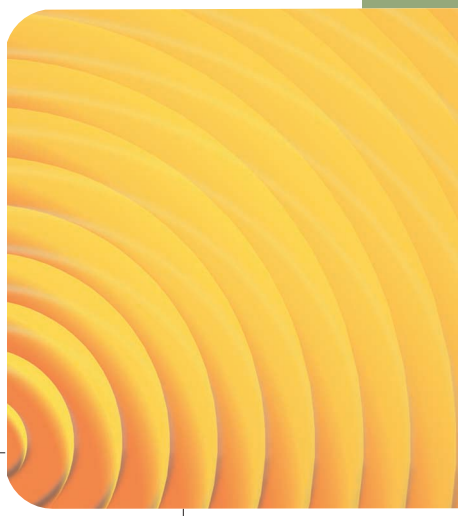
The Security and Privacy of Smart Vehicles

Road safety, traffic management, and driver convenience continue to improve, in large part thanks to appropriate usage of information technology. But this evolution has deep implications for security and privacy, which the research community has overlooked so far.



Jean-Pierre Hubaux, Srdjan Čapkun, and Jun Luo
EPFL

Current traffic-safety statistics are notoriously horrific. Approximately 40,000 people are killed each year on the European Union's roads, with around 1.7 million people incurring critical injuries; the US reports similar statistics (http://europa.eu.int/comm/transport/care/). The annual costs associated with traffic accidents (such as hospital bills and property damage) total nearly 3 percent of the world's gross domestic product (GDP), or roughly US$1 trillion.[1] Further compounding this predicament, the number of vehicles is increasing faster than the number of roads, leading to frequent traffic jams. Additional issues include pollution and scarce parking spaces.

In response to these problems, governments and manufacturers have launched several initiatives (such as mandatory safety-belt laws, airbags, and antiblocking brake systems), which have improved the situation somewhat. In October 1999, the US Federal Communications Commission allocated 75 MHz (the 5.85- to 5.925-GHz portion) of the spectrum in America for dedicated short-range communications (vehicle-vehicle or vehicle-roadside). Upcoming traffic safety initiatives rely heavily on information technology, which means that vehicles must be able to authenticate themselves and be traceable whenever necessary, be it for law enforcement (detection of speeding vehicles, for example), crash reconstruction, or toll collection. Today, most tracking operations rely on reading license plates; this obsolete and error-prone technique is the equivalent of reading a credit card with optical character recognition technology rather than with magnetic strips or embedded chips.

Reading plates has been replaced with authentication over a radio link (requesting an onboard device to transmit a cryptographic identity) in some cases, most noticeably at toll roads and bridges. As we will see, though, there is tremendous pressure to adopt generalized wireless authentication, especially in advanced safety mechanisms. However, this has deep implications for privacy, even greater than it does for cellular networks: a mobile phone can be switched off at any time, but a license plate can't. This article provides a brief overview of the relevant aspects of modern automotive technology and discusses in greater detail the role security will play.

Smart vehicles and roads

An important evolution for the automotive industry is the one toward *context awareness*, meaning that a vehicle is aware of its neighborhood (including the presence and location of other vehicles). Modern cars now possess a network of processors connected to a central computing platform that provides Ethernet, USB, Bluetooth, and IEEE 802.11 interfaces. Newer cars also have such features as

- an event data recorder (EDR), inspired by the "black boxes" found on airplanes (EDRs record all major data from the vehicle for crash reconstruction);
- a GPS receiver, the accuracy of which can be improved by knowledge of road topology (GPS is currently used in many navigation systems); and
- front-end radar for detecting obstacles at distances as far as 200 meters (such radar is often used for adaptive cruise control)[2] and short-distance radar or an ultrasound system, typically used for parking.

Inter-vehicle communication (IVC) supports many

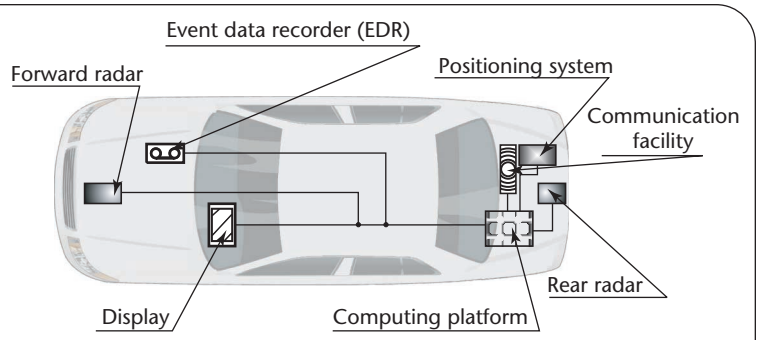


Figure 1. A smart vehicle's onboard instrumentation. The computing platform supervises protocol execution, including those related to security. The communication facility supports wireless data exchange with other vehicles or fixed stations.

important features, particularly in the area of crash prevention (for example, by informing vehicles about traffic congestion).[3] A set of communicating vehicles is an example of a mobile ad hoc network. The research community has devoted much attention to the security and privacy of such networks in the past few years,[4–6] but none of these contributions considers any such network for smart vehicles, which is what we'll study here.

In this article, we call a vehicle *smart* if it is equipped with recording, processing, positioning, and location capabilities and if it can run wireless security protocols (see Figure 1). Roads can be made smart, too. Fixed communication devices installed along a road can inform passing vehicles about the road's precise topology (see the PATH project, www.path.berkeley.edu). However, this approach's drawback is that it requires an enormous financial investment, which, at first, would benefit a small minority of drivers.

The observation of what happens on roads is called *traffic monitoring*,[7] which has a primary purpose of detecting anomalous situations, such as those generated by an accident or difficult driving conditions. It also optimizes traffic flow, most notably by synchronizing traffic lights with each other and with observed traffic, and civil engineers often use it to help plan construction of new roads. Traffic monitoring is based on different traffic measurement techniques; one of the most conventional (and popular) consists of inductive loop detectors buried in asphalt. Less "intrusive" techniques include video image processors, microwave radar, infrared laser radar, and acoustic/ultrasonic devices.

With more smart cars and roads, we can expect many changes. First, the number and severity of accidents should decrease: by integrating information about position and mutual distance with other vehicles, a given vehicle will be able to permanently assess the level of danger and trigger a warning to the driver, if necessary. In the more distant future, it could even override the driver—activating the brakes or taking control of the steering wheel, for example. Moreover, if an accident occurs, rescue teams will have immediate access to relevant information; a posteriori data will also help determine driver liability. With smart cars and roads, traffic monitoring itself will improve because it relies on much more accurate data. Ideally, traffic monitoring will eventually provide personalized advice to each driver via a personal navigation system. Ultimately, smart cars' benefits will range from simplifying the payment process for the driver (tolls, parking, and fuel), to helping the driver find an available parking place, to assisting authorities in fighting crime and terrorism. (Because terrorist activities often involve car bombs, automatic identification can help stop suspicious vehicles before they can access sensitive areas.)

However, a major hurdle in moving forward is that, for a lengthy time period, only a small subset of vehicles will be smart, yet the safety mechanisms we've described, especially those involving wireless authentication, require most—if not all—vehicles to be smart. As a result, bootstrapping the authentication mechanism's deployment is a formidable business challenge. An additional obstacle is the negative perception that the population might have about such mechanisms—especially the feeling of being permanently monitored by some arbitrary authority.

Devising an appropriate production and marketing strategy is beyond this article's scope, but we believe the solution is to deploy new features gradually, beginning with those that are operational even if only a small subset of vehicles can handle them—examples include access control to specific areas, wireless toll collection, personalized information about traffic congestion, and theft prevention. Another possibility for gradually deploying such systems without generating much resistance is to equip professional vehicles first—commercial trucks, buses, taxis, ambulances, and police cars, for example (in fact, many trucks already have EDRs).

Security and privacy

Surprisingly, most people overlook the security and privacy questions that vehicular technology's evolution raises. Currently, every vehicle is registered with its national or regional authority, which allocates a unique identifier to it, but in parts of the US and the EU, registration authorities have made substantial progress toward electronically identifying vehicles and similar progress is being made toward machine-readable driving licenses. To allow the wireless authentification of vehicles, these authorities must provide each vehicle with a private/public key pair, along with a shared symmetric key, and a digital certificate of its identity and public key. Such authorities will most likely be cross certified, making it possible for any vehicle to check any other vehicle's certificates.

To guard against misuse, the overall organization for such a system's security architecture must be very carefully designed, especially if it's deployed worldwide and

because of the information it will protect, so registration authorities must devise an appropriate Public Key Infrastructure. In magnitude, this challenge is equivalent to securing credit cards or mobile phones, but it also includes newer, more difficult problems: it must embed security features in stringent real-time protocols such as those used to prevent accidents, secure physical location and distance, and support communication within highly sporadic groups of participants.

Electronic tracking of vehicles could be derided as an incarnation of Big Brother, depending on your viewpoint, but it's a fact that the level of traffic monitoring is increasing. The public's acceptance of electronic tracking might be fuelled by the prospect of improved safety and optimized traffic for travelers and potential revenues for manufacturers. After all, privacy concerns haven't prevented the widespread acceptance of the Internet, cellular networks, or electronic payment systems. Therefore, the right question is not whether it should happen, but how to make it happen in the most desirable way.

An important task is to devise appropriate privacy-preserving protocols, which are typically based on anonymity schemes, relying on temporary pseudonyms. Fortunately, anonymity can be quantified, meaning that we can compare different proposals. Let's consider, for example, an anonymity metric based on entropy,[8] and let's assume that an attacker wants to retrieve a given vehicle's identity by sniffing identification messages the victim has transmitted.

Let X be a discrete random variable with probability function $p_i = Pr(X = i)$, where i represents each possible value that X can take. In our case, X represents the pseudonym under the attacker's scrutiny, and each i corresponds to an element (a vehicle) of the anonymity set. We use $H(X)$ to denote entropy after the attack occurs. For each vehicle belonging to the vehicle set of size N, an attacker assigns a probability p_i. We can calculate $H(X)$ as

$$H(X) = -\sum_{i=1}^{N} p_i \log_2 p_i,$$

thus the pseudonym's maximum entropy is

$$H_{\max} = \log_2 N,$$

where N is the anonymity set's size. Based on this, we compute the degree of anonymity d, provided by a given privacy-protection system, as

$$d = \frac{H(X)}{H_{\max}}.$$

The degree of anonymity quantifies the amount of information the system is leaking for a given pseudonym.

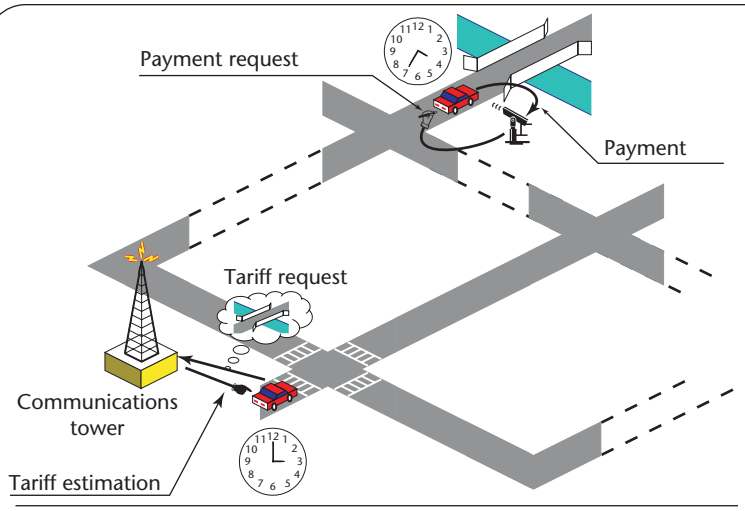


Figure 2. Dynamic pricing. The driver (possibly assisted by a navigation system) decides on a route; the payment of any tolls automatically occurs when entering the toll road or bridge.

Electronic license plates

We call the certified identity that a vehicle provides via a wireless link an *electronic license plate*. The protocols that use such license plates can be designed in different ways—when a vehicle's engine is on, for example, it can periodically broadcast a beacon containing its electronic license plate, road position, clock, and current speed. It also can store any data related to itself in an EDR. Alternatively, the vehicle can permanently listen to the environment and register the beacons it hears (that is, it can hear other vehicles' beacons regardless of whether the engine is on or off). This last design decision helps support sophisticated services, but it should be engineered carefully because it demands a lot of energy.

A possible application of electronic license plates is dynamic pricing. The onboard navigation system (or, alternatively, the driver can check a Web site before leaving or while en route from a cellular terminal) can propose a choice of routes to the driver, with an estimate of current toll prices. The vehicle will then be charged when it enters the related toll areas (see Figure 2).

Another way to use electronic license plates is to find drivers who flee the scene of an accident: even if no vehicle is in the radio power range, the culprit's vehicle likely will soon pass a parked car that can record its identity (see Figure 3). By interrogating the EDRs of nearby parked cars, police can retrieve the identities of all vehicles that have passed a specific spot at a given time.

Although powerful, electronic license plates are vulnerable to attack. A first, obvious threat is the attempt by the smart vehicle's owner (or thief) to disable, at least partially, its communication and storage capabilities (in particular, the EDR). Prevention is easier to automate for electronic license plates than it is for physical ones: we can

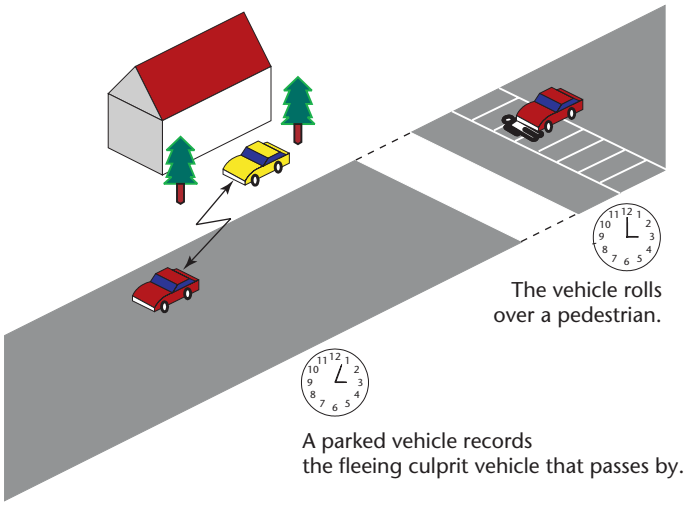


Figure 3. A parked vehicle recording a fleeing one. The recorded data can help the police identify the culprit.

try to protect the EDR physically, or trigger an alarm or alert law enforcement.

A second threat is the impersonation attack: a vehicle owner deliberately stealing another vehicle's identity and attributing it to his or her own car, or vice versa. We can prevent this type of attack by storing the vehicle's identity in tamper-resistant hardware, having it properly certified, and using modern authentication protocols. Electronic license plates are much more resistant to this sort of attack than physical ones.

A more dangerous attack is denial of service: an attacker systematically or selectively jamming the signals that vehicles exchange. There is no purely technical solution to such attacks, which is one of the reasons why we won't see a car overriding its driver in the near future.

To make the use of radio-transmitted information to track a given car's location (and therefore its driver) socially acceptable, it should protect driver privacy, at least as long as no collisions occur. For this reason, the broadcasted certified identity must be a pseudonym that changes over time; only the regional or national authorities should be able to determine the relationship between a pseudonym and its real identity. (Because the car's public key is broadcasted as well, it must also change periodically.) In this way, any personal information the electronic license plate transmits would be negligible when compared to that provided by its physical counterpart. The scheme's quality can be expressed by the degree of anonymity we defined earlier.

Location verification

Any car's location can be determined by using GPS or with the help of on-road infrastructure; IVC can also help. Existing positioning and distance estimation techniques assume that vehicles cooperate in determining or reporting their locations or distances, but some might try to report false distances or locations. Let's look at two solutions for verifying vehicle locations.

Tamper-proof GPS

Each vehicle should have a tamper-proof GPS receiver that registers its location at all times and provides this data to fixed stations or other vehicles in an authentic manner. Fortunately, this doesn't require any additional infrastructure and can be implemented independently in each vehicle. However, one drawback is its availability in urban environments: buildings, bridges, or tunnels often block GPS signals. Another disadvantage is that this option relies on tamper-resistant hardware, which has well-known weaknesses.[9]

The most serious problem with this approach is that GPS-based systems are vulnerable to several different kinds of attack, including blocking, jamming, spoofing, and physical attacks. Moreover, relatively unsophisticated adversaries can successfully execute them. The most dangerous attack involves fooling the GPS receiver with a GPS satellite simulator, which produces fake satellite radio signals that are stronger than legitimate ones. Such simulators are routinely used to test new GPS products and cost US$10,000 to $50,000. Some simple software changes to most GPS receivers would let them detect relatively unsophisticated spoofing attacks,[10] but more sophisticated ones would still be hard to detect.

Verifiable multilateration

A second solution for verifying vehicle location is based on roadside infrastructure and uses distance bounding and multilateration. (Distance bounding guarantees that the distance is no greater than a certain value; multilateration is the same operation in several dimensions.) This approach removes the need for tamper-proof hardware, but requires the installation of a set of base stations controlled by a central authority. The infrastructure covers an area of interest, such as specific roads or city blocks, and can verify vehicle locations in two or three dimensions.

Verifiable multilateration works as follows: Four verifying base stations with known locations perform distance bounding to the vehicle, the results of which give them four upper bounds on distance from the vehicle. If the verifiers can uniquely compute the vehicle's location using these distance bounds, and if this location falls into the triangular pyramid formed between the verifiers, then they conclude that the vehicle's location is correct. Equivalently, only three verifiers are needed to verify the vehicle's location in two dimensions; the verifiers still consider the car's location correct if they can be uniquely computed and if it falls in the triangle formed between them.

Verifiable multilateration relies on distance bounding; a claimant can always pretend to be further from the verifier than it really is, but it can't prove itself to be closer. Stefan

Brands and David Chaum first introduced the notion of distance-bounding protocols;[11] they proposed a technique that lets a party (the verifier) determine an upper bound on its physical distance to another party (the claimant). The main idea is simple but powerful: it's based on the fact that light travels at a finite speed, and with current technology, it's possible to measure (local) time with nanosecond precision. Their protocol was recently extended to support provable encounters in mobile wireless networks.[12]

Figure 4 shows an example of how the distance-bounding protocol unfolds. The protocol is performed between a verifier v (a fixed base station) and a vehicle C (which stands for claimant). After a mutual authentication phase (not shown in the figure), the vehicle commits to two random values N_C and N_C' by hashing them with a collision-resistant one-way hash function h and sending the result to v. The verifier then generates a challenge nonce N_v and sends it to C. On receiving the challenge, C is expected to respond immediately with $N_v \oplus N_C$. The verifier measures the challenge-response time of flight t_{vC} and estimates the distance to C, but because C can't send the correct response before receiving the challenge, it either delays the response or sends it immediately after receiving the challenge. In the last stage of the protocol, C signs the second part of the commitment N_C'. The verifier then uses the signature of the second part of the commitment to authenticate C and verify if the commitment corresponds to C's response.

When it estimates the distance to C, the verifier also takes into account C's processing delay. Here, this time is relatively short, given that C needs to perform only an XOR operation and does not need to perform any cryptographic operation until the end of the protocol.

Figure 5 shows an example of verifiable multilateration. The intuition behind the technique is that a vehicle might try to cheat about its location. As we mentioned earlier, the vehicle can only pretend that it is further from the verifier than it really is because of the distance-bounding property. However, if it increases the measured distance to one of the verifiers, it would need to prove that at least one of these distances is shorter than it actually is, to keep its claimed location consistent with the increased distance. This property holds only if the claimed location is within the triangular pyramid formed by the verifiers: if an object is located within the pyramid and it moves to a different location within the pyramid, it will certainly reduce its distance to at least one of the pyramid vertices. The same holds in two dimensions.

In a real deployment, the number of base stations would of course be much larger than what we see in Figure 5; as a result, a vehicle would always be within the geometric shape that three or four stations form.

Verifiable multilateration also detects *distance enlargement attacks* from outside attackers: If an attacker tries to jam the signal that the vehicle sends to the verifiers and delay its response, the verifiers detect this attack in the same way as if the vehicle itself performed the distance enlargement. The distance measurements' precision is very important. Today's technology based on time of flight and ultra wideband can achieve a precision of 15 cm for distances up to 2 km.[13]

C : generate random nonces N_C, N_C'
: generate commitment $commit = h(N_C, N_C')$
$C \rightarrow v$: C, $commit$

v : generate random nonce N_v
$v \rightarrow C$: v, N_v
$C \rightarrow v$: $N_v \oplus N_C$
v : measure the time t_{vC} between sending N_v and receiving $N_v \oplus N_C$

$C \rightarrow v$: C, N_C', $sig_{K_C}(C, N_C')$

v : verify if the signature is correct and if $commit = h(N_C, N_C')$

Figure 4. The distance-bounding protocol. The verifier (v) upper-bounds its distance to an untrusted vehicle C.

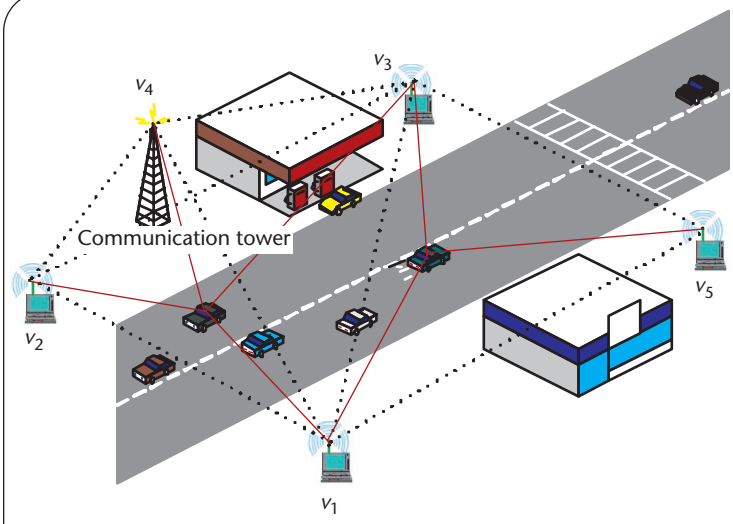
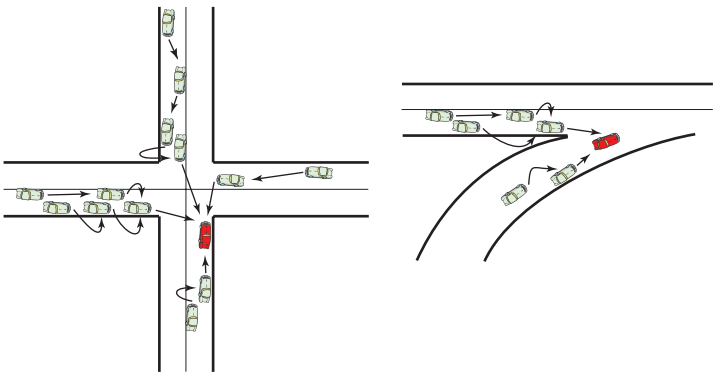


Figure 5. Two examples of verifiable multilateration. Base stations v_1, v_2, v_3, and v_4 can verify a vehicle's location in three dimensions if the vehicle is located in the triangular pyramid that v_1, v_2, v_3, and v_4 forms. Base stations v_1, v_3, and v_5 can verify a vehicle's location in two dimensions if the vehicle is located in the triangle formed by v_1, v_3, and v_5.

An example application: Cooperative driving

Once we verify a vehicle's identity (via its electronic license plate) and location (via the mechanisms we just de-



(a) (b)

Figure 6. Cooperative driving. The red car holds the token that lets it access the resource (a) at a blind crossing and (b) at a highway entrance.

scribed), we can implement several new functions, including cooperative driving.

Vehicles that pass through critical points such as highway entrances and blind crossings (those without light control) must coordinate to avoid collisions. With the IVC's support, this coordination can be at least partially automated. Coordination functions that share resources among a group of nodes are usually achieved by group communication primitives (such as mutual exclusion) in computer networks, but the problem we face here is more challenging: human lives are concerned, the nodes are mobile, the groups are highly transient, and the communications are wireless.

A potential solution to this challenge is a lightweight group communication system managed by a token (see Figure 6). Every vehicle sees the wireless link with one of its neighbors (other vehicles within the transmission range) as outgoing; the neighbors see this link as incoming. As a result, a directed acyclic graph (DAG) forms to link the members of a contention group (those vehicles contending for a common point) together. The sink (a node without an outgoing link) of the DAG is elected among the nodes closest to the critical point. This node then initiates a token (a small message that grants the right to access a resource) and goes across the point. The token then passes to one of the nodes that have outgoing links to the token holder, which lets that node move forward.

We can apply different policies to control the behavior of token passing; for example, the token can switch from vehicles on one road to those on the other one at a highway's entrance (which merges the two flows of vehicles). In any case, a policy would use each vehicle's verified position and identity to fine-tune the token's circulation and provide each driver with appropriate information.

A related problem is that when vehicles arrive at a given spot (such as at a crossroad) or travel together for a while (such as on a highway), they might need to exchange many messages and therefore may have to establish a shared symmetric key based on their certified public keys. Many people have proposed solutions for this recurring issue, usually based on so-called multiparty Diffie-Hellman agreement protocols.[14] Most of these protocols rely on an underlying group communication system to achieve fault tolerance, but in our case, the protocols must cope with stringent real-time constraints and the fact that human involvement is not possible. Obviously, such protocols still must be designed.

Because many safety features require some level of cooperation between vehicles, bootstrapping the adoption of the necessary hardware is a major business challenge. Of course, this push requires a substantial effort from the standardization bodies before it can materialize.

So far, the security and privacy challenges related to this area have been overlooked,[15] but the two solutions we've sketched in this article are a good place to start. In particular, electronic license plates have the potential benefit of allowing a much more accurate definition (and control) of what data law-enforcement agencies can access; this is likely to be one of the most relevant challenges in the area of wireless security. Location verification is the cornerstone of cooperative safety mechanisms, and the smarter vehicles become, the more their safety features will need to be secured. □

Acknowledgments

We are indebted to Mario Čagalj, Robert Dick, Markus Jakobsson, Ken Laberteaux, Jean-Yves Le Boudec, Christof Paar, and Pravin Varaiya for their comments on early versions of this article. Special thanks also to Matthias Grossglauser and Alcherio Martinoli for their thought-provoking discussions on this topic.

References

1. W. Jones, "Building Safer Cars," *IEEE Spectrum*, vol. 39, no. 1, 2002, pp. 82–85.
2. R. Moebus, A. Joos, and M. Morari, "Multi-Object Adaptive Cruise Control," *Proc. Hybrid Systems: Computation and Control*, LNCS vol. 2623, Springer Verlag, 2003, pp. 359–376.
3. W. Franz, R. Eberhardt, and T. Luckenbach, "FleetNet: Internet on the Road," *Proc. 8th World Congress on Intelligent Transport Systems*, 2001.
4. L. Zhou and Z. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, 1999, pp. 26–30.
5. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. 8th ACM Int'l Conf. Mobile Computing and Networking* (Mobicom), ACM Press, 2002, pp. 12–23.

6. J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks," *Proc. 4th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing*, ACM Press, 2003, pp. 291–302.
7. L. Klein, *Sensor Technologies and Data Requirements for ITS*, Artech House, 2001.
8. A. Serjantov and G. Danezis, "Toward an Information Theoretic Metric for Anonymity," *Proc. Privacy Enhancing Technologies* (PET), Springer-Verlag, 2002.
9. R. Anderson and M. Kuhn, "Tamper Resistance: A Cautionary Note," *Proc. 2nd Usenix Workshop on Electronic Commerce*, Usenix Assoc., 1996, pp. 1–11.
10. J. Warner and R. Johnston, *Think GPS Cargo Tracking = High Security? Think Again*, tech. report, Los Alamos Nat'l Lab., 2003.
11. S. Brands and D. Chaum, "Distance-Bounding Protocols," *Theory and Application of Cryptographic Techniques*, Springer-Verlag, 1993, pp. 344–359.
12. S. Čapkun, L. Buttyan, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks," *Proc. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, ACM Press, 2003.
13. J.-Y. Lee and R.A. Scholtz, "Ranging in a Dense Multipath Environment Using a UWB Radio Link," *IEEE J. Selected Areas in Comm.*, vol. 20, no. 9, 2002, pp. 1677–1683.
14. G. Ateniese, M. Steiner, and G. Tsudik, "New Multi-Party Authentication Services and Key Agreement Protocols," *IEEE J. Selected Areas in Comm.*, vol. 18, no. 4, 2000, pp. 628–639.
15. J. Luo and J.-P. Hubaux, *A Survey of Inter-Vehicle Communications*, tech. report IC/2004/04, EPFL, Mar. 2004.

Jean-Pierre Hubaux *is a professor at EPFL. His research interests are mobile networking and computing, with a special interest in fully self-organized wireless ad hoc networks. He also serves as an associate editor on* IEEE Transactions on Mobile Computing *and the* Elsevier Journal on Ad Hoc Networks. *He is a senior member of the IEEE and a member of ACM. Contact him at jean-pierre.hubaux@epfl.ch; http://lcawww.epfl.ch/hubaux.*

Srdjan Čapkun *is working toward his PhD at EPFL. His current research interests include security, privacy, and positioning in wireless networks. He received a BSc in electrical engineering and computer science from the University of Split, Croatia. He is a member of the IEEE Communications and Computer Societies and the ACM. Contact him at srdan.capkun@epfl.ch; http://lcawww.epfl.ch/capkun.*

Jun Luo *is working toward a PhD in communication systems at EPFL. His research interests include multicasting, mobile computing (especially in ad hoc networks), reliable group communication, and network security. He received a BS and MS, both in electrical engineering, from Tsinghua University, Beijing, PRC. He is a student member of ACM. Contact him at jun.luo@epfl.ch; http://lcawww.epfl.ch/luo.*