Interview with Kirill Levchenko

RIK FARROW

Kirill Levchenko is an Associate Professor at the University of Illinois at Urbana-Champaign. He received his PhD from the University of California, San Diego in 2008 and his BA in mathematics and computer science from the University of Illinois at Urbana-Champaign in 2001. His research applies evidence-based techniques to a broad range of computer security domains, including e-crime and cyber-physical systems. klevchen@illinois.edu

Rik is the editor of *;login:*. rik@usenix.org

As I read the Triton paper in the CSET '19 workshop [1], I found myself wanting to talk to some of the folks who had been working on this project. The recent software and documentation issues with Boeing's 737 Max that have led to the deaths of over 300 people provided some additional impetus. Karl Koscher, a member of the project, had written for *;login:* before about the automotive CAN bus [2], so I asked him for recommendations about who he thought I should talk to.

Karl suggested Kirill Levchenko. I don't recall ever meeting Kirill, but I'd certainly heard of him through various papers published by a large group of primarily West Coast researchers related to tracking Internet crime, work on hacking cars, and other topics [3].

As we worked on the interview, Kirill reminded me that the Triton Project was a collaboration of many people, something you can see right away by looking at the CSET paper [1]. Still, I found myself wanting to talk to Kirill, as I knew little about him beyond his published works.

Rik Farrow: Where did the idea for an avionics testbed come from?

Kirill Levchenko: Several years ago I and a group of researchers became interested in the security of electronic systems on aircraft (avionics). This was in part because of my own interest in aviation and in part because of the excellent work on automobile security done by my colleagues at UC San Diego and the University of Washington. Their experience with automobiles and my passion for aviation got us thinking about aircraft.

But unlike with the automobile work, we couldn't buy an airplane to test. So we had to focus on the parts of interest to us, the Line-Replaceable Units (LRUs) that might expose an electronic attack surface. We decided to start with the Communication Management Unit (CMU), which provides digital communications between aircraft and ground using a system called ACARS. To get this unit to work in the lab, we needed to recreate the environment it would have on board the aircraft, which meant building a testbed that would allow us to simulate parts of the aircraft—its communication networks and other LRUs.

RF: I'm hoping that avionics networks don't use TCP/IP. What do they use?

KL: The avionics of the aircraft we're looking at (everything designed before the Boeing 777, which includes the 737 and 747) uses the ARINC 429 bus, which transmits 32-bit frames at 12.5 kbps or 100 kbps.

ARINC 429 is unidirectional: there is one transmitter and one or more receivers. This provides some constraints on information flow. For example, the flight map in your in-flight entertainment system probably receives aircraft position information from the aircraft via ARINC 429, but, because ARINC 429 is unidirectional, the in-flight entertainment system cannot send any information back.

ARINC 429 is very similar to the CAN bus used in automobiles, with the notable difference that CAN is bi-directional—that is, there can be more than one transmitter on the bus.

Newer aircraft, such as the Boeing 787 and Airbus A380, use an Ethernet-based protocol called AFDX.

RF: Cars have telematics, usually via cellular networks, and Bluetooth. Both are connected to the CAN bus as vectors for attacks. What type of vectors are you considering for attacks against ARINC 429?

KL: Two of the most interesting vectors, from our point of view, are ACARS (handled by the CMU) and the software update process. These are the two vectors that originally motivated the testbed. ACARS (Aircraft Communications Addressing and Reporting System) provides short message digital communications between aircraft and ground systems. It was originally developed for reporting aircraft status (landed, at gate, etc.) but quickly came to be used for many other kinds of communications.

RF: Are updates to systems signed?

KL: Updates for most systems used on aircraft like the 737 and 747 are not signed.

Newer aircraft such as the Boeing 787 and A380 may use signed updates. This is something industry is working on.

There are no over-the-air updates while an aircraft is in the air, for obvious reasons. There are some products that allow you to do the update wirelessly when the aircraft is in for maintenance, but I am not aware of airlines using these. With the traditional ARINC 429-based data loader, there is no update verification built into the protocol. Of course, devices can implement their own checking, but we have not seen this in the avionics we've looked at.

RF: In Figure 2 in your CSET paper [1], you show USB 429 adapters. I assume these handle converting the serial protocol to USB, and the USB 429 driver portion is a Linux kernel module that acts as the device driver, so the emulated software you use as the bus will work, and daemons can present the 429 serial inputs or outputs as TCP ports?

KL: Yes, that's basically correct. To be specific, the driver is in userspace and connects to the USB 429 adapter using a library provided by the adapter vendor. The r429d daemon then provides access to the ARINC 429 bus over TCP (local access only). This allows us to create virtual devices that speak ARINC 429 to physical devices through the adapter.

RF: Was it hard to source the devices needed for the testbed?

KL: For aircraft such as the 737, no, we can get parts from avionics parts suppliers (who get them from aircraft that get torn down) and even from eBay. It's harder to get parts for newer aircraft, like the Boeing 777 and later, which don't have as large a parts market.

References

[1] S. Crow, B. Farinholt, B. Johannesmeyer, K. Koscher, S. Checkoway, S. Savage, A. Schulman, and A. C. Snoeren, and K. Levchenko, "Triton: A Software-Reconfigurable Federated Avionics Testbed," 12th USENIX Workshop on Cyber Security Experimentation and Test (CSET '19), USENIX Association, 2019: https://www.usenix.org/system/files/cset19-paper_crow.pdf.

[2] I. Foster and K. Koscher, "Exploring Controller Area Networks," *;login:*, vol. 40, no. 6 (December 2015): https://www.usenix.org/system/files/login/articles/login_dec15_02_foster.pdf.

[3] Published works of Kirill Levchenko: https://www.researchgate.net/scientific-contributions/70179178_Kirill_Levchenko.