دشمن پشت دروازه؛ هک شدن خودروها

چارلی میلر و کریس والاسک دو محقق حوزه امنیت با مشارکت مجله وایرد نشان دادند چطور می‌توان از راه دور یک جیپ چروکی مدل 2015 را هک و سیستم‌های حیاتی آن را کنترل کرد. این محققان معتقد هستند مشابه این هک را می‌توان روی صدها هزار خودرویی که روزانه در جاده‌ها تردد می‌کنند، پیاده کرد. هر دو این هکرها تجربه بالایی در حوزه امنیت دارند. میلر پیش از این به‌عنوان هکر با NAS و همین طور به‌عنوان کارشناس حوزه امنیت با توییتر همکاری داشته است. والاسک نیز هدایت تحقیقات حوزه امنیت IOActive را بر عهده داشته است.

در یک آزمایش، وقتی گزارش‌گر وایرد خودرو را در یک بزرگ‌راه می‌راند، این هکرها از راه دور و از فاصله ده مایلی قادر بودند رادیوی خودرو را دستکاری و حتی خودرو را خاموش کنند. بنا به ادعای این هکرها، آن‌ها قادر به اتصال به سیستم رسانه یا Head unit جیپ بودند و از این طریق این امکان برایشان فراهم می‌شود که سایر سیستم‌های این خودرو را نیز کنترل کنند. Head unit یک خودرو به‌طور معمول به چند ECU (واحد کنترل الکترونیکی) موجود در خودرو متصل است. ممکن است در یک خودرو تا دویست ECU وجود داشته باشد. نفوذ به Head unit این خودرو موسوم به UConnect برای این دو هکر حدود یک سال طول کشیده و به گفته میلر یک حمله سه‌مرحله‌ای است.
جان آلن تحلیل‌گر حوزه امنیت معتقد است این دو هکر برای اجرای حمله خود دسترسی فیزیکی به خودرو داشته‌اند: «آن‌ها پیش از این‌که خودرو را هک کنند دسترسی فیزیکی به آن داشته‌اند.» اما میلر می‌گوید آن‌ها می‌توانند به‌سادگی حمله مشابهی را روی هر یک از صدها هزار خودروی آسیب‌پذیر در حال تردد در جاده‌ها اجرا کنند: «دسترسی به خودرو فقط با بهره‌گیری از آسیب‌پذیری امنیتی موجود در Head unit و از طریق اینترنت صورت گرفته است. اجرای این هک به هیچ گونه دسترسی فیزیکی یا تغییر در خودرو نیاز ندارد.» آن‌ها از تجهیزات به نسبت ساده‌ای برای اجرای این هک کمک گرفته‌اند. میلر و والاسک از تلفن آندروییدی Kyocera متصل به لپ‌تاپ مک‌بوک به‌عنوان یک Hotspot وای‌فای استفاده کرده‌اند.
خودروسازان از طریق شبکه‌های ارتباطی سلولی به‌طور پیوسته اطلاعات خودرو را جمع‌آوری می‌کنند و در صورت نیاز به نگهداری یا تعمیر خودرو هشدارهای لازم را به رانندگان می‌دهند. امروزه خودروسازان در حال افزودن روترهای وای‌فای به محصولات خود هستند تا امکان اتصال به اینترنت همراه را نیز فراهم کنند. میلر می‌گوید مدل جیپی که در این هک استفاده شده، به وای‌فای هم مجهز بوده است، ولی این عملکرد سلولی خودرو بوده که اجازه دسترسی را داده است.

شرح شکل: میلر و والاسک از شبکه تلفن سلولی برای حمله به بخش سرگرمی خودرو جیپ که به اینترنت متصل است، استفاده کردند.

تاریخ انتشار:

18 مهر 1394
