# 1400 - Linux-Stack Based V2X Framework: All You Need to Hack Connected Vehicles

Saturday at 14:00 in Track 3
45 minutes | Demo, Tool
**p3n3troot0r (Duncan Woodbury)*Hacker***

**ginsback (Nicholas Haltmeyer)*Hacker***

Vehicle-to-vehicle (V2V) and, more generally, vehicle-to-everything (V2X) wireless communications enable semi-autonomous driving via the exchange of state information between a network of connected vehicles and infrastructure units. Following 10+ years of standards development, particularly of IEEE 802.11p and the IEEE 1609 family, a lack of available implementations has prevented the involvement of the security community in development and testing of these standards. Analysis of the WAVE/DSRC protocols in their existing form reveals the presence of vulnerabilities which have the potential to render the protocol unfit for use in safety-critical systems. We present a complete Linux-stack based implementation of IEEE 802.11p and IEEE 1609.3/4 which provide a means for hackers and academics to participate in the engineering of secure standards for intelligent transportation systems.
p3n3troot0r (Duncan Woodbury)
Car hacker by trade, embedded systems security engineer by day. Entered the field of cyberauto security in 2012 through the Battelle CAVE red team and had the opportunity to improve the world by hacking transportation systems. Co-founded multiple security companies focused on building tools for automated exploitation of automotive systems (http://www.silent-cyber.com/), open-source frameworks for V2X, secure digital asset management, and 3D printing electric cars (https://hackaday.com/tag/lost-pla/) out of your garage (http://fosscar.faikvm.com/trac/). DEF CON lurker since the age of 17, recently having joined forces with friends and mentors to organize and host the DEF CON Car Hacking Village.

p3n3troot0r began working V2X with ginsback two years ago and realized the opportunity, in lieu of any open-source or full-stack V2X implementation, to bring the security community in to the driver's seat in the development of next-gen cyberauto standards. Together they have engaged the thought leaders in this space, and via the long-awaited integration of this stack into the mainline Linux kernel, the global development community is given the opportunity to participate in the development of automated and connected transportation systems.
ginsback (Nicholas Haltmeyer)

AI researcher and security professional. Began work in automotive security through the DEF CON Car Hacking Village and have since developed V2X software and routing schemes. Extensive experience in signal processing and RF hacking, including vital sign monitoring, activity recognition, and biometric identification through RF.

Given the (abyssal) state of automotive cybersecurity, ginsback aims to develop and field tools for V2X that open collaboration with the hacker community. As intelligent transit reaches critical mass, attacks on V2X infrastructure have the potential to cause incredible damage. ginsback partnered with p3n3troot0r to develop a free as in freedom V2X interface and extend an invitation for the community to discover and fix flaws in the design of what will soon be a massive network of connected vehicles.

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday