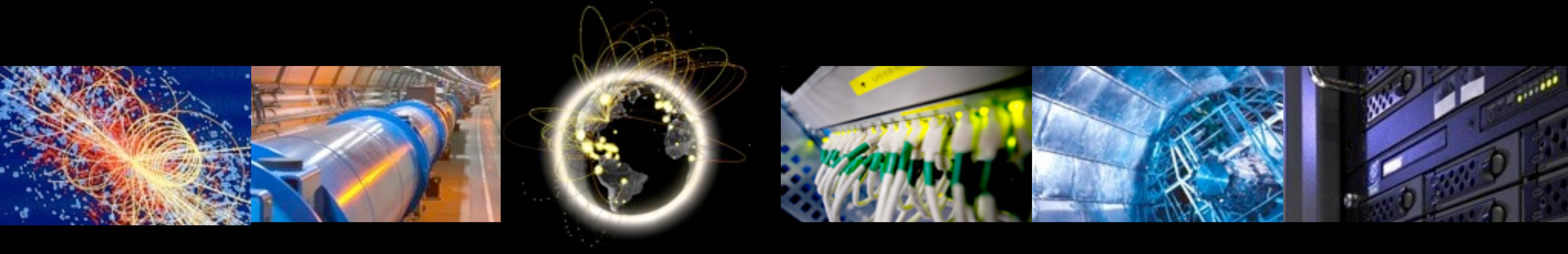
Update on the security TEG

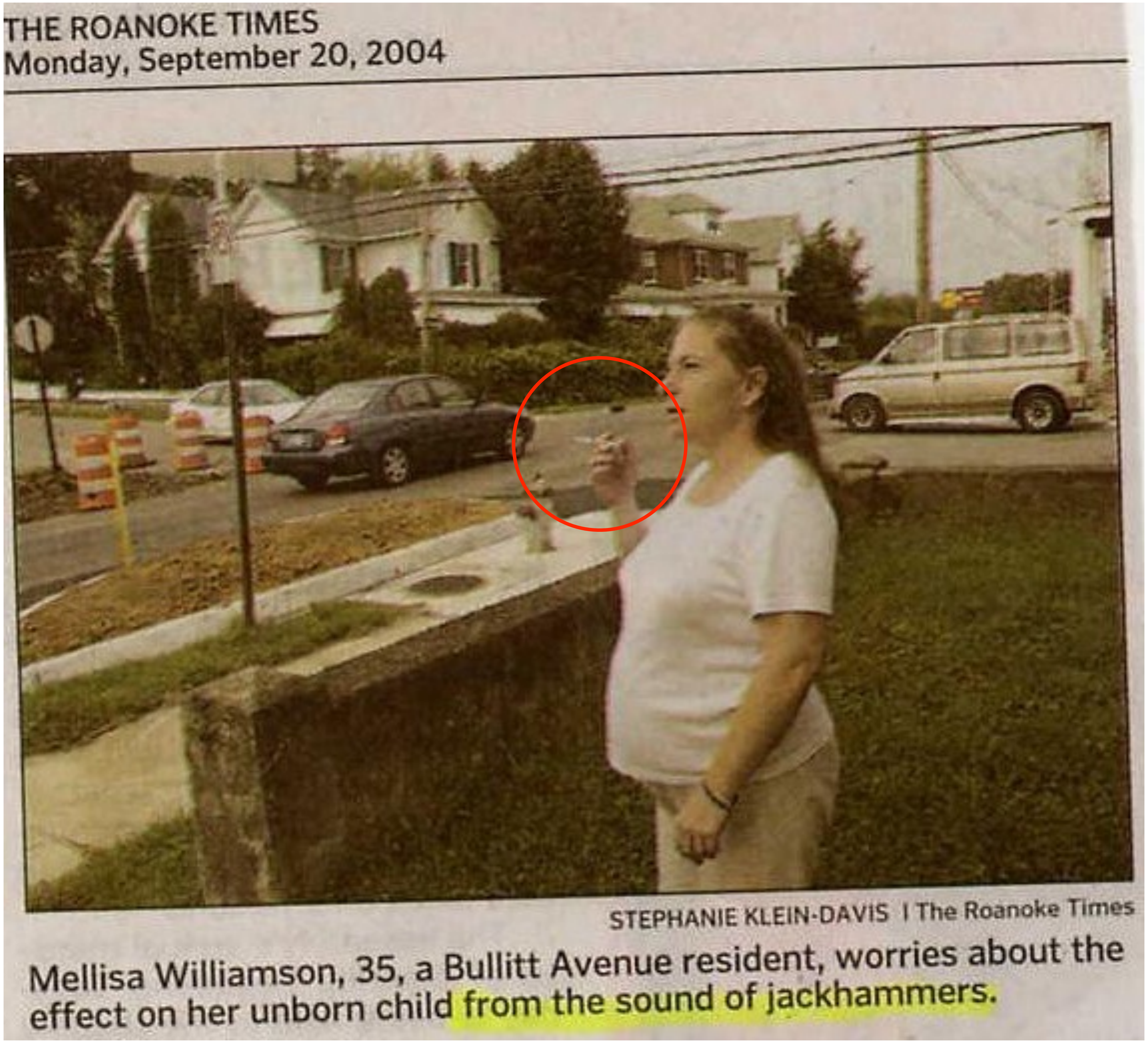
7th February 2012



General update

- Representation from the 4 LHC VOs + several sites
  - ~15 contributing members in total
- 3 face-to-face meeting so far, weekly phone meetings
- VERY large scope, covering many areas
- 5 different subtasks
  - WLCG risk assessment (in progress)
  - AAI on the worker nodes (in progress)
  - AAI on the storage systems (not started, but input has been received from the Data and Storage Management TEGs)
  - Identity federation (in progress)
  - Usability vs Security (just started)
- All details at:
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG
- A lot of feedback/complaints/frustration received....

Managing expectations



THE ROANOKE TIMES
Monday, September 20, 2004

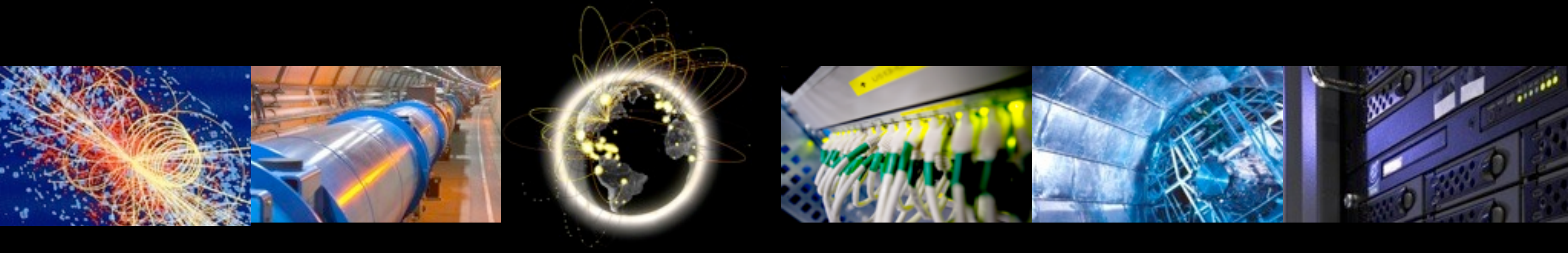
STEPHANIE KLEIN-DAVIS | The Roanoke Times

Mellisa Williamson, 35, a Bullitt Avenue resident, worries about the effect on her unborn child from the sound of jackhammers.

Managing expectations

http://www.flickr.com/photos/calavera/65098350

Risk Analysis



Risk assessment

- All services, sites, users, administrators, resources bear possible security issues
- Identify what we want/need to protect in WLCG
- Identify where the priorities should be
  - Some areas bring more risks than others
- Enable all participants to evaluate the effectiveness of a given security measure at protecting our assets

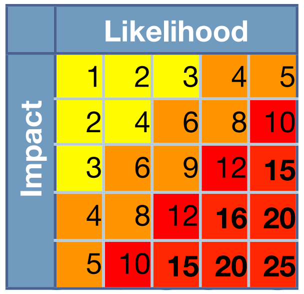
- Schneier on managing risks:
  - Too little security is too expensive
  - Too much security is too expensive
  - Aim at finding a “sweet spot”

Risk assessment

- This is a “live” document, work in progress!
- Latest version available from:
  - http://cern.ch/go/dt9S
- Objectives:
  - **[DONE]** Identify our assets
  - **[DONE]** Identify the main threats stemming from malicious intents
  - **[DONE]** Score and highlight the most important risks
    - Based on likelihood of each threat
    - Based on the typical impact of the realisation of the threat
  - **[DONE]** Discuss the risks and how they affect our assets
  - Propose recommendations for each of the risks
- All feedback welcome!

Risk scoring

- Likelihood: estimate of the number of expected events per year, mapped to a scale from 1 to 5.
- Impact:
  - Minimal impact on WLCG's ability to deliver its services
  - Minor impact, operational or financial costs, or local service disruption for less than a week
  - Serious localised disruption of some WLCG services for some users, for a week or more, leading to a productivity loss, or significant financial or operational costs
  - Serious global disruption of some WLCG services to all users, for a week or more, leading to a productivity loss, or significant financial or operational costs
  - WLCG is unable to deliver services to its users, for a week or more, or suffers risk to its funding or other business continuity issue



	Likelihood				
Impact	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	**15**
	4	8	12	**16**	**20**
	5	10	**15**	**20**	**25**

- The resulting color matters more than the resulting number

Main risks

Threat	Likelihood	Impact	Risk
Misused identities			**15**
Category 1 credentials (as defined in “Management of the risks”)			
Privileged user	2	**4**	**8**
Larger number of unprivileged users	2	**5**	**10**
Small number of unprivileged users	**5**	**3**	**15**
Category 2 credentials (as defined in “Management of the risks”)			
Privileged user	1	**4**	**4**
Larger number of unprivileged users	2	**5**	**10**
Small number of unprivileged users	2	**3**	**6**
Attack propagation between WLCG sites	**3**	**4**	**12**
Exploitation of a serious OS vulnerability	**4**	**3**	**12**
Threats originating from trust services	2	**4**	**8**
Negative publicity on a non-event	2	**4**	**8**
Insecure configuration leading to undesirable access	**3**	2	**6**
Insufficient protection of information leading to sensitive data leakage	**3**	2	**6**
Incidents on resources not bound by WLCG policies	1	**4**	**4**
Exploitation of a serious VO/middleware software vulnerability	2	2	**4**
Data removal/corruption/alteration	1	**3**	**3**
DoS from an external organisation	1	1	**1**

Credentials in WLCG

- Security depends on the typical deployment scenario
  - e.g. enabling x509 to authenticate against SSH would most likely not lead to a reduction of the number of SSH incidents.
- Two categories
  - Category 1: Where services accepting the credentials are directly accessible to an attacker. *For example username/password used to connect to an Internet service like SSH.*
  - Category 2: Where services accepting the credentials are not directly available to an attacker. Multiple ingredients are needed to obtain credentials to authenticate. *For example, the grid certificate of a user, accessible only on a host whose access requires SSH authentications with different credentials.*
- Category 1 is typically used for SSH authentication to UIs
- Category 2 is typically used by end users to generate a proxy certificate from their X509 certificate

Current summary

- Identities in WLCG is more than just x509

- Most important risks to be managed
  - Misused identities
  - Attack propagation between WLCG sites
  - Exploitation of serious OS vulnerabilities

- Containment and traceability are critical aspects there
  - Fine-grained traceability is necessary and an essential component of WLCG security
  - The only way to implement a reasonable level of traceability on multi-user systems is via physical identity switching - See next presentation
  - This is as very important step forward

Next steps

- The risk analysis will continue to evolve
  - What would be the next steps for the document?
  - Increasing part of the infrastructure managed by the experiments. Should they also conduct a brief risk assessment?
- Concentrate on the architecture and on the transition from the current system where needed
  - Difficult to steer directions at this level so far
- Work will be re-focused on producing recommendations
  - What degree of detail is needed?
  - What should be the scope of the recommendations?
  - Proposed recommendations will also depend on resources available
- Important to keep the work of the security TEG focused
  - If it becomes a catch-all for all security issues, more participation is required