Bowie Seniors Computer Club Minutes for February 5, 2015 Meeting

Carl Bulger presided.

New Member: Anita Babb

Presentation: Lightweight Portable Security by Glenn Bock, a NASA Goddard rocket scientist who works on the Integration and Testing of Hardware. His email is homsar44@gmail.com


Photo courtesy of Dennis Edgington

Glenn offered the outline of his talk on the following website: goo.gl/xvdszC This is Google's equivalent of tinyURL. Copy this into the URL address box of your browser and it will automatically convert to the very long URL of the site where he stored his talk.

On the webpage are three different versions of his talk. I've selected the second one and downloaded it here. It is an outline of his complex talk, which I will comment on slide-by-slide.

Apparently he calls our club the "Thursday Computer Club".
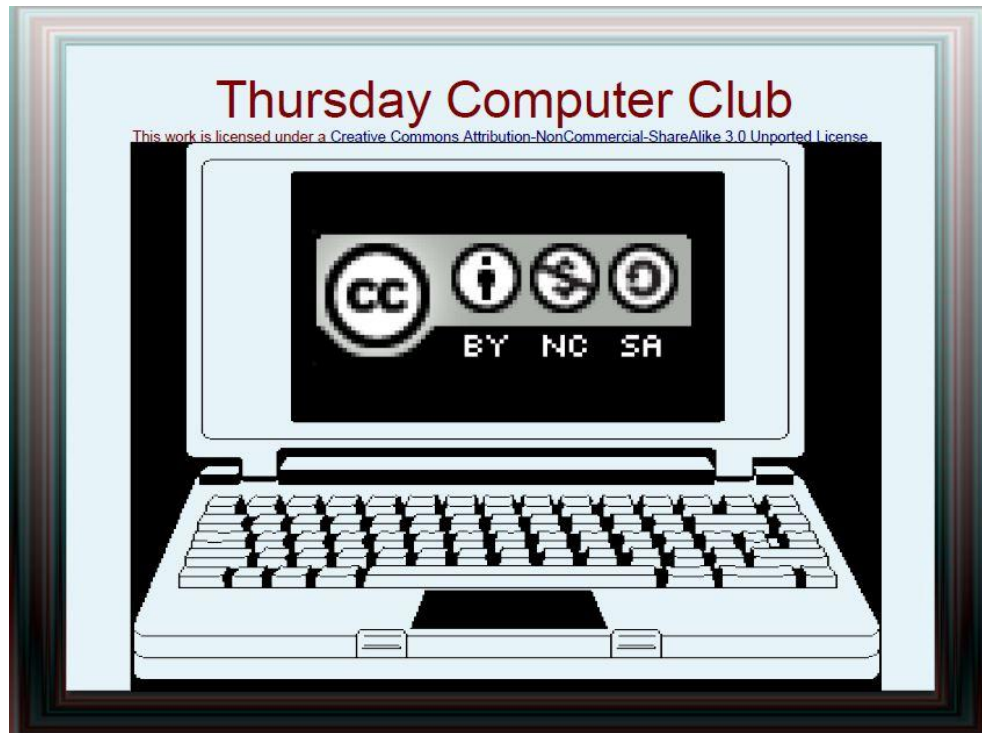
goo.gl/xvdszC is the Google equivalent of tinyURL for his webpage. If you have a smartphone with a camera and the QR app, you can take a picture of the QR pattern to take you to the website.

goo.gl/xvdsz<u>C</u>

The three MAIN topics of his talk. He added more, as you will see.

Tonight's Topics

- Lightweight Portable Security – RAM OS
- Nokia Lumia 520 off-contract smartphone
- Virtual Private Network (VPN)

Lightweight Portable Security is a DOD-developed Linux-based program that can be copied to a CD/DVD or a flash drive which then can be inserted in any computer to boot it up without accessing the hard drive, thus minimizing the possibility of encountering malware or harming the computer. Go to **spi.dod.mil** for a more detailed explanation of the organization and the application. Here you can download the public version of Lightweight Portable Security (LPS) and the Encryption Wizard.

A **live CD**, **live DVD**, or **live disc** is a complete bootable computer installation including operating system which runs in a computer's memory, rather than loading from a hard disk drive; the CD itself is read-only. It allows users to run an operating system for any purpose without installing it or making any changes to the computer's configuration. The functionality of a live CD is also available with a bootable live USB flash drive, or even an external USB drive. Ref: http://en.wikipedia.org/wiki/Live_CD

Don't use computer's installed OS

Boot computer from CD or USB with a
LIVE-CD operating system

A great idea for HOME online banking too

Take an old computer that doesn't even HAVE
a hard drive on travel, do everything in Cloud.

More on Lightweight Portable Security. An ISO file is a binary (.iso) file that is used to burn a bootable image to a CD/DVD or a flash drive. The CMOS Boot sequence is the boot sequence in the BIOS or UEFI. CMOS=Complementary Metal-Oxide-Semiconductor refers to the chip that stores the BIOS=Binary Input-Output System, or in the latest generation of computers, the UEFI=Unified Extensible Firmware Interface. A "keyring" is an electronic collection of images of your customer loyalty cards (grocery, drugstore, office supply store, electronics store, garden supply, etc.)

Lightweight Portable Security

- Free & updated several times a year
- Download ISO file, burn to CD, install USB boot
- Change CMOS Boot sequence to include CD/USB
- RAM Only, leaves Hard-Drive completely unused
- If machine happens to be infected, less threat
- Excellent compliment to "Cloud" Posture
- Strongly consider for banking & email from HOME
- Boot to generate new passwords & keyrings
- Use this exclusively on Public WiFi

The Lightweight Portable Security **desktop**
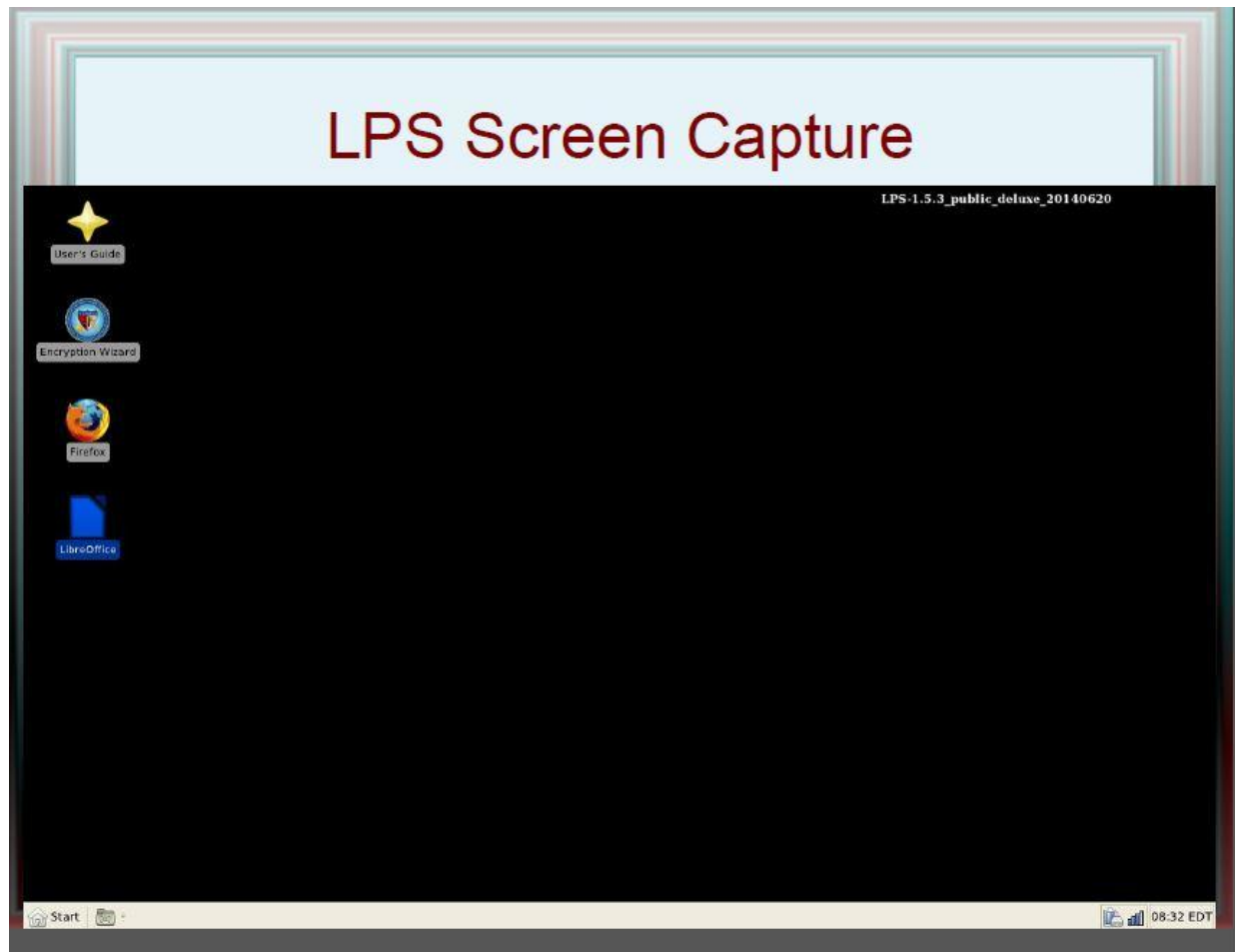
LPS "desktop" populated with several applications.
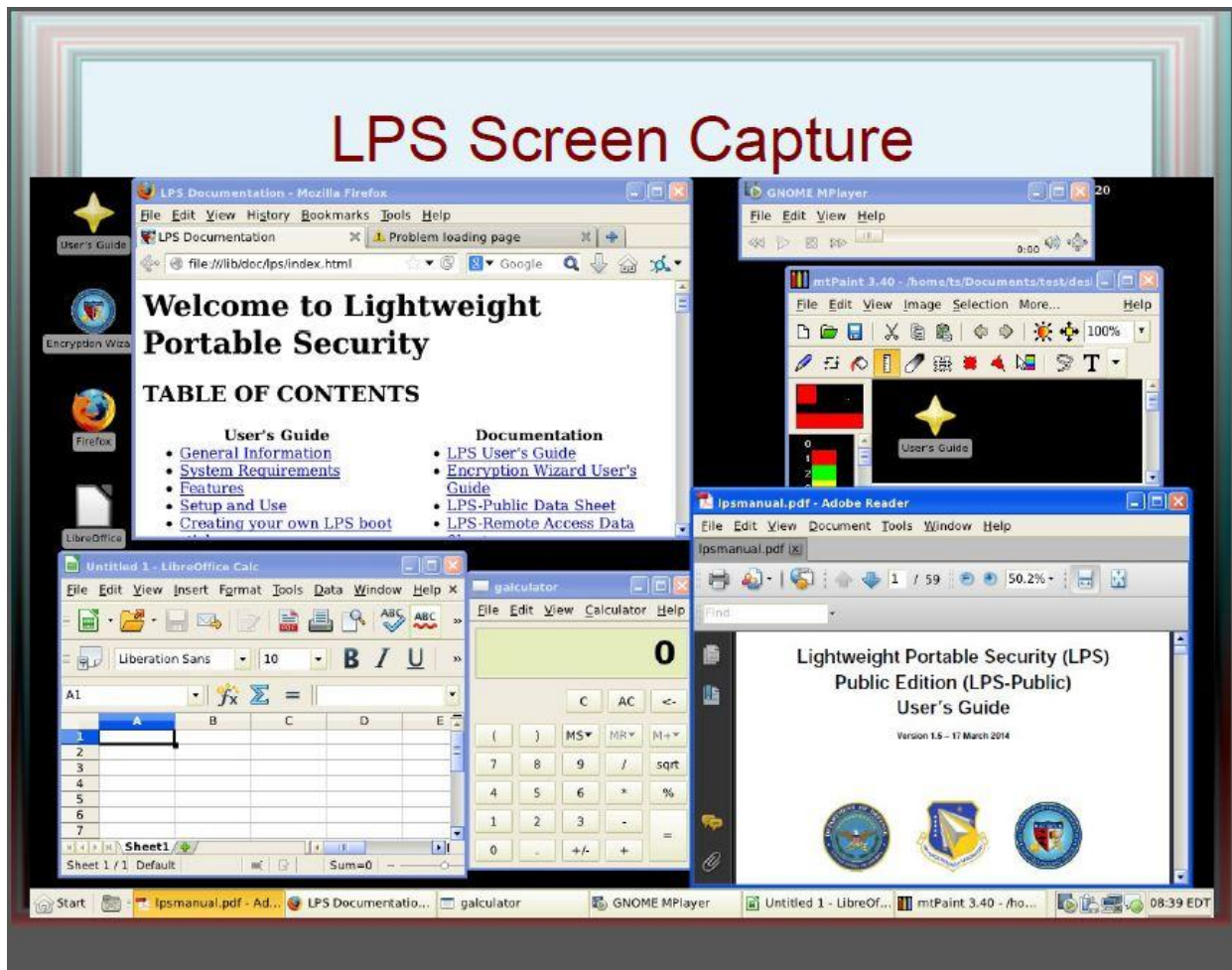
Nokia Lumia 520 Smartphone. Glenn's portable telephone is a small prepaid flip phone, but for modern smartphone functions, he uses a Nokia Lumia 520 Smartphone which you can buy from Amazon as an AT&T GO phone. He hasn't activated the SIM card; so he doesn't require a contract. He uses the wireless capability of the phone and the other functions (camera, GPS, web browser, etc. Nokia was bought by Microsoft, so this phone has a Windows 8.1 operating system. For a review of the phone: http://www.hardwaresecrets.com/article/Nokia-Lumia-520-Smartphone-Review/1861 You can buy it from Amazon for $40 http://www.amazon.com/Nokia-Lumia-520-GoPhone-AT/dp/B00E45043A or its successor Nokia Lumia 635 for $50. Glenn recommends the Reiko case for about $6 and a 32GB or 64GB memory card for storing pictures, etc.

Nokia Lumia 520 Smartphone

- Create live.com email/account
- Calendar, One-Note, GPS, Maps, Bing search engine, web-browser, app-store, (wallet if you want pay apps), MP3 Player, auto-sync podcasts
- Also available through regular internet
- Comes with micro-USB 120VAC charger

Nokia Lumia 520 Smartphone

- Available off-contract
- Pay-as-you-go "Go Phone" AT&T
- I only use as a WiFi device, never activated
- Available $30 amazon.com
- Suggest 32G or 64G memory card

Nokia Lumia 520 Smartphone

Nokia Lumia 520 Smartphone

- GSM/HSPA Phone
- Dual Core 1 GHz Qualcom MSM 8227
- 8G (SD card up to 64 G)
- WiFi 802.11 b/g/n
- GPS/Glonass
- Bluetooth
- FM Radio receiver (headphones antenna)
- 1430 mAh battery

Nokia Lumia 520 Smartphone

Click on https://proxpn.com for an advertisement of a Virtual Private Network available for free and an explanation of its advantages.

VPN = Virtual Private Network

- Encrypts all content transiting through local wireless/wired carrier.
- You exit at the other end, typically the company's server.
- Protects you from snooping and 'fire-sheep' type attacks
- https://proxpn.com/   Twit50 offer code

Backup Slides

- Multi-Factor Authentication

- Proxy

- Useful Firefox add-ins

Multifactor Authentication. **Multifactor authentication** (MFA) is a security system that requires more than one form of **authentication** to verify the legitimacy of a transaction. Glenn Bock noted that fingerprint images can be stolen, so don't depend on them. Passwords should be at least 16 characters including upper and lower case letters, numerals, and special characters. For those you can't remember, use a password manager such as RoboForm, LastPass, etc.

Multi-Factor Authentication

1. Know   **memorized** password
2. Have   phone application, device
3. Are   fingerprint, biometric
              (UPEK software fail & Disney)

4. They know You *or* You know Them,
   (typical of password recovery)

The remaining slides are either self-explanatory or you can go to the websites for more info.

Second Factor Application: Phone

Second Factor Authentication application. The number changes every 30 seconds, so even if someone steals password, you still deny them access.

Second Factor Device

Developing standard: user buys and can use with Chrome browser and Google-Mail. More adoption expected across industry.

My Mozilla modifications & Add-ins

'browse' to about:config
Search "privacy.sessionstore.privacy_level"
Change 0 to 2

Install:
HTTPs everywhere: https://www.eff.org/https-everywhere
Netcraft Anti-phishing toolbar: http://toolbar.netcraft.com/
Web-of-Trust tool: https://www.mywot.com/
NoScript: https://noscript.net/
Lightbeam: https://www.mozilla.org/en-US/lightbeam/

Privacy Badger: https://www.eff.org/privacybadger

HTTPS Everywhere

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM

HTTPS Everywhere

HTTPS
Everywhere

FAQ

Report Bugs /
Hack On The
Code

Creating HTTPS
Everywhere
Rulesets

How to Deploy
HTTPS Correctly

HTTPS Everywhere is a Firefox, Chrome, and Opera
extension that encrypts your communications with many
major websites, making your browsing more secure.
Encrypt the web: Install HTTPS Everywhere today.

**Install in
Firefox**
Version 4 Stable

**Install in
Firefox for
Android**
Version 4 Stable

**Install in
Chrome**
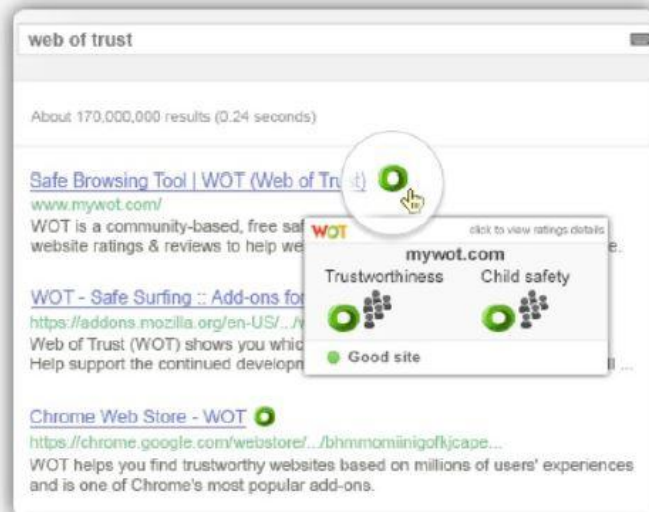Beta Version

**Install in
Opera**
Alpha Version

Netcraft Anti-Phishing Bar

WOT : Web of Trust

Hover over the bubbles for more information

web of trust

About 170,000,000 results (0.24 seconds)

Safe Browsing Tool | WOT (Web of Trust)
www.mywot.com/
WOT is a community-based, free safe
website ratings & reviews to help we...

WOT - Safe Surfing :: Add-ons for
https://addons.mozilla.org/en-US/.../w
Web of Trust (WOT) shows you which
Help support the continued developm...

Chrome Web Store - WOT
https://chrome.google.com/webstore/.../bhmmomiinigofkjcape...
WOT helps you find trustworthy websites based on millions of users' experiences
and is one of Chrome's most popular add-ons.

WOT
click to view ratings details
mywot.com
Trustworthiness   Child safety

● Good site

Rating symbols

Reputation icons are shown on popular
search engine results, social media
platforms, online email, shortened URLs,
and many popular sites.

They show how much other users trust a
site. Ratings are based on information from
millions of users and trusted third-party
sources.

No rating   Poor   Good

Very poor   Unsatisfactory   Excellent

NoScript

Mozilla Firefox Multiple Vulnerabilities

SA39240
2010-03-31
2010-04-05

1,251 view
0 comments

Highly critical
Security Byp...
System acces...
From remote

About NoScript...
Options...

Allow Scripts Globally (dangerous)
Allow all this page
Temporarily allow all this page

Untrusted

Allow secunia.com
Temporarily allow secunia.com

Lightbeam

Proxy

- Http can expose your traffic on Open WiFi

- Search Engine startpage.com offers proxy

New York, NY - National **Weather** Service
www.**weather**.gov/10001 - View by Ixquick Proxy - Highlight
New York City, Central Park (KNYC) ... New York, NY Local Forecast Office.

- Ixquick creates a tunnel to the page

start
page™ Proxy   nws weathe   Opening page via proxy...   Back   Unproxy

Press Release Newsletter update

Bowie Senior Center Computer Club Topics
Thursday, February 5 Noon-1:00 p.m.

Useful Windows Links

Keep the following up to date with current patches:

Windows (turn ON automatic updates)

Any Adobe product (UNinstall if not actually using: Acrobat Reader, Flash, Shockwave. Replace Reader with Foxit-Reader more secure http://www.foxitsoftware.com/Secure_PDF_Reader/ or even better, just view using Firefox's ability to display PDFs itself in a browser)

Java, uninstall unless REALLY need it, remember upgrading does NOT remove the malware prone previous versions, you have to manually uninstall them all! At the very least, disable Java in the browsers.

Keep anti-virus up to date, AVG, or MS-Security_Essentials
  (also download and use MSERT.exe
http://www.microsoft.com/security/scanner/en-gb/default.aspx)

Use HTTPS-Everywhere: (turn on the observatory or use Certificate Patrol)
https://www.eff.org/https-everywhere

Useful Windows Links

Add the link for AARP things happening in your neighborhood
Make a few slides of the social engineering techniques

Online Updates and references:
https://www.us-cert.gov/
http://www.verizonenterprise.com/DBIR/
https://www.onguardonline.gov/