OMG: They're Inside the Walls

Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu)

Association for Computing Professionals in Education (ACPE)
Spokane, WA
1:00-2:00 PM, March 4th, 2014

http://pages.uoregon.edu/joe/acpe-spokane/

Disclaimer: all opinions expressed are strictly my own and do not necessarily represent the opinion of any other entity.

Introduction

- I'd like to thank ACPE for the invitation to speak with you today, particularly since they put up with a version of this talk once before, in Ashland in December, and thus should really "know better."

- Given that our group today is relatively small, I'd like to have this be an interactive discussion and NOT just "me talking," "you listening. "

- In fact, I'd much rather just ask lots of questions, and let YOU talk. I always assume that I've got a lot to learn, and that every environment will be a little different, so I hope that you'll tell me about yours...

Why THIS Topic?

- **Why do you think this topic get chosen for this mini meeting? Is the security of personal devices connecting to school networks something that people have been worried about? If so, any particular reason WHY?**

- Have there been security **challenges**? Have their been security **disasters** in this community? **Or are we worrying about non-issues?** Are there even security **success stories** when it comes to connecting your teachers and your students and their devices?

- ***Is a desire for security (or a propensity toward risk aversion) getting in the way of why you have the network? Is this really a wireless network "usability" session?***

This Meeting: A Living WiFi Laboratory

- **WiFi at meetings may matter more than anything but coffee.**

- The **meeting hotel** is the Red Lion Spokane, a fairly typical convention hotel. After checking into the hotel, I went to my room and connected to the hotel's wireless network. I easily connected (without a password) after just clicking through a network policy statement (that I must confess I really didn't read). I then had the ability to use the web, **and to ssh back to the other systems I routinely use in Eugene.** This was terrific (and typical for hotels)

- Is the hotel doing the "wrong" thing? If so, why? (This is NOT a rhetorical question!)

- What could they do *differently?*

What About Eavesdropping Risks?

- Wireless is – obviously – a broadcast medium. It's a radio.

- Unless the transmissions are encrypted, potentially anyone can monitor that traffic.

- Some wireless connections may use WPA2 to encrypt connections between the user's laptop and the wireless access point.

- Other connections, such as the Red Lion's open wireless access point connections normally **aren't encrypted.**

You Can Manage Wireless Eavesdropping Risks In Different Ways

- For example...
  - If you're not transmitting passwords (or other confidential information), you may not strictly need to encrypt your wireless connectivity. But are you SURE that you're NEVER going to have sensitive info go over the wire?
  - The application itself may protect those credentials (example: a web page that uses https rather than http)... but what if some apps or some sites use https, but others don't?
  - You may use a VPN to encrypt your entire session (anyone offering VPN for all your wireless users, BTW?)
- **Sometimes though, none of those conditions will be fully satisfied.** That may be a problem, depending on the threats you worry about.

What's YOUR Threat Model?

- What do you worry about when it comes to wireless access?
  - Access by students to problematic content?
  - Ubiquitous access distracting students/keeping them from paying attention to what instructors are trying to teach them?
  - Use of your wireless to obtain unauthorized access to YOUR internal critical systems or records?
  - Unauthorized access (e.g., by spammers or hacker/crackers) who will then abuse that connectivity outbound?
  - Resource exhaustion? (you probably don't want to have to buy more bandwidth just to support your school's neighbors watching Netflix, Hulu, or Youtube videos, right?)
  - Other???

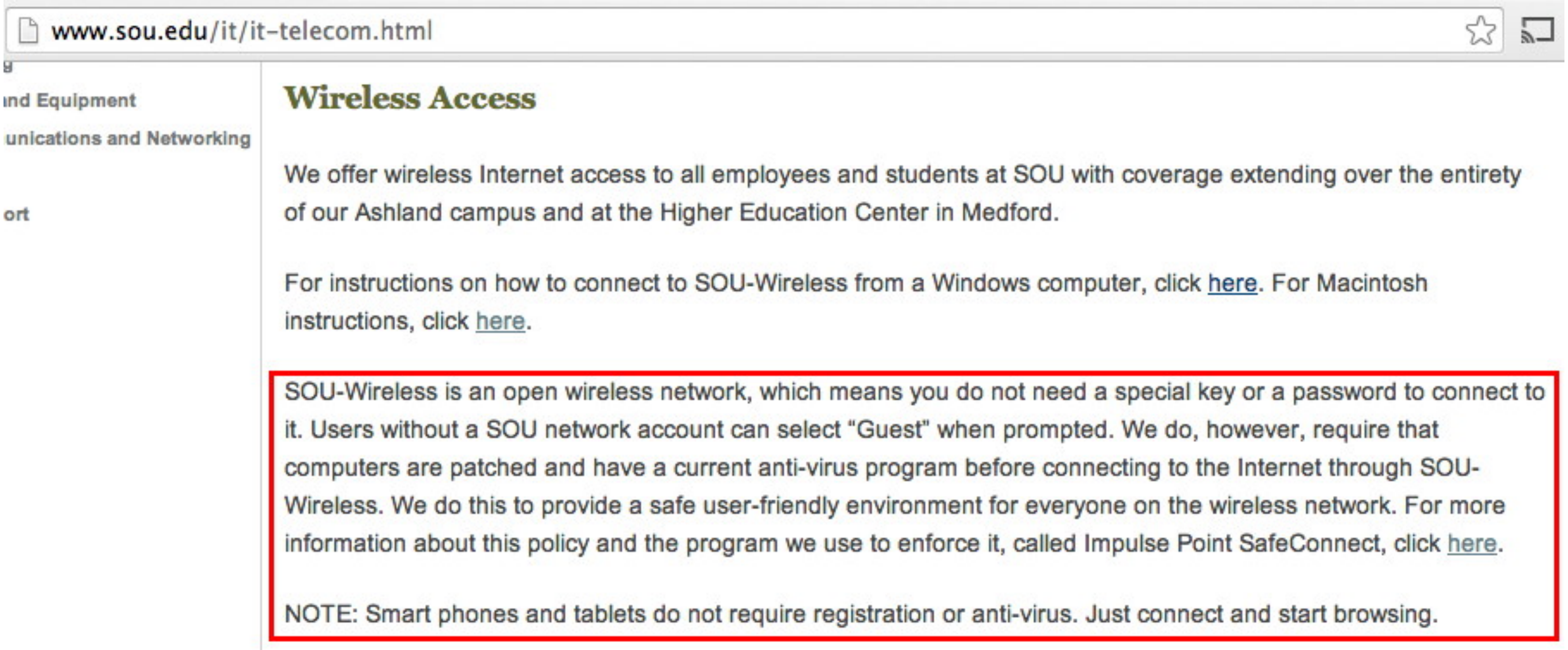
Should Access Require Authentication?

- I didn't need to enter a password to get access to the hotel's free wireless. That's because it was an open and unencrypted wireless network. I connected easily, but so could anyone else... including spammers, hackers and other "evil doers."
- If you want to enable WPA2 encryption, it's going to require authentication.
- One option (not a very good one) is to use a common password, much as you might on your home network. A secret shared across potentially hundreds of guests (and seldom if ever changed) doesn't really provide much security.
- Another option is per-user ("enterprise") authentication, but quite frankly, I normally only see that -- at least in hotels -- when the hotel is charging for wireless access.
- You could even use PKI client certificates for authentication (EAP-TTLSv0), but that's a unique "heck" all of its own. :-)

The Ashland Event Meeting Venue *Was* Different

- The Ashland ACPE event was held at Southern Oregon University, a beautiful campus.
- Like the Red Lion, no password was required to connect to their guest network.
- They did, however, do some things differently:
  - They required people to verify the security of their systems (e.g., do you have antivirus installed?), including requiring users to install an on-laptop agent
  - They blocked some services entirely, including ssh (which I routinely use and rely on)

SOU's Local Policy



Wireless Access

We offer wireless Internet access to all employees and students at SOU with coverage extending over the entirety of our Ashland campus and at the Higher Education Center in Medford.

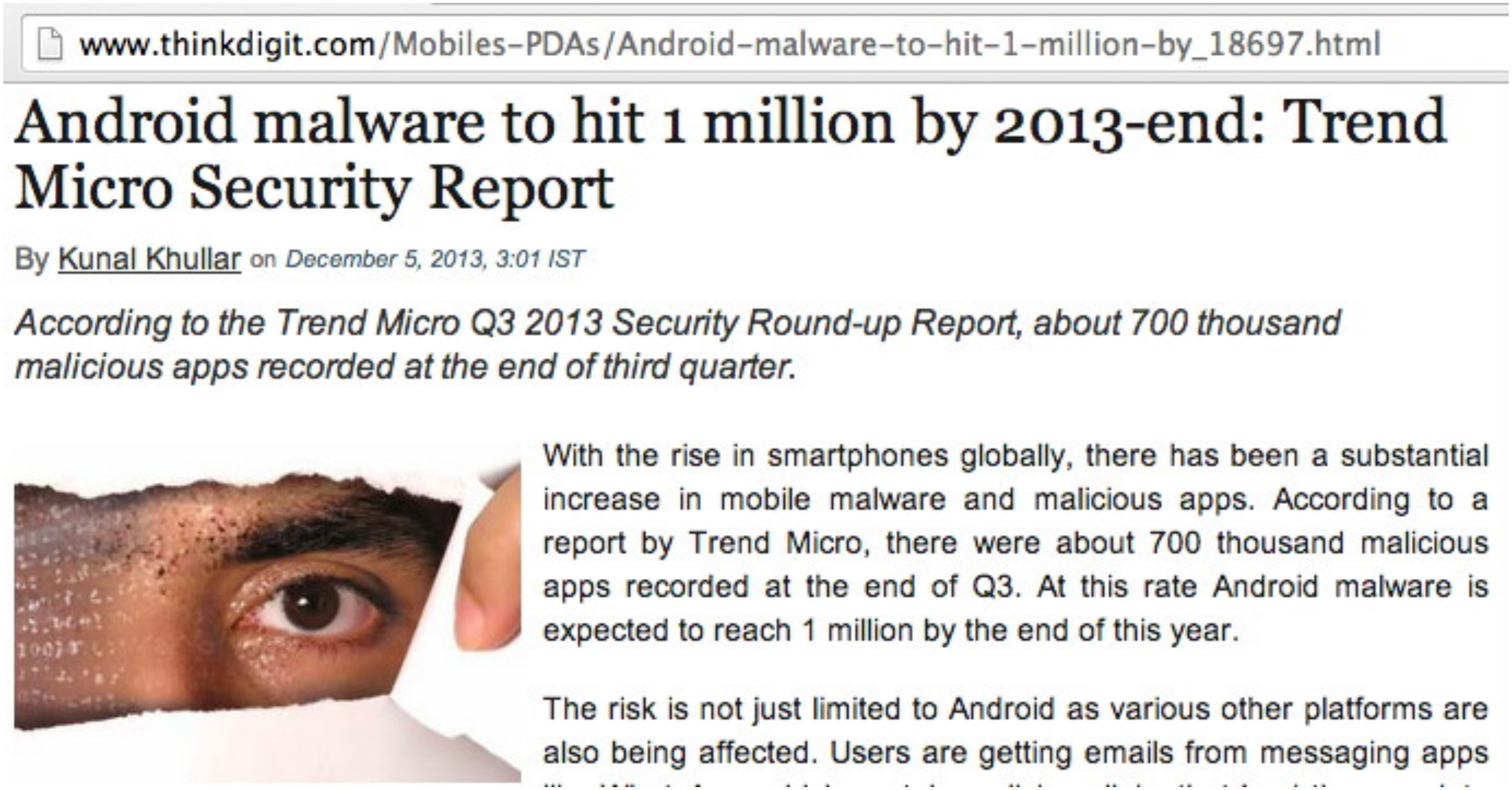
For instructions on how to connect to SOU-Wireless from a Windows computer, click here. For Macintosh instructions, click here.

SOU-Wireless is an open wireless network, which means you do not need a special key or a password to connect to it. Users without a SOU network account can select "Guest" when prompted. We do, however, require that computers are patched and have a current anti-virus program before connecting to the Internet through SOU-Wireless. We do this to provide a safe user-friendly environment for everyone on the wireless network. For more information about this policy and the program we use to enforce it, called Impulse Point SafeConnect, click here.

NOTE: Smart phones and tablets do not require registration or anti-virus. Just connect and start browsing.

- *Questions (if you know me, you know I **always** have questions):*
  -- Do users get what's implied to be on a non-encrypted network?
  -- Are you sure that the tool as deployed works as advertised?
  (For example: what A/V did I have installed on my Mac?)
  -- Why don't smart phones and tablets also require A/V here?

"Smart Phones and Tablets Don't Require A/V"



www.thinkdigit.com/Mobiles-PDAs/Android-malware-to-hit-1-million-by_18697.html

Android malware to hit 1 million by 2013-end: Trend Micro Security Report

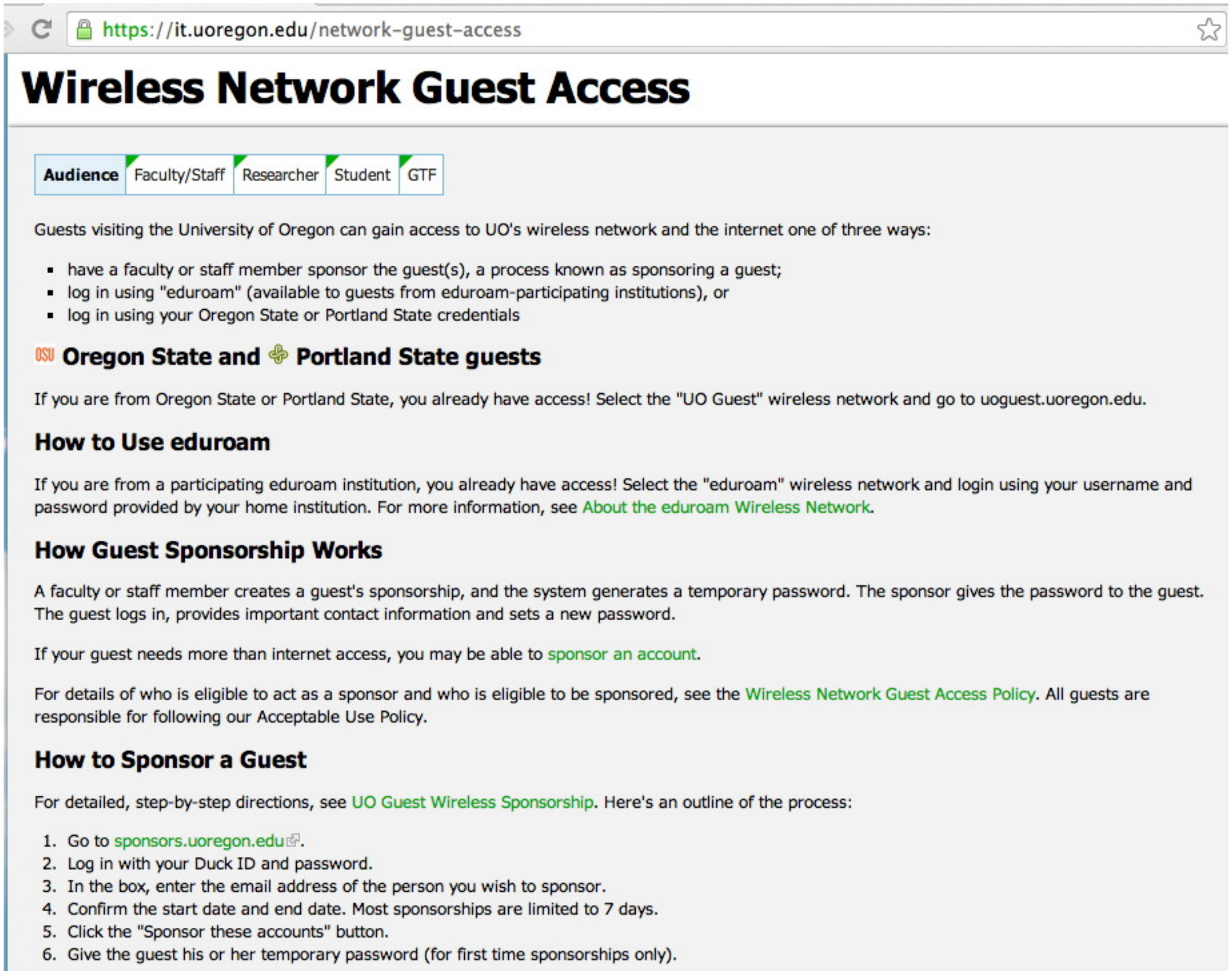
By Kunal Khullar on *December 5, 2013, 3:01 IST*

According to the Trend Micro Q3 2013 Security Round-up Report, about 700 thousand malicious apps recorded at the end of third quarter.

With the rise in smartphones globally, there has been a substantial increase in mobile malware and malicious apps. According to a report by Trend Micro, there were about 700 thousand malicious apps recorded at the end of Q3. At this rate Android malware is expected to reach 1 million by the end of this year.

The risk is not just limited to Android as various other platforms are also being affected. Users are getting emails from messaging apps

UO's Current Approach for Guest Wireless



Wireless Network Guest Access

Guests visiting the University of Oregon can gain access to UO's wireless network and the internet one of three ways:

- have a faculty or staff member sponsor the guest(s), a process known as sponsoring a guest;
- log in using "eduroam" (available to guests from eduroam-participating institutions), or
- log in using your Oregon State or Portland State credentials

OSU Oregon State and Portland State guests

If you are from Oregon State or Portland State, you already have access! Select the "UO Guest" wireless network and go to uoguest.uoregon.edu.

How to Use eduroam

If you are from a participating eduroam institution, you already have access! Select the "eduroam" wireless network and login using your username and password provided by your home institution. For more information, see About the eduroam Wireless Network.

How Guest Sponsorship Works

A faculty or staff member creates a guest's sponsorship, and the system generates a temporary password. The sponsor gives the password to the guest. The guest logs in, provides important contact information and sets a new password.

If your guest needs more than internet access, you may be able to sponsor an account.

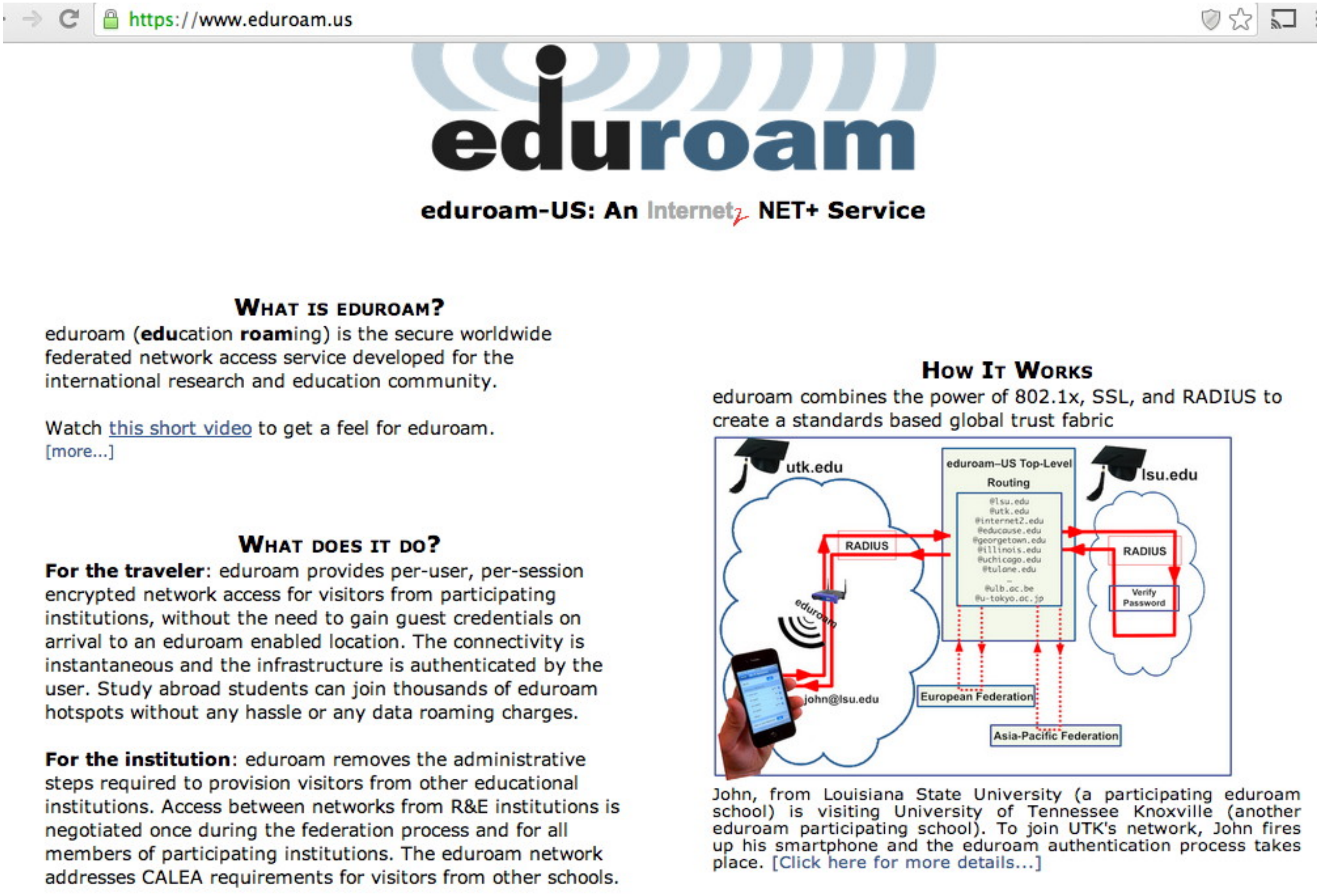
For details of who is eligible to act as a sponsor and who is eligible to be sponsored, see the Wireless Network Guest Access Policy. All guests are responsible for following our Acceptable Use Policy.

How to Sponsor a Guest

For detailed, step-by-step directions, see UO Guest Wireless Sponsorship. Here's an outline of the process:

1. Go to sponsors.uoregon.edu.
2. Log in with your Duck ID and password.
3. In the box, enter the email address of the person you wish to sponsor.
4. Confirm the start date and end date. Most sponsorships are limited to 7 days.
5. Click the "Sponsor these accounts" button.
6. Give the guest his or her temporary password (for first time sponsorships only).

Eduroam (As Mentioned on the Previous Page)



https://www.eduroam.us

eduroam

eduroam-US: An Internet2 NET+ Service

What is eduroam?

eduroam (**edu**cation **roam**ing) is the secure worldwide federated network access service developed for the international research and education community.

Watch this short video to get a feel for eduroam.
[more...]

What does it do?

For the traveler: eduroam provides per-user, per-session encrypted network access for visitors from participating institutions, without the need to gain guest credentials on arrival to an eduroam enabled location. The connectivity is instantaneous and the infrastructure is authenticated by the user. Study abroad students can join thousands of eduroam hotspots without any hassle or any data roaming charges.

For the institution: eduroam removes the administrative steps required to provision visitors from other educational institutions. Access between networks from R&E institutions is negotiated once during the federation process and for all members of participating institutions. The eduroam network addresses CALEA requirements for visitors from other schools.

How It Works

eduroam combines the power of 802.1x, SSL, and RADIUS to create a standards based global trust fabric

John, from Louisiana State University (a participating eduroam school) is visiting University of Tennessee Knoxville (another eduroam participating school). To join UTK's network, John fires up his smartphone and the eduroam authentication process takes place. [Click here for more details...]

BTW, I DO Get It That WiFi is Hard/Expensive

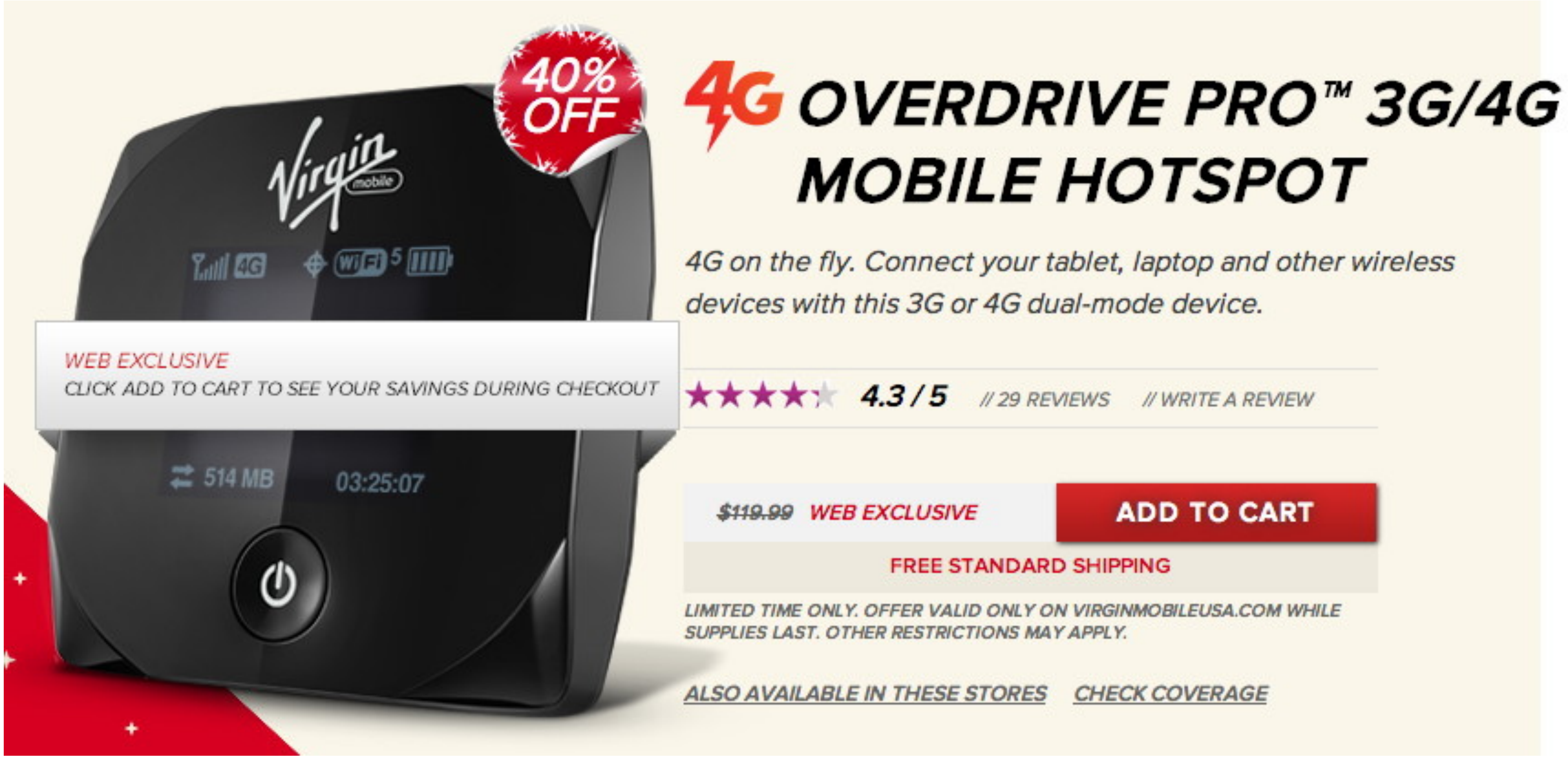
www.registerguard.com/rg/news/local/30551808-75/wifi-campus-students-wireless-dieni.html.csp

Missing links

UO has a hard time keeping the WiFi generation connected

University of Oregon student Amy Zhang, from China, texts on her smartphone while watching a video in the lounge of the Erb Memorial Student Building on campus. Students at the university are frustrated by problems with the WiFi network on campus as the number of mobile devices has skyrocketed. (Chris Pietsch (The Register-Guard)

Should I Just Stand Up My Own WiFi *Network?*



4G OVERDRIVE PRO™ 3G/4G MOBILE HOTSPOT

4G on the fly. Connect your tablet, laptop and other wireless devices with this 3G or 4G dual-mode device.

WEB EXCLUSIVE

CLICK ADD TO CART TO SEE YOUR SAVINGS DURING CHECKOUT

★★★★☆ 4.3 / 5 // 29 REVIEWS // WRITE A REVIEW

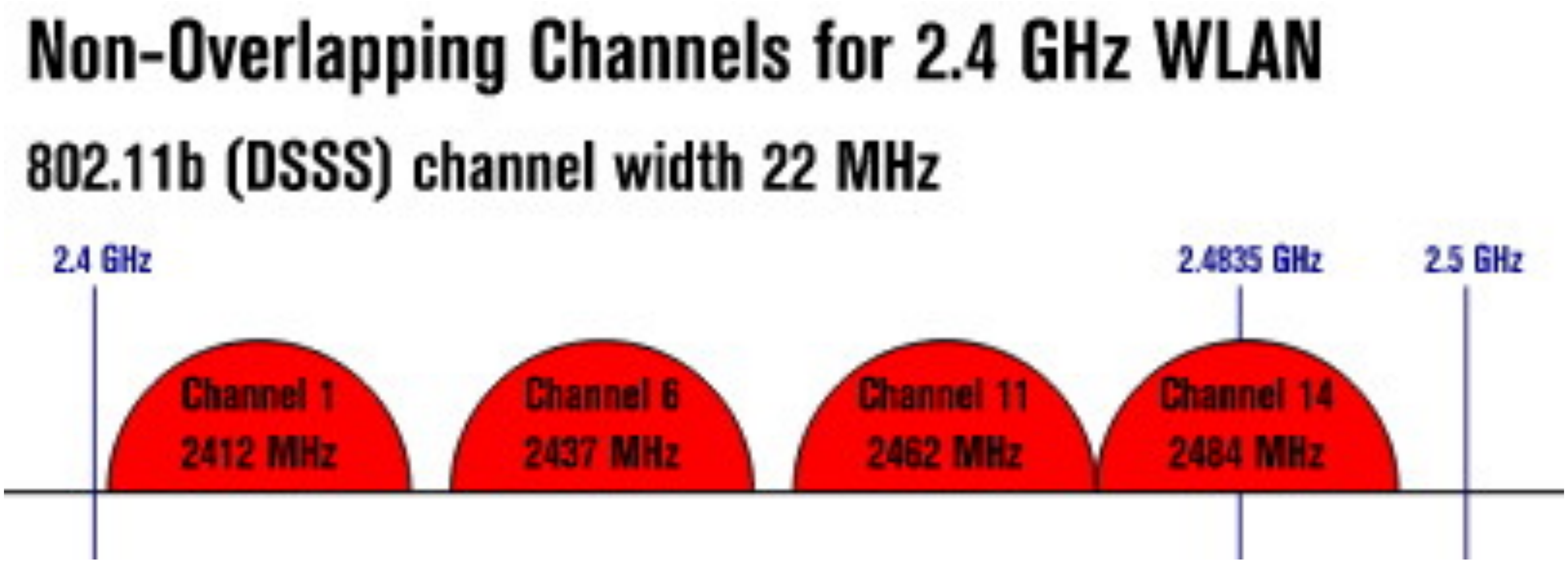
~~$119.99~~ WEB EXCLUSIVE

FREE STANDARD SHIPPING

LIMITED TIME ONLY. OFFER VALID ONLY ON VIRGINMOBILEUSA.COM WHILE SUPPLIES LAST. OTHER RESTRICTIONS MAY APPLY.

That's $72 (one time) plus $25/month for 1.5GB of data/month. Nice option -- as long as "everyone" doesn't do it, all competing for a limited number of channels.

Only 4 Real 802.11b Channels

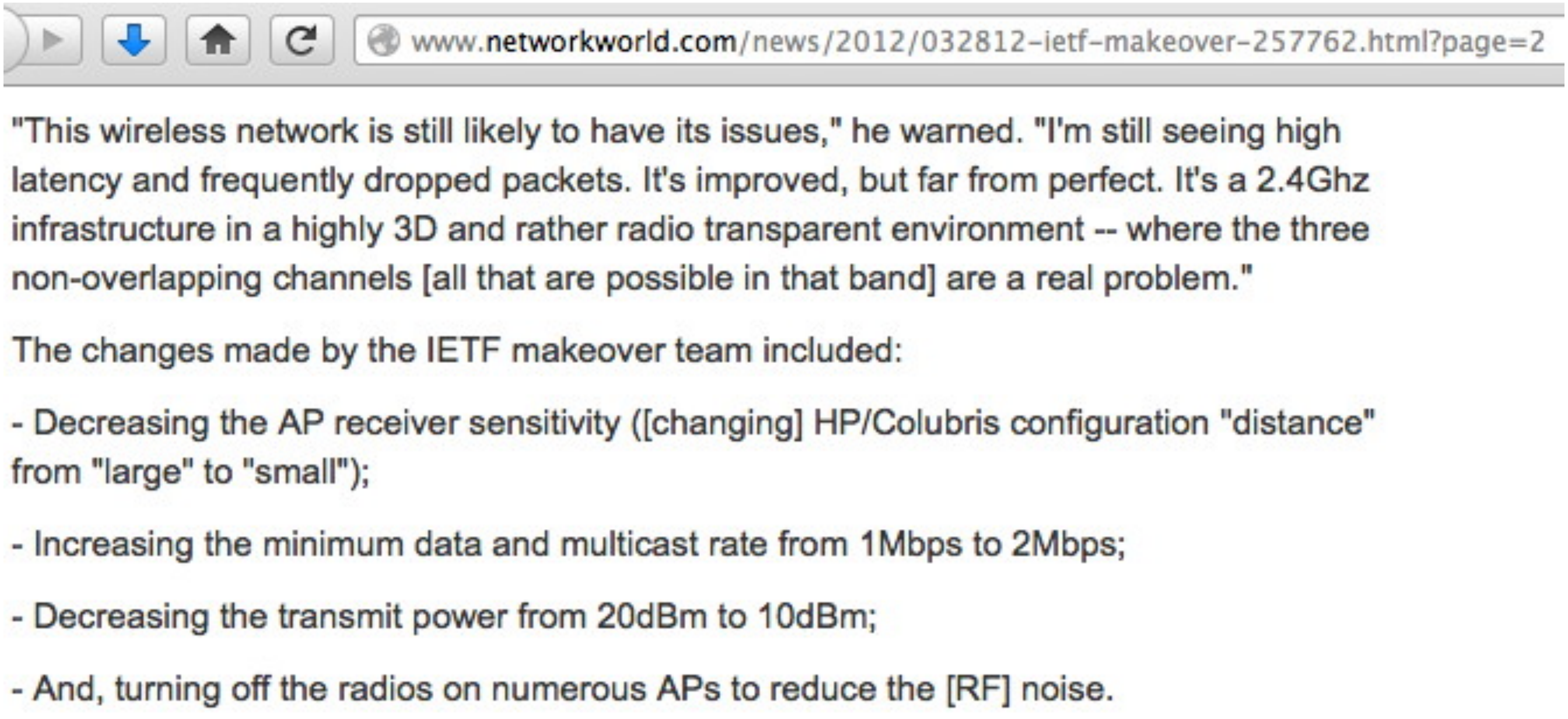


http://en.wikipedia.org/wiki/File:NonOverlappingChannels2.4GHz802.11-en.svg

If you only have four real channels, you need to use them with care. Random users standing up their own wireless access points are unlikely to choose their channels otimally.

Even the IETF has had to struggle to get meeting wireless work the way it should...

IETF Fixes For High Density WiFi Environment



"This wireless network is still likely to have its issues," he warned. "I'm still seeing high latency and frequently dropped packets. It's improved, but far from perfect. It's a 2.4Ghz infrastructure in a highly 3D and rather radio transparent environment -- where the three non-overlapping channels [all that are possible in that band] are a real problem."

The changes made by the IETF makeover team included:

- Decreasing the AP receiver sensitivity ([changing] HP/Colubris configuration "distance" from "large" to "small");

- Increasing the minimum data and multicast rate from 1Mbps to 2Mbps;

- Decreasing the transmit power from 20dBm to 10dBm;

- And, turning off the radios on numerous APs to reduce the [RF] noise.

"IETF attendees re-engineer their hotel's Wi-Fi network Extreme network makeover at Paris hotel boosts performance," http://www.networkworld.com/news/2012/032812-ietf-makeover-257762.html?page=2

Let's Talk About *YOUR* Normal Situation...

- **> [session reset] <**

- I know that K12 isn't the same as higher ed wireless (or hotel wireless or IETF wireless)

- Let's talk about **YOUR** world...

Are You Worried About Who's On Your Network?

- **Who** connects to the network at your site? Is **everyone** eligible for network access?

  Do they need to complete training or agree to an acceptable use policy (AUP) before they can get online? Does anyone actually read your AUP?

  If so, what gets covered in the training or in the policy? Are they learning they right things?

  When users connect, are they **accountable** for what they do online? For example, do they need to authenticate with a unique per-user username and password? Or does a shared password get used? Do you think that there's any unauthorized access going on?

Or Are You Worried About Their Systems?

- What sort of systems are your users using? PC laptops running Windows? Macs? iPads/iPods/iPhones? Android smart phones or tablets? Chromebooks? Is malware a problem on those systems?
- Are those systems provided by your school, or do users buy their own devices? Do you give users on **what to buy**, and **why**? (And what's the worst/weirdest thing you've seen?)
- Who maintains those systems? You? The user? No one?
- Upon connecting, do their systems get scanned with a network access control (NAC)-type system? Does a user have to download and install something? What if the user doesn't have administrative access as a matter of policy?
- Do you **monitor** what users do online? Do your users **know** this? What if the user wants to use encryption (as I do with ssh, or as someone else might do with SSL/TLS secured web connections)? Could a student even run Tor?

What If It's BYOD (Bring Your Own Device) on a TPN (Third Party Network) and There's NOYSDI (None of Your School's Data Involved): DYECWH (Do You Even Care What Happens)?

- If so, why? Its no longer about bandwidth consumption, right?

- Is it because it is disruptive and it distracts from teaching and learning?

- Do you have in-loco-parentis responsibilities?

- Or is the issue access to school PII by employees,
  no matter what they've promised?

Mobile Devices: Impossible to Resist Distraction or Mere Evil Incarnate Source of Non-Learning

- In classrooms lead by gifted teachers, mobile devices may be welcomed as an enabling tool, bringing the world to the classroom and enriching the student's learning experience.

- In other classrooms, with less dynamic teachers, mobile devices may be less welcome.

- Mobile device distraction may be a real instructional issue, but it isn't a cyber security issue, it's a teaching effectiveness/classroom management issue.

Students and In-Loco-Parentis Responsibilities

- In a K12 environment, a school may potentially have certain formal or implicit "in-loco-parentis" responsibilities related to student behavior online, just as they may in a face-to-face context.

- As a parent, I expect you to keep my kids safe from dangerous characters online, just as I do in the classroom or on the playground.

- But what if students end up in jeopardy while using their own mobile device, via their own telecom provider? Short of running cellular jamming equipment (illegal in the US), or banning all mobile devices from campus (and how would you enforce THAT?), can you, or should you even try to prevent users from doing what they will on their own devices on their own network?

Institutional Work on Personal Devices?

- Or is the issue **really** with *administrators, teachers and staff*, **not** *students*? Even if folks swear that they won't do sensitive work on their own devices (such as entering payroll information, or putting in student grades, or discussing student health conditions), will it still happen?
- If it does happen, what's the risk? Potentially, I suppose:
  -- a mobile device might get **lost or stolen**, and then, if it's not encrypted, you might have a PII spill to manage...
  -- un-backed-up mobile device data might **get lost** (are people paying attention to things like CryptoLocker?)
  -- after use of the mobile device becomes routine, and critical processes can't continue w/o using them, the institution ends up "having" to find $ to purchase/subsidize their continued use?
- How hard would you be willing to hammer someone who uses a personal device for work purposes when they shouldn't be?

Backups and WDE

- If the worry is that mobile devices will be lost, stolen, or destroyed with institutional data on them, can we make that worry go away with routine backups and pervasive deployment of whole disk encryption (WDE)?

- How are you handling those two issues now on your current site?

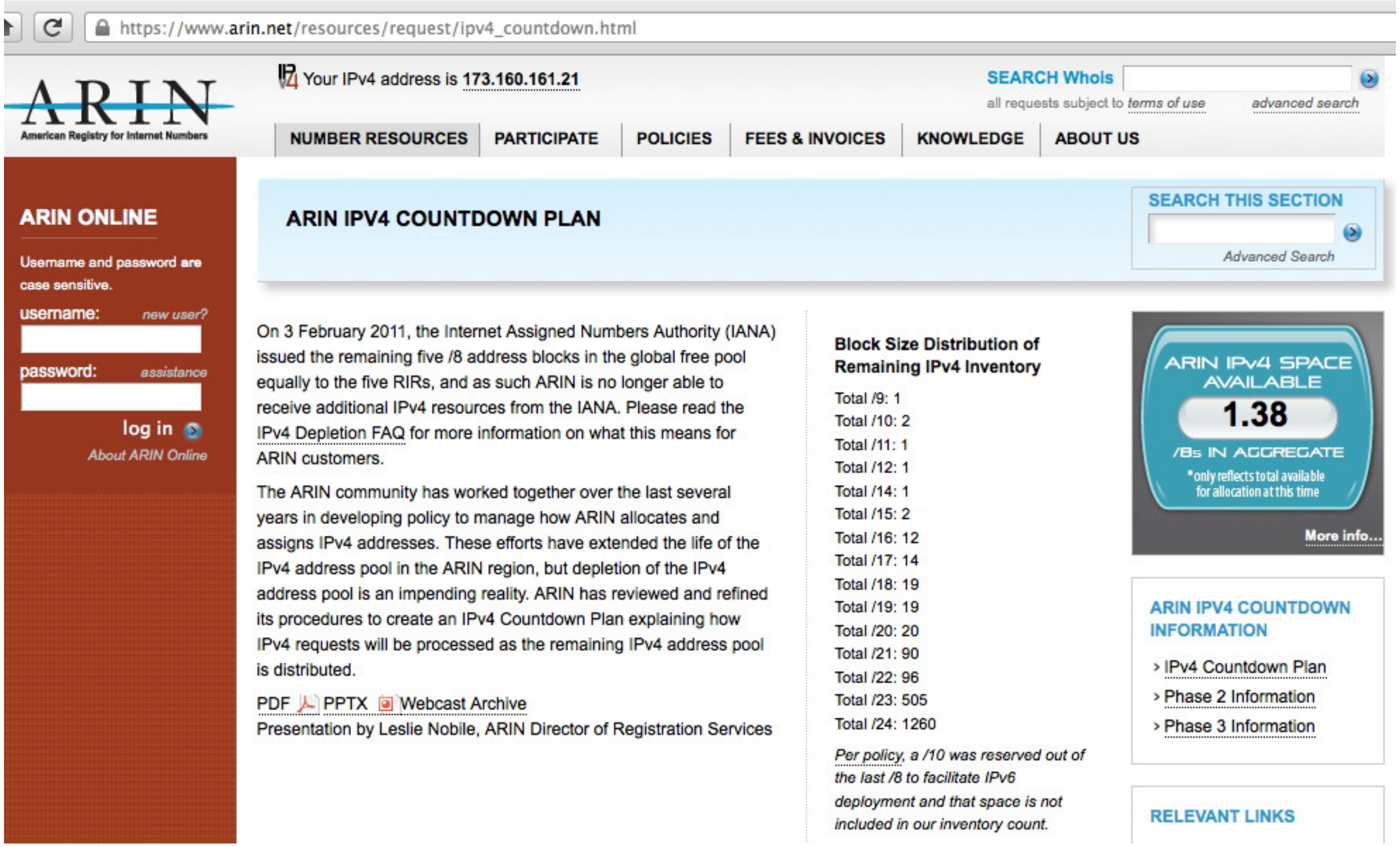
- Or is the issue the network, not the information on the device?

Do You Have A Network Firewall?

- What sort of firewall do you have, if you have one? Just router ACLs? A traditional stateful firewall? A next generation DPI box (such as a Palo Alto, etc.)? Some sort of specialized middlebox?
- WHY do you have a firewall?
  -- To block **scans/probes** from outside sources?
  -- To enforce **network policy** wrt internal users (e.g., permitted applications, allowed or blocked destinations, management of bandwidth consumption, etc.)?
  -- To **meet expectations** (perhaps from the administration/school board/parents/the media)?
  -- For **NAT/PAT** due to limited IPv4 space? (ARIN's almost out!)
- Has your firewall caused any problems? H.323? Does it make it hard for you to track abuse? Will your firewall "keep up" as bandwidth requirements scale up?

A Brief Diversion: IPv4 Address Space

- Let's assume for a second that growth in devices continues to increase. Will you have enough address space? If you need more address space you better be thinking about it now because ARIN, the regional Internet registry is just about out of space:



https://www.arin.net/resources/request/ipv4_countdown.html
ARIN
American Registry for Internet Numbers
Your IPv4 address is 173.160.161.21
SEARCH WhoIs
all requests subject to terms of use
advanced search
NUMBER RESOURCES
PARTICIPATE
POLICIES
FEES & INVOICES
KNOWLEDGE
ABOUT US
ARIN ONLINE
Username and password are case sensitive.
username:
new user?
password:
assistance
log in
About ARIN Online
SEARCH THIS SECTION
Advanced Search

ARIN IPV4 COUNTDOWN PLAN

On 3 February 2011, the Internet Assigned Numbers Authority (IANA) issued the remaining five /8 address blocks in the global free pool equally to the five RIRs, and as such ARIN is no longer able to receive additional IPv4 resources from the IANA. Please read the IPv4 Depletion FAQ for more information on what this means for ARIN customers.

The ARIN community has worked together over the last several years in developing policy to manage how ARIN allocates and assigns IPv4 addresses. These efforts have extended the life of the IPv4 address pool in the ARIN region, but depletion of the IPv4 address pool is an impending reality. ARIN has reviewed and refined its procedures to create an IPv4 Countdown Plan explaining how IPv4 requests will be processed as the remaining IPv4 address pool is distributed.

PDF PPTX Webcast Archive
Presentation by Leslie Nobile, ARIN Director of Registration Services

Block Size Distribution of Remaining IPv4 Inventory

Total /9: 1
Total /10: 2
Total /11: 1
Total /12: 1
Total /14: 1
Total /15: 2
Total /16: 12
Total /17: 14
Total /18: 19
Total /19: 19
Total /20: 20
Total /21: 90
Total /22: 96
Total /23: 505
Total /24: 1260

Per policy, a /10 was reserved out of the last /8 to facilitate IPv6 deployment and that space is not included in our inventory count.

ARIN IPv4 SPACE AVAILABLE
1.38
/8s IN AGGREGATE
*only reflects total available for allocation at this time
More info...

ARIN IPV4 COUNTDOWN INFORMATION

› IPv4 Countdown Plan
› Phase 2 Information
› Phase 3 Information

RELEVANT LINKS

Are You Thinking About IPv6?

- Even though we're almost out of IPv4 space, there's plenty of IPv6 space available.
- Are you even thinking about deploying IPv6?
- If not, you should really should be.
- But let's come back to the title of this session...

OMG, They're Inside The Walls! And/or OMG, They're NOT Inside The Walls!

- Which do you really want?
- One of the funny aspects about running any fortification (whether we're talking about a medieval castle, the Maginot Line in WW II, or a modern perimeter firewall) is that you're basically trying to balance two mutually conflicting objectives:

  -- the more people you've got "inside", the greater the chance that some of them may be untrustworthy (or infected and potentially contagious) or simply a drain on your limited support resources
  -- at the same time, you want to protect as much of your population as you can; if you leave them outside, they may get hammered.

- Will one enclave be able to balance both those factors?

Multiple Enclaves?

- Another possibility, if you wanted both the benefits of a firewalled environment yet you don't want to allow a large number of the "unwashed" "inside the walls" might be to use multiple enclaves -- one for high security assets, and another for routine user access.

- These might be adjacent/peer enclaves, or nested enclaves, with the high security enclave contained within the encompassing lower security enclave (much as medieval castles have traditionally had an outer wall around the central castle).

- Authorized users who need to access resources in the high security zone would presumably cross that boundary via a VPN or comparable solution.

Turning the Firewall Around?

- One of my colleagues from Connecticut is fairly famous for having said that if he could only afford one firewall, he'd turn it around and use it to protect the rest of his world from his users.

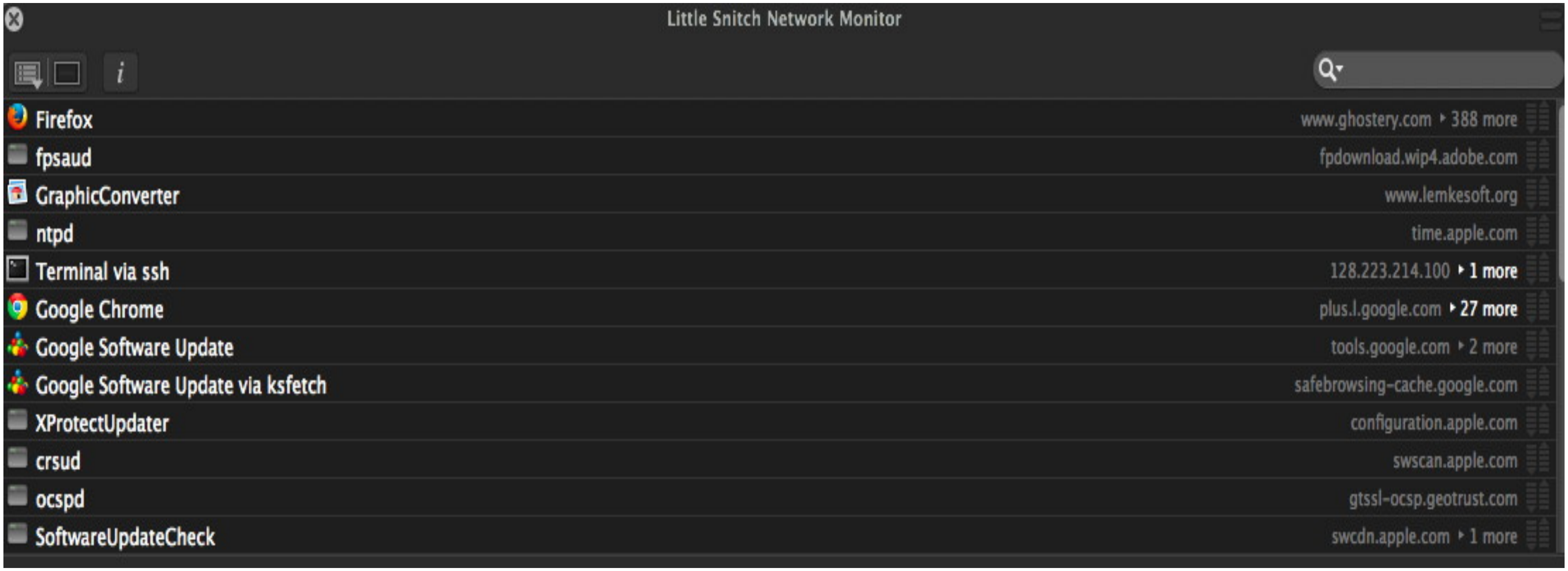
- Is THAT how we're supposed to be deploying these things? :-;

- I suppose we'd have to call that a walled garden, not a firewall. Oh wait: some sites do have those, for dealing with botted users, vulnerable systems, etc., now don't they...

  If you had the ability to isolate a problematic user when they connected, would it be easier to expand who/how many users you allowed to connect?

The "Secret Life" Of Your Workstation

- If you use a Mac, try installing Little Snitch on it some time.
- Unlike the firewall that you normally run on a system, Little Snitch is focused on what gets sent OUTBOUND. More stuff is happening outbound than you might expect...



Little Snitch Network Monitor

Firefox	www.ghostery.com ‣ 388 more
fpsaud	fpdownload.wip4.adobe.com
GraphicConverter	www.lemkesoft.org
ntpd	time.apple.com
Terminal via ssh	128.223.214.100 ‣ 1 more
Google Chrome	plus.l.google.com ‣ 27 more
Google Software Update	tools.google.com ‣ 2 more
Google Software Update via ksfetch	safebrowsing-cache.google.com
XProtectUpdater	configuration.apple.com
crsud	swscan.apple.com
ocspd	gtssl-ocsp.geotrust.com
SoftwareUpdateCheck	swcdn.apple.com ‣ 1 more

Firewalls Can't Fix "Everything"

- While firewalls can be great when it comes to blocking old fashioned scan-and-'sploit attacks, or things like brute force login attacks, they can't protect you and your users from everything.
  A perimeter firewall can't protect your network from a user who:
  -- plugs in an infected thumb drive or touches a tainted web site
  -- opens an infected attachment that his or her A/V product missed
- Firewalls also can't protect your network if:
  -- the firewall is SUPPOSED to pass the traffic (e.g., web traffic to a web server, email traffic to an SMTP server, etc.), and you're not doing DPI
  -- the attack is a DDoS, particularly if the DDoS attack is actually trying to do state exhaustion on the firewall itself
  -- the traffic doesn't go near your firewall (example: 4G traffic)
  -- the traffic is encrypted
  -- your users take steps to intentionally circumvent the firewall

What About Running Without A Firewall?

- Another alternative is to have no perimeter firewall at all. I know that this seems like running with scissors, but many universities with large networks do precisely this. Potential mitigating factors:
  -- Encourage use of non-MS Windows solutions since most malware targets MS Windows (or Android in the mobile world)
  -- Run a firewall on the device itself
  -- Make sure systems are patched up-to-date, including any/all browser helper applications (Secunia is terrific)
  -- Anti-virus isn't perfect, but can still help, so run it, too
  -- Don't install and run any publicly exposed network services
  -- Consider mitigating threats via DNS (example: OpenDNS.com)
  -- Instrument your network with an IDS (Snort, Bro, etc.)
  -- Make sure you have good abuse reporting contacts for your domain, netblocks, and autonomous system number
  -- Other things?

While We're Talking About Security...

- Are there other security things you should be worried about instead of firewalls?

- For example, given the increasing importance of the cloud, how are you doing **identity management?** And are you thinking about using something better than just plain old passwords? (e.g., **multifactor authentication**?)

- Or, since so many people are doing so many things in the cloud that really require uninterruptable network access, **is your connectivity fully redundant at every level**? What's your target SLA for network availability?

- Or how about **IPv6**? Is "security" holding up deploying that?

What Else ***Should*** We Have Talked About Today?

- What did we miss? What questions do you still have?

- Will you be more relaxed about this issue when you go back home, or are you leaving with more questions than you started with? I'd be happy either way!