PWC G8 Gals@Technology

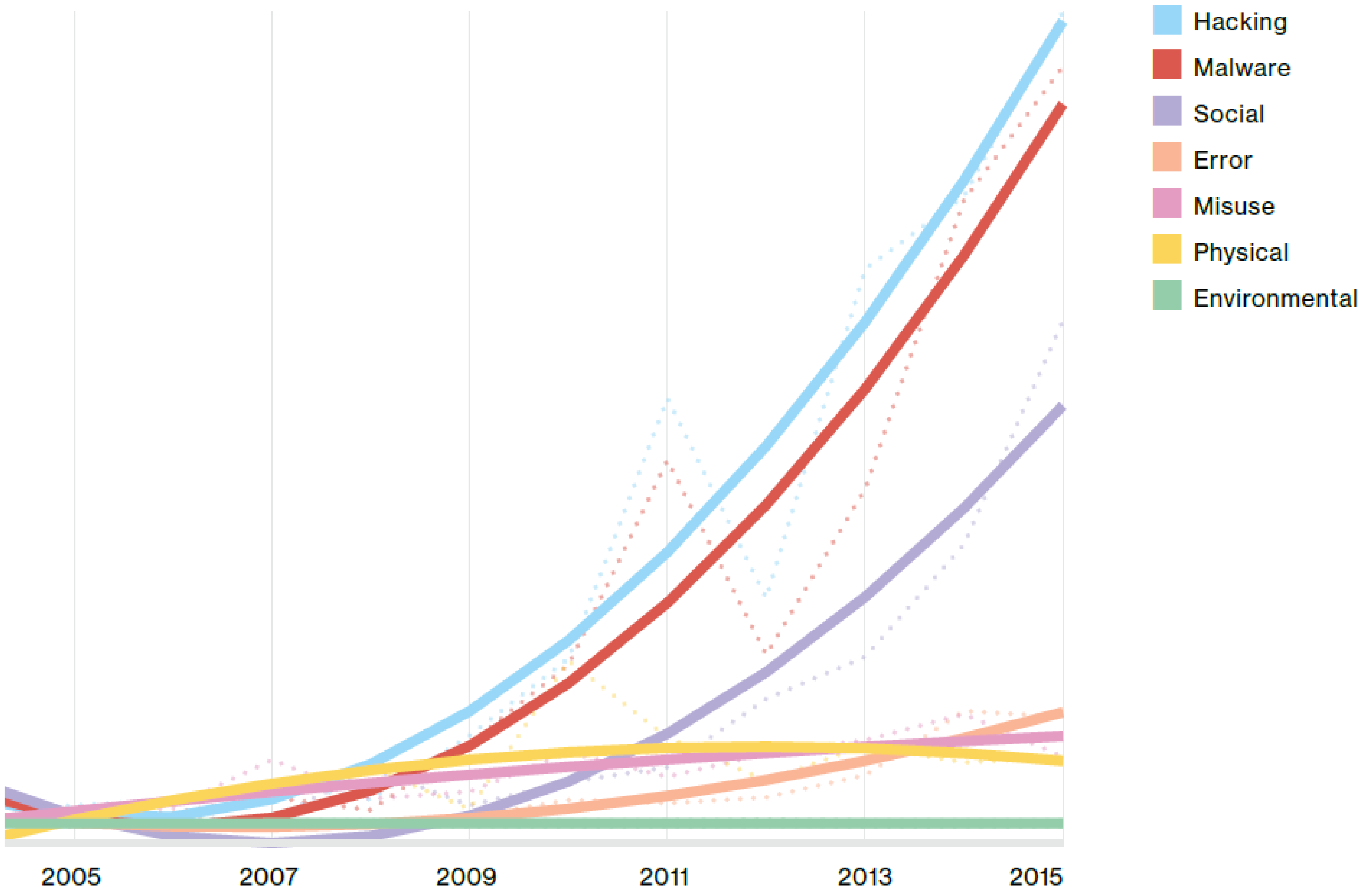
Security Update

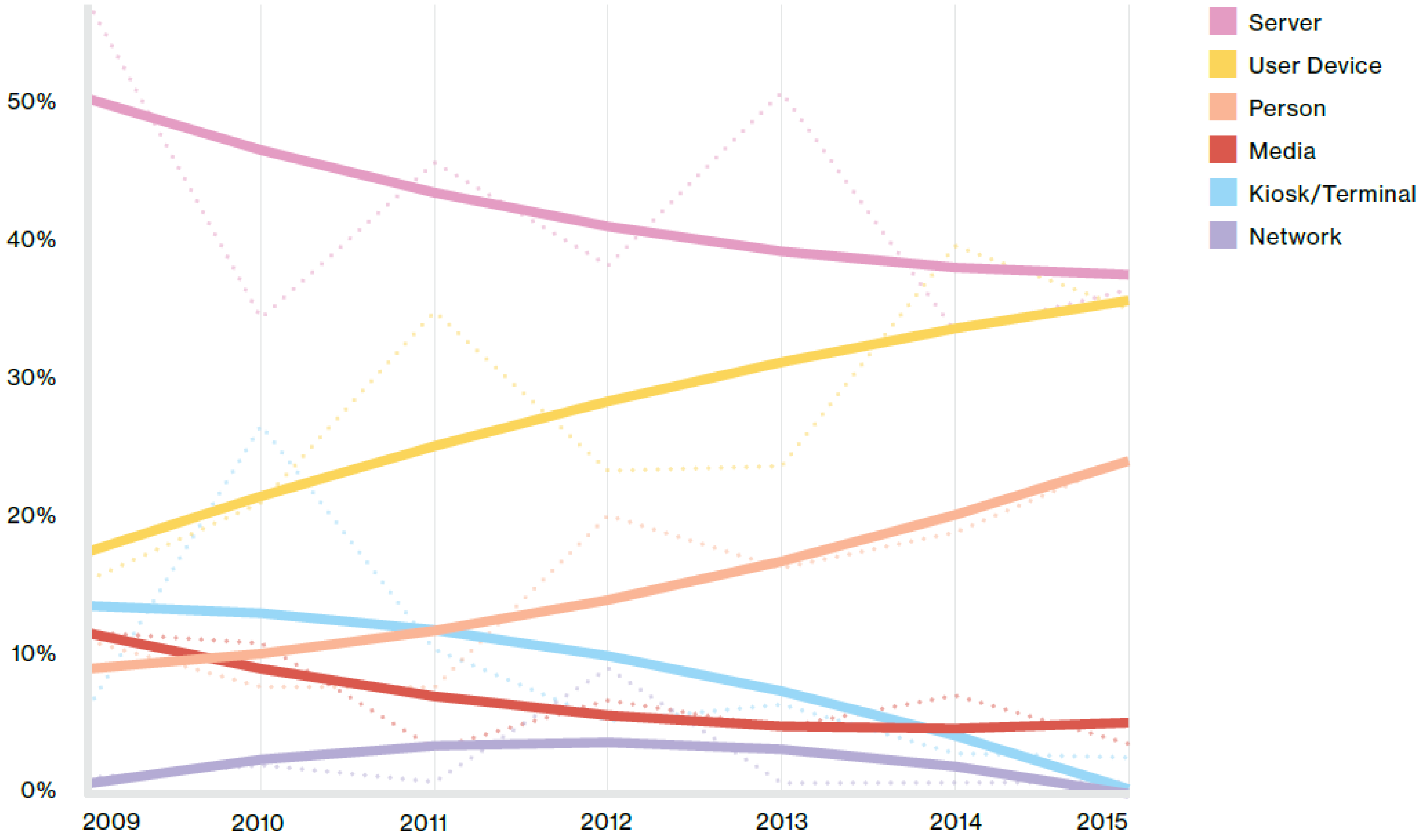
Current Topics

- Samsung Note 7– FIRE!!!!
- Google “Pixel” Phone – possible “best” Android phone ($650)

Agenda

- State of the world
- What Can I Do?
- Backup & Restore Point
- Secure Networks
- Online Shopping
- Social Media
- Resources


Hacking
Malware
Social
Error
Misuse
Physical
Environmental
2005
2007
2009
2011
2013
2015

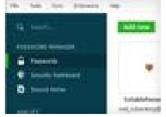
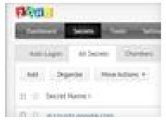
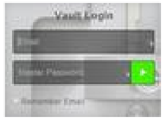
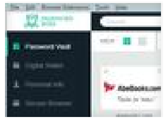
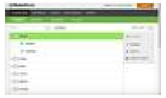
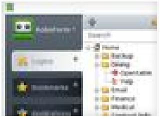
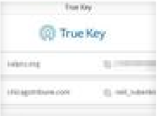

50%
40%
30%
20%
10%
0%
2009
2010
2011
2012
2013
2014
2015
Server
User Device
Person
Media
Kiosk/Terminal
Network

The Situation in 2016

- Ransomware is dominating the malware market
- Cyber-espionage
- Exploit kits becoming better. 80% involve Adobe Flash exploits.
- Vulnerability in enterprise applications are providing new vectors
- Users not installing patches in a timely manner giving more “time to operate” for hackers.

What Can I Do?

- ***Create*** strong passwords
    - Never a valid word in any language dictionary
    - Use special characters
    - At least 8 characters

Name	Dashlane 4	Zoho Vault	LastPass 4.0 Premium	Sticky Password Premium	Keeper Password Manager & Digital Vault 8	LogMeOnce Password Management Suite Ultimate	Password Boss Premium	RoboForm Everywhere 7	RoboForm Desktop 7	True Key by Intel Security
										
Lowest Price	$39.99 Dashlane - Synced SEE IT	$12.00 Zoho SEE IT	$12.00 LastPass SEE IT	$14.99 Special Offer SEE IT	$29.99 Keeper Security SEE IT	$39.00 LogMeOnce SEE IT	$29.99 Password Boss SEE IT	$19.95 RoboForm SEE IT	$29.95 RoboForm SEE IT	$19.99 MSRP
Editor Rating	●●●●● EC	●●●◐○	●●●●● EC	●●●●◐ EC	●●●●○	●●●●○	●●●●○	●●●●○	●●●◐○	●●●◐○
Import From Browsers	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓
Import From Competitors	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Export Data	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Automatic Password Capture	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Automatic Password Replay	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
Fill Web Forms	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗
Multiple Form-Filling Identities	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗

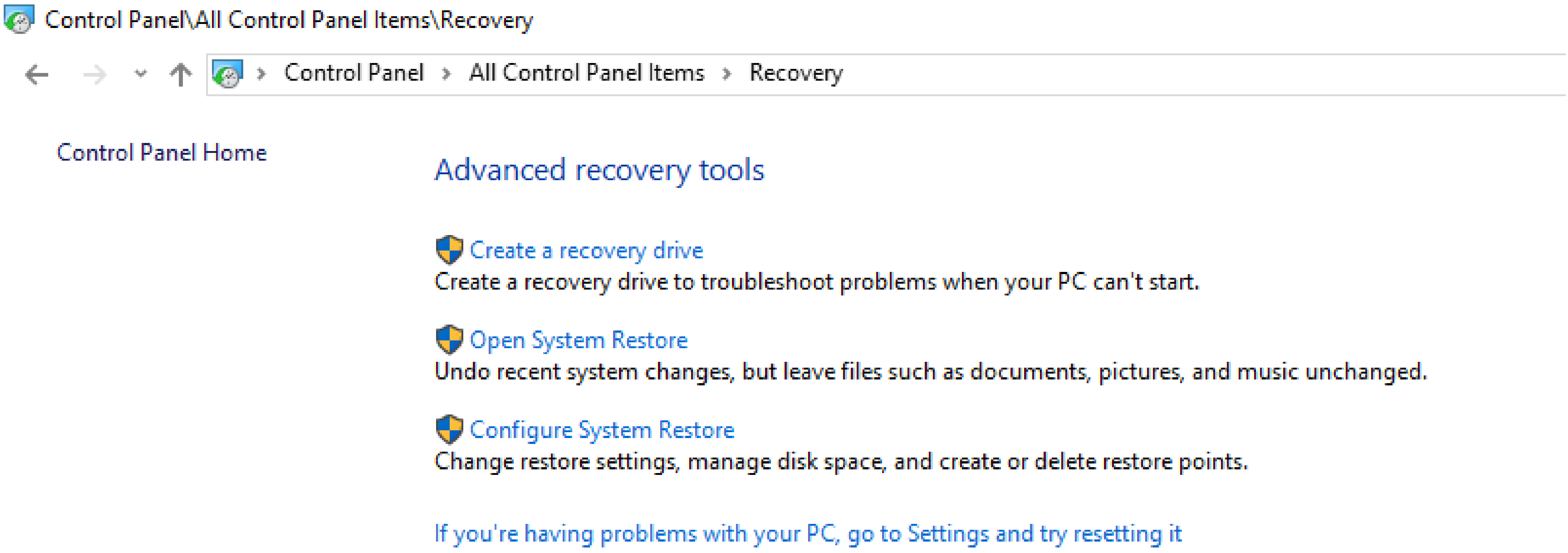
What Can I Do?

- ***Create*** strong passwords
- Install and ***maintain*** antivirus software
- ***Apply*** software patches as soon as possible/reasonable
- Be ***cautious*** with email attachments and links
- ***Remove*** unused and/or unnecessary software
- ***Secure*** your web browser settings
- Enable and ***configure*** firewalls

What Can I Do?

- ***Maintain*** backups and restore plan
- ***Create*** full disk image backup/recovery drive
  - Microsoft Windows Capability
  - Commercial software (e.g. Acronis True Image $22/$35/$50)

Restore Point



Control Panel\All Control Panel Items\Recovery

Advanced recovery tools

Create a recovery drive

Create a recovery drive to troubleshoot problems when your PC can't start.

Open System Restore

Undo recent system changes, but leave files such as documents, pictures, and music unchanged.

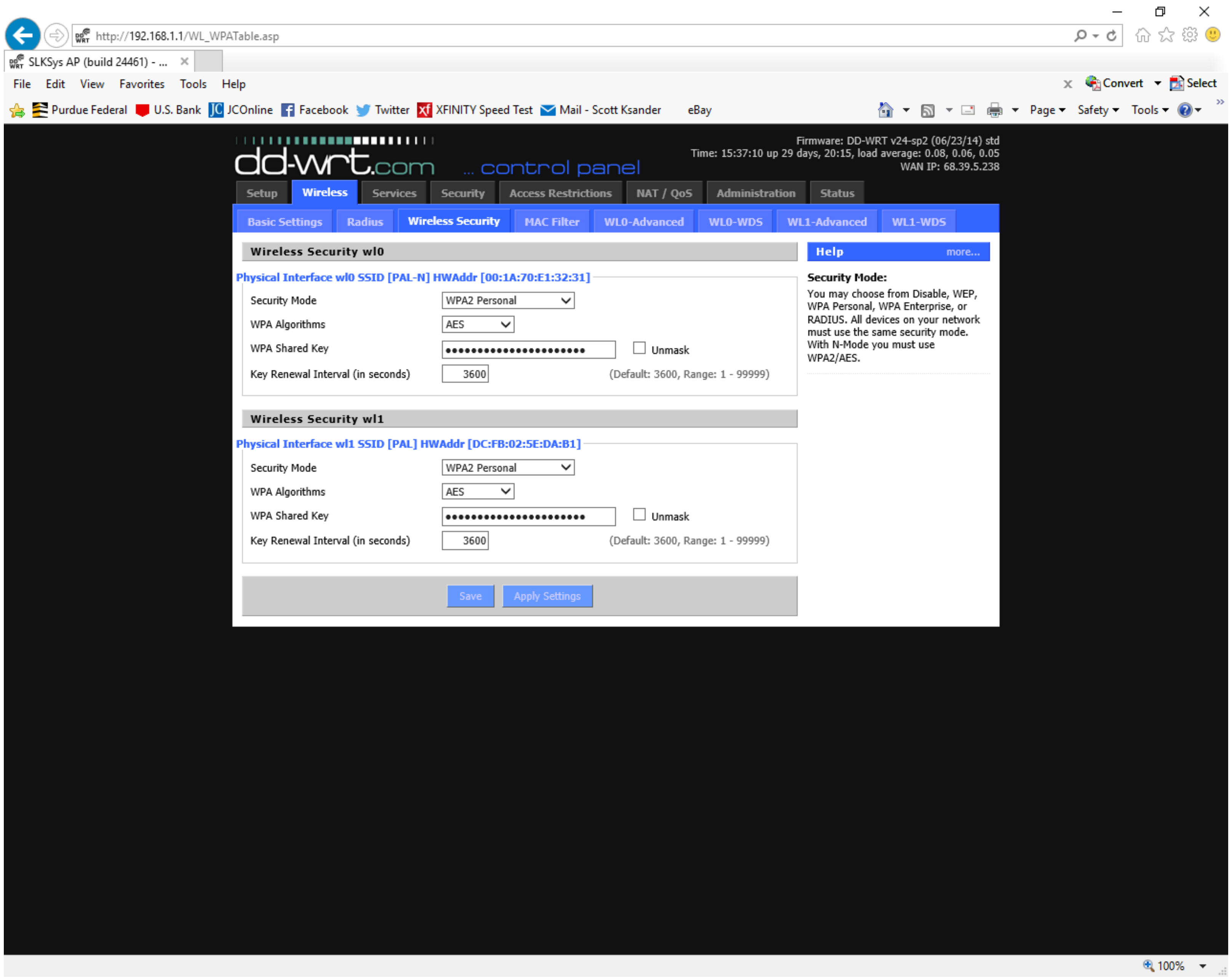
Configure System Restore

Change restore settings, manage disk space, and create or delete restore points.

If you're having problems with your PC, go to Settings and try resetting it

What Can I Do?

- Only connect to “secure” networks
- Secure your home network
  - Change default user id and password
  - Change default SSID
  - Disable WPS
  - Disable UPnP
  - Use WPA2/AES encryption
  - Limit WLAN signal strength is possible
  - Use current firmware
  - Disable remote management
  - Monitor for unknown devices


http://192.168.1.1/WL_WPATable.asp
SLKSys AP (build 24461) - ...
File Edit View Favorites Tools Help
Convert Select
Purdue Federal U.S. Bank JCOnline Facebook Twitter XFINITY Speed Test Mail - Scott Ksander eBay
Page Safety Tools
dd-wrt.com ... control panel
Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status
Basic Settings Radius Wireless Security MAC Filter WL0-Advanced WL0-WDS WL1-Advanced WL1-WDS
Help more...
Save Apply Settings
100%

Firmware: DD-WRT v24-sp2 (06/23/14) std
Time: 15:37:10 up 29 days, 20:15, load average: 0.08, 0.06, 0.05
WAN IP: 68.39.5.238

Wireless Security wl0

Physical Interface wl0 SSID [PAL-N] HWAddr [00:1A:70:E1:32:31]

Security Mode	WPA2 Personal
WPA Algorithms	AES
WPA Shared Key	••••••••••••••••••••• □ Unmask
Key Renewal Interval (in seconds)	3600 (Default: 3600, Range: 1 - 99999)

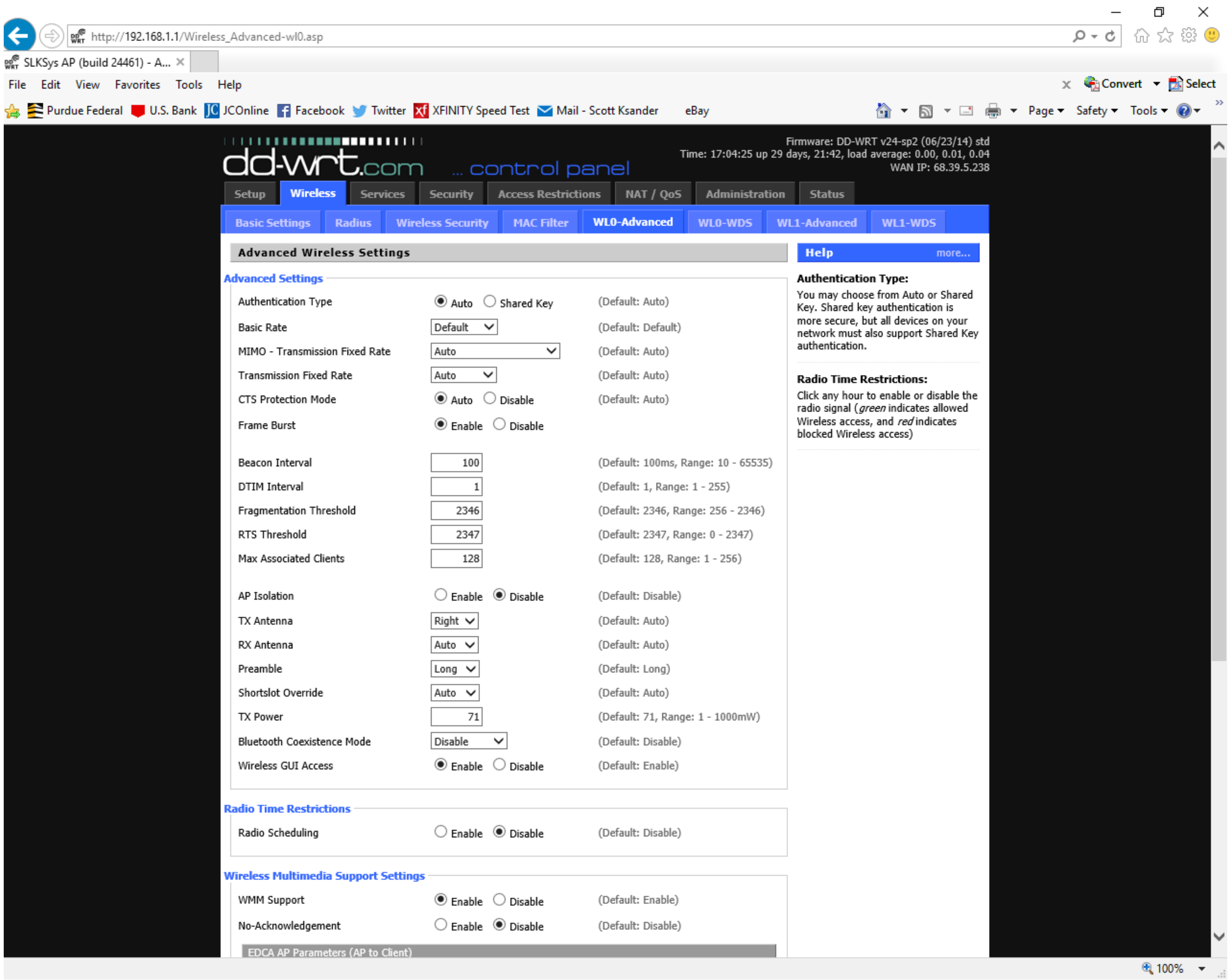
Wireless Security wl1

Physical Interface wl1 SSID [PAL] HWAddr [DC:FB:02:5E:DA:B1]

Security Mode	WPA2 Personal
WPA Algorithms	AES
WPA Shared Key	••••••••••••••••••••• □ Unmask
Key Renewal Interval (in seconds)	3600 (Default: 3600, Range: 1 - 99999)

Security Mode:

You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode. With N-Mode you must use WPA2/AES.



Firmware: DD-WRT v24-sp2 (06/23/14) std
Time: 17:04:25 up 29 days, 21:42, load average: 0.00, 0.01, 0.04
WAN IP: 68.39.5.238

Advanced Wireless Settings

Advanced Settings

Authentication Type	● Auto ○ Shared Key	(Default: Auto)
Basic Rate	Default	(Default: Default)
MIMO - Transmission Fixed Rate	Auto	(Default: Auto)
Transmission Fixed Rate	Auto	(Default: Auto)
CTS Protection Mode	● Auto ○ Disable	(Default: Auto)
Frame Burst	● Enable ○ Disable	
Beacon Interval	100	(Default: 100ms, Range: 10 - 65535)
DTIM Interval	1	(Default: 1, Range: 1 - 255)
Fragmentation Threshold	2346	(Default: 2346, Range: 256 - 2346)
RTS Threshold	2347	(Default: 2347, Range: 0 - 2347)
Max Associated Clients	128	(Default: 128, Range: 1 - 256)
AP Isolation	○ Enable ● Disable	(Default: Disable)
TX Antenna	Right	(Default: Auto)
RX Antenna	Auto	(Default: Auto)
Preamble	Long	(Default: Long)
Shortslot Override	Auto	(Default: Auto)
TX Power	71	(Default: 71, Range: 1 - 1000mW)
Bluetooth Coexistence Mode	Disable	(Default: Disable)
Wireless GUI Access	● Enable ○ Disable	(Default: Enable)

Radio Time Restrictions

Radio Scheduling	○ Enable ● Disable	(Default: Disable)

Wireless Multimedia Support Settings

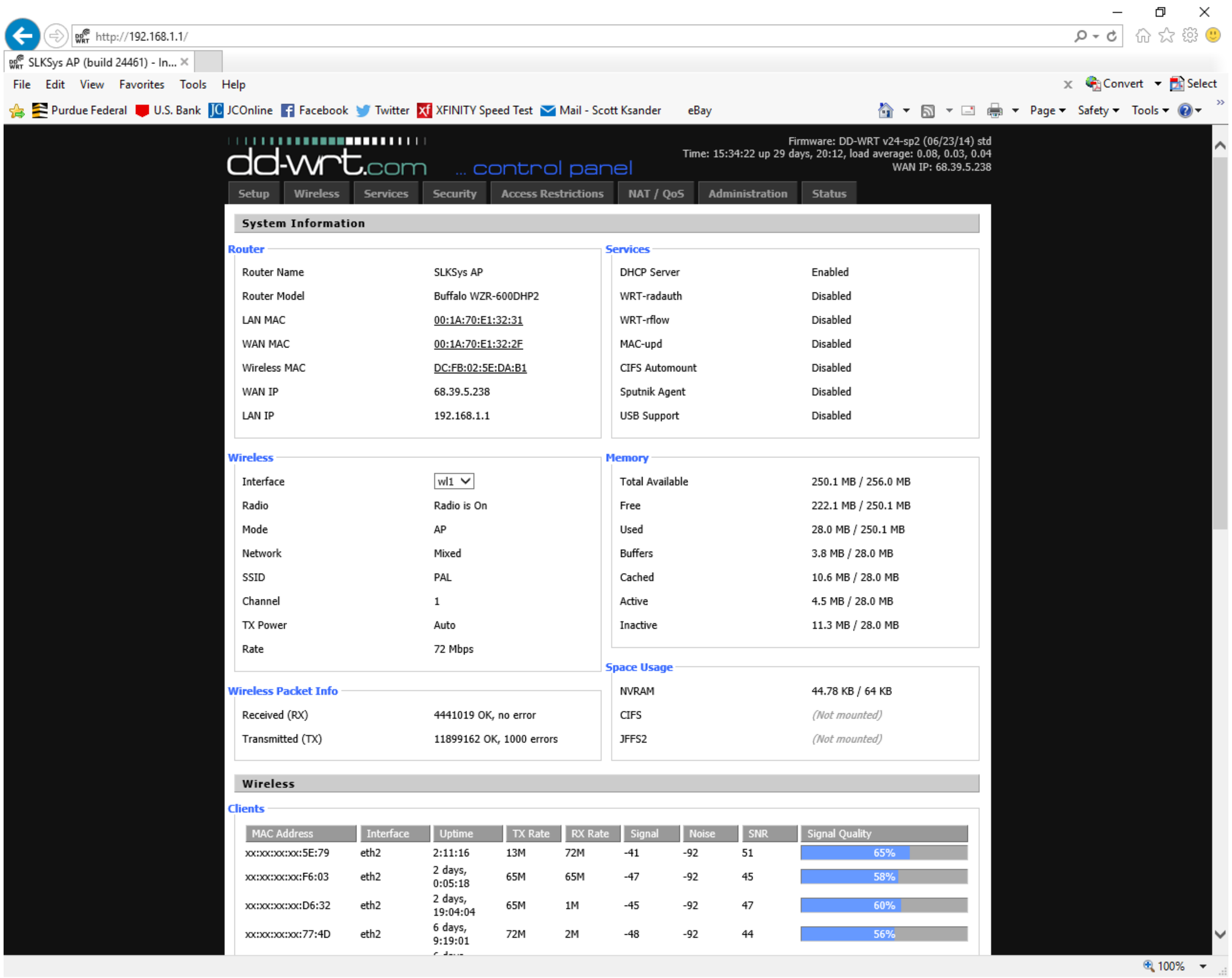
WMM Support	● Enable ○ Disable	(Default: Enable)
No-Acknowledgement	○ Enable ● Disable	(Default: Disable)

EDCA AP Parameters (AP to Client)

Help

Authentication Type:
You may choose from Auto or Shared Key. Shared key authentication is more secure, but all devices on your network must also support Shared Key authentication.

Radio Time Restrictions:
Click any hour to enable or disable the radio signal (*green* indicates allowed Wireless access, and *red* indicates blocked Wireless access)



Firmware: DD-WRT v24-sp2 (06/23/14) std
Time: 15:34:22 up 29 days, 20:12, load average: 0.08, 0.03, 0.04
WAN IP: 68.39.5.238

System Information

Router

Router Name	SLKSys AP
Router Model	Buffalo WZR-600DHP2
LAN MAC	00:1A:70:E1:32:31
WAN MAC	00:1A:70:E1:32:2F
Wireless MAC	DC:FB:02:5E:DA:B1
WAN IP	68.39.5.238
LAN IP	192.168.1.1

Services

DHCP Server	Enabled
WRT-radauth	Disabled
WRT-rflow	Disabled
MAC-upd	Disabled
CIFS Automount	Disabled
Sputnik Agent	Disabled
USB Support	Disabled

Wireless

Interface	wl1
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	PAL
Channel	1
TX Power	Auto
Rate	72 Mbps

Memory

Total Available	250.1 MB / 256.0 MB
Free	222.1 MB / 250.1 MB
Used	28.0 MB / 250.1 MB
Buffers	3.8 MB / 28.0 MB
Cached	10.6 MB / 28.0 MB
Active	4.5 MB / 28.0 MB
Inactive	11.3 MB / 28.0 MB

Space Usage

NVRAM	44.78 KB / 64 KB
CIFS	*(Not mounted)*
JFFS2	*(Not mounted)*

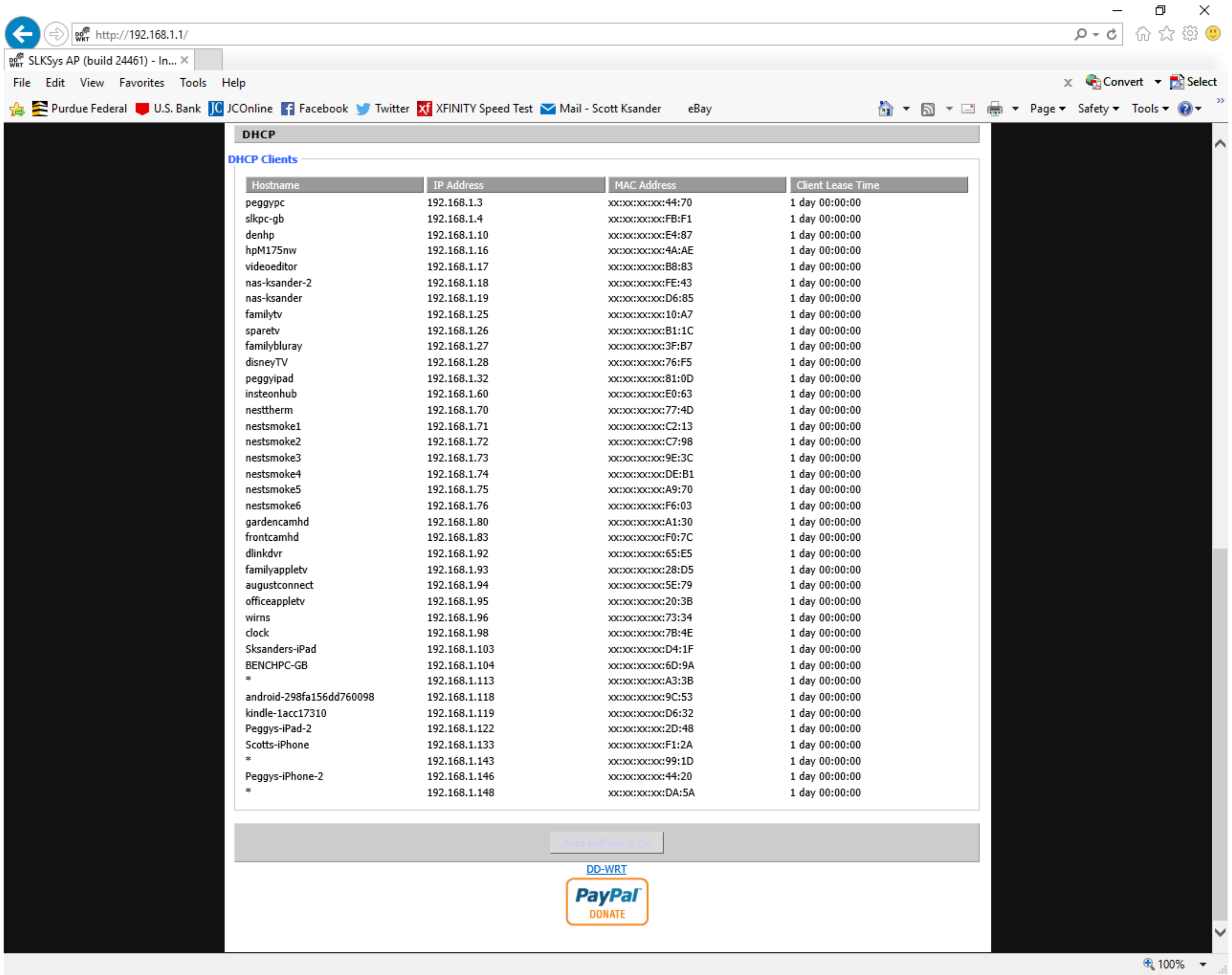
Wireless Packet Info

Received (RX)	4441019 OK, no error
Transmitted (TX)	11899162 OK, 1000 errors

Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
xx:xx:xx:xx:5E:79	eth2	2:11:16	13M	72M	-41	-92	51	65%
xx:xx:xx:xx:F6:03	eth2	2 days, 0:05:18	65M	65M	-47	-92	45	58%
xx:xx:xx:xx:D6:32	eth2	2 days, 19:04:04	65M	1M	-45	-92	47	60%
xx:xx:xx:xx:77:4D	eth2	6 days, 9:19:01	72M	2M	-48	-92	44	56%
		6 days,						



DHCP

DHCP Clients

Hostname	IP Address	MAC Address	Client Lease Time
peggypc	192.168.1.3	xx:xx:xx:xx:44:70	1 day 00:00:00
slkpc-gb	192.168.1.4	xx:xx:xx:xx:FB:F1	1 day 00:00:00
denhp	192.168.1.10	xx:xx:xx:xx:E4:87	1 day 00:00:00
hpM175nw	192.168.1.16	xx:xx:xx:xx:4A:AE	1 day 00:00:00
videoeditor	192.168.1.17	xx:xx:xx:xx:B8:83	1 day 00:00:00
nas-ksander-2	192.168.1.18	xx:xx:xx:xx:FE:43	1 day 00:00:00
nas-ksander	192.168.1.19	xx:xx:xx:xx:D6:85	1 day 00:00:00
familytv	192.168.1.25	xx:xx:xx:xx:10:A7	1 day 00:00:00
sparetv	192.168.1.26	xx:xx:xx:xx:B1:1C	1 day 00:00:00
familybluray	192.168.1.27	xx:xx:xx:xx:3F:B7	1 day 00:00:00
disneyTV	192.168.1.28	xx:xx:xx:xx:76:F5	1 day 00:00:00
peggyipad	192.168.1.32	xx:xx:xx:xx:81:0D	1 day 00:00:00
insteonhub	192.168.1.60	xx:xx:xx:xx:E0:63	1 day 00:00:00
nesttherm	192.168.1.70	xx:xx:xx:xx:77:4D	1 day 00:00:00
nestsmoke1	192.168.1.71	xx:xx:xx:xx:C2:13	1 day 00:00:00
nestsmoke2	192.168.1.72	xx:xx:xx:xx:C7:98	1 day 00:00:00
nestsmoke3	192.168.1.73	xx:xx:xx:xx:9E:3C	1 day 00:00:00
nestsmoke4	192.168.1.74	xx:xx:xx:xx:DE:B1	1 day 00:00:00
nestsmoke5	192.168.1.75	xx:xx:xx:xx:A9:70	1 day 00:00:00
nestsmoke6	192.168.1.76	xx:xx:xx:xx:F6:03	1 day 00:00:00
gardencamhd	192.168.1.80	xx:xx:xx:xx:A1:30	1 day 00:00:00
frontcamhd	192.168.1.83	xx:xx:xx:xx:F0:7C	1 day 00:00:00
dlinkdvr	192.168.1.92	xx:xx:xx:xx:65:E5	1 day 00:00:00
familyappletv	192.168.1.93	xx:xx:xx:xx:28:D5	1 day 00:00:00
augustconnect	192.168.1.94	xx:xx:xx:xx:5E:79	1 day 00:00:00
officeappletv	192.168.1.95	xx:xx:xx:xx:20:3B	1 day 00:00:00
wirns	192.168.1.96	xx:xx:xx:xx:73:34	1 day 00:00:00
clock	192.168.1.98	xx:xx:xx:xx:7B:4E	1 day 00:00:00
Sksanders-iPad	192.168.1.103	xx:xx:xx:xx:D4:1F	1 day 00:00:00
BENCHPC-GB	192.168.1.104	xx:xx:xx:xx:6D:9A	1 day 00:00:00
*	192.168.1.113	xx:xx:xx:xx:A3:3B	1 day 00:00:00
android-298fa156dd760098	192.168.1.118	xx:xx:xx:xx:9C:53	1 day 00:00:00
kindle-1acc17310	192.168.1.119	xx:xx:xx:xx:D6:32	1 day 00:00:00
Peggys-iPad-2	192.168.1.122	xx:xx:xx:xx:2D:48	1 day 00:00:00
Scotts-iPhone	192.168.1.133	xx:xx:xx:xx:F1:2A	1 day 00:00:00
*	192.168.1.143	xx:xx:xx:xx:99:1D	1 day 00:00:00
Peggys-iPhone-2	192.168.1.146	xx:xx:xx:xx:44:20	1 day 00:00:00
*	192.168.1.148	xx:xx:xx:xx:DA:5A	1 day 00:00:00

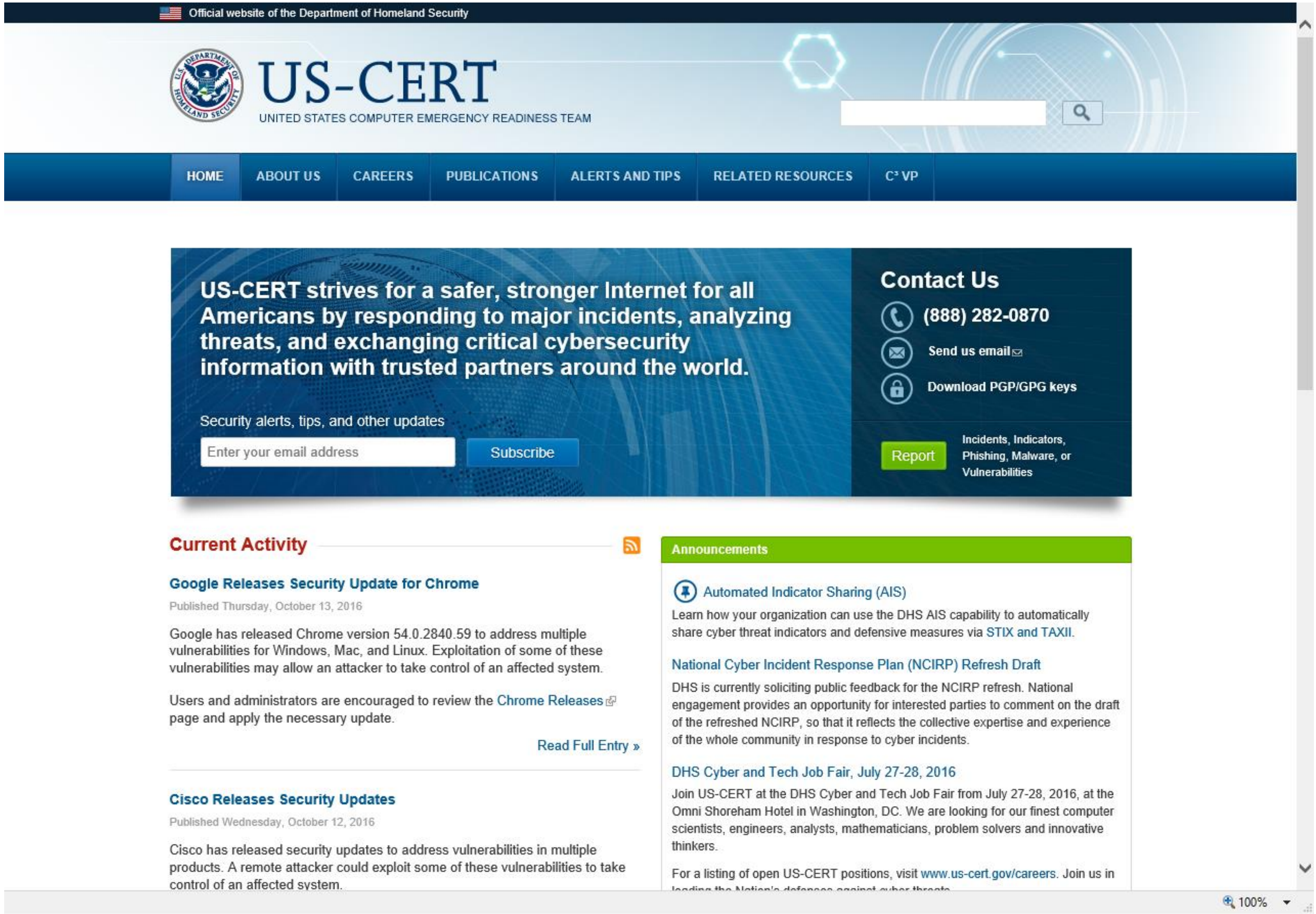
Online Shopping

- Use reputable sites
- Be sure site uses HTTPS
- Limit information request vs. value
- Use a “online credit card” that you monitor
- Check statements often

Social Media

- Limit personal information
- Be wary of strangers and know you friends
- Be skeptical
- Use strong passwords
- Remember, internet is public

Resources – www.us-cert.org



US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

Security alerts, tips, and other updates

Contact Us

☎ (888) 282-0870

Send us email

Download PGP/GPG keys

Report Incidents, Indicators, Phishing, Malware, or Vulnerabilities

Current Activity

Google Releases Security Update for Chrome

Published Thursday, October 13, 2016

Google has released Chrome version 54.0.2840.59 to address multiple vulnerabilities for Windows, Mac, and Linux. Exploitation of some of these vulnerabilities may allow an attacker to take control of an affected system.

Users and administrators are encouraged to review the Chrome Releases page and apply the necessary update.

Read Full Entry »

Cisco Releases Security Updates

Published Wednesday, October 12, 2016

Cisco has released security updates to address vulnerabilities in multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

Announcements

Automated Indicator Sharing (AIS)

Learn how your organization can use the DHS AIS capability to automatically share cyber threat indicators and defensive measures via STIX and TAXII.

National Cyber Incident Response Plan (NCIRP) Refresh Draft

DHS is currently soliciting public feedback for the NCIRP refresh. National engagement provides an opportunity for interested parties to comment on the draft of the refreshed NCIRP, so that it reflects the collective expertise and experience of the whole community in response to cyber incidents.

DHS Cyber and Tech Job Fair, July 27-28, 2016

Join US-CERT at the DHS Cyber and Tech Job Fair from July 27-28, 2016, at the Omni Shoreham Hotel in Washington, DC. We are looking for our finest computer scientists, engineers, analysts, mathematicians, problem solvers and innovative thinkers.

For a listing of open US-CERT positions, visit www.us-cert.gov/careers. Join us in leading the Nation's defenses against cyber threats.

"I keep our secure files in a coffee can
buried behind the office. You can't
hack into that with a computer!"