

Chapter 17

Dimensions of Cybersecurity Risk Management



Kendall E. Nygard, Aakanksha Rastogi, Mostofa Ahsan, and Rashmi Satyal

17.1 Introduction

In December 2020, it was revealed that multiple federal departments in the United States were victims of major cyberattacks originating from foreign nation-states [1]. Massive data breaches occurred. Exploiting vulnerabilities in software products from several major firms in the United States, the intruders had access to extremely sensitive information for a period of several months. In addition to the federal government, other victims of the attack include government agencies and departments in many states and localities as well as companies in the private sector. The cyberattacks broadly eluded detection, circumvented security controls, and exploited vulnerabilities. Although there have been great many attacks in the past on many targets, the scale and impact on security of these attacks were unprecedented. Trust and reliability of basic systems that underpin society today were diminished. Some have described the impact of the attacks as being so severe that they are essentially a declaration of war.

The concept of risk is broadly understood by people through recognition that bad outcomes can occur in many systems and situations that impact lives, and associated losses can occur. From a technical perspective, specifically, the 2020 attacks illustrate that multiple security shortcomings and vulnerabilities can exist within the systems and networks. Firewalls were unable to detect and block the entry of destructive malware through the boundaries of the systems. Intrusion detection systems monitoring input streams failed to recognize and report suspicious activity. Breach detection and database security routines failed to find unauthorized alterations when updates and change management processes occurred.

K. E. Nygard (✉) · A. Rastogi · M. Ahsan · R. Satyal
North Dakota State University, Fargo, ND, USA
e-mail: kendall.nygard@ndsu.edu; aakanksha.rastogi@ndsu.edu; mostofa.ahsan@ndsu.edu;
rashmi.satyal@ndsu.edu

Technical security is typically associated with a specific element or component, such as a device on the Internet of things, cloud, or firewall. The component may be software, such as a developed system employing secure methodologies, an operating system, or a penetration testing protocol. At the technical level, risk management is concerned with these kinds of aspects.

At a level much broader than purely technical, risk is well understood within societies and cultures. At a very high level, bad outcomes and/or losses affect people through things such as accidents, health issues, floods, fires, and crimes. However, these traditional sources of loss all literally have a digital underpinning in nearly all cases. At these high levels, an example of risk management is the existence and widespread use of insurance products of many kinds, with each type designed to protect against losses. Risk management also extends into commitments to physical systems, such as locks on doors to deter intruders, enforce privacy, and prevent unauthorized access. Vaults and safes exist to keep valuables secure. Police, emergency management teams, and fire departments exist for protection against losses associated with disasters. A great deal of infrastructure and many laws and regulations are designed to reduce or mitigate risk. Examples include mandatory speed limits, buckling of seat belts, and wearing of masks during a pandemic. Risk management in the large has dimensions that go well beyond technical considerations, reaching broadly into societal impacts and the need for policies and regulations. In addition to the prominent technical components, the 2020 data breach incidents are an example of significant impacts on the well-being and livelihoods of many people and the society in the large.

In considering risk management, we take a special interest in cyber-physical systems, with self-driving cars being a prototypical example. Trust, reputation, autonomy, and anti-autonomy are of high importance in analyses and modeling of risk for self-driving cars. Threats can originate from network intrusions, failures of electronic or mechanical components, and external conditions such as dangers posed by other vehicles or pedestrians and weather. There are many points of vulnerability. When a mishap occurs, impacts are often severe, including injuries, deaths, and expensive property damage. Details of threats, vulnerabilities, and impacts that apply to self-driving cars are reported in Sect. 17.3. We also take special interest in modeling and analyses for intrusion detection, authentication, and identity management in relation to risk as reported in Sect. 17.4. We also include descriptions of recent state-of-the-art machine learning approaches that are effective in intrusion detection.

17.2 Systems of Interest

In the digital world of today, there have been many advances in computing and networked systems, including cyber-physical systems; cloud computing; the Internet of things; and mobile and distributed computing. Security is of high importance in all of these areas of computing and cyber sciences, particularly as

bad actors become increasingly knowledgeable and sophisticated in the use of their techniques and actions. The principles of risk management that we discuss in this chapter have applicability to these diverse types of systems. We primarily focus our attention on risk in the context of cyber-physical systems, with self-driving cars as our exemplar.

A cyber-physical system (CPS) integrates software, hardware, and networking with physical processes or devices. Examples include self-driving cars, drones, manufacturing equipment, and weapons of war. In Sect. 17.3, we focus in detail on self-driving cars. CPS technologies account for many improvements in the performance of machines, controllers, and diagnostic systems. In self-driving cars, specifically, many advanced technological advances reduce vulnerabilities and blunt the risk associated with threats. Some prominent ones include: (1) on-board diagnostics, (2) adaptive cruise control, (3) collision warnings, and (4) dynamic monitoring and adjustment systems (lighting optimizers, temperature regulators, cylinder controls, fuel consumption regulators, brake interventions, and lane keepers). Route guidance and traffic assistance also enhance safety.

Figure 17.1 illustrates a generic semi-autonomous cyber-physical system that shows possible disruptions due to a device failure, external attack, or originating from external hackers. For simplicity, only a few of the many points of vulnerability are illustrated. The structure allows for a human on the loop who can exercise control under certain circumstances as needed.

Local networks within the CPS provide communication among mechanisms, embedded processors, devices, sensors, and actuators that work in concert with

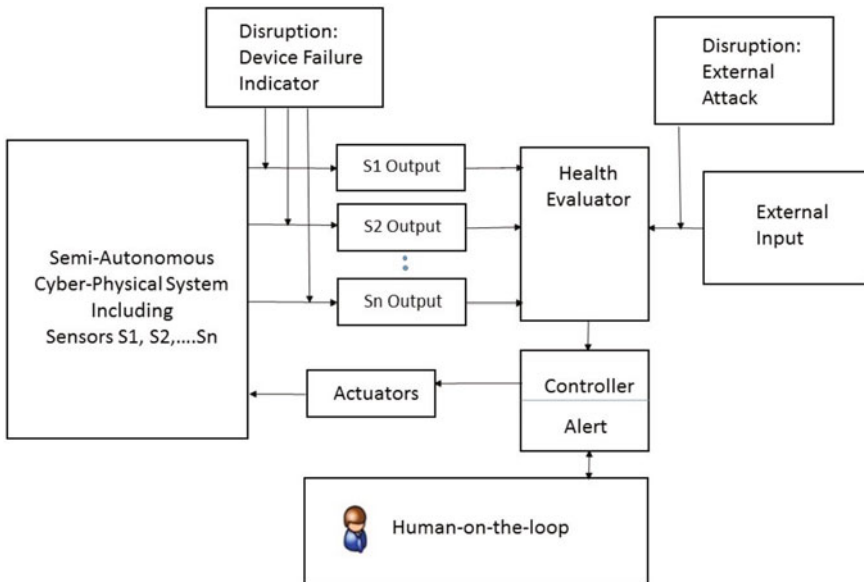


Fig. 17.1 Cyber-physical system control with human on-the-loop

the sensors that report to the explicit health evaluator that is illustrated. Any CPS requires constant monitoring and evaluation for system health. The role of the human-on-the-loop is characterized by an intermittent supervisory control such as that implemented in systems like air traffic control, fighter aircrafts, crisis response, or process controls in manufacturing. The human could receive detailed readouts, visual alerts, or audible alarms and take action that influences the operation of the CPS. For example, in a self-driving car in autonomous operation, the human might receive an indicator that current conditions, such as adverse weather or a disruption, may make it inadvisable to continue autonomous operation and that the human should take over driving.

Critical infrastructure refers to the systems that are so vital to the society that limiting their functionality or incapacitating them in any way would have a debilitating impact on the vitality of the nation. Examples of infrastructure sectors of high importance include electricity, water, energy, chemical processing, and health. Federal government systems, like the ones recently hacked, are a somewhat different type of infrastructure but critical, nevertheless. Most critical infrastructure systems have cyber-physical components that include real-time networking, embedded controllers, and specialized communication protocols that make them vulnerable in specific and interdependent ways. Traditional techniques for cyber-physical systems (CPS) security either treat the cyber and physical systems independently or fail to address the specific vulnerabilities of real-time embedded controllers and networks used to monitor and control physical processes. This is a major weakness of most risk management processes currently in use.

17.3 Characterizing and Modeling Risk

The famous triad of confidentiality, integrity, and availability are the foundational components of information security. Confidentiality is the principle that systems, applications, and data should be accessible only to authorized users. Confidentiality can be violated in many ways, including direct attacks, human error, or lapses in authentication procedures. Integrity concerns ensuring that systems and data have not been modified in any way. Encryption, hashing, and certificates are mechanisms to enforce integrity. Availability refers to ensuring that authorized users have reliable access to resources when needed. Many kinds of attacks, such as denial of service, threaten availability.

Within cybersecurity, in an abstract sense, risk is a concept that includes three types of elements: threat, vulnerability, and impact.

Threat. Any occurrence or presence of something that can jeopardize the confidentiality, integrity, or availability of a system and thus cause harm, hazard, or undesirable performance.

Vulnerability. A condition of being susceptible to a threat through a flaw or weakness in security. The cause could be in design or implementation and lead to being exploited intentionally or accidentally.

Impact. An inimical effect or outcome that can possibly occur.

It is easily understood that all three elements must be simultaneously present for non-zero risk to be present. For example, in the 2020 cyberattack, the initial threat was the arrival of the modified software that was installed, which in turn rendered the systems vulnerable and thus resulted in external hackers gaining access. The impacts are in the form of the importance of the highly sensitive government data that were purloined. The implications for safety, privacy, and national security are far-reaching. When quantitative measures of threat, vulnerability, and impact can be devised, risk can be evaluated as a function of the three elements as shown in Eq. (17.1) below.

$$\text{Risk} = f(\text{Threat}, \text{Vulnerability}, \text{Impact}) \quad (17.1)$$

The challenges in calculating a measure of risk lie in the type of function used in the computation and in the scaling of the measures of Threat, Vulnerability, and Impact. For example, there is a simplistic but popular assumption given by Eq. (17.2). More detailed treatments are described in [2].

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Impact} \quad (17.2)$$

The second term in Eq. (17.2) can be measured using the Common Vulnerability Scoring System Calculator (CVSS) popularized by the National Institute of Standards and Technology (NIST), which is described in [3]. The components of the CVSS calculation basically include low, medium, and high fuzzy measures of exploitability metrics (attack vector type and complexity, privileges required, and user interaction), and temporal scoring. Vulnerability can then be normalized to the interval [0,1] to provide an estimate of the probability that an attack will succeed in doing something harmful. The measure of impact must conflate the elements that comprise the multi-aspect and multilevel nature of risk in that there are direct technical impacts concerning confidentiality, integrity, and availability and also non-technical impacts such as financial harm, legal and regulatory violations, or even loss of life. If an input-monitoring system such as an intrusion detection system or firewall sounds an alert that there is a threat, it is possible to collect data aimed at producing an estimate of a rate per unit time at which a given threat is incident to the system and use it as the threat term in Eq. (17.2). Multiplying by the normalized vulnerability factor yields a rate per unit time at which the threat succeeds in its malicious mission. Finally, multiplying by the impact measure in Eq. (17.2) yields a rate at which the associated harm occurs, which is then a reasonable measure of risk. In notation, let K be a set of possible threats, vulnerabilities, and their impacts, and $k \in K$ be their index. Over a unit of time, such as a year for example, expression (17.3) yields the rate at which harm is caused by a given threat over that time period.

$$\text{AnnualRisk}_k = \text{threatrate}_k + \text{vulnerability}_k + \text{impact}_k \quad (17.3)$$

Summed over the entire set of possible threats, expression (17.4) yields the total harm incurred over the time period.

$$\text{TotalAnnualRisk} = \sum_{k=1}^K (\text{threatrate}_k + \text{vulnerability}_k + \text{impact}_k) \quad (17.4)$$

In practice, probability distributions would apply to all three factors. Expression (17.4) could then be applied with expected values to yield the expected annual risk incurred by individual threats that occur. Since the number of possible risks is typically quite high, statistical methods for approximating the probability distribution of *TotalAnnualRisk* can be utilized. This then provides for using analyses such as the Chebyshev inequality for calculation of probability expressions like confidence intervals at a given significance level or answers to questions aimed at estimating the probability that *TotalAnnualRisk* would be below or above a given level. These types of calculations are invaluable in a risk management process.

We use self-driving cars as a prototypical example of a cyber-physical system. In this context, Table 17.1 shows the primary types of threats, vulnerabilities, and impacts for self-driving cars as well as for more general systems.

17.4 Autonomy, Trust, Identity Management, and Risk

Systems that can run autonomously have provided many enhancements to the lives of people in areas such as transportation, logistics, energy, healthcare, medicine, and aviation. Cyber-physical systems such as intelligent autonomous automobiles hold promise to help improve travel and conveyance with minimal to zero human driving effort. With the inclusion of smart, diversified, and robust technological features and security aspects, many of these systems have gained a positive-level trust and positive reputation scores from the users. Drones are regularly being put to new and varied uses. However, hackers are seeking and developing security vulnerabilities, loopholes, and attack strategies to compromise the operation of autonomous systems. These vulnerabilities influence degrees of trust, risk, safety, and anti-autonomy.

In autonomous vehicles, manufacturers continue to embed new and advanced driver assistance systems. White hat hackers doing important work help prevent and mitigate the risks associated with intrusions that can disrupt vehicle operations. However, compromises still can occur, and once the internal computational systems of the vehicles are compromised by insiders or outsiders, not only are such vehicles a source risk to themselves but also pose a great danger to those around them through their actions and behaviors. These actions and behaviors are a source of mistrust and negatively impact their reputation. Anti-autonomy refers to actions and

Table 17.1 Sources of risk in cyber-physical systems

Type of attack/threat	Description	Vulnerabilities	Impacts
Sybil attack	<p>The identity of an autonomous vehicle is subverted into multiple dissociated identities with the intention of sabotaging its reputation system. Ideally, when an autonomous vehicle only has one distinct identity while communicating with a Roadside Unit (RSU), a Sybil attack generates multiple counterfeit identities appearing as multiple distinct nodes, each misusing the system by propagating false messages</p>	<p>Vehicular Ad-Hoc Network (VANET), Global Positioning System (GPS), RSU</p>	<p>A Sybil attack impacts the authentication, availability, trust, and reputation system of autonomous vehicle by leaking data on a back-end wired channel via exposure of nonencrypted messages and routing table flaws [4]</p>

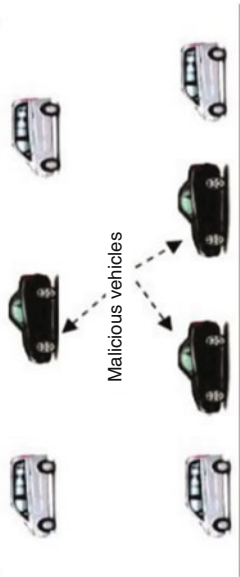


Fig. 17.2 Sybil attack [5]

Figure 17.2 depicts how malicious vehicles can create an illusion of the presence of multiple vehicles on the road and confuse other vehicles into thinking they are in heavy traffic. A Sybil attack is very impactful since the attacker can spoof the identity and location of the vehicle and can implement several other types of attacks in the network [5]

(continued)

Table 17.1 (continued)

Type of attack/threat	Description	Vulnerabilities	Impacts
Black hole attack	A malicious node presents itself as being on a route that provides the shortest total distance to the destination node. Subsequently, the malicious node creates a new route and receives packets from the originating node. Upon establishing the route, the malicious node either drops the packets, or inhibits their forwarding to a genuine node	VANET	A Black Hole attack compromises the network protocol performance and efficiency of a VANET, disrupts the availability of network services, and has impacts associated with the delay of information on traffic congestion, accidents, and road conditions
Grey hole attack	A malicious node, upon receipt of packets from a neighboring node, promises to forward them to another node but drops the packets	VANET	A Grey Hole attack is a variant of black hole attack that compromises a VANET network protocol performance and efficiency, disrupts the availability of network services, and impacts by delaying information on traffic congestion, accidents, and road conditions. The attack also impacts authentication

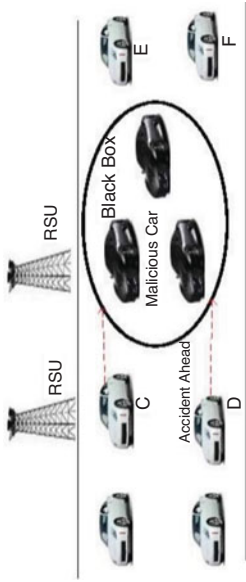
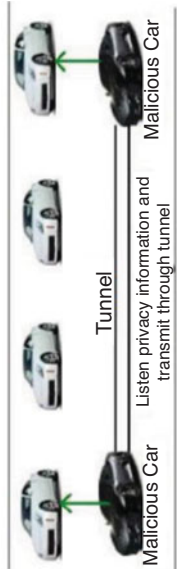
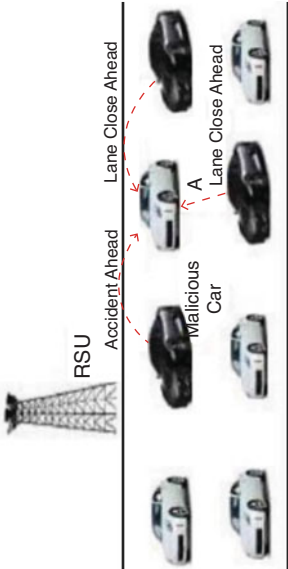


Fig. 17.3 Black hole attack [5]

Figure 17.3 depicts malicious cars (in black) forming a black hole network and preventing the packets received from genuine cars C and D from transmission to other genuine cars E and F [5]

<p>Worm hole attack</p>	<p>Two attacker nodes work together in creating a worm hole or a sort of tunnel route making other nodes believe that these two nodes are close to each other and have the shortest route to the destination. This results in tunnel getting large number of messages which are subject to being dropped</p>	<p>VANET</p>	 <p>Fig. 17.4 Worm hole attack [5]</p> <p>Figure 17.4 depicts how two cars can create a worm hole or a tunnel for transmitting data between genuine source and destination [5]</p>
<p>Distributed Denial of Service (DDoS) attack</p>	<p>A Denial-of-Service attack launched from different locations</p>	<p>GPS, RSU, Electronic Control Unit (ECU), Onboard Unit (OBU), Controller Area Network (CAN) bus</p>	 <p>Fig. 17.5 Distributed Denial-of-Service attack [5]</p> <p>Figure 17.5 depicts malicious cars initiating a DDoS attack on a genuine car from different locations at different times, thus impairing the ability of the genuine car to communicate with other trusted cars [5]</p>

(continued)

Table 17.1 (continued)

Type of attack/threat	Description	Vulnerabilities	Impacts
GPS spoofing	An attacker utilizes a GPS satellite simulator to generate stronger signals than the one generated by genuine satellites [6]	GPS, Light Detection, and Ranging (LiDAR), vehicle's data transmission	This attack impacts authentication and identification wherein the attacker produces false data into GPS devices and fools the nodes into thinking that they are in a different location [6]. An attacker can mislead the car by providing wrong directions
GPS Jamming	An attacker purposely decreases the signal-to-noise ratio by repeatedly transmitting radio signals to disrupt communication with the GPS satellite [7]	GPS, LiDAR, OBU	A GPS Jamming attack impacts availability by effectively blocking the warning messages related to emergency vehicles, accidents, hazardous road conditions. Failing to receive these messages can endanger driver and passenger safety [7]
Sensor Jamming attack	An attacker injects similar and stronger signals or ambient noises that suppress the original sensor signals and causes interference [8]. Often, strong interference can cause sensor denial of service [8]	Vehicle sensors/hardware, OBU	Sensor jamming attacks that cause sensor denial of service can lead automobiles into taking wrong and misinformed decisions and cause fatal accidents. For instance, a sensor that informs a driver that there is a moving object near the vehicle or the sensor that assists in a lane change operation is jammed, it can cause accidents and collisions on the road
Sensor Spoofing attack	An attacker emits carefully constructed signals with ultrasound pulses, frequencies, and modulations identical to the signals emitted by the true sensors [8]	Vehicle sensors/hardware	A Sensor spoofing attack impacts authentication and can result in sensors interpreting the spoofed signal as original and can lead to false detection of obstacles that do not exist
Sensor Relay attack	An attacker deliberately places devices between senders and receivers of signals and relays signals between them with the intention of breaking the distance restrictions in the communication system [8]	Vehicle sensor/hardware	A Relay attack can abuse the Passive Keyless Entry and Start (PKES) system and gain access to the car door, open it and start the engine. This impacts authentication and availability
Camera attack	An attacker can blind the cameras or permanently damage them with strong light, thus impairing its ability to assist advanced driver assistance features that use camera-based functionalities	Vehicle camera/hardware	The Cameras attack targets driver assistance systems used for detection of lane markings, identifying road signs, parking assistance, moving objects, pedestrians, and bicyclists. Blinded or damaged cameras and any changes to its physical configuration can lead to serious or fatal accidents

<p>Malware</p>	<p>Malware refers to malicious software and is a term for viruses, trojans, spyware, worms, and other harmful programs that hackers use to gain access to information. Malware is often spread by a user clicking a link that appears benign. Ransomware intimidates a user by threatening to destroy or block access to their data unless a ransom is paid. Trojans appear to be normal software but are designed to steal important information from the victim. A drive-day attack broadcasts malware to multiple victims and may transfer browser control to an alternative website [9]</p>	<p>Onboard Diagnostics (OBD), CAN bus, OBU components such as LiDAR, camera, radar</p>	<p>Destructive malware has impacts through the demanding of ransoms, stealing data, or affecting availability</p>
<p>Phishing</p>	<p>Phishing is a type of social engineering that fools a user into clicking into a site where they are persuaded into revealing information that they would normally guard [10]</p>	<p>Personal efficacy of the user</p>	<p>A phishing attack can target an individual, a member of a corporate organization, military unit, or government agency. The impacts include loss of secret information or financial assets. Whale phishing refers to targeting high-profile people in an organization [11]</p>
<p>Man-in-middle attack</p>	<p>Refers to an intelligent version of eavesdropping, where the intruder intercepts communication between two parties</p>	<p>Unsecured public Wi-Fi [12]. OBU, VANET, Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and RSU In autonomous vehicles</p>	<p>The impacts are many, all associated with loss of confidentiality of the information. Losses can involve safety, health, and finances</p>

Table 17.1 (continued)

Type of attack/threat	Description	Vulnerabilities	Impacts
DoS attack	<p>An attack type that impairs services and makes systems inaccessible by generating large traffic volumes that consume resources and bandwidth and overwhelms the system [13]</p> <p>In autonomous vehicles, DoS occurs at every network layer for which an attacker controls the vehicle resources, jams communication channels, and denies network access to legal vehicles</p>	<p>RSU, Electronic Control Unit (ECU), OBU, CAN bus in autonomous vehicles</p>	<p>There are large financial loss impacts that occur when servers of financial institutions, government, trade, and e-commerce platforms are brought down [14]. For autonomous vehicles, there are direct impacts related to authentication, availability, and integrity, with severe safety implications and fatalities</p>

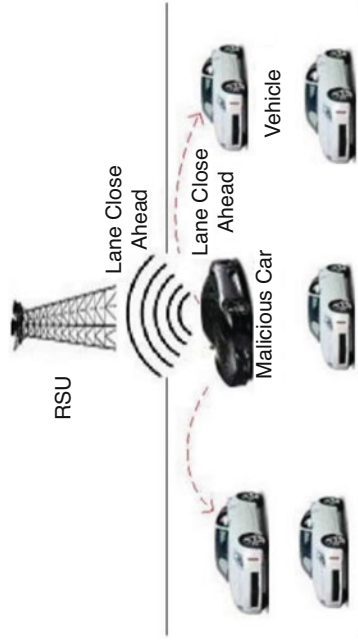


Fig. 17.6 Denial of Service (DoS) attack [5]

Figure 17.6 depicts a malicious car demolishing communication between V2I and V2V by transmitting bogus messages such as ‘Lane closure ahead’ to the nearest RSU or the vehicles near it. This misleads genuine vehicles into making wrong decisions based on the false information they received [5]

<p>Structured Query Language (SQL) Injection</p>	<p>Exploits a vulnerable point that allows an attacker to interfere with the queries associated with a database. This allows changes to stored data or the introduction of malicious queries [15]</p>	<p>The database itself or the SQL, communications and management interacting with the database</p>	<p>Impacts can be very severe and sweeping, since the integrity of stored data is of fundamental importance in how systems are utilized and controlled. Data is the most important asset in many organizations, and does play a role in many cyber-physical systems</p>
<p>Zero-day Exploit attack</p>	<p>An exploit attack that occurs when a new application is installed or when a new vulnerability is revealed with no patch yet installed. Often the vulnerability is not yet known to the developer [16]</p>	<p>When software is updated, fresh vulnerabilities are often introduced. Also, hackers may quickly spread information about newly discovered vulnerabilities</p>	<p>There are many impacts associated with a period of time in which hackers can gain unauthorized access to the system. When tools are stolen in this way and widely distributed, the primary assets of an organization are gone, destroying their business and financial vitality. The attacks can also result in bridges that broadcast malware of multiple types widely [17]</p>
<p>Domain Name System (DNS)-Tunneling</p>	<p>Transferring to an attacker the DNS translation of the human-readable Uniform Resource Locator (URL) into a machine readable IP address over port 53 [18]. DNS tunneling for non-malicious intent is legitimate, but attackers use it to disguise outbound traffic as intended DNS and conceal secured data</p>	<p>Access to the DNS functionality. Gateways, servers, and routers</p>	<p>Severe impacts related to the hijacking of the data</p>

behaviors gone awry. In some cases, the autonomous systems do not align with human comprehension, intentions, and beliefs as many think they should. The laws of robotics can be defiled, pose risk to human life, and cause significant damage.

Advance driver assistance systems and semi-autonomous features in self-driving cars can help avoid certain threats and vulnerabilities. Over the air updates to vehicle's security system and incorporation of self-reboot technology in the vehicle's computer system can also help mitigate risks. Road-side units (RSUs), Vehicular Ad Hoc Networks (VANETs), Vehicle to Vehicle (V2V), and Vehicle to Infrastructure (V2I) technologies, when programmed to inform the vehicles of a potential risk and threat, can help spread risk awareness and help drive risk mitigation approaches.

Risk management becomes a bidirectional issue when applied to the programmed operation of autonomous systems. When these systems are programmed to exhibit anti-autonomous capabilities in interactions with others, they can be enormously helpful. This is the case, for example, in detection of attack strategies from other intelligent systems when battlefield robots are programmed to disarm other battlefield machines that pose threats. One anxiety-inducing military question concerns authorization to engage and fire in battlefield situations when civilian casualties and collateral damages can happen. There have been instances of downsides to the countermeasures and protections against automated attacks. An example is the Counter Unmanned Aerial System (C-UAS) jamming system designed to stop Unmanned Aerial Vehicle (UAV) communication that can inadvertently jam the networks in small airplanes in the vicinity. Additional examples include electro-optical systems and acoustic sensors, which can confuse drones with birds or other airplanes, and electromagnetic and radio frequency interference that can disrupt air traffic control systems when in use near airports [19].

Risks associated with identified threats and vulnerabilities described in Sect. 17.3 results in damaged reputations through inimical impacts on availability, authentication, identity, and integrity. In particular, there are impacts associated with compromise of authentication and identity management protocols employed in V2V and V2I network communications between vehicles. Authentication and identity management issues can also inhibit the sharing of information between vehicles concerning the presence of dangerous conditions such as accidents, dangerous roadway surfaces, road closures, or construction zones. Trust, trustworthiness, anti-autonomy, and their relationships with risk are all influenced. When vehicles are compromised with attacks such as Sybil, black hole, DoS, and DDoS, other nearby vehicles often regard them as anti-autonomous. Once vulnerabilities, threats, and attack strategies to autonomous vehicles are fully understood, their mitigation, remediation, and countermeasures can be designed and developed. Abueh and Liu presented a message authentication scheme for protecting vehicles from fake messages and making VANETs resistant to DoS attacks [20].

Multiple dependencies exist within the topological structure of the communication networks that interconnect devices within complex cyber-physical systems such as self-driving cars. Risk and reliability lessons can be learned through analogy with the smart electrical grid. More specifically, in the smart grid, there is great risk of cascading failures when a problem such as a failed voltage controller or a

downed power line propagates rapidly through the network. Optimization models that direct strategic placements of monitoring devices called Phasor Measurement Units (PMUs) can provide alerts and automatically take corrective actions (such as redirecting power or tripping breakers) when a problem occurs to minimize the risk of dependencies causing widespread disruptions [21]. Similar approaches apply to self-driving cars.

Apart from the risks associated to jeopardized network protocols, corruption of driver authentication systems employed as part of advanced driver assistance systems (ADAS) also pose life risk to the drivers and passengers of the vehicle. The demonstrated success of hackers gaining access to the vehicle infotainment system, onboard diagnostics, steering wheel, anti-lock braking system (ABS), and the CAN bus network reveal many sources of risk.

Risks related to operation of autonomous vehicles are often categorized on the basis of the presence of pedestrians, bicyclists, other human drivers, roadway surface, roadway conditions, weather conditions, lighting conditions, and the preceding movement of the vehicle. Any of these factors can trigger potential malfunctions in the operation of autonomous vehicles. A sudden appearance of a pedestrian or bicyclist in front of the vehicle at an intersection or the actions of vehicle trying to stop at an intersection can result in paralysis of the sensor mechanics of the vehicle. Unprecedented road conditions such as construction repair zones, potholes, loose material, or flooding on the roadway also impact autonomous vehicle operations. When these roadway conditions combine with adverse weather conditions such as fog, rain, snow, or wind, the associated accident and collision risks become higher. Many collisions are reported on a rainy day since rain makes the road surface slippery and also impairs the sensors of the vehicles. Autonomous vehicles do employ LiDAR technology but can still fail to reconstruct point cloud data in poor weather conditions. It is known that rain droplets can partially reflect the light pulses that the LiDAR system emits, leading to increased noise that affects the data and impairs the system.

Interdependencies among multiple risk factors can help draw important correlations among them, which can be utilized toward safety and risk assessment and mitigation. For instance, rainy or snowy weather conditions are correlated with slippery roadway surface resulting in asphalt roads being more slippery than concrete. Also, dirt and gravel roads become muddy in rain or melting snow. Another correlation exists between rainy or snowy weather conditions and roadway surface and lighting. The effect is that asphalt roads are very slippery and dangerous on dark nights with no street lights during heavy rains or snowfall. Moreover, the likelihood of collisions and accidents in pedestrians or bicyclists crossing the streets under darkness on roads with limited street lights during adverse weather conditions increases. Several other studies have contributed to drawing substantial correlations between these factors [22–24].

17.4.1 Authentication and Identity Management

Trust in a system cannot be achieved without a guarantee of confidentiality and integrity. To ensure confidentiality and integrity, user authentication is employed. Authentication establishes the identity of a user. A user must authenticate when they first attempt to establish a connection. Three factors come into play when a system authenticates the user. Use of one or a combination of these factors determines the type of authentication. The factors are as shown below [25].

1. The knowledge factor: something the user knows or has memorized, such as a Personal Identification Number (PIN) or password.
2. The possession factor: something the user has, such as a token or card that can be scanned.
3. The inherence factor: something the user has, such as a biometric like a fingerprint or retina pattern.

Passwords are rapidly becoming obsolete. Knowledge factors are easily misused and stolen. Different measures like recurring password changes, strengthening phrases, and using combinations of different character sets are employed to reduce password vulnerability. However, these are still weak defenses. Possession factors such as tokens and card keys increased in popularity, as they provide better protection than standard passwords. But this factor has the issues of mobility and recovery. Biometrics provide good security against intruders, but many of the devices do not have webcams or fingerprint system installed. To enhance the account security and mitigate these issues, Multi-factor Authentication (MFA) plays a high-performance role. MFA is offered by many websites, applications, and devices to authenticate the user from multiple devices and accounts. Based on the number of validators, MFA is known as Two-Factor Authentication (2FA) and Three-Factor Authentication (3FA). There are several methods to authenticate a user through multiple devices or accounts, including:

1. **Device application push:** The host pushes a message to authenticate the user. Applies to mobile devices and other platforms.
2. **Mobile application code:** The user inputs a unique and time-sensitive code sent by the authenticator application on mobile device. These codes are relatively short and their short time frame for validity enhances the security of the method.
3. **SMS code:** Similar to the Mobile Application Code but uses an SMS text message for the second code. The method does not apply if the user does not use a smartphone.
4. **Email code:** Uses an e-mail message as a second factor for authentication. The e-mail must be registered to the account.
5. **Physical token:** A physical token provides the second validation. The code is unique and is continuously changed by the device.

17.4.2 Trust and Deception

Trust is defined as a belief that an entity will act dependably, reliably, and securely within a specific context. Viewed as a transitive verb, we could write $A \rightarrow B$ to convey the meaning that A trusts B to fulfill some purpose. This also implies the trust can be specific to a domain with intended goals and purpose. The purpose has a context, such as accessing resources or information, controlling or monitoring a process, providing a service, or making a decision. In online systems, trusted message passing is a phrase used to describe public/private key encryption, including digital signatures. However, this restricts trust to the meaning that the message got through from sender to receiver and with no issues of interception, modification, etc. Effective cybersecurity is important in ensuring this type of trust, but unacceptable outcomes can and often do occur even when all of the communication between A and B is trusted in the sense of being accurate and fully secure. Such outcomes can be the result of things such as misinformation, misunderstandings, deceptions, or timing issues. The unacceptable outcomes again illustrate the larger meanings of risk beyond technological trust.

Trust among parties is often built on evidence that is related to reputation. Most retail electronic commerce systems provide measures of reputation, such as five-star rankings or written reviews. When a person hesitates to purchase an item online because the reputation of the seller is low, they may say that they do not trust the seller or, alternatively, that they are taking a risk if they commit to buy. The concept of resilience is also related to trust and risk. For example, consider the many ways in which a self-driving car can experience a problem through a failure of a hardware or a software component because it is compromised, incorrectly instantiated, or wears out. A highly resilient vehicle will avert disaster by failing gracefully, self-healing, or continuing to provide required service by some means. High levels of resilience may be the result of fail-safe machine design by a person, or, alternatively, the result of excellent intelligence on the part of the machine.

There is also the issue of machines trusting people. For a computer system, the traditional meaning of trust is simply effective access control. Authentication methods that can verify that a user is legitimate fall into the three categories that were described above. However, an autonomous and intelligent machine that gets instructions and controls from a human user may require a form of authentication that goes beyond the usual verification methods. It may be the case that the machine would have choices as to which human it should empower to complete their side of a task within a domain, making the “machine trusting man” decisions quite complex. Finally, it is now feasible for machines to capture information about the behaviors of users and utilize them to uniquely model and identify the individual. Departures from the normal ways in which a user interacts with the system can reveal deception, hacking attempts, fatigue, illness, or confusion, all of which are cause for concern if the user is allowed into the system.

Trust and trustworthiness share an inversely proportional relationship with risk. Higher involvement of autonomous vehicles in collisions and accidents increases

the associated risks of technology and decreases the overall trust in autonomous vehicles. Unexpected and incomprehensible behavior of the autonomous vehicles on the roads resulting in collisions and accidents also leads to overall declining levels of trust.

Unique security challenges are present in cloud security. Data stored on the cloud is managed by a third-party provider which is accessed over the Internet. The user does little visibility and control over the stored data on the cloud, which introduces trust issues. Many cybersecurity researchers have indicated that customers should have full access and control over their data stored on cloud for the sake of better security. There are many examples where cloud services providers fail to live up to their service agreement contracts. For example, a provider may enter into a contract that specifies data security and access within a specified time frame but in practice does not always provide the prescribed level of service. Another fact is that cloud storage and facilities are installed all over the world. This raises the question of trusting the cloud provider, including the country where the facility is located and the laws and regulations that apply in the region. However, cloud providers will state that trust reduces controls and access, which introduces a question into trustworthiness. Users should consider that trust is a much broader concept than security, compliance, and privacy.

The digital revolution is a great opportunity for financial institutions like banks and trading platforms. It required many years for these industries to earn high levels of trust by their customers, placing them second only to health care in the importance of trust. Many lending banks have invested heavily in cyber trust, realizing the importance to their business model [26]. Major data breaches reveal that the financial sector is under immense pressure to keep the money and data of their customers safe from attackers. The financial industry is rapidly transitioning all operations to fully online, which increases the needs to utilize advanced cybersecurity practices. In just the past decade, nearly half of all bank teller jobs have been replaced by online systems. People are comfortable with conducting their banking through smartphones. Authentication and identify management are also of high importance in financial institutions, indicating that bi-directional trust is of key importance. A long-term view of trust, safety, and confidence combined with growing customer expectation has made this financial platform an example of high performance in cybersecurity risk management.

17.5 Intrusion Detection and Machine Learning

Intrusion detection refers to practices for identifying outside threats initiated by malicious actors who wish to breach or compromise a system. Machine learning is an approach to intrusion detection that has achieved high credibility and accuracy in identifying intrusions. An important reason is that machine learning methods have the ability to adapt to changes in threat profiles that occur very frequently.

17.5.1 Role of Intrusion Detection

Ubiquitous access to the Internet has encouraged more and more organizations to operate completely over networks, which have the effect of increasing the risks of cyberattacks. Intrusion detection is the process of detecting abnormalities caused by any unauthorized activity in the computer network. The growing popularity of high-bandwidth Internet and the associated dependence of individuals and organizations on Internet connectivity make it essential to protect from external attacks over the network. An intrusion detection system (IDS) is implemented as a wall of defense between such attacks and the network. It is common practice for organizations to use intrusion detection system to detect both internal and external intruders.

Based on the detection approach, IDSs are divided into two categories: signature based and anomaly based. A signature is an identifier derived from patterns of known threats to the system. Signature-based detection systems search for known signatures to identify possible attacks. Based on the data source, an IDS can be classified as host based or network based. While a network-based IDS detects malicious packets and input streams, a host-based IDS detects internal changes and analyzes activities in a single system [27]. Figure 17.7 summarizes an IDS taxonomy.

Anomaly-based detection systems search for significant deviations from what is considered normal behavior of a system or user of the system. Unlike a signature-based IDS, anomaly-based detectors are capable of identifying previously unknown threats or zero-days attacks. The most popular implementation of anomaly detection systems involves machine learning techniques. An IDS that makes use of machine learning techniques relies heavily on feature engineering to learn useful information from network traffic data [29]. The performance of an intrusion detection system depends on the accuracy of classification. Thus, machine learning techniques that can provide high accuracy by keeping false-positive rates low, and maintaining a high attack detection rate is highly desirable [10].

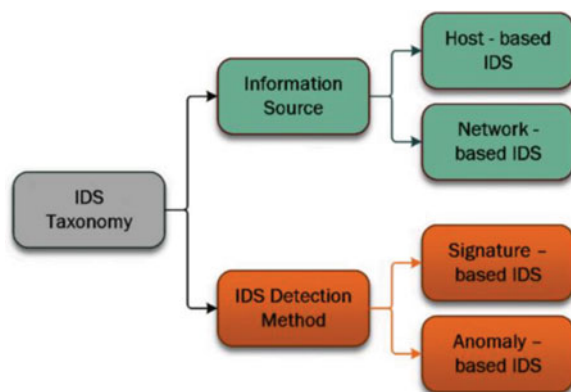


Fig. 17.7 Basic IDS classification [28]

While intrusion detection systems work in altering and protecting systems to an attack underway, intrusion prevention systems are a step ahead and are the act to stop an invasion from occurring. As we describe security, it is considered an impossibility to completely shield a system from every possible attack.

17.5.2 Machine Learning Approaches

Learning, the process of acquiring new knowledge, is an ability with which every living being is born. Machine learning (ML) is an approach that aims to impart this ability into machines. The process of learning in humans and machines is similar in the sense that both acquire knowledge based on experiences [30]. While human learning relies mostly on knowledge transfer from one human being to another, machine learning makes use of “transfer knowledge” which is the method of reusing stored knowledge gained while solving a problem and using it later to solve other related problems.

There have been rapid advancements in machine learning and artificial intelligence in the past decade. Machine learning finds its place in more and more households in applications such as Alexa, Google maps, and virtual assistants. Problem domains such as image recognition, traffic prediction, recommendation systems, self-driving cars, spam filters, speech recognition systems, fraud detection systems, and medical diagnosis are seeing an increasing use of machine learning techniques. In autonomous vehicles, the use of machine learning approaches plays a role in every routine task. For example, ML components, specifically applied to object detection and classification, are the fundamental method used in an Automated Driving System (ADS) to determine relative distances of the vehicle from objects [31]. Incorrect classification of objects is a major challenge for autonomous vehicles. Employing improved ML methods in the context of autonomous vehicles can also help to avoid judgment errors such as incorrectly identifying a stop sign as a speed limit sign, which can be a crucial mistake [32].

There are three fundamental approaches for machine learning. In the first approach, called supervised learning, the learning is accomplished by inducing understanding of trends and patterns that have been observed in the past. The supervised approach uses training data sets tagged with labels from which the algorithm learns patterns.

The second approach, unsupervised learning, employs natural groupings of data items without predefined labels. The third approach, semi-supervised learning, uses domain knowledge to partition unlabeled data. The semi-supervised approach combines large sets of unlabeled data with a smaller proportion of labeled data, with the effect of cutting training effort and possibly accomplishing high accuracy [33]. Regardless of the approach used, a machine learning task typically involves the following steps:

1. Problem identification
2. Data preparation
3. Model training
4. Evaluation and parameter tuning
5. Prediction

Supervised learning is used mostly for problems involving classification and regression. A model based on supervised learning undergoes training and then makes predictions. The model is corrected when it makes wrong predictions, and this training process is repeated until a desired level of accuracy is attained [34].

Unsupervised learning is often used for problems involving clustering. A model based on unsupervised learning finds structures in the input on its own. In pattern recognition problems, where the goal is to discover similar patterns, the training dataset may consist of an input vector with no target values.

Supervised and unsupervised learning methods are popularly used to solve different pattern recognition problems, commonly used in IDS implementation [17]. For self-driving cars, unsupervised learning is an important approach for identifying threats that were previously unknown.

The input data used in training a machine learning model comprises of many features, represented by columns in the data. However, not all features are relevant to the machine learning task [35, 36]. Using a threshold feature selection technique, features relevant to the model can be selected. However, there is always a risk of losing data associated with this approach. Selecting the appropriate threshold is challenging but necessary, as dealing with all features in the data set is expensive [37].

17.5.3 Fuzzy Logic Intrusion Detection Systems

We consider an Intrusion Detection System (IDS) that primarily focuses on identifying anomalous events in computer networks and distributed network systems. Classification and clustering are the most used techniques for recognizing different cyberattacks. Fuzzy classification relaxes the concept of a membership function by allowing continuous values between end points 0 and 1 [38]. This is useful in intrusion detection because certain attack vectors have similarities that make them difficult to distinguish from each other. For example, an attack mounted by a malicious intruder aimed at disrupting the operation of a self-driving car through a wireless connection may utilize a black hole or gray hole attack, which presents themselves in similar ways. Since the nature of attacks is often uncertain, fuzzy logic can play a role in discovering known or unknown intrusion patterns. It is desirable to keep false alarm rates low. Fuzzy logic is considered to be highly accurate for low-level decision-making rather than high-level artificial intelligence. Since fuzzy logic is well suited and effective for reasoning involving consistently vague concepts, it is useful for feature generation or reduction of many machine

learning models. Fuzzy logic can be used to label data for further investigation [39]. Fuzzy rules and functions provide expertise in reasoning with data without using Boolean logic. The set of rules used in a fuzzy expert system are referred to as the rule or knowledge base. The general inference process of an expert fuzzy system consists of four segments, given below.

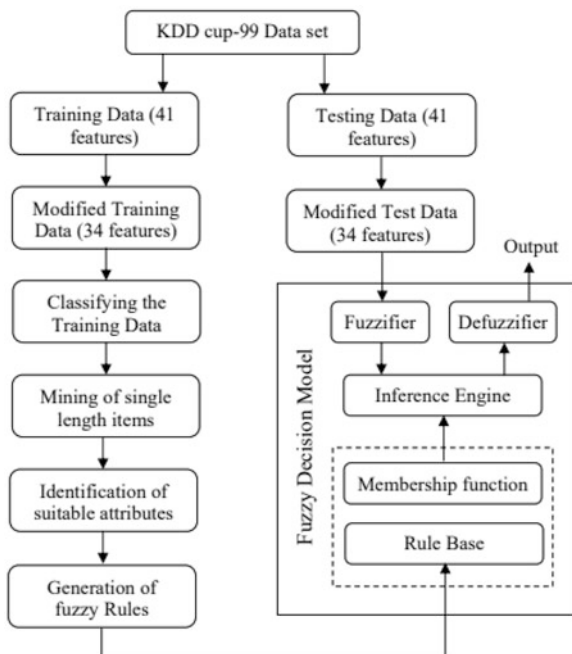
1. **Fuzzification:** Determine the degree of truth of a fuzzy function based on applying actual values to the input variables.
2. **Inference:** Provide a truth value calculation for each fuzzy rule and apply the value to the parts of every rule. Often MIN and PRODUCT operations are used within the inference rules.
3. **Composition:** Combine the fuzzy functions and rules associated with different output variables to form a single subset for an output variable. Often MAX, SUM, and OR functions are used.
4. **Defuzzification:** Converts the fuzzy output set to a crisp number. Often CENTROID and MAXIMUM methods are used.

Fuzzy logic has been used in various intrusion detection systems in combination with other machine learning algorithms. Association rule mining is one of the widely used approaches to finding hidden patterns or rules behind unlabeled data. Fuzzy logic has made this process very reliable and interpretable in comparison to association rule mining [40]. Hybrid cybersecurity frameworks use fuzzy functions to filter out suspicious and harmless data according to the instructions of domain specialists [41]. Fuzzy measures help the feature reduction process through sets of primary logics or functions [42]. A novel Fuzzy Intrusion Recognition Engine was introduced by the authors which was proven effective on TCP packet data to extract metrics of different network attacks, including Distributed Denial of Service [43]. The authors used an anomaly-based fuzzy logic to assess if there are any malicious activities on the network. A high-level fuzzy implementation for network profiling was experimented with the KDD Cup-99 standard data set for binary classification of attack status, resulting in an interpretable high-performance outcome [44]. The proposed system was validated by sets of experiments, including classification of the training data, fuzzy rules generation, building a fuzzy decision module, and classifying test inputs. Figure 17.8 shows a flow diagram of the system.

The NSL KDD is among the most used cybersecurity data set among researchers, particularly for evaluating techniques for modeling and detecting distributed denial of service attacks. Machine learning algorithms have made this prediction nearly perfect using state-of-the-art algorithms [13]. Figure 17.8 illustrates a classification approach used with KDD cup-99 data used as input to a Fuzzy Decision model, resulting in extremely high classification accuracy.

With respect to self-driving cars, fuzzy logic intrusion detection systems have enabled high-performance countermeasures and protection mechanisms against several kinds of attack strategies, such as black hole, sybil, denial of service, and distributed denial of service attacks in vehicular ad hoc networks (VANETs). Alheeti and McDonald-Maier presented an Intelligent Intrusion Detection System that selected important features, extracted them, and then applied fuzzification to

Fig. 17.8 Flow diagram of an intrusion detection system using fuzzy logics [44]



detect and block malicious behavior in the layers of VANETs and provide adequate security to these network layers [21].

17.5.4 Dynamic Risk Monitoring

In cybersecurity risk assessment, there is a need to monitor live networks in near real time. This presents a major challenge for many techniques that have a significant computational burden. Machine learning in particular, although useful in detecting known threats when trained with sets of appropriate historical data, can encounter difficulties when forced to retrain under new conditions. There is a substantial need for research to provide high threat identification accuracy in the presence of shifting and dynamically changing environments with new attack patterns. Some issues in dynamically evolving environments are listed below:

1. **Resource allocation to monitor risk:** Information Technology assets are limited, and resources needed to identify and counter risks are substantial. Estimates indicate that well over half of successful attacks occur at least in part to the scarcity of resources to defend network security [44]. Needed resources include the human expertise needed to deploy, maintain, and coordinate management of and interpret the risks.

2. **The impact of insider attack:** The most dangerous and harmful cyberattack happens from someone who is already inside the organization. It is very difficult to detect an attack when the trust between an insider and the organization is violated. Appropriate risk-monitoring platforms could devote resources to detecting insider attacks based on anomalous user behavior. Accuracy at this point in time is limited.
3. **Deception and diversion:** The expertise of attackers is high, up to date, and extensive. In a diversion activity, an attacker may feign interest in one part of a system to direct assets accordingly. The next step may be to seek access to another asset while the guard is down. Dynamic risk monitors have difficulty in detecting diversion activity. Deliberate deception is a somewhat similar approach. One form is to utilize the system for a long period of time to establish a good reputation. After a solid reputation is established, the time is ripe for an attack since the system has established high trust in the user. Another type of deception concerns the use of machine learning intrusion detection methodologies. Training deception, operating in real-time, will deliberately influence the machine learning system to recognize input only other than the type that the attacker intends to utilize. After the intrusion detection system is skewed to identify threats only in the different input stream, the pathway to breach the system in another way is open.
4. **Backdoors:** Backdoors that remain undetectable from the users are used by the attackers to get access to the system. A standard risk-monitoring system often overlooks backdoors, which can be detected by comprehensive penetration testing. This underscores the need for advanced education and training in ethical hacking.
5. **Predicting potential attack:** Many tools and techniques are implemented to sound alerts to future attack. Every security practitioner wishes to predict attacks before they occur. Although the goal is clear, there are many challenges in implementing this type of system [45]. Predicting imminent attacks requires combinations of tools for dynamic risk monitoring, multiple metrics, and complex statistical correlation and causation procedures to address the desired predictions.
6. **Zero-day attacks:** The use of historical data is often not useful in avoiding zero-day attacks. Once attackers find a zero-day vulnerability, it can be exploited quickly and extensively, sometimes before an approach to developing a patch is identified. Again, dynamic risk monitoring can be helpful to minimize damage from this type of attack.

Dynamic risk monitoring is a largely unmet need in cybersecurity risk assessment and management. Faster and more targeted computational procedures can help address this need. In self-driving cars, dynamic risk monitoring can be facilitated with the incorporation of frequent performance checks at the RSUs and VANETs that are responsible for maintaining communications between vehicles and the roadside units. Incorporation of effective and advanced network communication protocols in V2V and V2I can also significantly supplement efficient risk monitoring

and management in terms of communicating threats to vehicles just in time. These network protocols can also be programmed to deploy fail-safe mechanisms and updates to the vehicles in the event that they are compromised in an attack.

17.6 Conclusions

We focus on risk management, particularly as it applies to cyber-physical systems. Foundations of risk that occur through types of attacks and threats, the nature of vulnerabilities, and types of impacts are explored. Self-driving cars are an important example for which details are provided. Relationships among multiple concepts, including trust and reputation, are developed. Identity management and intrusion detection are characterized. The role of machine learning in the analytics is characterized as it applies to intrusion detection and in real-time monitoring. The overall importance of serious attention to risk management across technological and managerial levels at multiple levels described, including the importance of policies, procedures, and regulations. Dimensions of risk at multiple levels are illustrated.

References

1. Wolff, J. (2020, December 16). *What we do and don't know about the massive federal government hack*. Slate Archive.
2. Kanoun, W., Cuppens-Boualahia, N., Cuppens, F., & Autrel, F. (2007). Advanced reaction using risk assessment in intrusion detection systems. In *Proceedings of the International Workshop on Critical Information Infrastructures Security*.
3. National Vulnerability Database. Retrieved December 20, 2020, from <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>
4. Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. (2020). Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access*, 8, 207308–207342.
5. Zaidi, T., & Faisal, S. (2018). An overview: Various attacks in VANET. In *Proceedings of the 4th International Conference on Computing Communication and Automation (ICCCA)*.
6. Hezam Al Junaid, M., Syed, A., Mohd Warip, M., Fazira Ku Azir, K., & Romli, N. (2018). Classification of security attacks in VANET: A review of requirements and perspectives. In *MATEC Web of Conferences* (Vol. 150).
7. Malebary, S., & Xu, W. (2015). A survey on jamming in VANET. *International Journal of Scientific Research and Innovative Technology*, 2(1).
8. Xu, W., Yan, C., Jia, W., Ji, X., & Liu, J. (2018). Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6).
9. Bilge, L., & Dumitraş, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*.
10. Ahsan, M., Gomes, R., & Denton, A. (2018). Smote implementation on phishing data to enhance cybersecurity. In *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT)*.
11. Ramzan, Z. (2010). Phishing attacks and countermeasures. In *Handbook of information and communication security*.

12. Vallivaara, V. A., Sailio, M., & Halunen, K. (2014). Detecting man-in-the-middle attacks on non-mobile systems. In *Proceedings of the 4th ACM conference on Data and Application Security and Privacy*.
13. Ahsan, M., & Nygard, K. E. (2020, March). Convolutional neural networks with LSTM for intrusion detection. In *Proceedings of the 34th International Conference on Computers and Their Applications*.
14. Bose, S., & Kannan, A. (2008). Detecting denial of service attacks using cross layer based intrusion detection system in wireless ad hoc networks. In *Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking*.
15. Tajpour, A., & Shooshtari, M. J. (2010). Evaluation of SQL injection detection and prevention techniques. In *Proceedings of the IEEE 2nd International Conference on Computational Intelligence, Communication Systems and Networks*
16. Ahmed, M. R., Kim, H., & Park, M. (2017). Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking. In *Proceedings of the IEEE MILCOM Military Communications Conference*.
17. Gomes, R., Ahsan, M., & Denton, A. (2018). Random forest classifier in SDN framework for user-based indoor localization. In *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT)*.
18. Engelstad, P., Feng, B., & van Do, T. (2017). Detection of DNS tunneling in mobile networks using machine learning. In *Proceedings of the International Conference on Information Science and Applications*.
19. Rastogi, A., & Nygard, K. E. (2019). Trust and security in intelligent autonomous systems. *International Journal of Computers and their Applications*, 26(1).
20. Abueh, Y. J., & Liu, H. (2016). Message authentication in driverless cars. In *Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST)*.
21. Alheeti, K. M. A., & McDonald-Maier, K. (2016). Hybrid intrusion detection in connected self-driving vehicles. In *Proceedings of the 22nd International Conference on Automation and Computing (ICAC)*.
22. Boggs, A., Wali, B., & Khattak, A. (2020). Exploratory analysis of automated vehicle crashes in California: A text analytics & hierarchical Bayesian heterogeneity-based approach. *Accident Analysis & Prevention*, 135.
23. Das, S., Dutta, A., & Tsapakis, I. (2020). Automated vehicle collisions in California: Applying Bayesian latent class model. *IATSS Research*, 44, 300–308.
24. Dixit, V., Chand, S., & Nair, D. (2016). Autonomous vehicles: Disengagements, accidents and reaction times. *PLoS One*, 11(12).
25. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1).
26. Chowdhury, M., & Nygard, K. (2018). Machine learning within a con resistant trust model. In *Proceedings of the 33rd International Conference on Computers and their Applications*.
27. Soniya, S. S., & Vigila, S. M. C. (2016). Intrusion detection system: Classification and techniques. In *Proceedings of the IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT)*.
28. Alamiedy, T. A., Anbar, M., Alqattan, Z. N. M., et al. (2020). Anomaly-based intrusion detection system using multi-objective grey wolf optimization algorithm. *Journal of Ambient Intelligent Human Computing*, 11.
29. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunication Technologies*.
30. Janardhanan, P. S. *Human Learning and Machine Learning—How they differ?* Retrieved December 2020, from <https://www.datasciencecentral.com/profiles/blogs/human-learning-and-machine-learning-how-they-differ>
31. Tuncali, C. E., Fainekos, G., Prokhorov, D., Ito, H., & Kapinski, J. (2020). Requirements-driven test generation for autonomous vehicles with machine learning components. *IEEE Transaction on Intelligent Vehicles*, 5.

32. Ors, A. O. (2020, January). *The role of machine learning in autonomous vehicles*. Retrieved January 2021, from <https://www.electronicdesign.com/markets/automotive/article/21147200/nxp-semiconductors-the-role-of-machine-learning-in-autonomous-vehicles>
33. Denton, A. M., Ahsan, M., Franzen, D., & Nowatzki, J. (2016). Multi-scalar analysis of geospatial agricultural data for sustainability. In *Proceedings of the IEEE International Conference on Big Data*.
34. Brownlee, J. (2019). *A tour of machine learning algorithms*. Retrieved December 2020, from <https://machinelearningmastery.com/a-tour-of-machine-learning-algorithms>
35. Li, J., & Liu, H. (2017). Challenges of feature selection for big data analytics. *IEEE Intelligent Systems*, 32(2).
36. Ahsan, M., Gomes, R., & Denton, A. (2019). Application of a convolutional neural network using transfer learning for tuberculosis detection. In *Proceedings of the IEEE International Conference on Electro Information Technology (EIT)*.
37. Pavlenco, T. (2003). On feature selection, curse-of-dimensionality and error probability in discriminant analysis. *Journal of Statistical Planning and Inference*, 115(2).
38. Zadeh, L. A. (1996). *Fuzzy sets, Fuzzy logic, Fuzzy systems*. World Scientific Press.
39. Salome, J., & Ravishankar, R. (2007). Fuzzy data mining and genetic algorithms applied to intrusion detection. *i-manager's Journal on Software Engineering*, 1(4).
40. Tajbakhsh, A., Rahmati, M., & Mirzaei, A. (2009). Intrusion detection using Fuzzy association rules. *Applied Soft Computing*, 9(2).
41. Shanmugam, B., & Idris, N. B. (2009). Improved intrusion detection system using fuzzy logic for detecting anomaly and misuse type of attacks. In *Proceedings of the IEEE International Conference of Soft Computing and Pattern Recognition*.
42. Yao, J. T., Zhao, S. I., & Saxton, L. V. (2005). A study on Fuzzy intrusion detection. In *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, International Society for Optics and Photonics* (Vol. 5812).
43. Dickerson, J. E., & Dickerson, J. A. (2000). Fuzzy network profiling for intrusion detection. In *Proceedings of the IEEE 19th International Conference of the North American Fuzzy Information Processing Society-NAFIPS*.
44. Shanmugavadivu, R., & Nagarajan, N. (2011). Network intrusion detection system using Fuzzy logic. *Indian Journal of Computer Science and Engineering (IJCSE)*, 2(1).
45. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In *Insider threats in cyber security*. Springer.
46. Ren, K., Wang, Q., Wang, C., Qin, Z., & Lin, X. (2020). The security of autonomous driving: Threats, defenses, and future directions. *Proceedings of the IEEE*, 108(2).
47. Sokri, A. (2018). Optimal resource allocation in cyber-security: A game theoretic Approach. *Procedia Computer Science*, 134.
48. Khiabani, V., Erdem, K., Farahmand, K., & Nygard, K. E. (2014). Smart grid PMU allocation using genetic algorithm. *Journal of Network and Innovative Computing*, 2.