

Chapter 2

Security Threats in Cyber-Physical Systems

Traditional security terminology describes high-level attacking scenarios:

- A *fabrication* is a scenario that an unauthorized party generates additional data or objects on a network or in some storage.
- A *modification* is a scenario that an unauthorized party changes existing data or objects on a network or in some storage.
- An *interception* is a scenario that an unauthorized party reads data or objects on a network or in some storage.
- An *interruption* is a scenario that an unauthorized party makes data, objects, or services become unavailable.

A modification and a fabrication can be generalized as an unauthorized write, and an interception can be generalized as an unauthorized read. Regarding security protections, there are also some high-level properties:

- *Integrity* is satisfied if data or objects are not changed (written) or generated by an unauthorized party.
- *Authenticity* is satisfied if an author of data or an object is who it claims to be.
- *Confidentiality* is satisfied if data or objects are not read by an unauthorized party.
- *Availability* is satisfied if data, objects, or services are available.

The following paragraphs will describe existing security threats and protections for different cyber-physical systems.

Security has become a pressing issue for automotive electronic systems, as modern vehicles can be attacked from a variety of interfaces, including direct or indirect physical access, short-range wireless access, and long-range wireless channels [6, 39]. One critical threat is compromising one automotive Electronic Control Unit (ECU) through those interfaces [26]. An attacker may then conduct various attacks by getting access to other ECUs and safety-critical components such as brakes and engines through in-vehicle communications. Another critical threat is directly generating a message on a network through diagnostics ports, empty ports, or wireless networks [55]. ECUs and safety-critical components may thus behave aberrantly.

An overview of in-vehicle security threats and protections was provided by Kleberger et al. [25]. For in-vehicle communication, the Controller Area Network (CAN) protocol has been the most attractive protocol for attackers since it is the most widely used one, and there is no direct support for security protection. Hoppe et al. [13] showed the weakness of the CAN protocol that may affect the operations of electric window lift, warning lights, and airbag control system of a vehicle. Koscher et al. [26] demonstrated that an attacker is able to take over an ECU and execute many functions such as those of body control modules, engine control modules, and electronic brake control modules. Furthermore, denial-of-service attacks are also possible so that inputs from the driver are ignored. Besides the CAN protocol, Rouf et al. [39] studied wireless tire pressure monitoring systems and demonstrated that eavesdropping and spoofing are possible for messages sent from a tire pressure sensor. Checkoway et al. [6] conducted comprehensive analysis and experiments on the attack surface of an automotive system. Seifert and Obermaisser [48] developed anomalies and failures detection on the gateway, which can secure in-vehicle network from both external and internal attacks. Wolf and Gendrullis [56] presented a vehicular hardware security module that enables a holistic protection to in-vehicle ECUs and their communications. However, with these potential gateway and hardware protections, protections over communication are still desired. This is because the gateway protections may not be able to protect against all threats (especially those within the same network), while an existing ECU may also be compromised.

Integrity and authenticity are believed to be more important than confidentiality for automotive communications. This is because automotive systems taken control by an attacker may behave aberrantly and thus have immediate danger, while, regarding confidentiality, the moving behavior of automotive systems is mostly observable by an attacker. As a result, most existing security mechanisms [9, 12, 34] focused on authenticating messages with Message Authentication Codes (MACs) for the CAN protocol. Since a frame of the CAN protocol has only 64 bits for the data payload and the automotive CAN bus speed is typically at only 500 kbps, these mechanisms try to reduce the communication overhead of the MACs through various approaches.

The security threats to automotive systems are becoming broader and more challenging with the emerging of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. For instance, Wasicek et al. [54] demonstrated potential security threats through V2V communications by modeling a platoon of vehicles accelerating or braking simultaneously under adaptive cruise controls. The major standard for V2V and V2I applications is the Dedicated Short-Range Communications (DSRC). At the message sublayer (above the transport layer) in DSRC, SAE J2735 [43] defines standard message types including a Basic Safety Message (BSM) which contains time, position, velocity, direction, size, and other important information of a vehicle. It enables the development of many safety applications such as forward collision avoidance, lane change warning (blind spot warning), and left turn assist [11]. IEEE 1609.2 [21] provides security services at the DSRC middle layers (network layer, transport layer and message sublayer). Message authentication is supported by using the Elliptic Curve Digital Signature Algorithm (ECDSA), which is an asymmetric cryptographic algorithm. When a vehicle intends to send a

message, it signs the message with its private key and sends the message with its signature and certificate digest. A vehicle receiving the message then uses the public key corresponding to the private key to verify the message. The generation time of a message and the location of a vehicle are optionally included in a signed message to protect against replay attacks. Message encryption is also supported in DSRC. More details of DSRC were introduced in some previous works [21, 23].

Besides automotive systems, security is also a rising concern for other cyber-physical systems. Aircraft communicates with ground stations, other aircraft, and satellites through global positioning systems, Automatic Dependent Surveillance Broadcast (ADS-B) [40], and Internet-Protocol-Based Aeronautical Telecommunication Network (IP ATN) [14]. These protocols fulfill the modernization of air transportation systems which become safer, more time and fuel efficient, and more convenient, but there are some potential security risks in global positioning systems and these protocols. Sampigethaya et al. [46] introduced current and next-generation aircraft communication protocols and provided an overview of the standardization progress. Especially, security was highlighted due to the risk of attacks from “brought-in” devices of passengers and the higher dependence of flight on data communications. However, most aviation standards have not included security considerations. Zeng et al. [58] and Gong et al. [8] showed spoofing attacks for global positioning systems. These attacks may lead global positioning systems to be out of synchronization and affect other systems using global positioning systems, such as aircraft systems and smart grids [8]. By observing the dynamic ranges of successful detection rates, a detection mechanism was proposed to protect against these attacks [58]. Among different types of security properties, integrity, authenticity, and availability are more important than confidentiality for control systems of aircraft [5].

Since many of medical devices utilize wireless communications, possible attacks are also pointed out recently. Halperin et al. [10] targeted on an implantable cardioverter defibrillator. By reverse-engineering the implantable cardioverter defibrillator, they successfully performed security attacks, including eavesdropping and spoofing, by replaying signals. They proposed three low-power security mechanisms based on RF power harvesting to protect against these attacks. Furthermore, Li et al. [29] demonstrated security attacks on a glucose monitoring and insulin delivery system. They successfully performed passive attacks (eavesdropping of the wireless communication) and active attacks (impersonation and control of the system), which can compromise safety and privacy of patients. They also proposed security mechanisms with cryptographic protocols and body-coupled communication to protect against these attacks.

Security issues in smart grids have also been identified, and some protection guidelines have also been provided. Khurana et al. [24] gave an overview of security issues of smart grids. They emphasized the communication and device security as well as privacy and introduced the challenges of security management, such as the complexity and scalability of smart grids. McDaniel and McLaughlin [30] also provided an overview of security issues of smart grids. The privacy concern and vulnerability of devices and systems are emphasized again. Khurana et al. [24] worked from authentication principles in Internet protocols and discussed potential constraints of smart

grids. They presented several design principles and engineering practices that help ensure the correctness and effectiveness of authentication mechanisms. Metke and Ekl [31] presented several security technologies including public key infrastructures and trusted computing for smart grids. Lastly, due to global positioning systems out of synchronization, fault detection, voltage stability monitoring, and event positioning of smart grids may also be affected [8].

Security-Aware Design for Cyber-Physical Systems

A Platform-Based Approach

Lin, C.-W.; Sangiovanni-Vincentelli, A.

2017, VII, 102 p. 31 illus., 2 illus. in color., Hardcover

ISBN: 978-3-319-51327-0