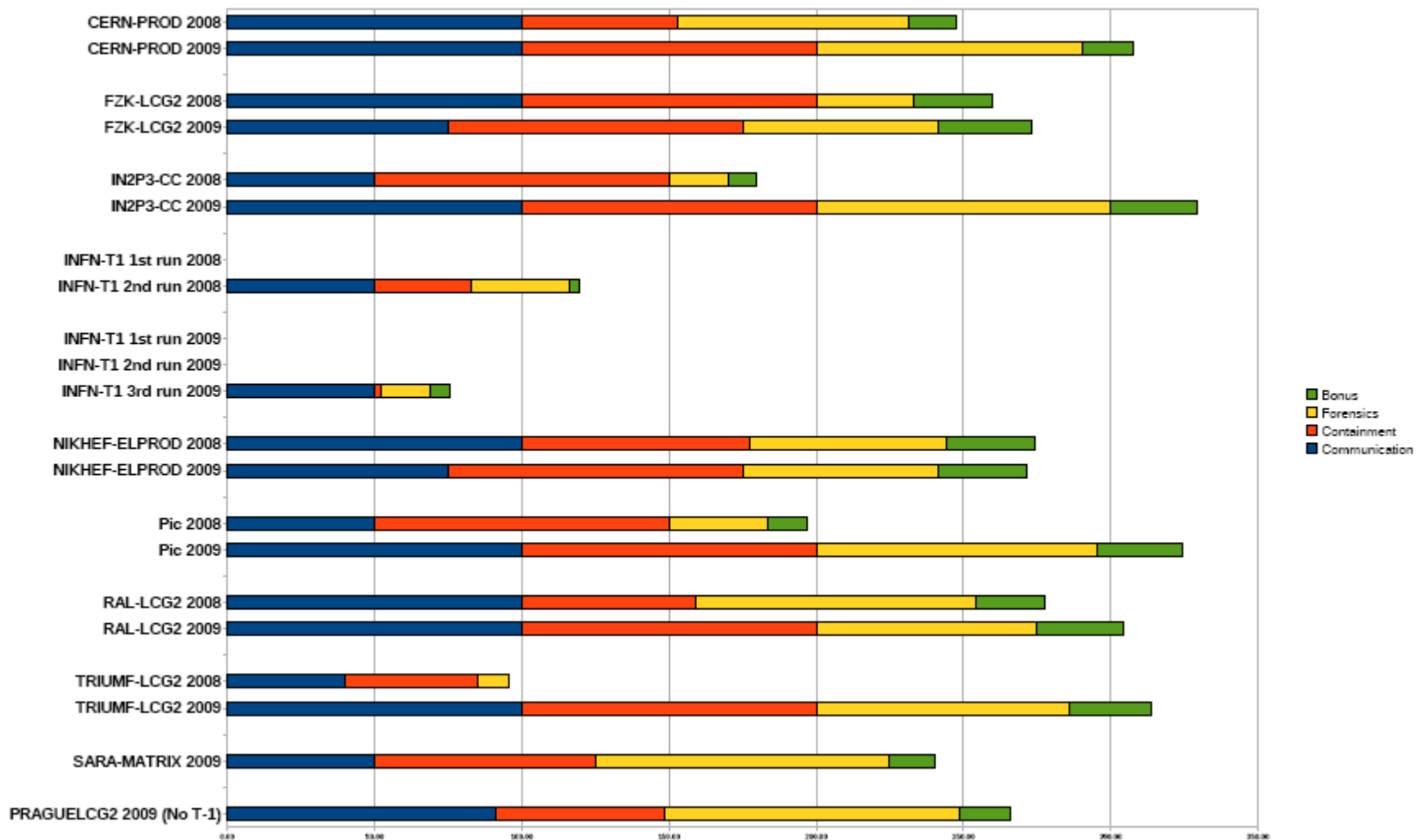
<https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge>

# SSC3 Result - UKI Tier2 Sites

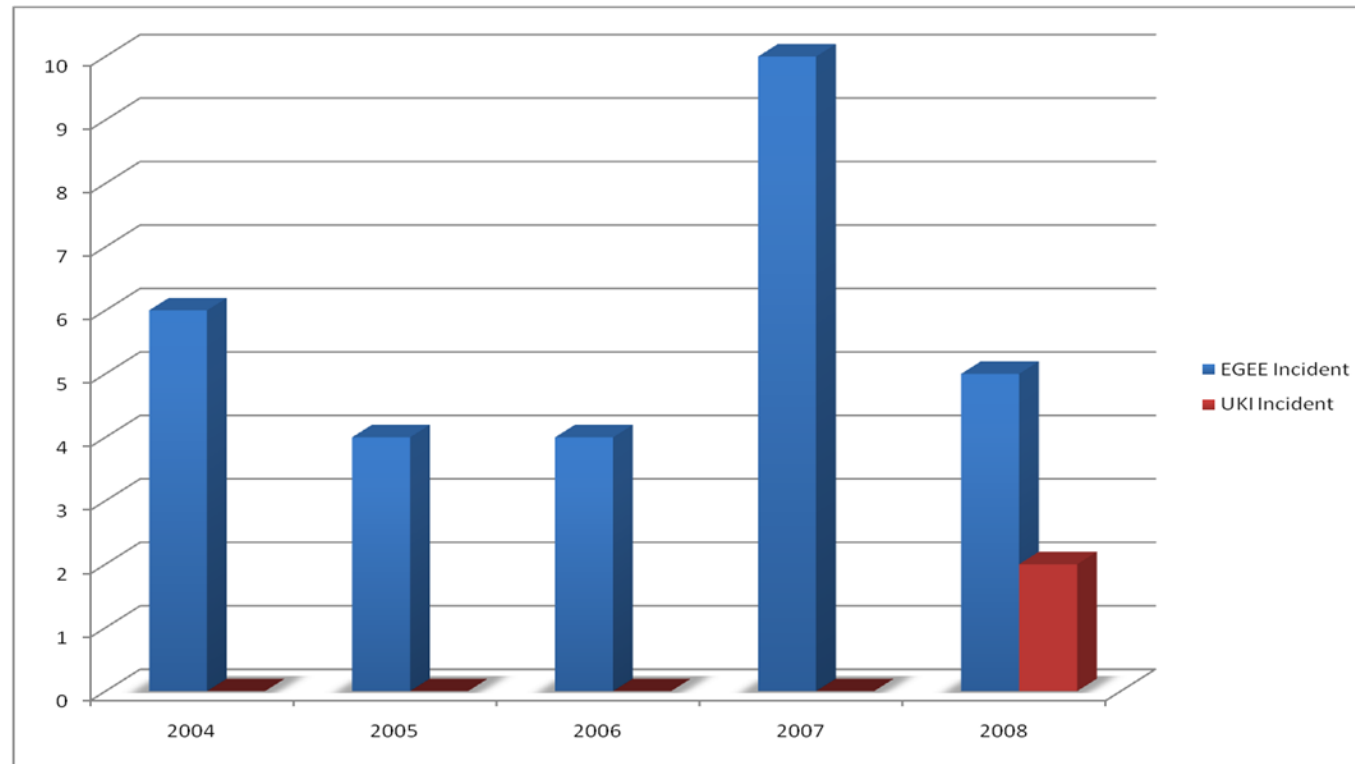


# SSC3 Result - Tier1 Sites

SSC\_3 Overview Run 2008/2009



# Grid Incident



- Of which, 2 incidents involved GridPP sites in 2008
- A few vulnerabilities such as Debian OpenSSL, Linux Kernel and DNS poisoning vulnerabilities etc.
- Some Grid middleware vulnerabilities as well

## The Grid

- Grids are not (yet) a primary target
  - Currently home users are the easier target
  - But this may change soon
- Grids are valuable to attackers
  - Large numbers of distributed hosts
  - High availability
  - High throughput network

## The Grid (cont.)

- Grids are also particularly exposed
  - Transparent access/attack propagation from one site to another
  - Large number of identical hosts
  - Heterogeneous skills, staffing and security standards
- So far no “grid incident”, where the grid is the attack vector, but ...
- It might change SOON!

# Risk?

# Unexpected

- Natural Disaster
  - Hurricanes, tornadoes, floods, earthquake;
- Terrorist Activities
  - Terrorist attack/bomb threat
- Massive widespread power outage
  - E.g. Northeast blackout 2003
  - 10 million people in the Canadian province of Ontario and 45 million people in eight U.S. states.

## Expected

- Technical failures
  - Loss of a communications line; Power failure; Internet connection failure; Mis-configuration;
- Security incidents
  - System compromised
  - Attack (e.g. DDOS) to other organizations
  - Illegal or inappropriate material;

## Potential Consequence

- Service disruption
  - One or a few sites down;
  - A partial or complete shut down in the UK;
- Damage or lose of user data
- Damage to the project/sites reputation
  - A minor incident might result in a PR disaster
- Legal/financial actions against participants

# Threat

- Highly motivated attackers, many are professional
- Organized criminal syndicate
- Highly sophisticated malwares
- User-friendly and affordable attacking toolkits
- Immense power

## An Example

- Computing Magazine on 19<sup>th</sup> March 2009
  - “Foiling a thoroughly modern bank heist”
  - Organised criminals aiming for big money (£229m)
  - Targeted attack on the bank system
  - Tailored malware sophisticated enough to avoid bank anti-virus software
- Money is not the only motivation
  - Hacktivism
    - “the nonviolent use of illegal or legally ambiguous digital tools in pursuit of **political** ends...” - Wikipedia

## Another Example

- 10 September 2008 - CMS website defaced
  - “Although the current incident was of **no technical consequence** there has been an awful lot of misinformation made available and it has generated a lot of bad publicity and has wasted an awful lot of time. Clearly the reason we were targeted, as well as the interest it generated, was **due to the publicity surrounding the start-up of LHC...** ” - David, CSO at CERN

### Lesson-learned:

- The motivation
- The timing
- The media attention and PR “disaster”

## One More

- BBC - Click program on 13<sup>th</sup> March
  - BBC paid a few thousands USDs to buy a botnet of 22,000 computers
  - To send spam
  - To launch a DDOS attack on a website
    - Only 60 machines took down a website with decent bandwidth in a few minutes

## Lessons Learned

- Know what might happen
  - Risk Assessment
  - No perfect security
- Know what to do before it happened
  - Simple, well-understood documented procedures
- Know who can help you
  - Local CSIRT team, network team etc.



## Lessons Learned (cont.)

- Communication
  - Very important to the Grid
  - Main channel via Email/Mailing list
    - Site security contacts/Tier2 Coordinators
    - Telephone?
  - Alternative Channel (Emergency)
    - JANET CSIRT
    - University CSIRTs
  - Site and local security team (e.g. CSIRT)?
  - VOs, Experiments, Users, peer grids ... ..

## Lessons Learned

- Multiple layers defence - defence in depth
  - One single mistake isn't enough to sink the ship
- Know what is going on
  - Security monitoring at different levels: host, network, site, ROC etc.
- Know what had happened
  - a central log facilities
- Know how to deal with media
  - To have a single point of contact

# Are We Ready?