If you haven't seen Lightweight Portable Security (LPS), you ought to take a look at it. It's a bootable "hardened" Linux CD that the Air Force Research Lab put together and got approved for use. It allows users to process sensitive information on their EOIS (home computers) and access restricted websites and networks.

There are two versions of LPS:

- LPS-Remote Access is approved for telework and has an Army CoN. For use at a given installation, the Air Force will create a custom build that has VPN info, remote desktop client software, etc., hard-coded in.

- LPS-Public Edition allows users to access AKO, OWA, etc., from their home computers. It contains CAC middleware and drivers for the common USB CAC readers. It's also a great tool for non-government use (e.g., banking from home, browsing websites which may be malicious, etc.). It comes with a web browser and, if desired, OpenOffice.

More info at http://www.spi.dod.mil/lipose.htm. Below is an e-mail I sent to my command's IA folks recently; it references a couple of good articles about LPS.

May be time for DoD and DA policy to be updated a bit ...

Vr,

Ed

IA folks,

We've been tracking the U.S. Air Force's development and accreditation of a Linux bootable distribution known as Lightweight Portable Security (LPS) since last May. If you're not aware of this software, I recommend you read about its two flavors and consider how they can be beneficial for your users. Here's a brief description from the Government Computing News Oct 2010 issue:

"LPS is a simple, inexpensive tool to create trusted endpoints for government and the public. It is bootable, open-source software that can be used with most Windows, Macintosh or Linux computers to create a nonpersistent trusted end node for secure browsing, cloud computing or network access. It boots a Linux operating system from a LiveCD and installs nothing on the client computer, running only in RAM to bypass any local malware and leave no record of the session" (http://gcn.com/articles/2010/10/18/gcn-awards-air-force-lightweight-portable-security.aspx).

In other words, LPS allows personally-owned or public computers to connect to restricted government websites and networks. No data from the session is saved to the computer's hard drive. In addition to the GCN article, there was a good article in an IATAC IAnewsletters last spring (see page 42), and the LPS website contains a lot of information (http://spi.dod.mil/lipose.htm). Here's an excerpt from the IATAC article:

"Because LPS-Public operates only in Random Access Memory (RAM), users may visit risky, malware-infected sites with very little permanent risk. Likewise, user's private sessions and sensitive transactions occur within a leave–no–local–trace browsing environment. LPS-Public provides a thin, secure, end-node for cloud computing. Created by the Software Protection Initiative at the Air Force Research Laboratory (AFRL), LPS-Public boots from a CD, runs only in RAM, installs nothing to the hard drive, and does not require administrative rights. LPS-Public provides a Firefox browser with plug-ins, CAC middleware, certificates, and a PDF viewer within a very thin Linux operating system. It's a great solution for users with Mac, Linux, or Windows 7 systems, or those using others' computers.

A derived and accredited version, LPS-Remote Access, offers teleworkers remote desktop virtualization of their company's or agency's network. This means far fewer government laptops. Now one only needs to carry a CAC-reader and a custom CD and then use almost any personal, public, or corporate computer to use a NIPRNet computer remotely."

I can see a lot of uses for LPS:

- teleworkers could use it to connect to their installation LAN

- distance learning students could use it to access restricted websites securely from their home computers. Since LPS comes preconfigured with CAC reader drivers and middleware, the students wouldn't have to learn how to install and configure them

- intel personnel and students studying foreign languages could use it to browse websites that are likely to contain malicious software

- if TDY personnel with government laptops used LPS to connect through hotel or airport networks, they wouldn't have to worry about the Road Warrior BBP requirement that "DAAs and SAs shall check any IS that has been on travel or was connected to an external or untrusted network for ... contamination"

- personnel could use LPS at home or while travelling to conduct on-line banking or other activities which could compromise their personally-identifiable information if the computer's hard drive contained malware

The Government Remote Access Edition (LPS-Remote Access) just received Networthiness approval (i.e., a Con).

Vr,

Ed

Ed Rietscha
Information Assurance Program Manager / Director,
U.S. Army Training and Doctrine Command

(757) 788-3653
DSN 680-3653