From the desk of Rouzbeh

Dr. Rouzbeh Yassini

"Typically the end user has no knowledge that the low layer 802 network he relies on for access to his information can be used to identify where he is physically located and, via pattern recognition, provide information about the types of end points he may be connecting to..."

Hello,

Our first quarter of 2017 has contained some twists and turns, some in politics and others in industry, including within the broadband world. As we touched upon in our February issue, connected cars remain a hot spot with Intel announcing in mid-March a deal to spend $15B **TO BUY** a company called Mobileye. We, on the other hand, turn our eyes to new topics this month.

Privacy and Security in a Networked World

UNH BCoE April 2017 Newsletter Contribution by Paul Nikolich, Chairman of IEEE 802 LAN/MAN Standards Committee

Firstly, let me wish my good friend Rouzbeh a Happy Persian New Year 2017 (also known as Nowruz, the beginning of spring) which occurred at 6:29 AM Eastern Daylight Time March 20, 2017.

Now, on to our topic of the month: Privacy and Security in a networked world. I recently returned from the March IEEE 802 LAN/MAN Standards session held in Vancouver, BC, Canada, where we had hundreds of data networking technology experts from all over the globe meet to develop IEEE 802 networking standards. Two important classes of the standards 802 develops are in the areas of security and privacy. This work is primarily done in the higher layer 802.1 **ARCHITECTURE WORKING GROUP**, although some of the security work is also done in the lower layer Working Groups such as 802.11 Wireless LANs to address each group's particular operating environment.

The 802.1 Working Group has a project under development, P802E, which specifies a privacy threat model for IEEE 802 technologies and recommendations on how to protect against privacy threats. The P802E is concerned with the 802 network information (such as the Medium Access Control [MAC] addresses contained in all 802 packets) that may be used to identify a person, called Personally Identifiable Information (PII) and how an individual may control exposure of their PII to a passive eavesdropper.

Typically the end user has no knowledge that the low layer 802 network he relies on for access to his information can be used to identify where he is physically located and, via pattern recognition, provide information about the types of end points he may be connecting to, even if they are protected by the many higher layers of secure communications via encryption and virtual private network techniques. This is known as device fingerprinting. One of the mitigation approaches to this intrusion is obfuscating the individual's source MAC address through randomization of the address and the times the changes take place, while not disrupting the higher layer connections.

This helps to reduce the likelihood of association of an individual to the device he is using for connection to the Internet, its location and the types of traffic that are being accessed. More public information is available at the IEEE 802 document repository **HERE** and **HERE**.

This work parallels work done in the IETF: Privacy Considerations for **INTERNET PROTOCOLS**. This document intends to provide guidance for considering privacy in protocol design.

From an end user perspective, the bottom line is this — a persistent network connection, especially a wireless one, comes with a significant risk to your Personally Identifiable Information.

Congress Repeals Privacy Rules

Following on the heels of FCC Chairman Ajit Pai's move to alter the broadband privacy rules, the US Congress voted to **OVERTURN** the rules in late March. A key point made by the Republicans was the rules were too much government intrusion and they were unfair since ISPs like Verizon and Comcast were being treated tougher than Google and Facebook. It's expected President Trump will sign the repeal measure.

And, the Pai-led FCC also is also taking aim at the network neutrality rules that treat broadband as a 21st century utility, getting the attention of the *NY Times* **EDITORIAL BOARD**. What is likely to follow on the heels of network neutrality's demise? Here's a view from **MIT TECHNOLOGY REVIEW**.

Meanwhile, at the FCC...

There have been positive developments with the Broadcast Incentive Auction. As you might remember the auction was established to repurpose valuable "low-band" spectrum previously used for analog broadcast TV for wireless broadband services, both licensed and un-licensed. The auction was comprised of two separate but interdependent auctions called the reverse auction and the forward auction, and is well described on the **FCC SITE** if you are interested in the details. The conditions to meet the "final stage rules" were met on January 18, 2017 with the auction ultimately repurposing 84 MHz of spectrum, 70 MHz for licensed use and 14 MHz for unlicensed use.

As of March 30th the assignment phase, during which winning bidders placed additional bids to try and secure their desired placement in the spectrum, was completed. This marks the completion of the final phase of the Broadcast Incentive Auction, bringing in total proceeds of $19,768,437,378 of which a little over 10 billion goes to the TV broadcasters. The FCC will soon make a public announcement of the winning bidders for both auctions and those broadcasters that will be reassigned to new channels (repacking). The announcement will kick off a 39-month post-auction **TRANSITION PERIOD** on which we will periodically report.

As my colleague Paul wished me earlier in the newsletter, I extend to you thoughts for a great and peaceful Spring 2017.

Rouzbeh