Vehicle Telematics: The Good, Bad, and Ugly

Hal Berghel, University of Nevada, Las Vegas

Vehicle telematics may be thought of as an Internet of Things (IoT) on wheels. And just as with the IoT, the technology is a mixed blessing, with serious privacy and security implications.

Just as the shifts changed at Jaguars, a noted Las Vegas "gentleman's club," one afternoon in May 2003, FBI agents burst into the manager's office, guns in hand. So, according to the *L.A. Times*,[1] began Operation G-Sting, the federal sting that convicted four Clark County (Nevada) Commission members and two San Diego, California, city councilmen on bribery charges.

Flash forward to March 2010. A disgruntled former employee of the Texas Auto Center (TAC) in Austin remotely triggers the installed aftermarket GPS devices to set off car alarms, activate headlights, and shut off the engine starting systems for roughly 100 of TAC's customers' personal vehicles, leaving them stranded with disabled or unusable automobiles.[2]

What does the conviction of four county commissioners from Las Vegas have to do with the TAC hack? The answer is vehicle telematics, one of the emerging digital threat vectors in use by hackers, criminals, terrorists, governments, and invasive businesses.

FAITH-BASED SECURITY

The TAC (www.texasautocenter.com/) is apparently one of the car dealers of last resort for those who are credit challenged. These car centers have been a staple in poor communities for many years, specializing in high-interest and no income, no job, no assets (NINJA) loans. The trick to making such loans profitable is the ability to recover the car if the payments are in arrears. In years past, this was the purview of the repo man. Now, we throw new wave repo technology at the problem in the form of a digital, remotely operated "real-world asset protection" system like Payteck (http://www.payteck.cc/).

TAC used Payteck's GPS and starter-interrupt systems for asset management (i.e., theft reduction)—apparently a winning combo for finance companies that specialize in NINJA car loans. Unlike the GPS trackers used formerly, Payteck's system enables finance and used car companies to both locate and disable the car if payments became delinquent. This sounds fine in practice, but what if a disgruntled former employee of TAC used a coworker's login credentials to go rogue on the unsuspecting used car buyers—which is exactly what happened when that former employee disabled roughly 100 recently sold vehicles as an

Digital Object Identifier 10.1109/MC.2019.2891334
Date of publication: 11 March 2019

0018-9162/19©2019IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

act of revenge against TAC. This reads like a bad NSA surveillance expose: one has to ask, "Where were the checks and balances?" Apparently, the Payteck and TAC folks assumed that theft or unauthorized elevation of authentication privilege could never happen to them and that it would be impossible for an employee or hacker to behave improperly. This is an example of what I have called *faith-based security* (*FBS*),[3] a cousin of security through obscurity (STO). If such strategies are effective, it's by accident rather than design.

Even if you are financially well heeled, your cars aren't immune to FBS and STO measures. Don't get lulled into complacency because you avoid NINJA financing. One may accomplish the same objective with any car through the internal computer system—even by hacking the audio system.[4] I will return to this theme.

Operation G-Sting was a hack of a different color; this time, it was the Feds who took advantage of the vehicle telematics system. The convicted bagman, the head of the Clark County Commission and a former cop, decided that to best avoid government eavesdropping, he'd conduct all sensitive discussions regarding the bribing of elected officials in his car, which just happened to have OnStar enabled. Much to his chagrin, the preinstalled General Motors' OnStar folks were all too willing to activate the microphone for the FBI, thereby allowing the latter to listen in on conversations in the vehicle (all without benefit of warrant). These recorded conversations provided the key evidence for the convictions. In one of life's little ironies, after the county commissioners had been released from prison, the Ninth Circuit Court (which includes both California and Nevada) ruled that such OnStar spying was illegal because it required tampering or disabling the OnStar vehicle recovery mode, which violates the customer's terms of service.[5] That is, the Ninth Circuit Court ruled that OnStar wiretapping and surveillance represented an egregious violation of a corporate term of service under current law (http://www.law.cornell.edu/uscode/text/18/2518)—but not that it in any way violated the customer/citizen's expectation of privacy!

In a bizarre twist, the 2011 OnStar revised terms of service extended OnStar's promised focus on continuous vehicle recovery mode and specifically allowed OnStar to collect driving and location data from car owners even if they had cancelled their OnStar subscriptions. This produced a public relations nightmare for OnStar, which, temporarily at least, stopped this practice[6] at the behest of former Senator Al Franken (D, Minnesota) and Senator Chris Coons (D, Delaware). OnStar has since resumed the practice of collecting any information, for any purpose, at any time (https://www.onstar.com/content/tcps/us/20180227/privacy_statement.html).

These prosecutions were interesting from several perspectives. One of the two San Diego city councilmen was exonerated in 2010 (http://www.sddt.com/News/article.cfm?SourceCode=20101014tza). The convicted former politicians who made up the Las Vegas contingent of bribe recipients have apparently set aside their political aspirations for the moment and directed their attention to less visible vocations in public relations, marketing, and the law.[7]

BIG BROTHER TELEMATICS

Vehicular telematics is but one of the later instantiations of Orwellian digital dystopia, but with its own distinctive twists including the increased exposure to malicious hacking and the potential for abuse of individual privacy.

As with other innovative technologies, modern vehicular telematics is a mixed blessing. There is no doubt that some telematics associated with convenience, safety, mechanical reliability, and entertainment are welcomed by many consumers and to varying degrees. With my latest vehicle, I most appreciate features like forward collision alert, 360° surround vision, distance indication, front pedestrian braking, cross traffic alerts, active cruise control, lane-keeping assistance, parking sensors, blind-spot monitoring, navigation systems with traffic alert, adaptive lighting, and a host of other warnings and driver assistance features. I'm confident the roads would be safer if such features were available on all modern vehicles, and I'm pleased to see that some car manufacturers like Subaru and Toyota now include most of these in their base models.

No matter how useful, these telematics features are the least interesting from the point of view of security and privacy. The more intriguing features are those that entail security and privacy vulnerabilities. I'll begin with a convenience feature that largely goes unnoticed these days: the vehicle remote, also called the *wireless fob*, which is used in lieu of a key to control access to a vehicle or remotely initiate some action on the vehicle (e.g., remote start). Originally designed about 40 years ago for remote keyless entry, fobs are functionally similar to more feature-rich mobile devices.

Used as a substitute for the keypad on the driver's door, the fob is a short-range radio-frequency (RF) transceiver. In my case, the fob passively exchanges proximity information with the car so that, when it is within a few meters of the car, a logo is projected on the ground where a sensor detects motion, opens the rear hatch, turns on various lights, and activates the opening buttons on the door handles. Additionally, push buttons on the fob enable it to communicate instructions to the car

to remotely start the engine, lock or unlock the doors, open the rear deck hatch, and set off the car alarm. Many of these features are further configurable. Thus, the modern fob has taken on the role of the modern remote controller associated with multimedia devices.

What's the problem then? To begin with, RF appliances are never optimal for security-sensitive applications; RF neither respects individual privacy nor obeys property lines. So any communications between car and fob should be viewed as broadcasts throughout the immediate neighborhood. This makes them susceptible to a gamut of hacks, ranging from denial-of-service (e.g., to deny vehicle access) to replay attacks, to name but two.

And this is nothing new. Computer scientist Avi Rubin has been lecturing about such vehicle insecurities for many years.[8] The Center for Automotive Embedded Systems Security at the University of Washington, Seattle, and the University of California, San Diego, (www.autosec.org) has been conducting research on vehicle telematics vulnerabilities for even longer. One of the center's classic papers from 2010[9] references articles on vehicle vulnerabilities as far back as the early 2000s. In a subsequent paper,[10] these same researchers evaluate a cornucopia of attack vectors that affect modern automobiles. One of this center's projects, CarShark, provides working demonstrations of these vulnerabilities. Researchers there have since extended their work to include using vehicle telematics for driver profiling and fingerprinting. The irony that this research has been covered so extensively over the past 10 years that it has been featured in *Popular* Science[11] should not be overlooked.

Confirmation of these problems isn't hard to obtain. Samy Kamkar (https://samy.pl) recently developed a suite of such attacks[12] and reported the same in a 2015 DEFCON talk.[13] His tool, OwnStar, runs a replay attack against OnStar fobs by inserting itself between a GM vehicle's transceiver and either OnStar apps on mobile devices or the fobs themselves. His video explains all of this in detail.

While OwnStar targets older RF-based keyless entry systems, modern vehicles use rolling code systems that prevent OwnStar replay attacks. Rolling codes use algorithms to generate code sequences based on pseudorandom numbers. As long as the vehicle transceiver and the fob/mobile app transceiver use the same seeds and rolling code algorithm, the sequences can be validated even if the codes are nonconsecutive. This means that, while continuously changing, rolling code generators suffer from the serious defect of predictability: once the algorithm is known, an endless sequence may be generated, each element of which can be determined to be legitimate. Based on this observation, Kamkar developed RollJam,[14] which offers a replay attack for modern RF-based keyless entry systems that use rolling codes. This reaffirms our observation that RF is really not effective when security is important (i.e., if you want to prevent car, boat, or airplane theft; garages from being opened by home invaders; proximity card lock compromises; and so on).

A question naturally arises: Why do car companies use digital technologies that are so easily compromised? In this case, challenge-response authentication based on a reasonable key derivation function would go a long way toward avoiding replay attacks. Such technology has been well understood and successfully deployed for decades, so why isn't it used for keyless access systems? The answer is that manufacturers' cost benefit analyses suggest that their legal exposure to the resulting safety deficiencies and security vulnerabilities from nonuse will not cost them much. In the absence of regulations with teeth or large-scale public blowback, there is little incentive to protect the customer. Since the beginning of the industrial revolution, the absence of risk has always been a strong disincentive to serious process improvement where product safety is at issue. (Note, by the way, that these same vulnerabilities may apply to other remote access systems including remote garage door openers, proximity card access systems, and so on).

But keyless access is not the greatest security and privacy vulnerability; far greater is the new cell phone synchronization environment. A decade or so ago, Bluetooth synchronization between a cell phone and the vehicle's communication systems was focused on hands-free use of the phone. The vehicle's voice recognition system sent the appropriate codes to the phone (for dialing, searching contact lists, and so forth) but otherwise played a passive, facilitative role in the communication. On modern GM systems I'm familiar with, and presumably other systems as well, the Bluetooth synchronization actually uploads data from the cell phone and stores the data in the vehicle's computer database—without the user's permission and possibly without the user's knowledge. This compounds the privacy problem of a lost cell phone.

Even if cell phone data are encrypted and the phone is locked, it is not that difficult to retrieve PINs, passwords, and encrypted data in plain text. Companies such as Cellebrite (www.cellebrite.com) have, for decades, offered mobile forensics devices that serve this purpose. But the lowest hanging fruit in this attack vector is the automobile. The only data access protection that my car offers is a four-number PIN valet lock. This bad idea is both polished and refined: it offers limited data protection against a determined adversary while at the same time making vehicular telematics inconvenient for the owner. Such bad ideas don't just happen naturally; they require serious effort from incompetent designers. This isn't innovation: it's enervation.

A similar situation applies to the access of data through the onboard diagnostics (OBD) ports under the dash. While it seems reasonable to make diagnostic data available to manage

engine performance, optimize safety systems, and so on, when OBD ports became the preferred option for smog tests a decade or so ago, that opened an entirely new vulnerability to the car owner. While automobile manufacturers could have restricted OBD information sharing to just those data of use to smog inspectors, instead they opened the OBD ports to a much wider variety of data—including historical accelerometer data, speed data, GPS data, and trip timings and usage data.

Originally, these "black box" OBD devices were used by insurance companies (e.g., Progressive's Snapshot program) to award user premium rate discounts, i.e., drivers were even given discounts to have them installed in their vehicles. As any good personal injury attorney will attest, one of the first questions attorneys ask of accident investigators is whether the "other" vehicle had one installed so that it may be subpoenaed as evidence in court. Sans black box, an attempt will be made to recover vehicle data directly from the automobile. This information can be used by an insurance company to confirm good driving behavior, but it can also be used by personal injury attorneys and prosecutors to justify liability claims for allegedly bad driving behavior. Somehow this equivalence just never seemed to register with the public. Incidentally, OBD black box devices are now popular general aftermarket automobile appliances for GPS tracking, monitoring driving behavior, and so on (https://www.blackboxgps.com/products/blackbox-gps-3s-locator-obd-ii).

MARKETING VERSUS PRIVACY PROTECTION

I don't mean to impart any special blame to General Motors or OnStar for breaches in personal security and privacy. All car manufacturers offer similar services. Ford SYNC, based on Microsoft's Auto OS, offers the same range of services as GM/OnStar. The same may be said for LexusLink, BMW Assist, Mercedes Mbrace, and so forth. As near as I can tell, all manufacturers approached telematics exclusively from a marketing point of view with little or no consideration for consumer privacy protection. This is not to deny the potential advantage to collision detection and reporting capabilities. Nor is it to criticize the use of motor vehicle event data recorders (MVEDR) per se. However, for detection and reporting accidents, MVEDRs don't require more than a few minutes of precrash recorded data collection to serve the passenger's public safety interests. So, even if we assume that vehicle speed, engine revolutions per minute, service brake status, lateral acceleration, roll angles, antilock braking system status, seatbelt status, steering wheel position, and airbag-related data would be useful to first responders, a simple first-in, first-out data collection strategy that would retain only the most recent data would serve perfectly well. In other words, the claim that event data recorder information has to be retained for longer periods or shared with the manufacturer via telephone or satellite links doesn't pass my smell test. That was essentially the issue that Sens. Franken and Coons raised with OnStar.

At the heart of privacy vulnerability is the manufacturer's insistence on a simple, integrated vehicle data retention policy that will serve all demands, e.g., crash reporting, smog inspection, manufacturer's revenue potential from the sale of telematics options, manufacturer and third-party marketing and advertising revenue, and so forth. It is this oversimplistic integration that leads to the problem. Of course, the rationale is obvious: automobile manufacturers have discovered that using and selling access to these data can be enormously profitable.[15] Car companies and dealers are finding that the sale of customer data is another lucrative source of profit along with the interest and fees associated with car loans. However, unlike with car loans, the customer has no right of refusal regarding the sale of his or her personal data.

It is quite telling that automobile manufacturers have not packaged these data collection technologies in the form of optional modules that the customer may or may not purchase and that may be removed if the service is no longer desired. Manufacturers do not want to give customers that choice because 1) many would choose not to purchase these options and 2) the manufacturer would lose the opportunity to repurpose the data for profit. In the case of my new car, the OnStar equipment is built into the car. Any attempt to disable or remove it not only disables other nonprivacy invasive systems like navigation, the entertainment system, and Bluetooth connectivity, but it also voids the manufacturer's warranty. And there's no way to avoid Internet connectivity on modern premium cars.[16] My car will attempt to authenticate with all insecure proximate Wi-Fi networks whenever the car is started. If there's a way to disable this feature, I haven't found it. One need only read up on Operation G-Sting to confirm the dangers of all of this insecurity. The FBI aren't the only ones listening!

Car companies and dealers are finding that the sale of customer data is another lucrative source of profit along with the interest and fees associated with car loans.

With the proliferation of unwanted and unneeded passive interfaces like Bluetooth; Internet and Wi-Fi connectivity; the ability to invasively record passenger compartment audio and

video; the integration of myriad sensors, cameras, and microphones; and the megaintegration of all of these components into an insecure multimedia and networked infrastructure, the potential for privacy abuse in modern automobiles is enormous. Add to that the profit motive for the manufactures to use or sell these data, and we have a new frontier for privacy abuse, fraud, and theft. The question isn't whether these new automobile systems will be exploited to our cost, but when and to what degree.

This is not to deny that there are other manufacturers capturing these data. Mobile device manufactures do the same thing. Literally hundreds of smartphone apps are known to share such data as real-time GPS location with third-party vendors.[17] It is not easy (and may not be possible) to shut such features off because the manufacture/provider ultimately has control over enabling/disabling services. However, at least in the case of mobile devices, you have the ability to shut the device off. That's not an option with modern automobiles.

There are also more mundane privacy exposures with such "large scale and covert collection of personal data" through Microsoft Offices' ProPlus subscription,[18] which shares motivations with vehicle telematics and mobile apps, but under the office productivity suite rubric. I'll expand on this in a future column.

REFERENCES

1. J. Johnson, "The talk of Las Vegas is Operation G-String," *Los Angeles Times*, Dec. 21, 2003. [Online]. Available: http://articles.latimes.com/2003/dec/21/nation/na-strippers21
2. K. Poulsen, "Hacker disables more than 100 cars remotely," Wired. Mar. 17, 2010. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/
3. H. Berghel, "*Faith*-based security," *Commun. ACM*, vol. 51, no. 4, pp. 13–17, Apr. 2008.
4. R. McMillan, "With hacking, music can take control of your car," IT World, Mar. 14, 2011. [Online]. Available: http://www.itworld.com/security/139794/with-hacking-music-can-take-control-your-car?page=0%2C1)
5. D. McCullagh, "Court to FBI: No spying on in-car computers," c|net, Nov. 19, 2003. [Online]. Available: http://news.cnet.com/Court-to-FBI-No-spying-on-in-car-computers/2100-1029_3-5109435.html
6. K. Hill, "OnStar kills its terrible plan to monitor non-customers' driving," Forbes, Sept. 27, 2011. [Online]. Available: http://www.forbes.com/sites/kashmirhill/2011/09/27/onstar-kills-its-terrible-plan-to-track-non-customers-driving-data/
7. J. A. Morrison, "Politicians come and go after serving corruption sentences," The Las Vegas Rev.-J., Mar. 21, 2010. [Online]. Available: https://www.reviewjournal.com/news/news-columns/jane-ann-morrison/politicians-come-and-go-after-serving-corruption-sentences/
8. TED, "All your devices can be hacked," 2011. [Online]. Available: https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked
9. K. Koscher et al., "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Security and Privacy*, 2010, pp. 1–16.
10. S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Security Symp.*, 2011, pp. 77–92.
11. R. Boyle, "Proof-of-concept CarShark software hacks car computers, shutting down brakes, engines, *and* more," Popular Science, May 14, 2010. [Online]. Available: https://www.popsci.com/cars/article/2010-05/researchers-hack-car-computers-shutting-down-brakes-engine-and-more
12. A. Greenberg, "The greatest hits of Samy Kamkar, YouTube's favorite hacker," *Wired*, Dec. 17, 2015. [Online]. Available: https://www.wired.com/2015/12/the-greatest-hits-of-samy-kamkar-youtubes-favorite-hacker/)
13. YouTube, "Drive it like you hacked it: New attacks and tools to wirelessly steal cars," 2015. [Online]. Available: https://www.youtube.com/watch?v=UNgvShN4USU
14. A. Greenberg, "This hacker's tiny device unlocks cars and opens garages," *Wired*, Aug. 16, 2015. [Online]. Available: https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/
15. P. W. Howard, "Data could be what Ford sells next as it looks for new revenue," Detroit Free Press, Nov. 13, 2018. [Online]. Available: https://www.freep.com/story/money/cars/2018/11/13/ford-motor-credit-data-new-revenue/1967077002/
16. B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. New York: Norton, 2018.
17. J. DeVries, N. Singer, M. H. Keller, and A. Krolik, "Your apps know where you were last night, and they're not keeping it secret," *New York Times*, Dec. 10, 2018. [Online]. Available: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?emc=edit_nn_p_20181210&nl=morning-briefing&nlid=76619836&section=topNews&te=1&fbclid=IwAR2MfaMW_jC9wK25lywuCNFWiSs2xa4SC-C3o61eaowMAeAcR7_ew_g0cYsY
18. C. Cimpanu, "Dutch government report says Microsoft Office telemetry collection breaks GDPR," ZDNet, Nov. 14, 2018 [Online]. Available: https://www.zdnet.com/article/dutch-government-report-says-microsoft-office-telemetry-collection-breaks-gdpr/

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.