The Car Hacker's Handbook: A Guide for the Penetration Tester - Craig Smith (2016)

Chapter 10. VEHICLE-TO-VEHICLE COMMUNICATION

The latest trend in vehicle technology is *vehicle-to-vehicle (V2V) communication*—or in the case of vehicles communicating with roadside devices, *vehicle-to-infrastructure (V2I) communication*. V2V communication is primarily designed to communicate safety and traffic warnings to vehicles through a dynamic mesh network between vehicles and roadside devices called the *intelligent transportation system*. This mesh connects various nodes—

vehicles or devices—in the network and relays information between them.

The promise of V2V is so great that in February 2014 the US Department of Transportation announced its desire to implement a mandate requiring that V2V-based communication be included in all new light vehicles, though as of this writing nothing has been finalized.

V2V is the first automotive protocol to consider cybersecurity threats at the design stage, rather than after the fact. The details of V2V implementation and interoperation between countries are still being determined, so many processes and security measures are still undecided. Nevertheless, in this chapter, we'll review the current design considerations in an attempt to offer guidelines for what to expect. We'll detail the thinking behind different approaches and discuss the types of technologies likely to be deployed in the V2V space. We'll also discuss several protocols used in V2V communications and the types of data they'll transmit, and we'll review V2V's security considerations as well as areas for security researchers to focus on.

NOTE

Because this chapter focuses on a technology yet to be implemented, we won't cover the reasons behind various

features, nor will we discuss the ways that manufacturers can implement each feature because all of that detail is subject to change.

Methods of V2V Communication

In the world of V2V communication, vehicles and roadside devices interact in one of three ways: via existing cellular networks; using *dedicated short-range communication (DSRC)*, which is a short-range communication protocol; or via a combination of communication methods. In this chapter we'll focus on DSRC, as it's the most common method of V2V communication.

Cellular Networks

Cellular communication doesn't require roadside sensors, and existing cellular networks already have a security system in place, so communication can rely on security methods provided by the cellular carriers. The security provided by cellular networks is at the wireless level (GSM), not the protocol level. If the connected device is using IP traffic, then standard IP security, such as an encryption and reduction of attack surfaces, still needs to be applied.

DSRC

DSRC requires the installation of specialized equipment in modern vehicles and new roadside equipment. Because

DSRC is designed specifically for V2V communication, security measures can be implemented prior to widespread adoption. DSRC is also more reliable than cellular communication, with lower latency. (See "The DSRC Protocol" on page 179 for more on DSRC.)

Hybrid

The hybrid approach combines cellular networks with DSRC, Wi-Fi, satellite, and any other communication that makes sense, such as future wireless communication protocols.

In this chapter, we'll focus on DSRC because it's unique to the V2V infrastructure. The DSRC protocol will be the main protocol deployed by V2V, and you may see it mixed with other communication methods.

NOTE

You can use traditional methods to analyze communication, such as cellular, Wi-Fi, satellite, and so on. Evidence of these signals communicating doesn't necessarily mean the vehicle is using V2V communication. However, if you see DSRC being transmitted, you'll know that V2V has been implemented in that vehicle.

FUN WITH V2V ACRONYMS

The auto industry loves acronyms as much as any

government does, and V2V is no exception. In fact, the lack of any universal V2V standard between countries means that the world of V2V acronyms can be especially messy because there's little consistency and a good dose of confusion. To help you out, here are some acronyms that you'll run into when researching V2V-related topics:

ASD Aftermarket safety device

DSRC Dedicated short-range communication

OBE Onboard equipment

RSE Roadside equipment

SCMS Security Credentials Management System

V2I, C2I Vehicle-to-infrastructure, or car-to-infrastructure (Europe)

V2V, C2C Vehicle-to-vehicle, or car-to-car (Europe)

V2X, C2X Vehicle-to-anything, or car-to-anything (Europe)

VAD Vehicle awareness device

VII, ITS Vehicle infrastructure integration, intelligent transportation system

WAVE Wireless access for vehicle environments

WSMP WAVE short-message protocol

The DSRC Protocol

DRSC is a one- or two-way short-range wireless communication system specifically built for vehicle communications between vehicles and roadside devices, or from vehicle to vehicle.

DSRC operates in the 5.85 to 5.925 GHz band reserved for V2V and V2I. The transmit power used by a DSRC device will dictate its range. Roadside equipment can transmit at higher-power ranges, allowing up to a 1,000 m specification, while vehicles can broadcast only at a power level that provides closer to 300 m ranges.

DSRC is based on the wireless 802.11p and 1609.x protocols. DSRC-and Wi-Fi-based systems, such as wireless access for vehicle environments (WAVE), use IEEE 1609.3 specification or the WAVE short-message protocol (WSMP). These messages are single packets with no more than 1,500 bytes and typically less than 500 bytes. (Network sniffers such as Wireshark can decode WAVE packets, which allows for easy sniffing of traffic.)

DSRC data rates depend on the number of users accessing the local system at the same time. A single user on the system would typically see data rates of 6 to 12Mbps, while

users in a high-traffic area—say, an eight-lane freeway—would likely see 100 to 500Kbps. A typical DSRC system can handle almost 100 users in high-traffic conditions, but if the vehicles are traveling around 60 km/h, or 37 mph, it'll usually support around only 32 users. (These data rates are estimated from the Department of Transportation's paper "Communications Data Delivery System Analysis for Connected Vehicles."[1])

The number of channels dedicated to the 5.9 GHz range of the DSRC system varies between countries. For example, the US system is designed to support seven channels with one channel that acts as a dedicated control channel reserved for sending short high-priority management packets. The European design supports three channels with no dedicated control channel. This disparity is largely due to the fact that each country has different drivers for the technology: Europe's system is market driven, while the US system has a strong vehicle safety initiative behind it. Therefore, while the protocols will interoperate, the types of messages supported and sent will differ significantly. (In Japan, DSRC is currently being used for toll collection, but the Japanese are also planning to use a 760 MHz band for crash avoidance. The Japanese 5.8 GHz channels don't use 802.11p, but they should still support the 1609.2 V2V security framework.)

NOTE

While both Europe and the United States use 802.11p with ECDSA-256 encryption, the two systems are not 100 percent compatible. As of this writing, they incorporate various technical differences, such as where the signing stack is placed in the packet. There's no good technical reason for this lack of standardization, so this will hopefully be fixed before widespread adoption.

Features and Uses

All DSRC implementations offer convenience and safety features, but their features differ. For example, the European DSRC system will use DSRC for the following:

Car sharing Would work like today's vehicle sharing, such as car2go, except that instead of using a third-party vehicle dongle attached to the OBD-II connector to control the vehicle, it would use the V2I protocols

Connections to points of interest Similar to the points of interest, such as restaurants or gas stations, in a traditional navigation system but would be broadcast to passing vehicles

Diagnostics and maintenance Would report the reason why a vehicle's engine light is on via DSRC instead of having to read codes from an OBD connector

Driving profiles for insurance purposes Would replace

insurance-style dongles that record driving behavior

Electronic toll notification Would allow for automated payments at toll booths (already being tested in Japan)

Fleet management Would allow for the monitoring of fleets of vehicles, such as those used for trucking and transportation services

Parking information Would record duration of parking and could displace traditional parking meters

Security-driven areas like the United States are more concerned with communicating warnings about things like the following:

Emergency vehicles approaching Would notify vehicles of an approaching emergency vehicle

Hazardous locations Would warn drivers of hazards, such as an icy bridge or road surface, or falling rocks

Motorcycle approaches Would signal the approach of a passing motorcycle

Road works Would notify drivers of upcoming construction

Slow vehicles Would provide early notification of traffic congestion or traffic slowdowns due to slow-moving farm or oversized vehicles

Stationary (crash) vehicles Would warn of vehicles that have broken down or were in a recent collision

Stolen vehicle recovery Might work similarly to a LoJack-like service in that it would allow law enforcement to locate a stolen vehicle based on a radio beacon

Additional types of communication categories that could be implemented via DSRC include traffic management; law enforcement, such as communicating speeds or tracking vehicles; driver assistance, such as parking assistance or lane guidance; and highway automation projects, such as self-driving vehicles that use V2I roadways to assist in guidance.

Roadside DSRC Systems

Roadside DSRC systems are also used to pass standardized messages and updates to vehicles with information such as traffic data and hazard or road works warnings. The European Telecommunications Standards Institute (ETSI) has designed two formats for continuous traffic data, both of which use 802.11p: the cooperative awareness message (CAM) and the decentralized environmental notification message (DENM).

CAMs for Periodic Vehicle Status Exchanges

CAMs are broadcast periodically through the V2X network.

ETSI defines the packet size of a CAM as 800 bytes and the reporting rate at 2 Hz. This protocol is still in its preliminary stages. If you encounter CAMs in the future, they may vary from the proposal, but we're including the current proposed characteristics to give you a sense of what you can expect from the CAM protocol in the future.

CAM packets consist of an ITS PDU header and station ID as well as one or more station characteristics and vehicle common parameters.

Station characteristics may include the following:

- Mobile ITS station
- Physical relevant ITS station
- Private ITS station
- Profile parameters
- Reference position

Vehicle common parameters may consist of the following:

- Acceleration
- Acceleration confidence
- Acceleration controllability

- Confidence ellipse
- Crash status (optional)
- Curvature
- Curvature change (optional)
- Curvature confidence
- Dangerous goods (optional)
- Distance-to-stop line (optional)
- Door open (optional)
- Exterior lights
- Heading confidence
- Occupancy (optional)
- Station length
- Station-length confidence (optional)
- Station width
- Station-width confidence (optional)
- Turn advice (optional)

- Vehicle speed
- Vehicle-speed confidence
- Vehicle type
- Yaw rate
- Yaw rate confidence

Although some of these parameters are marked as optional, they're actually mandatory in certain situations. For example, a basic vehicle profile—station ID of 111 in binary—must report crash status and whether the vehicle is carrying dangerous goods, if known. An emergency vehicle—station ID of 101 in binary—must report whether its lights and sirens are in use. Public transportation vehicles—station ID also 101—are required to report when their entry door is open or closed and may also report schedule deviation and occupancy count.

DENMs for Event-Triggered Safety Notifications

DENMs are event-driven messages. While CAMs are periodically sent so that they're regularly updated, DENMs are triggered by safety and road hazard warnings. Messages might be sent in cases of:

- Collision risks (determined by roadside devices)

- Entering hazardous locations
- Hard braking
- High wind levels
- Poor visibility
- Precipitation
- Road adhesion
- Road work
- Signal violations
- Traffic jams
- Vehicles involved in an accident
- Wrong-way driving

These messages stop either when the condition that triggered them is gone or after a set expiry period.

DENMs can also be sent to cancel or negate an event. For instance, if roadside equipment identified that a vehicle was going the wrong way down a street, it could send an event to notify nearby drivers. Once that driver had moved the vehicle into the proper lane, the equipment could send a cancel event to signal that the risk had passed.

Table 10-1 shows the packet structure and byte position of a DENM packet.

Table 10-1: Packet Structure and Byte Position of a DENM Packet

Container	Name	Byte start position	Byte end position	Notes
ITS Header	Protocol Version	1	1	ITS Versio
	Message ID	2	2	Message Type
	Generation Time	3	8	Timestam
Management	Originator ID	9	12	ITS Static ID
	Sequence Number	13	14	
	Data Version	15	15	255 = Cancel
	Expiry Time	16	21	Timestam
	Frequency	21	21	Transmiss Frequenc
	Reliability	22	22	Probabilit event is t Bit 1..7
	IsNegation	22	22	1 == Nega Bit 0

Situation	CauseCode	23	23	
	SubCauseCode	24	24	
	Severity	25	25	
Location	Latitude	26	29	
	Longitude	30	33	
	Altitude	34	35	
	Accuracy	36	39	
	Reserved	40	*n*	Variable s

There are optional messages as well. For example, the situation container could include TrafficFlowEffect, LinkedCause, EventCharacteristics, VehicleCommonParameters, and ProfileParameters, just as in the CAN structure.

WAVE Standard

The WAVE standard is a DSRC-based system used in the United States for vehicle packet communication. The WAVE standard incorporates the 802.11p standard as well as the range of 1609.x standards across the OSI model. The purposes of these standards are as follows:

802.11p Defines the 5.9 GHz WAVE protocol (a modification of the Wi-Fi standard); also has random local MAC addressing

1609.2 Security services

1609.3 UDP/TCP IPv6 and LLC support

1609.4 Defines channel usage

1609.5 Communication manager

1609.11 Over-the-air electronic payment and data exchange protocol

1609.12 WAVE identifier

NOTE

To explore the WAVE standard in more detail, you can use the OSI numbers in the preceding list to pull up the relevant reference documentation online.

WSMP is used in both service and control channels. WAVE uses IPv6, the most recent Internet protocol, for service channels only. IPv6 is configured by the WAVE management entity (WME) and also handles channel assignments and monitors service announcements. (The WME is unique to WAVE and handles the overhead and maintenance of the protocol.) Control channels are used for service announcements and short messages from safety applications.

WSMP messages are formatted as shown in Figure 10-1.

WSMP Version	PSID	Channel Number	Data Rate	Transmission Power	WAVE Element ID	WAVE Length	WSMP Data

Figure 10-1: WSMP message format

The type of application provided by a roadside device, or hosted by a vehicle, is defined by the provider service identifier (PSID). The actual announcement of a service comes from a WAVE service announcement (WSA) packet, the structure of which is shown in Table 10-2.

Table 10-2: WAVE Service Announcement Packet

Section	Elements
WSA header	WAVE version EXT Fields
Service Info	WAVE Element ID PSID Service Priority Channel Index EXT Fields
Channel Info	WAVE Element Operating Channel Channel Number Adaptable Data Rate Transmit Power EXT. Fields
WAVE Routing Advertisement	WAVE Element Router Lifetime IP Prefix Prefix Length

	Default Gateway Gateway MAC Primary DNS EXT. Fields

If the vehicle's PSID matches that of an advertised PSID, the vehicle will begin communications.

Tracking Vehicles with DSRC

One attack that utilizes DSRC communications is vehicle tracking. If attackers can create their own DSRC receiver by buying a DSRC-capable device or using software-defined radio (SDR), they could receive information about vehicles within the receiver's range—such as the size, location, speed, direction, and historical path up to the last 300 m—and use this information to track a target vehicle. For example, if an attacker knew the make and model of a target vehicle and the size of the target, they could set up a receiver near the target's home to remotely detect when the target moves out of range of the DSRC receiver. This would tell the attacker when the owner had left their house. This method would allow an attacker to continue to track and identify vehicle activity despite the owner's attempts to obscure identifying information.

Information on vehicle size is transmitted in the following four fields:

- Length
- Body width
- Body height
- Bumper height (optional)

This information should be accurate to within a fraction of an inch because it's set by the manufacturer. The attacker could use this size information to accurately determine the make and model of a car. For instance, Table 10-3 lists the dimensions for a Honda Accord.

Table 10-3: Honda Accord Dimensions

Length	Body width	Body height	Bumper height
191.4 inches	72.8 inches	57.5 inches	5.8 inches

Given these dimensions and a bit more information, such as the estimated time a target might pass a sensor, an attacker could determine whether a target has passed a sensor and track that target.

Security Concerns

There are other attack potentials in the implementation of V2V, as was investigated by the Crash Avoidance Metrics Partnership (CAMP), a group of several auto manufacturers

working to conduct different safety-related studies, in December of 2010. CAMP performed an attack analysis on V2V systems through its Vehicle Safety Consortium (VSC3). The analysis focused primarily on the core DSRC/WAVE protocol, and attempted to match attacker objectives with potential attacks. Figure 10-2 shows a summary of the consortium's findings by attacker objective.

			Attacker Objectives						
			O1.1	O1.2	O1.3	O1.4	O1.5	O1.6	O1.7
			Cause an accident	Cause congestion	Cause a driver to change their route	Erode user's faith in the system	Identify a particular driver or track their route	Conceal bad driving behavior	Falsely accuse/report misbehavior
Attacks	A2.1	Cause a false positive to be presented to a driver	X	X	X	X			
	A2.2	Suppress a message that should be presented to the driver (i.e., cause a false negative)	X	X	X	X		X	
	A2.3	Cause the system to be made unreliable, unknown to the driver	X	X	X	X			
	A2.4	Cause the system to be made unreliable, known to the driver	X	X	X	X			
	A2.5	Collect a set of messages from other vehicles and use them to identify a particular vehicle/driver					X		
	A2.6	Prevent the attacker's own vehicle from sending a message						X	
	A2.7	Create messages that will be attributed by the system to a vehicle that did not send them							X
	A2.8	Create messages from "ghost" vehicles to make a target's behavior seem more dangerous than it is, or the attacker's behavior seem safer than it is, from the point of view of an authority reviewing the record						X	X

Figure 10-2: Attacker objectives crossed with attacks

This table shows some of the goals a malicious actor may have when attacking V2V systems and the types of attacks they might launch in order to achieve those objectives. The

top columns of the chart define an attacker's possible objectives and the areas they might focus on. The chart is rather simplistic but might give you some idea as to which areas to research further.

PKI-Based Security Measures

While much of the technology and security behind V2V is still being ironed out, we do know that the security for cellular, DSRC, and hybrid communications is based on a public key infrastructure (PKI) model much like the SSL model on websites. By generating public and private key pairs, PKI systems allow users to create digital signatures for use in encrypting and decrypting documents sent over networks. Public keys can be openly exchanged and are used to encrypt data between destinations. Once encrypted, only private keys can be used to decrypt the data. The data is signed with the sender's private key in order to verify its origin.

PKI uses public key cryptography and central certificate authorities (CAs) to validate public keys. The CA is a trusted source that can hand out and revoke public keys for a given destination. The V2V PKI system is sometimes also referred to as the *Security Credentials Management System (SCMS)*.

For a PKI system to function, it must enforce the following:

Accountability Identities should be verifiable using trusted signatures.

Integrity Signed data must be verifiable to make sure that it hasn't been altered in transit.

Nonrepudiation Transactions must be signed.

Privacy Traffic must be encrypted.

Trust The CA must be trusted.

V2V and V2I systems rely on PKI and a CA to secure data transmission, though the identity of the CA has yet to be determined. This is the same system that your browser uses on the Internet. On your browser's Settings screen, you should find a HTTPS/SSL section listing all authorized root authorities. When you buy a certificate from one of these CAs and use it on a web server, other browsers will verify this certificate against the CA to ensure it's trusted. In a normal PKI system, the company that set up the environment controls the CA, but in V2V, government groups or countries will likely control the CA.

Vehicle Certificates

The PKI systems used to secure today's Internet communication have large certificate files, but due to limited storage space and the need to avoid congestion on the

DSRC channels, vehicle PKI systems require shorter keys. To accommodate this need, vehicle PKI systems use elliptical curve cryptography (ECDSA-256) keys, which generate certificates that are one-eighth the size of Internet certificates.

The vehicles participating in V2V communication use two types of certificates:

Long-term certificate (LTC)

This certificate contains vehicle identifiers and can be revoked. It's used to get short-term certificate refills.

Short-term, pseudonym certificate (PC)

This certificate has a short expiry time and, therefore, doesn't need to be revoked because it simply expires. It's used for anonymous transfers, which are designed for common messages like braking or road conditions.

Anonymous Certificates

PKI systems are traditionally set up to identify the sender, but with information being broadcast to unknown vehicles and devices, it's important to ensure that V2V systems don't send information that can be traced back, such as packets signed by the source.

For that reason, there's a provision in the V2V spec that allows you to sign packets anonymously, with only enough information to show that the packet came from a "certified terminal." Though this is more secure than sending packets signed by the author, it would still be possible for someone to examine the anonymous certificate signature on a given route and determine the route that vehicle is traveling (in the same way that you might use the unique ID transmitted from a tire pressure monitor sensor to track a vehicle's progress). To compensate for this, the spec states that the device should use short-lived certificates that will last for only five minutes.

Currently, however, the systems being developed are planning to use 20 or more certificates that are all simultaneously valid with a lifetime of a week, which could prove to be a security flaw.

Certificate Provisioning

Certificates are generated through a process called certificate provisioning. V2V systems use a lot of short-term certificates, which need to be provisioned on a regular basis in order to replenish a device's certificates so that it can use them for anonymous messaging. The full details of how privacy works in V2V certificate systems is actually quite complicated, as the CAMP diagram in Figure 10-3 shows.

Prepare yourself for a lot of larvae references—as in caterpillar, cocoon, and butterfly—as we review how the certificate-provisioning process works:

1. First, the device—that is, the vehicle—generates what's known as a "caterpillar" keypair, which sends the public key and an Advanced Encryption Standard (AES) expansion number to the Registration Authority (RA).

2. The RA generates a bunch of what are known as "cocoon" public keys from the caterpillar public key as well as the expansion number. These become new private keys. The number of keys is arbitrary and not correlated with the device requesting the keys. (As of this writing, the request includes some ID information from the linkage authorities and *should* shuffle the request with requests from other vehicles. This shuffling is designed to help obscure which vehicle made each request in an attempt to improve privacy.)

3. The Pseudonym Certificate Authority (PCA) randomizes the cocoon keys and generates the "butterfly" keys. These are then returned to the originating device over an encrypted channel so the RA can't see the contents.

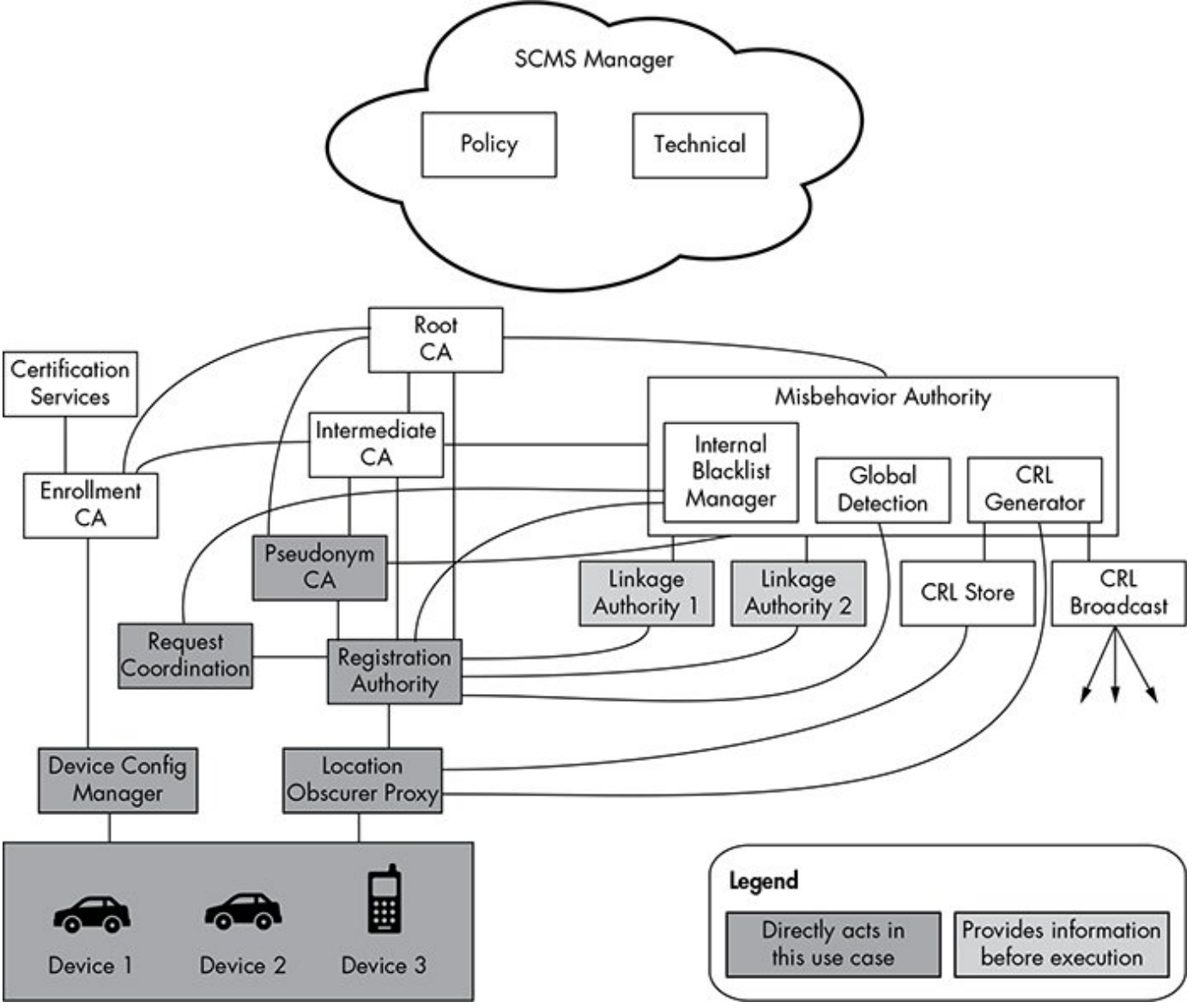

Figure 10-3: Certificate-provisioning flow graph

In theory, the originating device can request enough short-term keys to last the vehicle's lifetime, which is why the certificate revocation list (CRL)is important. If a vehicle has one month's worth of certificates, it won't check for new updates until that month is up, so a bad actor can continue to communicate with this vehicle until there's an update. If the vehicle has a year's worth or more of certificates and no CRL functionality, then things can get real bad real fast because it won't be able to identify bad actors.

NOTE

Notice the location obscurer proxy (LOP) in the certificate-provisioning chart. This is a filter to remove identifiable information, such as location, from the request. A request should *get through an LOP before the RA sees it.*

Updating the Certificate Revocation List

The CRL is a list of "bad" certificates. Certificates sometimes go bad because they're compromised by an attacker or lost by their owner or because a device is misbehaving for some reason that the CA considers detrimental. A device must update its CRL so that it can determine which certificates, if any, are no longer trustworthy.

The CRL can be large, and it isn't always feasible to download the entire list through DSRC or opportunistic Wi-Fi. Therefore, most systems will implement an incremental update period, which the manufacturer decides, but even that can cause issues. DSRC requires roadside devices to send the list, but in order to receive large chunks of data, the vehicle must travel past the roadside devices slowly enough that they have enough time to receive the CRL. Because most devices will be situated on major highways, with only a few on side roads, the only opportunity a vehicle might have to receive an updated list is during a traffic jam. The best

way to retrieve an updated CRL is, therefore, through cellular or full-satellite communication, though that's still slow. With high-speed cellular or full-satellite links, it would be possible to receive incremental updates or full downloads if required.

One possible way to distribute an updated CRL is to have vehicles communicate updates to each other via the V2V interface itself. While a vehicle may not be in contact with a roadside device long enough to complete an update, it's sure to encounter hundreds, if not thousands, of other vehicles on a journey.

Risks of V2V Updates

While updating via the V2V interface is very tempting because it lowers the infrastructure cost and overhead significantly (because you don't need to invest in lots of additional roadside infrastructure) it has its limits. For one, a vehicle could receive a CRL download only from nearby cars traveling in the same direction long enough to complete the download; cars going in opposite directions may pass by too quickly. This V2V method also provides the opportunity for a bad actor to inject a bad CRL that could either block legitimate devices or hide bad actors, and that bad CRL could then circulate through traffic like a virus.

Unfortunately, V2V protocol security focuses entirely on communication protocols. The onboard system, such as the

ECU, is responsible for requesting and storing CRLs, reporting misbehavior, and sending vehicle information, but this unsecured system provides an easy gateway for attackers to inject their code. Instead of taking over the device performing the actual V2V communication, they could simply modify the ECU firmware or spoof packets on the bus, and the V2V device would then faithfully sign and send the information out to the network. It's because of this latter vulnerability that this method has been unofficially dubbed the *epidemic distribution model*.

Linkage Authorities

When dealing with thousands of pseudonym, or short-term, certificates, revocation can be a nightmare, and that's where the linkage authority (LA) comes in. The LA can revoke all generated certificates from a vehicle with just one CRL entry. In this way, even if bad actors gather numerous certificates before being identified and blocked, the LA can still shut them down.

NOTE

Most V2V systems are being designed to support an internal blacklist that's separate from the CRL. A manufacturer or device may blacklist any device.

Misbehavior Reports

V2V and V2I systems are being designed to allow for the ability to send misbehavior reports on anything from standard vehicle malfunctions to notifications of hackers messing with the system. These misbehavior reports are then supposed to trigger the revocation of certificates. But how does a vehicle know whether it has a hacked packet? The answer differs for each automotive industry, but the general concept is that the ECU—or some other device—would receive a packet and check whether it "makes sense." For example, the receiving device might validate a message against a GPS signal or identify reports of a vehicle traveling at improbable speeds, say 500 mph. When something erroneous is detected, the vehicle should send a misbehavior report, which would eventually lead to revocation of that certificate. A misbehavior authority (MA) would be tasked with identifying and revoking certificates from the misbehaving device.

One interesting scenario to consider is that of a vehicle with a low CRL update interval—or that of a vehicle that hasn't been near a roadside device in awhile—leaving it with an outdated revocation list. Such a vehicle might unknowingly forward incorrect information, which would cause it to be reported as a bad actor and which might lead to revocation of its certificate. What happens then? When can the vehicle be trusted again?

When performing security testing, make sure to include these possible scenarios in your research.

Summary

This chapter discussed the plan for V2V communication. V2V devices are still in development and many deployment decisions are still to be made. As this technology rolls out, the various vendors will interpret the rules differently and in ways that could lead to interesting security gaps. Hopefully as these early devices start to trickle out into the marketplace, this chapter will be a useful guide for performing security audits.