Community Expectations for Campus Computer and Network Security: A Wrapup

Joe St Sauver, Ph.D.
joe@uoregon.edu or joe@internet2.edu
Internet2 Security Programs Manager

Wednesday, November 3rd, 2010, 10:30-11:45AM, Wilton
Internet2 Member Meeting, Atlanta GA

http://www.uoregon.edu/~joe/expectations-wrapup/

Disclaimer: The opinions expressed are those of the author and do not necessarily represent the opinion of any other party.

Introduction

- We've been having a conversation about community expectations for computer and network security at both the April 2010 Internet2 Member Meeting and the July 2010 Joint Techs Meeting.

  If you participated in those sessions, thank you!

- For those of you who may not have been able to participate in this conversation until now, let's begin by taking just a few minutes to recap how this whole effort began...

The Original Campus Expectations Task Force

- The original charge for the Campus Expectations Task Force (CETF), circa 2005, was described by Bill Decker, head of the Task Force, in a talk he did for the Fall 2005 Internet2 Member Meeting, see www.internet2.edu/presentations/fall05/20050920-cetf-decker.ppt

  Articulate a current set of expectations for what it means to be an Internet2 member campus.
  - *Consider focusing on what the campus infrastructure needs to be 2-5 years out in order to support advanced applications.*
  - *Areas considered should include campus network configurations, campus directory implementations, privilege management, data storage, image transfer/management, computation,* ***security,*** *campus bandwidth management, collaboration environments, and others.* [JES-emphasis added]
  - *Consider the responsibilities that come with supporting sponsored participants and SEGPs.*
  - *A series of case studies that illustrate the best practices of campuses in resolving these issues will also be created.*
  - *Seek input from a broad range of constituency groups, including but not limited to CIOs, application developers, GigaPoP operators, network engineers, support staff, faculty, researchers and other users.*

Expectations Function #1: Minimum Standards

- It was clear by 2005 that it made little sense to have a high speed nationwide backbone (such as Internet2), if existing campus or regional networks were slow and congested, or if key servers and researchers were only connected via 10Mbps chokepoint links.
- Put another way, if you made the effort to connect to an advanced national R&E network, other sites might reasonably expect that your network had more than just "vanilla IPv4" capabilities, perhaps including the ability to support advanced network protocols such as:

  -- IPv6,
  -- IP multicast, and
  -- jumbo frames (e.g., 9K MTUs)

Expectations Function #2: Keeping Us All Stretching Just A Bit

- The CETF process was also envisioned as serving an important "forward looking" role, going beyond just saying "where should we be now?" to laying out "where should we be two to five years from now?"
- In the simplest of terms, if campuses had 100Mbps backbones in 2005, we needed to be actively working to get upgraded to gig backbones, while planning for 10 gig backbones (and maybe even doing basic research needed to make 100 gig backbones a reality when they're needed)
- The general expectation was/is that we should be "challenging" ourselves at least just a little; Internet2 shouldn't be just about living comfortably at a currently adequate but not exceptional level.

Note: Not All Expectations Were Purely Technical

- While some expectations were technical, others were not.
- One might also expect organizational commitment to advanced networking, including support from institutional executive management, appropriate institutional financial commitments, commitment of personnel and facilities, etc.
- Metaphorically, if you were going to be part of the "club," you were expected to actively participate, making a reasonable effort to "stay up with the pack" and to contribute to advancing the good of the order.
- Explicit articulation of community expectations has the potential to serve an important normative function, allowing people to identify areas where success has already been attained locally, and areas where more effort is still required.

Expectations Also Served to Reassure

- For instance, note the explicit reference to supporting SEGPs and sponsored participants in the original charge.
- At the time that charge was prepared, there were worries that when Internet2 allowed connection of state K12 networks (as SEGPs), or smaller institutions with less of an instituional emphasis on advanced networking (as sponsored participants), that that step might result in the creation of substantial new operational burdens, burdens which might be born by the community as a whole rather than by the sponsored or sponsoring site.
- Of course, in retrospect, we know that anticipated deluge of potential problems didn't occur, but at the time, some were worried and wanted reassurances.

Expectations Also Were Meant to Educate, And To Be Demonstrably/Provably Attainable

- In particular, the case studies mentioned in the charge were meant to illustrate how members of the community were actually meeting the community's articulated expectations, thereby showing peer institutions at least one proven path that presumably could also be replicated by others.

- "Let me show you what we did. When you check out what we did, you'll see that it's worked well for us."

- Those are the sorts of things that were originally envisioned (or at least that's my recollecton)

The CETF Final Report Was Issued Spring 2006

- A final report from the CETF was produced in Spring 2006, and remains available online at http://www.internet2.edu/files/CETF-FinalReport.pdf

- A discussion of that final report is also available, see http://www.internet2.edu/presentations/spring06/200604225-cetf-decker.ppt

- Somewhere along the line, though, we all got a little distracted, and work on shared community expectations got postponed or deferred, even though the need for shared community expectations was ongoing (and we never got any security expectations articulated!)

Fast Forward Now to The Fall of 2009

- In the Fall of 2009, during discussions of the Internet2 SALSA Security Advisory group, the issue of community expectations came back up, with input from SALSA members including members of the Applications, Middleware and Services Advisory Council.

- Consistent with Internet2 Strategic Plan Tasks G ("Implement Security Best Pracatices") and J ("Cooperate on Security Challenges"), the Internet2 community has been working with Educause and the REN-ISAC in providing security information to our colleges and universities.

- But that information has been informative/descriptive, not normative/prescriptive.

So What *Does* The Internet2 Community Expect?

- During sessions at the April 2010 Internet2 Member Meeting in Arlington Virginia, as well as at the July 2010 Joint Techs Meeting in Columbus Ohio, we held sessions at which participants shared their expectations for system and network security.
- Our role in that process was one of convening those sessions and facilitating the brainstorming process, and now we want to bring you a summary of what we think we heard for your review and validation.
- So with no further ado, let me tell you about the ten items making up those draft community expectations. (I've got printed copies of these expectations for you, too)

The Draft Community Security Expectations

"All Internet2 members should strive to meet community computer and network security expectations.

"Specifically, Internet2 members should --

* Have an **information security officer** and an adequately staffed information security team with executive management support, real operational authority, and sufficient budget.

* Have a comprehensive institutional **information security plan** (including information classification and PII stewardship policies), and an acceptable use policy (AUP).

* Firewall important administrative assets at the subnet level (as may be required by PCI-DSS and similar policies, and by audit practice), but **minimize or eliminate firewall obstacles** in front of non-administrative research and education users to preserve network transparency and protect network performance (encourage hardening at the host level)

* Have a site-wide **intrusion detection capability** (Snort, Bro, etc.), and be prepared to address any compromised systems.

* Be prepared to **cope with malware**: promote alternative operating systems; site license an antivirus product; facilitate patching of all software; offer help for infected users, including potentially deploying quarantine networks for online self-remediation of infected hosts, etc.

* **Manage password authentication**: deploy scalable institutional identity management/federated authentication; secure any apps still using unencrypted passwords; offer two factor auth for high security scenarios; secure the password reset processes.

* **Harden DNS** at your site. At a minimum, you should control any open recursive resolvers and work to develop a plan for deploying DNSSEC.

* **Control emission of spoofed network traffic** (do BCP38 filtering at the subnet level and at your network border).

* Work to **overcome potential security objections** that might inhibit deployment of critical advanced networking services (such as IPv6).

* Be active in the information security community, including participating in the **REN-ISAC**.

[Note: these items are not listed in priority order; all items should be considered equally important]

Discussion

- **I'd like to spend most of the rest of this session talking about the draft list of ten items, and then spend a little time talking about potential next steps.**

- ***Are*** these the right items? Did we miss anything critical? If so, what? If we do need to add something that's not there now, what existing item should we remove to make room for that new item? (I'd really like to see us resist the urge to increase the size of that list – I think it's very important that we keep the size of the security expectations list to a doable (and not overwhelming!) size, at least for now).

- Have we described the expectations in a useful way? Is there any "wordsmithing" we need to do?

Next Steps

- Assuming we have the right set of community expectations, the next step will be to run these security expectations past some additional entities:

  -- Internet2's Security Advisory Committee (SALSA)
  -- Internet2's Network Technical Advisory Committee
  -- Internet2's governance councils, including the Applications, Middleware and Services Advisory Council
  -- Internet2 senior management, and
  -- The Internet2/Educause HEISC (Higher Education Information Security Council).

- We hope those groups will endorse the security community expectations document, and work with all of us to promote progress toward sites meeting those expectations.

Case Studies

- Once we have the community aligned behind a common set of expectations, we'd also like to develop some case studies that illustrate how Internet2 sites are meeting each of these expectations.

- Would any of you be interested in working on those case studies?