Update from CSAC Aug 2008

For the new UEC members (who all know me, I think) -- if not:

I'm Martin Purschke, Physics Department, PHENIX DAQ coordinator

In my free time I'm the current chairman of BNL's Cyber Security Advisory Council (CSAC)

"The Cyber Security Advisory Council (CSAC) participates in formulating, establishing and reviewing BNL's security policies, plans and strategy, and advises the Information Technology Division Manager on security and other issues."

Most of the cyber folks are computer professionals, and have only a vague idea what scientists do... we are all sitting in front of our windows machine doing spreadsheets. Or?

That's where CSAC comes in. We actually have quite some power (in suggesting as well as vetoing) things and bump critical issues up one floor (meaning Sam, eventually, if there absolutely is no middle ground)

Status Update

I was originally asked to present here news and status about the (never-ending) Internet-in-the-Apartments story

This, however, is largely a no-news area, summer lull, etc; I prepared a few slides with a re-cap.

On the phone with Abhay, we discussed that many of you are probably only vaguely aware in which smoke-filled room BNL's cyber policies are hashed out, so I'll give a quick overview of who does what...

...and give a quick run-down of recent issues.

Internet Access in Dorms and Apartments

Several issues have caused some consternation recently.

The Facts:

The housing areas are part of BNL. The network is provided by BNL.

Users of the network are subject to BNL's cyber rules.

Traffic from there is seen as coming from BNL. It's DOE's network.

Users sign a Computer Use Agreement.

Problems:

The network is subject to filtering rules, users got spooked by the "inappropriate content" message that BNL displays when the filter thinks this is not kosher

No hard numbers on true and false positives, lots of information is anecdotal

Team housing and family members using the internet muddle the "ownership" of a given network hub -- who signs the CUA?

Recent Problems and Silver Linings

It is fair to say that the Computer Use Agreement for the Dorms/Apts has taken up a major share of meeting time for CSAC and related committees

Lots of discussions how to make the CUA least intrusive and easy to understand/follow

That was (and is) the status – that it is and will be the DOE/BNL network.

Then something unexpected happened – we had long written off external ISPs as not interested, and the “Suffolk Wireless Network” as too far in the future.

Out of the blue (think: the economy), Optimum/Lightpath signalled modest interest in wiring the apartments and try their hand in being the external ISP for the housing areas

It all comes down to hard dollars, if there is a business case, it might happen.

Initial talks between BNL and O/L, but please don't get your hopes up (yet).

The number of potential show-stopper issues are staggering – would there then be only Optimum Internet? Billing? Part of the rent? The BNL Network manager is not so optimistic that a business case remains in the end.

But I personally consider the interest by O/L a breakthrough. We'll see.

Policy Making

- You may wonder how BNL's Cyber Rules are brokered..
- First off, there's some stuff that simply gets handed down from DOE. Non-negotiable, we can only interpret and implement a rule so the impact is as small as possible
- A lot of discussion before an issue goes to full-blown CSAC takes place in the Cyber Security Policy Working Group (CSPWG).

Tom Schlagel, Chair
Martin Purschke
Keith Lally
Tom Throwe
Brett Viren
Rich Casella

Lisa Soto
Frank Quarant
Mark Sakitt
Anand Kandasamy
Alan L
Jerome Lauret

And interested others + adhoc experts on specific issues

CSPWG & CSAC

- We were inaugurated at a time when the DOE panicked and handed down a long list of so-called “Technical Management Requirements” (TMRs) (which I was speaking about about a year ago here in this forum)
- We were somewhat successful fending off the worst, and that laid the groundwork for an effective collaboration between CS and “us”.
- We meet every other Friday, although there are gaps
- Group is small enough to be effective, and has all the right experts, and is open to interested folks
- We almost always come out with a very good solution (many things are technical issues)
- Policies and rules are then resented to CSAC for discussion and comments, and, eventally, acceptance or rejection.
- In CSAC, we usually have a lively discussion; we meet each 1st Tuesday of the month

A Selection of Hot Issues

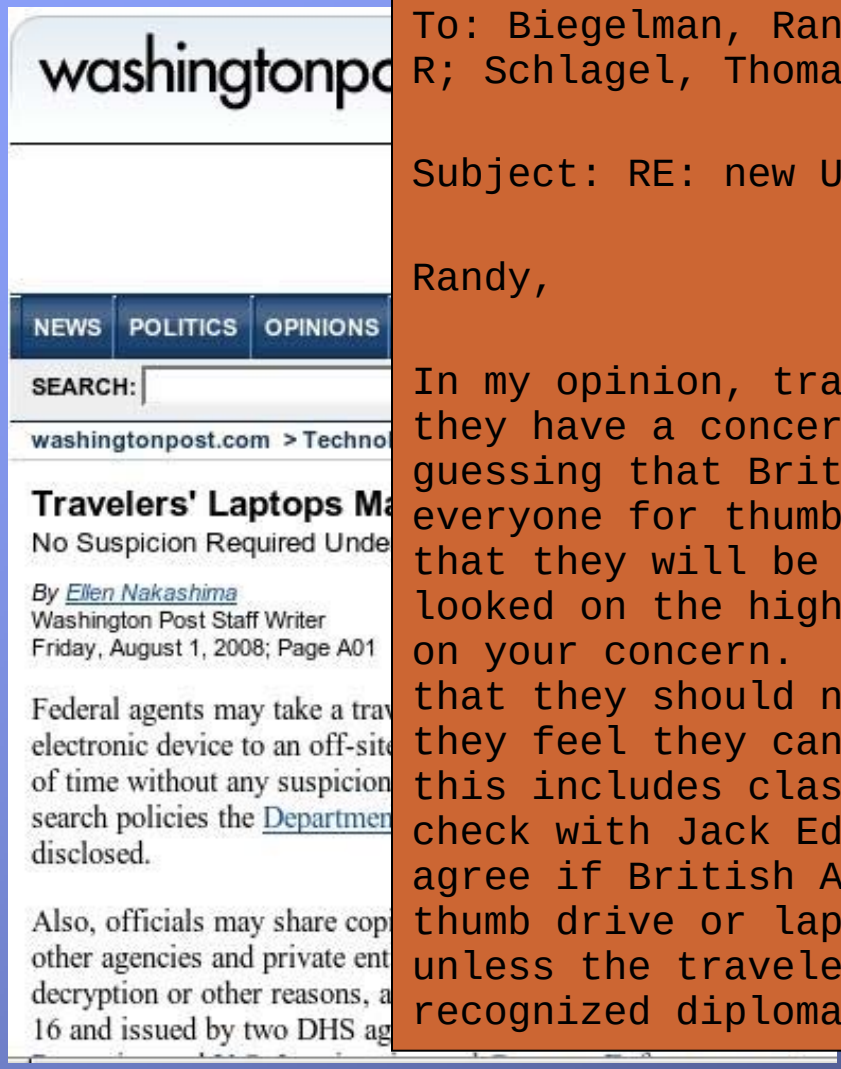
- The Computer Use Agreement,
- the Computer Use Agreement, and
- the Computer Use Agreement. Yes, that has taken *a lot* of time over the last year.
- Every sentence in there is carefully crafted, vetted by BNL's Legal Dept, some have been revised a hundred times. This was a major piece of work.
- (I am really proud of the outcome.)

- Laptop Encryption, and alternate technologies
- Guidance for travellers in light of the DHS rules w.r.t. Laptop searches/confiscations at the border, also new UK rules
- Clarifications of BNL computer seizing for suspected policy violations
- Guidance and help for foreign travellers (the China incident)
- Upcoming next week: a VPN survey to better streamline access and improve the security posture

Initiatives

- CSAC and the CSPWG often take the initiative to try to improve our life
- The items in blue on the last slide were initiated by “us”
- Some go as far as the DOE legal counsel
- We are fulfilling or role as advisors, I think

Border Laptop Searches



From the News Desk

To: Biegelman, Randy; Purschke, Martin Cc: Lally, Keith R; Schlagel, Thomas; Richards, Mitchell; Edsall, John M

Subject: RE: new UK crypto law ... guidance

Randy,

In my opinion, travelers should never take information they have a concern about being compromised. I am guessing that British officials are not going to screen everyone for thumb drives or check everybody's laptops; that they will be targeting specific individuals. I looked on the high side and found no further information on your concern. I recommend you advise your travelers that they should never travel with electronic information they feel they cannot risk being compromised. Of course this includes classified information. You can double check with Jack Edsall but, I am confident that he'll agree if British Authorities want you to un-encrypt your thumb drive or laptop, you're going to have to do it unless the travelers are traveling under some sort of recognized diplomatic status.

VPN Survey

- Another item that we brought up:
- We feel that the use of Virtual Private Networks (VPNs) is getting a bit out of hand
- Especially in light of the new BNL rule that you can work from home, we fear that employees will VPN in all the time.
- VPNs have the potential to compromise the network security (you “connect” your home PC to the internal BNL network without the safeguards)
- You funnel all access through BNL, including sites in violation of the CUA
- Using a VPN to, say, access your timecard, or filling out a purchase order, is equivalent to opening the main Swiss Bank vault just to take out change for the vending machine. More secure alternatives exist (I virtually never use VPNs)
- The (neutrally-worded) survey will give us an overview what VPNs are used for
- I (on behalf of CSAC) will send out a mail for people to participate today or Monday

Summary

- We have a very active group of people working with ITD to shape CS policies
- With few exceptions, policies and guidelines are developed with user input from the get-go
- CSAC has quite a bit of power to make the users' point of view heard
- Often, we take the initiative to ask for change, or improve services, or provide alternative, easier solutions for technical issues that affect us
- Also, we watch out for inadvertent status-quo changes

You can contact your Department CSAC rep (or me) for any issue that irks you.