IPv6 Implementation

A presentation to SLUUG by David Forrest

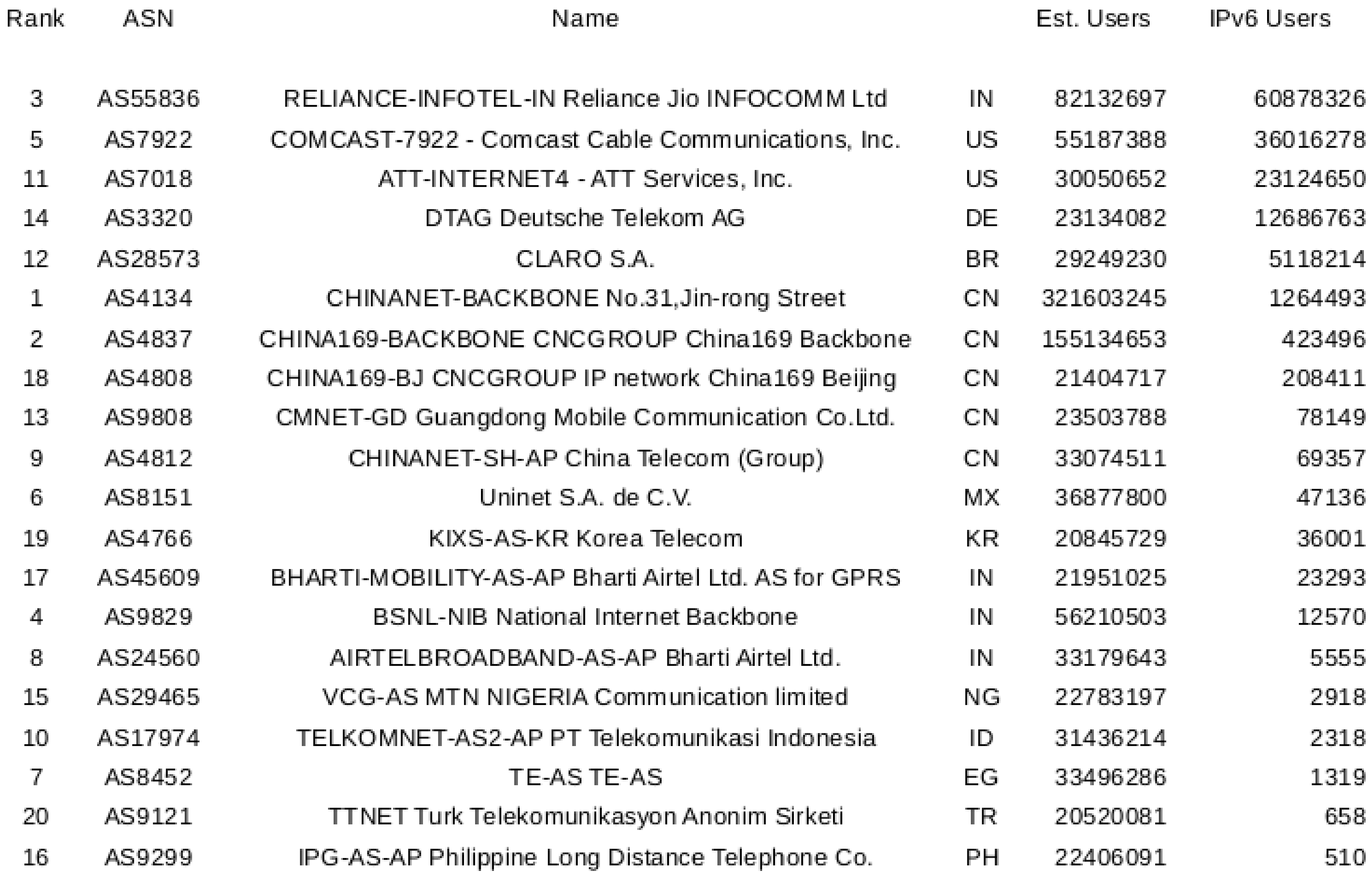
8 February 2017

David Forrest graduated from Oregon State University with a BS in BA. Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6 & 7, Raspbian, Mint, and Chrome on various local and cloud machines.

https://stats.labs.apnic.net/v6pop

Note: This is a large site – over 21,000 lines!

Autonomous Systems



Rank	ASN	Name		Est. Users	IPv6 Users
3	AS55836	RELIANCE-INFOTEL-IN Reliance Jio INFOCOMM Ltd	IN	82132697	60878326
5	AS7922	COMCAST-7922 - Comcast Cable Communications, Inc.	US	55187388	36016278
11	AS7018	ATT-INTERNET4 - ATT Services, Inc.	US	30050652	23124650
14	AS3320	DTAG Deutsche Telekom AG	DE	23134082	12686763
12	AS28573	CLARO S.A.	BR	29249230	5118214
1	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	CN	321603245	1264493
2	AS4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	CN	155134653	423496
18	AS4808	CHINA169-BJ CNCGROUP IP network China169 Beijing	CN	21404717	208411
13	AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd.	CN	23503788	78149
9	AS4812	CHINANET-SH-AP China Telecom (Group)	CN	33074511	69357
6	AS8151	Uninet S.A. de C.V.	MX	36877800	47136
19	AS4766	KIXS-AS-KR Korea Telecom	KR	20845729	36001
17	AS45609	BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd. AS for GPRS	IN	21951025	23293
4	AS9829	BSNL-NIB National Internet Backbone	IN	56210503	12570
8	AS24560	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd.	IN	33179643	5555
15	AS29465	VCG-AS MTN NIGERIA Communication limited	NG	22783197	2918
10	AS17974	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia	ID	31436214	2318
7	AS8452	TE-AS TE-AS	EG	33496286	1319
20	AS9121	TTNET Turk Telekomunikasyon Anonim Sirketi	TR	20520081	658
16	AS9299	IPG-AS-AP Philippine Long Distance Telephone Co.	PH	22406091	510

What is IPv6

The simple answer is 128 binary bits of internet addressing.

1111111100000000111111110000000011111111000000001111111100000000
1111111100000000111111110000000011111111000000001111111100000000

ff00:ff00:ff00:ff00:ff00:ff00:ff00:ff00

IPv4 uses 32 binary bits

11111111000000001111111100000000

ff00:ff00 (hex)

256.0.256.0 (octal)

A,B,C,Hosts (class)

What is IPv6

The 128 bits are divided into a “Prefix” of 64 bits
used for routing,
and a “Link-Local” network of 64 bits.

The local interface is initialized to the standard
Modified EUI-64 without special configuration

CDIR Prefix Allocations

2001:4978:000f:8640::/64

|||| |||| |||| ||||/64   Single End-user network (default prefix size for SLAAC)

- |||| |||| |||| |||/60   6rd deployments, like AT&T
- |||| |||| |||| ||/56   Minimal end sites assignments (size of a Class C V4 network) 8 binary bits 256
- |||| |||| ||||/48   Typical assignment for larger sites (size of a Class B V4 network) 256*256 containing 65,536 routeable discrete networks

Larger allocations are possible

- |||| |||| |||/44
- |||| |||| ||/40   the size of an old IPv4 Class A net
- |||| |||| |/36   possible future Local Internet registry extra-small allocations

What is IPv6

F000::/4 Unroutable – Special purposes

ff00::/8 Multicast – Big topic for later

fec0::/10 Deprecated (old site local)

fd00::/8 Site Local – (Mine is fd82:bc70:4324::/48)

fe80::/10 Link Local – Local MAC or whatever

::1/128 loopback address

All others are global addresses

2000::/3 Assigned global addresses Note: 2000::/3 in binary includes 001X (and 0011 is a hex 3)

What is IPv6

Site local addressing:

unroutable, like 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 in IPv4.

FEC0::/10 (deprecated)   (1111 1110 11 bin /10)

Better to use FD00::/8. (1111 1101 bin /8) The next 40 bits complete the global fd00::/48 prefix and are randomly set. The following 16 bits are the subnet ID, which can be used for hierarchical addresses within an organization. As usual, the final 64 address bits are the interface ID.

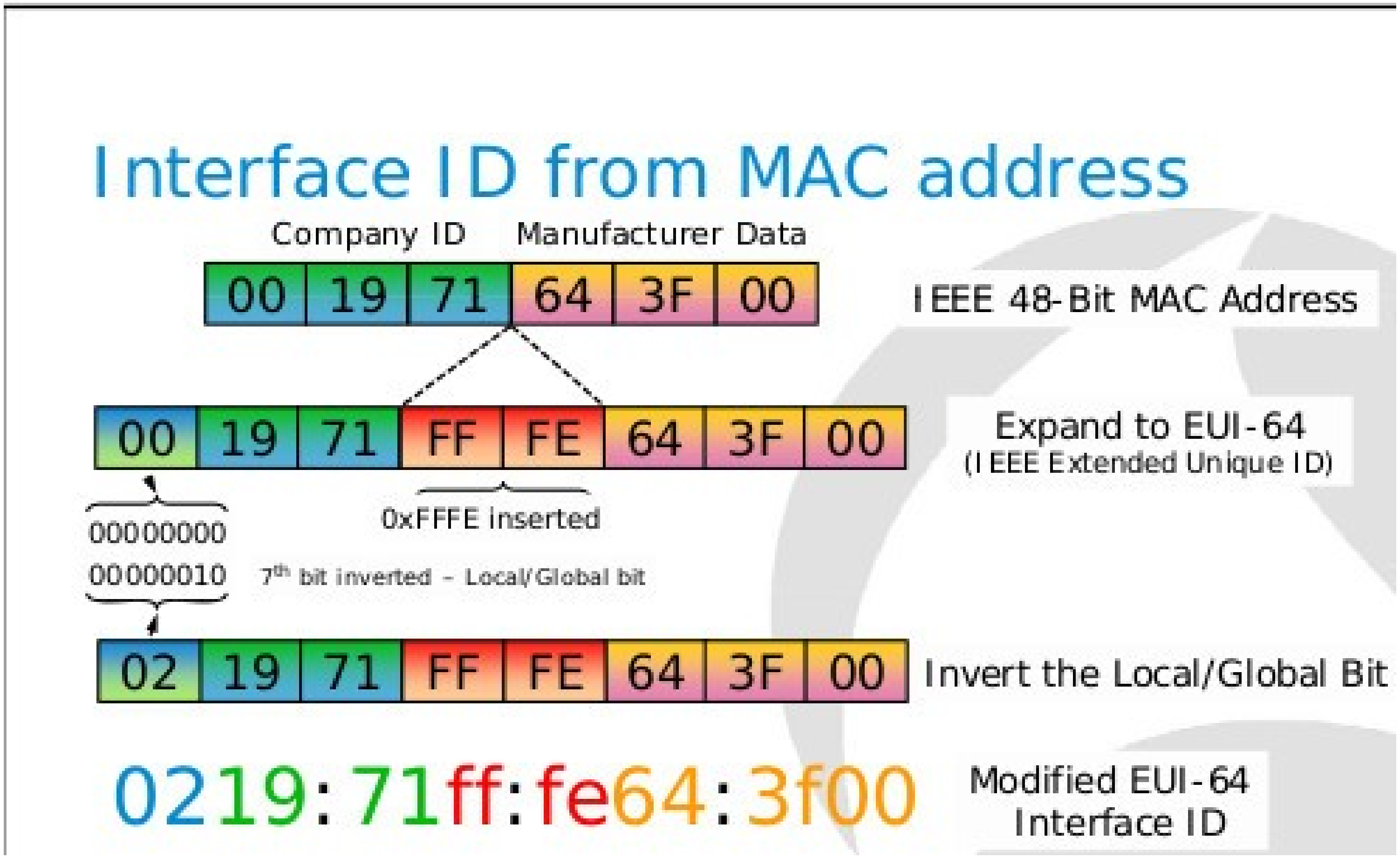
http://unique-local-ipv6.com   Website generates random unique local /48 prefixes.

fd82:bc70:4324::/48   (host -6 maplepark.com 8.8.8.8 returns: 2600:3c00::f03c:91ff:fe56:7e17)

David Forrest   Maple Park Development Corporation   http://maplepark.com

I would like to defer this topic for a possible more in depth presentation

Modified EUI-64 IPv6



Interface ID from MAC address

00 19 71 64 3F 00 IEEE 48-Bit MAC Address

00 19 71 FF FE 64 3F 00 Expand to EUI-64 (IEEE Extended Unique ID)

02 19 71 FF FE 64 3F 00 Invert the Local/Global Bit

0219:71ff:fe64:3f00 Modified EUI-64 Interface ID

What is IPv6

MPDC of Kirkwood MO ↔ Paris, FR

- IPv4 speed 99.26.132.228/9 (32 bit long dynamic address)
- ISP AT&T Internet Services
- Speed 11.5 Mbit/s

16*1+10=26;   16*8+4=132;   16*15+4=228

- IPv6 speed 2602:306:31a8:4e40:8073:a095:3096:3d85

  (128 bit long global unique address - AT&T 6rd rapid deployment)
- ISP AT&T Internet Services
- Speed 12.9 Mbit/s

```
[drf@ns1:~]$ ip a show dev br0
4: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1472 qdisc noqueue state UNKNOWN
    link/ether 00:50:04:68:d5:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.78/24 brd 192.168.1.255 scope global br0
    inet 99.178.153.41/8 brd 99.255.255.255 scope global br0
    inet 99.26.132.228/32 scope global br0
    inet6 2001:4978:f:8640::63b2:9929/128 scope global
       valid_lft forever preferred_lft forever
    inet6 2602:306:31a8:4e40::63b2:9929/128 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::0250:04ff:fe68:d5be/64 scope link
       valid_lft forever preferred_lft forever
[drf@ns1:~]$
```

CPE Residential IPv6 Security

An interesting poll last September had many comments about IPv6 security in the discussion group ipv6-ops:

http://lists.cluenet.de/pipermail/ipv6-ops/2016-September/

World wide ASN IPv6

http://v6asns.ripe.net/v/6

CPE Residential IPv6 Security

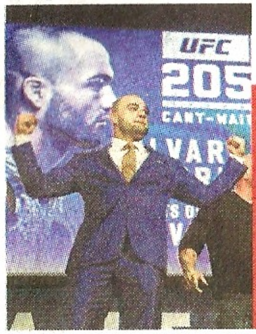
“Nobody with brains is going to go online and badmouth an ISP that supplies a CPE that has defaults that error on the side of protection-of-morons.   But they are going to badmouth an ISP that supplies a CPE that has defaults that allow morons to get easily broken into – because it's them who are going to be sucked into putting those systems back together. And they are really going to badmouth an ISP that supplies a CPE that can't have it's internal firewall turned off.”

CPE Residential IPv6 Security

I'm using AT&T U-verse and it has decided to block all incoming connections through its residential 2-Wire 3800 CPE so I'm not able to host anything globally through them. I've set up cloud machines giving 24/7 100 Mbit service D/L at low cost and believe that's best for me.

I host locally and rsync to my cloud websites hourly via crontabs and maybe upon manual changes. Happy with it too.

BUSINESS & TECH.



Ultimate Fighting Goes Hollywood Bigtime

SPORTS | B3

Tesla Gives Car Makers A Jolt of Electricity

AUTOS | B8

© 2016 Dow Jones & Company. All Rights Reserved. * * THE WALL STREET JOURNAL. Friday, September 30, 2016 | B1

Hackers Hijack Video Cameras

Attackers launched massive web assaults, fueling fresh worries about 'smart' devices

By Drew FitzGerald

Attackers used an army of hijacked security cameras and video recorders to launch several massive internet assaults last week, prompting fresh concern about the vulnerability of millions of "smart" devices in homes and businesses connected to the internet.

The assaults raised eyebrows among security experts both for their size and for the machines that made them happen. The attackers used as many as one million Chinese-made security cameras, digital video recorders and other infected devices to generate webpage requests and data that knocked their targets offline, security experts said. It is unclear whether the attackers had access to video feeds from the devices.

Those affected include French web hosting provider **OVH** and U.S. security researcher Brian Krebs, whose website was disabled temporarily.

"We need to address this as a clear and present threat not just to censorship but to critical infrastructure," Mr. Krebs said.

Closely held OVH confirmed the attack, but declined to comment further.

"We're thinking this is the tip of the iceberg," said Dale Drew, head of security at **Level 3 Communications** Inc., which runs one of the world's largest internet backbones, giving it a window into many of the attacks that cross the net.

The proliferation of internet-connected devices from televisions to thermostats provide attackers a bigger arsenal of weapons to infiltrate. Many are intended to be plugged in and forgotten. These devices are "designed to be remote controlled over the internet," said Andy Ellis, security chief at network operator Akamai Technologies Inc., some of whose clients were affected. "They're also never going to be updated."

Experts have long warned that machines without their own screens are less likely to receive fixes designed to protect them. Researchers have found flaws in gadgets ranging from "smart" lightbulbs to internet-connected cars. Wi-Fi routers are a growing source of concern as many manufacturers put the onus on consumers to do the updating.

1 Million

Estimated number of security cameras and other devices that were accessed as part of the global breach.

Level 3 identified cameras and video recorders made by Chinese manufacturer **Dahua Technology Co.** as the sources of a large share of the recent attacks, but Level 3 said other devices are being roped into a new attack network currently being assembled. Hackers often hijack the machines through computers that are already infected or poorly protected Wi-Fi routers.

A Dahua spokeswoman said Thursday the company is reviewing Level 3's research. She cautioned that malware could succeed in attacking older devices with outdated software.

"We strongly recommend users to upgrade the firmware of devices" and set a strong password to reduce risks, she added.

Dahua, which claims it is one of the world's biggest makers of security cameras and digital recorders, sells directly to consumers and businesses through its website and retailers like

Please see HACK page B6

Salesforce Battles Microsoft, LinkedIn

By Rachael King

Salesforce.com Inc. said it would press regulators in the U.S. and Europe to block **Microsoft** Corp.'s $26.2 billion acquisition of **LinkedIn** Corp., arguing the deal would hurt competition by giving its business-software rival too much control over the social-networking company's vast pool of data.

Salesforce's public broadside against the deal on Thursday came three months after it lost a bidding war for LinkedIn

UPnP

Shorewall includes support for UPnP (Universal Plug and Play) using linux-igd (http://linux-igd.sourceforge.net).

UPnP is required by a number of popular applications including MSN IM.

Warning

From a security architecture viewpoint, UPnP is a disaster. It assumes that:

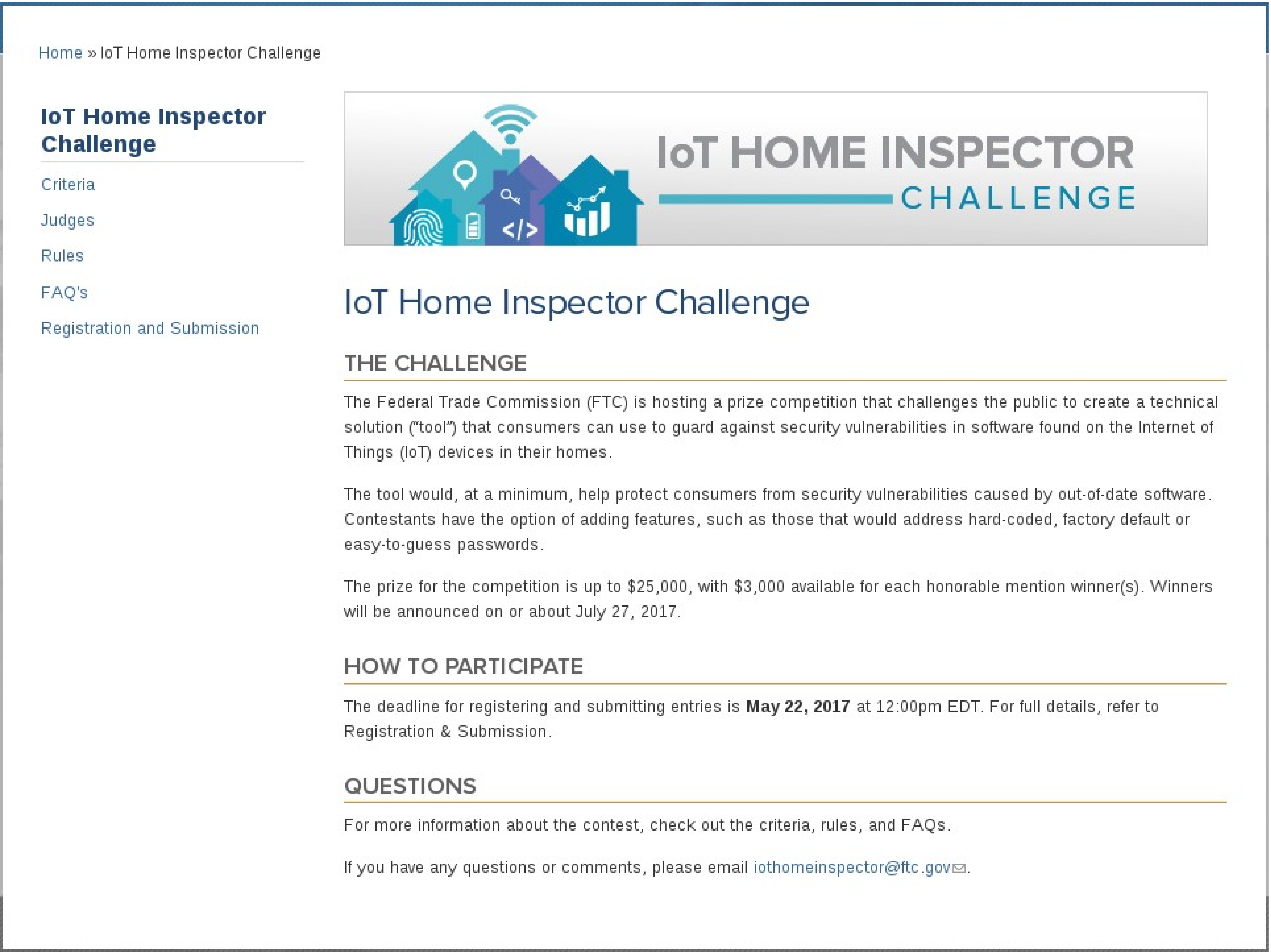
All local systems and their users are completely trustworthy.

No local system is infected with any worm or trojan.

If either of these assumptions are not true then UPnP can be used to totally defeat your firewall and to allow incoming connections to arbitrary local systems on any port whatsoever. In short: USE UPnP AT YOUR OWN RISK.

Important

Shorewall and linux-igd implement a UPnP Internet Gateway Device. It will not allow clients on one LAN subnet to access a UPnP Media Server on another subnet.



Home » IoT Home Inspector Challenge

IoT Home Inspector Challenge

- Criteria
- Judges
- Rules
- FAQ's
- Registration and Submission

IoT Home Inspector Challenge

THE CHALLENGE

The Federal Trade Commission (FTC) is hosting a prize competition that challenges the public to create a technical solution ("tool") that consumers can use to guard against security vulnerabilities in software found on the Internet of Things (IoT) devices in their homes.

The tool would, at a minimum, help protect consumers from security vulnerabilities caused by out-of-date software. Contestants have the option of adding features, such as those that would address hard-coded, factory default or easy-to-guess passwords.

The prize for the competition is up to $25,000, with $3,000 available for each honorable mention winner(s). Winners will be announced on or about July 27, 2017.

HOW TO PARTICIPATE

The deadline for registering and submitting entries is **May 22, 2017** at 12:00pm EDT. For full details, refer to Registration & Submission.

QUESTIONS

For more information about the contest, check out the criteria, rules, and FAQs.

If you have any questions or comments, please email iothomeinspector@ftc.gov✉.

Network Address Translation

NAT or Natting is used in IPv4 (PnP, VPNs etc) to add additional host addressing as required for unique situations. Not needed/used in IPv6 as the routing occurs in the prefix. It's often thought as a security enhancement but requires local routing adjustments by who? IPv6 allows end-to-end interface routing with administrative control of the prefix.

In my opinion, NAT is a hack; IPv6 is a solution.

IoT Privacy and Security

"You spelled 'confidential' wrong."

Security is a technology ~ Privacy is a policy

And proxy servers are back

With NATTING off the table, proxy servers at hierarchical network boundaries, and a good SLIP avoidance program, significant security enhancements can be effected. Of course using private addresses make us feel better but we can talk further about that.

Here's a site that describes how proxy servers help with built-in ACL

https://www.youtube.com/watch?v=qRx_RkdvpS4

appyling TECH

Where to from here?

- Multicast?
- Unique Local Addresses?
- 6to4 (2002:[IPv4]::/48)
- Tunnel Brokers?
- THE INHERENT SECURITY OF OUR SYSTEMS

  Remember, they all have a weak link: and it is us
- ??

  Questions?

  Thanks