Summary of the Cyber Event for the UGBoD

Mark M. Ito

February 28, 2012

At the last UGBoD meeting Sebastian asked that I summarize the Cyber Event of the Summer of '11. Some of these observations will be from my personal perspective. I was not privy to all of the details of the incident; as noted below a comprehensive report of the facts was not made to anyone outside of IT and Lab management.

The original event that alerted IT about a problem was a large amount of data being transferred out from the Lab from machines that would normally not be involved in large volume data exchanges. I will use their term and call this the "exfiltration event." This kicked off a set of actions and an investigation.

There was an compromise of two outward-facing web servers through ColdFusion applications running on them. One was a Windows machine, another a Linux machine. Allegedly, the problem was a day-one vulnerability. This happened roughly a month before the exfiltration event.

The intruders gained administrative access to several Windows machines at the Lab.

The suspicion was that intruders gained access to the Lab, took a month surveying who worked on which projects, and wanted to download technical information (drawings, specifications, etc) for their own purposes. I do not know how this was determined.

At roughly the same time a similar attack was discovered at Pacific Northwest National Lab. During the investigation, people at the Lab were consulting back and forth with people from PNNL.

There have been several reports of similar intrusions at other technical facilities.

IT decided on an ambitious plan to mitigate this and future incidents.

They instituted a more secure architecture for the internal network. This plan was mostly in place before the cyber event, but was supposed to be rolled out over a six-month period.

Access to classes of desktop machines, for example, those involved in business services, were made more restrictive. Thought was given to preventing Lab employees from inadvertently placing sensitive data on systems outside the restricted enclaves.

Public Affairs decided to restructure the Lab's web architecture. Again plans to do this had been in place, but implementation was put on the front-burner with an aggressive schedule.

IT removed user-created content being served from www.jlab.org to address data exfiltration concerns.

These plans were proposed, discussed, implemented, revised, re-discussed and re-implemented over several weeks as information from the investigation became available and problems with the initial actions were discovered.

All of this activity was occurring in "real-time". Late hours were logged by certain pieces of IT Division trying to meet aggressive deadlines, mainly Computer and Network Infrastructure (CNI) and parts of Management Information Services (MIS). Consultants from DOE arrived to help. One telling indication of the level of activity was that a coffee, doughnut, and candy bar station was established. Pizza was delivered, etc.

"User space" web sites, those served from /home/<username>/public_html directories were moved from the /home partition to a new /userweb partition and put into /userweb/<username>/public_html.

- The initial move was to dis-allow access to all public_html areas. The old public_html directories were suspect because of the possibility of intruders staging data there, thus making it visible to the outside world.
- For a while there was a plan to manually review all of the files in these directories to detect an exfiltration attempt. This was rejected as too hard to do reliably.
- The new /userweb partition was created and users were required to get approval to have access to a new public_html directory. This served two purposes:
    - Since all users in the old system had potential access to a public_html, the new opt-in system eliminated the number of such users.
    - By forcing users to move their data from the old areas to the new ones, and agree to screen their data before doing so, data staged for exfiltration had a chance of getting caught in the screening process.

IT Division had multiple audiences while they did this:

- Lab management
- DOE Office of Science
- Lab employees from outside IT Division
- Non-Lab user community
- The infiltrators
- General public

There were different concerns regarding each audience. Satisfying all of them (except the infiltrators, of course) is obviously not easy. The limited amount of communication coming from IT Division reflects this difficulty. Technical information about steps to mitigate future attacks was kept private as much as possible, to mitigate future attacks.

Information given to the user community was limited to a series of email messages announcing when and in what form services were planned to be restored.

Eight days after the event started, IT Division held a briefing in the CEBAF Center Auditorium to describe the situation to people on-site. The nature of the attack itself was described, including the data-collection period and the data exfiltration event, and a schedule for bringing systems back online was outlined. No equivalent communication was ever issued to the user community.