UNIT _IV

SECURITY OF CYBER PHYSICAL SYSTEMS

Security of Cyber Physical Systems -Embedded and CPS security - attacks and countermeasures, authentication, identification, confidentiality, data integrity, authorization, access control, malware attacks and counter-measures, security protocols. Privacy issues - vehicular devices and smart metering. Applications of public key and symmetric cryptography, - digital certificates, credentials. Security and vulnerability of cyber-physical infrastructure networks - Mobile and wireless network security, Robust wireless infrastructure - Cloud computing and data security, Event Awareness and System Monitoring for Cyber Physical Infrastructure.

Security of Cyber Physical Systems

Cyber-physical systems (CPSs) are broadly used across technology and industrial domains to enable process optimization and previously unachievable functionality. However, CPSs have been key targets in some of the most highly publicized security breaches over the last decade. Neither cyber- nor physical-security concepts alone can protect CPSs because the complex interdependencies and crossover effects can introduce unexpected vulnerabilities: Physical attacks may damage or compromise the information system on the device, and cyber-attacks can cause physical malfunctions. Because of the many critical applications where CPSs are employed, either kind of attack can result in dire real-world consequences. As a result, security and privacy must be key concerns for CPS design, development, and operation

Security and privacy have in common the concepts of appropriate use and protection of information. Privacy is often thought of as freedom from observation, disturbance, or unwanted public attention and the ability of an individual or group to limit its self-expression. Privacy is often seen as an aspect of security, an affordance of confidentiality, because a secure system should protect the privacy of its users. Confidentiality usually means that information is not released to unauthorized parties, but privacy has a more dynamic dimension of allowing owners to control the dissemination of their information themselves. At the same time, security may be considered contrary to privacy. For instance, politicians and industry leaders endure reduced privacy to protect the public trust .

Information security is generally characterized by three core principles, which Pfleeger and Pfleeger (2007) and Cherdantseva and Hilton (2013) defined as follows:

- **Confidentiality – Only authorized parties can access computer-related assets.**

- **Integrity – Assets can be modified only by authorized parties or only in authorized ways.**

• Availability – Assets are accessible to authorized parties at appropriate times.

Together these are known as the **"CIA triad,"** and they ensure reliable access to correct information for the right people/programs/machines.The CIA triad is the heart of information security but is widely thought to be incomplete. Cherdantseva and Hilton (2013) discuss attempts to amend the triad and propose an information assurance and security octet that starts with CIA but also includes accountability, authentication and trustworthiness, auditability, nonrepudiation, and privacy.

The complete list of security goals Overview of Security and Privacy in Cyber-Physical Systems 3 has not been definitively agreed upon, but we elect to add to the triad two additional elements that are most germane to the physical side of our discussion of CPSs.

The **last two principles are often bundled into the principle of integrity, but they are important enough to deserve separate attention:**

• Authentication – Verifies the identity, often as a prerequisite to access (Committee on National Security Systems, 2010).

• Nonrepudiation – Protects against an individual's false denial of having performed a particular action and captures whether a user performed particular actions (i.e., sending or receiving a message) (NIST, 2013).

There are a number of means of implementing each of these cybersecurity principles. For example, encryption provides confidentiality, protecting data and system functions from unauthorized use.

Digital signatures and secure hashes provide integrity, ensuring data or software updates are not modified. Redundancy of resources keeps the system available for the intended users for proper use at any time even under stress. Identities, certificates, and passwords are examples of authentication mechanisms that guarantee only authorized users may access resources protected by confidentiality measures.

Authentication ensures integrity by verifying the authority of actors who would change an asset. Automatically collected records and logs of these changes may show which user accessed or modified specific parts of the system. When these logs are protected by some integrity mechanism, the result is a system with nonrepudiation.

Nonrepudiation makes violations of integrity clear and provides forensically useful information when security fails. Privacy in the information sense of the word usually refers to the principle of confidentiality, but it is also related to controlled disclosure of information. People want to be able to disclose information to some and not to others and they want to be able to control what is done with the information disclosed. Thus, privacy is a facet of personal information integrity because although data about a person may be transmitted, the information it bears is always the property of the person identified by it.

We divide the CPS domain into two broad categories: **infrastructural and personal**. While functional CPS concepts are consistent between the two categories, the security risks and concerns are often different. **Infrastructural CPSs include ICSs that operate factories, refineries, and other types of industrial infrastructure. Personal CPSs include end-user devices such as smartphones, watches, appliances, and home systems.**

Infrastructural CPSs

Infrastructural CPSs are found everywhere in industry and are critical to modern life. In ICS, the physical side is emphasized, and the cyber side is added for convenient access and control of physical machinery, and so on. However, the points of connection between the machinery and external computer networks may be undocumented or poorly understood as connectivity has often evolved over long periods of time. Some grave concerns are to avoid property damage, economic loss, and physical harm. However, for industrial systems that are part of critical infrastructures providing vital services such as power and water, availability is the overriding concern, as modern societies are largely dependent upon them.

Example: Electric Power CPSs that meet the NSTAC IoT criteria abound in many industrial domains including oil and gas, water and wastewater, chemical, and manufacturing. Infrastructural CPSs are used to monitor every part of the electric grid from power generation through transmission to consumption by end users and accounting for power used. These CPSs must monitor and control turbines, power lines, transformers, feeders, and other critical equipment that are highly distributed, spanning large geographic regions. Sometimes, CPSs are located on remote poles and substations without direct human supervision. Their distributed nature makes it difficult to monitor the CPSs that monitor the system creating security vulnerabilities both in cyber and physical domains. In the last decade, the smart grid trend has increasingly pushed to automate more networked devices throughout the power domain driven by the desire to operate power grids much more efficiently, to reduce strain on current systems, and to lower the cost of deploying future systems.

Smart meters, home energy-management systems, and smart appliances promise to be better stewards of limited energy resources in assisting the populace. However, human operator interaction compounds the challenge of securing these systems because humans routinely cross over system boundaries and may expose sensitive data and services to unanticipated risks, creating additional vulnerabilities not typically accounted for.

Through the smart grid, infrastructural CPSs may invisibly reach down into personal spaces such as homes and create inadvertent risks including loss of services, energy theft, and loss of privacy by enabling pattern-of-life analysis.

Personal CPSs

Personal CPS technologies were meant to produce economic value by automating routine tasks. In personal CPSs, the cyber side is emphasized and the physical dimension is added to enhance the utility of the information system.

The ubiquity of these devices

close physical proximity was required to observe and study the patterns of our lives. Now these devices may provide the possibility to do this from anywhere in the world via their Internet connectivity. For this reason, privacy is the principal concern with personal CPSs. However, safety may be the primary concern in personal medical devices while privacy is secondary. Because personal CPSs may share trust relationships with office or industrial systems and ICS, security is an important tertiary issue.

Example: Smart Appliances Personal CPSs include appliances, wearable utilities, novelty items, toys, tracking tags, medical devices, and a host of devices that enter our lives on a personal level while being connected to the broader Internet. Homes frequently have high-speed Internet access that smart appliances increasingly take advantage of to make their services viewable or accessible online. Refrigerators can order groceries and tell when food is going bad, televisions learn favorite stations and programs, and even light bulbs may detect motion and can monitor home status. Because persons in the home use these items regularly, they must be protected to avoid leaking information that would enable pattern-of-life analysis. Information leakage could subject the homeowner to the unwanted attentions of advertisers or opportunistic thieves. In addition, these appliances are often created to “phone home” to their parent company or its affiliates, passing potentially sensitive information outside the home to unknown parties. Thus, personal CPSs may invisibly reach up into infrastructural and commercial spaces providing undetectable exposure to outside entities

Lack of physical protections using measures such as cameras and better physical barriers. In addition, adding alarms would both increase detection and facilitate a better response. To enhance authentication, the system should require users to have unique identifiers and passwords so that even if someone plugged a laptop directly into the PLC he or she would not be able to use the system without logging in. Barriers and identifiers would also increase the delay time to use the system, giving authorities more time to react.

Nonrepudiation mechanisms such as encrypted log files with redundant, off-site copies would have helped the forensic team reconstruct the breach definitively. Timely detection alarms would have alerted the operators when the system was under attack. An integrity-checking mechanism such as two or more component systems that continually check each other's integrity could have detected the breach in the camera system or changes to the programs that regulated the flow of oil

Anonymity: Separating Owner from Data Deidentification of data (removing direct identifiers and information that easily derives them from a data set) remains an active area of research with uncertain results. For example, Dr Latanya Sweeney of Harvard University demonstrated that deidentified information including only gender, birth date, and zip code of residence is sufficient to distinguish an individual identity over 85% of the time (Sweeney, 2000). Anecdotes and systematic studies of such data reidentification are commonplace.

One key difficulty in assuring the deidentified data cannot be reidentified (i.e., associated with the identity of its subject human) is that adversaries have access to large and diverse public data sets that can be combined with deidentified data to reconstruct identification. Such attacks are often called intersection attacks. At present, we know of no practical deidentification techniques to achieve privacy of individual data while retaining reasonable utility.

While deidentification provides little or no anonymity, differential privacy offers the promise that data of an individual may successfully "hide in the crowd" of other similar data.

Authentication: Verifying User Privileges for Access to Data

The practice of identity authentication has historic roots. As early as 200 BCE or so, fingerprints were used as a means of authentication on written contracts in ancient Babylon. Even earlier, government documents in China were commonly authenticated by the addition of fingerprints of the issuing official. Today, authentication is often achieved on computer systems by the presentation of a prearranged password or phrase. Unfortunately, passwords tend to be either easy to "break" or difficult to remember. In addition, passwords can be stolen by an adversary in many ways.

As a result, the emerging standard for authentication requires more than a password. So-called **multifactor authentication** is often described as combining "something you know" (e.g., a password) with "something you have" such as a randomization token. Effective multifactor systems insist that one of the factors be changed frequently, to avoid replay attacks, where a previously captured combination of multiple factors can simply be reused by an adversary. RSA tokens or virtual tokens such as Google Authenticator provide such dynamic factors. Biometrics are increasingly popular as authentication factors. However, many biometrics (including fingerprints) offer uncertain security.

For example, in September 2013, Jan Krissler demonstrated how to compromise Apple's fingerprint-based Touch ID iPhone technology (Fiebig et al., 2014) using the camera to create an impression. Even high-resolution photographs can reveal iris patterns or fingerprints with sufficient detail to fool biometric authentication systems.

Biometric signatures have the additional problem of being irrevocable: once a user's fingerprints are compromised, they stay compromised. In contrast, passwords and even authentication certificates can be revoked and issued anew. Thus, choosing biometric signatures as authenticators is a potentially poor choice, at least if used in a single-factor authentication system**. Geolocation is a potentially valuable factor for a multifactor authentication system.**

Allowing user authentication only in a specific area, along with verifying a password or a cryptographic token provides substantial assurance in authentication but may not be useful for mobile systems.

Multichannel authentication is an emerging technology that may help in avoiding credential theft due to man-in-the-middle attacks. Such attacks may gather credentials, for example, by using keystroke loggers (particularly on shared computers), by leveraging malicious plug-ins in web browsers, or by interjecting malicious websites between a user's client system and intended web service.

A multichannel authentication system uses a second secure communication channel to authenticate the user without revealing passwords in a way vulnerable to such attacks. For example, a website may display a machine-readable cryptographic code (perhaps as a QR code) when a user browses to the site. The user may then use an app provisioned to her smartphone to take a photograph of the QR code, and use the information encoded there (including a web server session identity number) to contact an authentication service.

The authentication service then contacts the desired server on a secure channel and authenticates the user and associated session number. The web server then logs the user in without 190 Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications requiring direct disclosure of credentials. Such a system can be made into a multifactor authentication system by requiring system users to provide a PIN code during the authentication process.

For example, in May 2016, an Android app was released with the capability to read the barcode on US military CAC cards, part of a system typically used for US government authentication at some secure facilities. The app, called CAC Scan, is reported to be able to retrieve the card owner’s Social Security number, first and last name, and military rank, among other identity details. Including such personal information in an authentication token puts that information at risk in the event of credential theft.

Because even the most secure authentication system is likely still vulnerable to some form of credential theft, authentication fraud detection systems are commonplace. Credit card companies have combated such theft and related credit fraud for years by applying anomaly detection technologies to identify likely credential theft

CPS COMMUNICATION and CPS PROTOCOLS

ICSs used many specialized protocols designed for industrial automation and control, with the key goal of efficiency and reliability. The operational requirements for ICSs were real-time synchronization to support precision operation and deterministic communication of both monitoring and control data. The ICS devices initially only worked over serial channels like RS232 at low speeds, but many have evolved to operate over Ethernet networks using routable protocols like TCP/IP and UDP/IP. In general, the industrial protocols can be divided into two common categories, **Fieldbus protocols and backend protocols.**

Fieldbus is a broad category of protocols that are commonly found in process and control. They are commonly deployed to connect process connected devices, like sensors or actuators. Examples include Modicon Communication Bus or Modbus and the Distributed Network Protocol or DNP3.

Backend protocols are protocols that are deployed on or above supervisor networks and are used to provide efficient system-to-system communication. Backend protocols connect an ICS from one supplier to another supplier’s systems. Examples include the Open Process Communication, OPC, and the Inter-Control Center Protocol, ICCP

Fieldbus protocols :

The Modbus (Modicon communication bus) protocol, designed in 1979 by Modicon, is one of the most popular protocols used in ICS architectures, and it enables process controllers to communicate with real-time computers. Modbus is an open standard, is widely adopted, and has also been enhanced over the years into several distinct variants. Modbus communicates raw messages without the restriction of authentication or obsessive overhead. Modbus is an application layer protocol and allows for communication between interconnected assets based on the request-reply methodology. This enables extremely simple devices, such as sensors and motors, to use Modbus to communicate with more complex computers. During communication, it uses three distinct protocol data units, or PDUs, which are Modbus request,

■ Advances in Security, Privacy, and Trust for IoT and CPS Modbus response, and Modbus exception response14. A transaction begins with the transmission of an initial function code and a data request within a request PDU. The receiving device responds in one of two ways. If there are no errors, it will respond with a function code and data response within a response PDU. If there are errors, the device will respond with an exception function code.

An exception code within a Modbus exception response. Modbus can be implemented on either an RS-232C, which is point to point or RS-45, which is a multidrop physical layer. Up to 32 devices can be implemented on a single RS45 serial link, requiring each device communication via Modbus to be assigned a unique address. A command is addressed to a specific Modbus address, and while other devices may receive a message, only the addressed device will respond. Data are represented in Modbus using four primary tables. They include the discrete input data table, the coil table, the input register table, and the holding register table. The method of handling each of these tables is device-specific, as some may offer a single data table for all types, while others offer unique tables.

Modbus has several variants. These include Modbus RTU, and Modbus ASCII, which support binary and ASCII transmissions over serial buses, respectively. Additionally, Modbus TCP is a variant of Modbus developed to operate on modern networks. And Modbus Plus is a variant designed to extend the reach of Modbus via interconnected buses using token passing techniques. Here we have the Modbus RTU and Modbus ASCII frames. The similar variance of Modbus is used in asynchronous serial communication, and they are the simplest of the variants based on the original spec. Modbus RTU uses a binary representation, whereas Modbus ASCII uses ASCII characters to represent data when transmitting over the serial to your link.

Like Modbus, the distributed network protocol or DNP3 began as a serial protocol for use between master stations or control stations, and slave devices called outstations. It is also commonly used to connect RTUs configured as master stations to IED outstations in electric substations. DNP3 was initially introduced in 1990 by Westronic and was based on early drafts of the IEC 60780-5 standard. The primary motivation for this protocol was to provide reliable communications in environments common within the electric utility industry that include a high level of electromagnetic interference. DNP3 was extended to work over IP via encapsulation in TCP or UDP packets in 1998. And is now widely used in not only electric utility, but also oil and gas, water, and wastewater industries. DNP3 was based on the IEC One of the leading reasons for some industry migration from Modbus to DNP3, includes features that apply to these other industries.

Common cyber-attacks

Some examples of common cyber-attacks are man-in-the-middle attacks, information harvesting, denial-of-service attacks, and replay attacks. The primary reason for this is a combination of insecure communications protocols, little device-to-device authentication, and also less computing power in embedded devices.

• Man-in-the-Middle Attack: In a man-in-the-middle attack, the attacker seeks to get in the middle of the communication between devices, and if the connection lacks encryption and authentication, the attacker can read the data. The adversary then is able to impersonate the device to the hub and vice versa. This could lead to the wrong data being sent to the physician or the monitoring system.

• Information Harvesting: Information harvesting is a significant threat to CPS healthcare devices than CPSs in other domains. Of all the personal data that is available online, personal health information is deemed as a big gold mine. In the black market, the value Cyber-Physical Systems in Healthcare

■ 39 of a person's health record is estimated to be $50, compared to $3 for a social security number and $1.50 for a credit card10 and a lot more focus is on SSN and credit card fraud while the big danger posed by IMDs and other medical sensors is increasing by the day. Disclosure threat, Identity theft, and patient's prescription leakage could be the outcomes of information harvesting from the devices or network. Many times, the information gathered may be used for other purposes.

For example, data from a wearable device like Fitbit could be used to commit burglaries since that could give information about when the person is not available at their homes. The same goes for video footage by unmanned aircraft or driverless cars. The data that is used to enable Machine Learning can also be exploited for malintent in these cases. Moreover, if the data is from influential people or high net worth individuals, then it is more valuable, and people could be subject to extortion or other threats if their private data is compromised.

• Denial-of-Service (DoS) Attack: Denial-of-service attack is a broad category of attacks that include crashing critical devices or flooding the network with a deluge of data, resulting in the loss of availability of the system thereby preventing the system from doing its job. The attacker could try to request power-consuming tasks that might drain CPS devices and networks that are generally LPWN (Low power wireless network) devices. An attacker might use a signal jamming device to scramble responses from a device to the hub, rendering the sensor useless from the hub's perspective. In the case of IMDs with magnetic switches, an attacker could exert a magnetic field near the patient to trigger automatic shut off

DOS attacks could escalate into catastrophic damages in CPSs, unlike online services or websites. A CPS system could be controlling the flow of crude oil in a pipeline, converting steam into electricity, or controlling ignition timing in an automobile engine, and if that gets disrupted, the results can be disastrous. It could lead to not only the hospital or the industry where it is deployed but also cause environmental damages. When a system fails as a result of an attack, one of the following failure modes could be activated:

(i) Fail-stop where the system operation stops,

(ii) (ii) Fail-safe where the system enters a safe mode to avoid any hazardous effects,

(iii) (iii) Fail-loud where the system sounds an alarm, or

(iv) (iv) Fail-quiet where the system allows unauthorized access so that the pattern can be studied

Replay Attack: This is similar to man-in-the-middle attack but more dangerous. Here the attacker eavesdrops on the channel and replays the traffic many times by modifying the data. A replay attack could be made even if the message is encrypted.

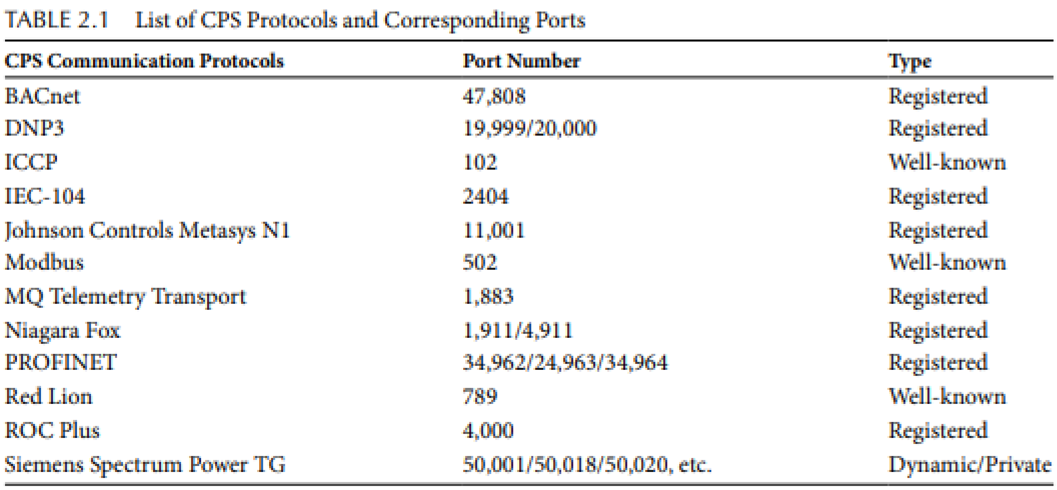
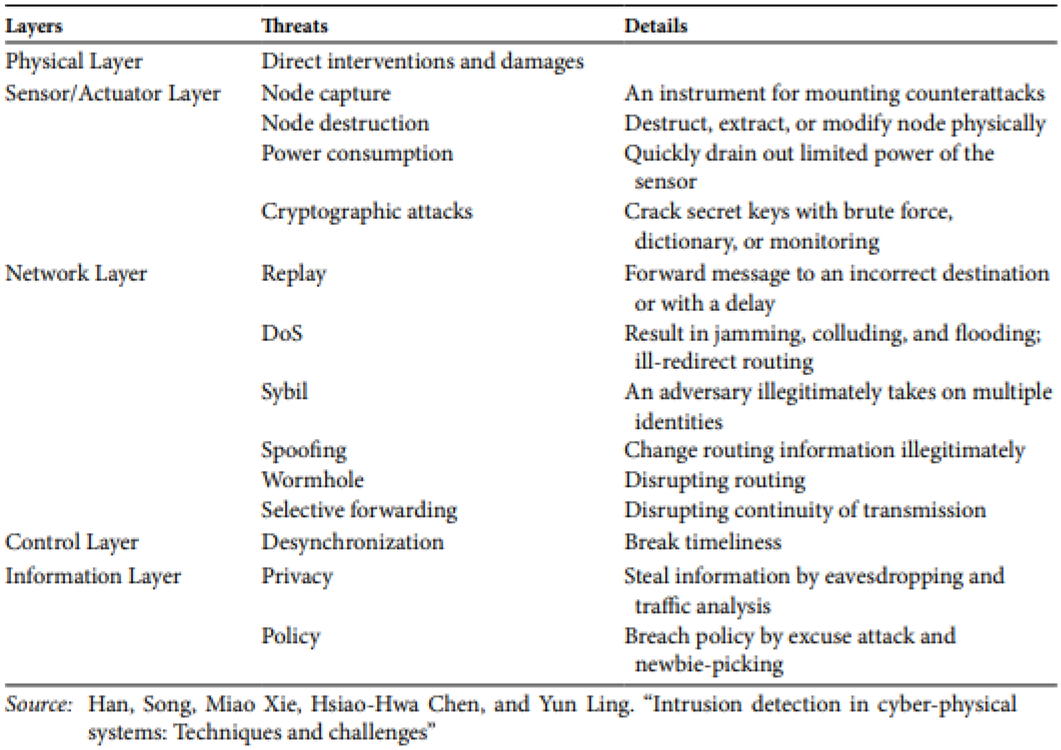


TABLE 2.1 List of CPS Protocols and Corresponding Ports

CPS Communication Protocols	Port Number	Type
BACnet	47,808	Registered
DNP3	19,999/20,000	Registered
ICCP	102	Well-known
IEC-104	2404	Registered
Johnson Controls Metasys N1	11,001	Registered
Modbus	502	Well-known
MQ Telemetry Transport	1,883	Registered
Niagara Fox	1,911/4,911	Registered
PROFINET	34,962/24,963/34,964	Registered
Red Lion	789	Well-known
ROC Plus	4,000	Registered
Siemens Spectrum Power TG	50,001/50,018/50,020, etc.	Dynamic/Private

Security threats against CPS at each layer



Layers	Threats	Details
Physical Layer	Direct interventions and damages	
Sensor/Actuator Layer	Node capture	An instrument for mounting counterattacks
	Node destruction	Destruct, extract, or modify node physically
	Power consumption	Quickly drain out limited power of the sensor
	Cryptographic attacks	Crack secret keys with brute force, dictionary, or monitoring
Network Layer	Replay	Forward message to an incorrect destination or with a delay
	DoS	Result in jamming, colluding, and flooding; ill-redirect routing
	Sybil	An adversary illegitimately takes on multiple identities
	Spoofing	Change routing information illegitimately
	Wormhole	Disrupting routing
	Selective forwarding	Disrupting continuity of transmission
Control Layer	Desynchronization	Break timeliness
Information Layer	Privacy	Steal information by eavesdropping and traffic analysis
	Policy	Breach policy by excuse attack and newbie-picking

Source: Han, Song, Miao Xie, Hsiao-Hwa Chen, and Yun Ling. "Intrusion detection in cyber-physical systems: Techniques and challenges"

Physical Security and Privacy

Physical protection aims to defend an area in space according to the following principles adapted from the U.S. Department of Defense (2016) and U.S. Department of Energy (2005):

• Deterrence – A credible threat of countermeasures that prevents actions against the system by making the perceived cost of an attack outweigh the perceived benefits.

• Detection – The positive assessment that a specific object caused the alarm and/or the announcement of a potential malevolent act through alarms.

• Delay – Impediments that slow or prevent an adversary from accessing a protected asset or from completing a malevolent act.

• Response – Actions taken with appropriate force and at locations and times designed to stop the advancement of the adversary.

• Neutralization – Rendering enemy forces incapable of interfering with a particular operation. Deterrence can be as innocuous as a sign indicating the presence of physical-security components or a guard posted in a visible location to warn the potential adversary of the consequences of an attack.

The interconnectedness of CPSs leads to interdependencies and system interactions that are not obvious to even careful inspection. The very nature of CPSs affords both cyber and physical attack pathways, greatly increasing the adversary's options. Separate sets of vulnerabilities on the cyber and physical sides do not simply add up; they multiply. Having physical access to a cyber system makes possible certain attacks that would not be otherwise. Adding a networked cyber dimension to a physical system increases the complexity of the system, the scope of what may be attacked, and the distance from where the attack may be conducted.

The separate attack pathways may be fully protected in only one domain or the other, but only parts of the system where both domains are simultaneously protected are truly protected. At the same time, defenses in either the cyber or physical component can be used to protect the other component in more ways than a pure cyber or physical system.

For example, computerized skid detectors protect drivers from the physical danger of icy roads. Thus, adding the two domains makes determining the security of the conjoined system much more difficult to assess. Security and privacy attack points in CPSs may be at the interfaces between devices, on the devices themselves, in the infrastructure that supports them, from the Internet, and even from malicious users. Figure 1.1 illustrates a few possible points of Security and Privacy in Cyber-Physical Systems

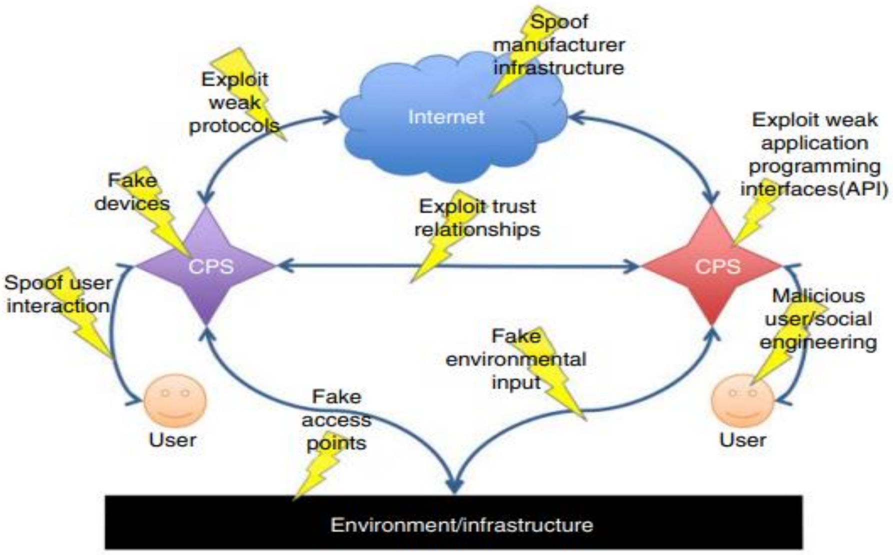

Spoof manufacturer infrastructure
Exploit weak protocols
Internet
Exploit weak application programming interfaces(API)
Fake devices
Exploit trust relationships
CPS
CPS
Spoof user interaction
Malicious user/social engineering
Fake environmental input
Fake access points
User
User
Environment/infrastructure

Figure 1.1 Security attack points in CPSs.

1st DIMENSION OF ATTACK TYPE(S): SERVICE-ORIENTED ATTACKS

1. **Attacks Based on Information** Disruption Ready to be processed and stored health data can be obtained, manipulated, or altered by a malefic attacker to provide wrong information and remove information integrity. Such attacks include the following

   Interruption: An adversary initiates a series of denial-of-service (DoS) attacks to cause communication links to become lost or unresponsive. This attack-type explicitly threatens healthcare availability, standard network functionality, and device responsibility.

   Interception: An adversary eavesdrops on medical data included in transmitted messages to threaten data privacy and confidentiality. Modification: An adversary gains unauthorized access to health data and performs tampering attacks to create confusion and false identities in the IoT health network.

   Fabrication: An adversary forges messages by injecting false information to threaten message integrity and authenticity. Replay: An adversary performs replay attacks to threaten message freshness, and cause network confusion.

2. **Attacks Based on Host Properties** Three possible types of attacks can be launched based on host properties

   User Compromise: An adversary compromises the user's health devices and networks by cheating or stealing cryptographic primitives. This type of attack reveals sensitive information, such as passwords, cryptographic keys, and user data.

   Hardware Compromise: An adversary tampers with physical devices and components and may extract device program-codes, keys, and data. Furthermore, an attacker may reprogram compromised devices with malicious codes.

   Software Compromise: An attacker exploits several software (i.e., operating systems, system software, and applications) vulnerabilities and forces IoT health devices to malfunction states (i.e., buffer overflow and resource exhaustion).

   3**. Attacks Based on Network Properties** This type of attack comes in two necessary forms: protocol- and layer-specific security compromise. Standard Protocol Compromise: An attacker utilizes standard protocols (software and networking protocols) and acts maliciously to threaten service availability, message privacy, integrity, and authenticity.

   Network Protocol Stack Attack: As shown in Figure 3.310, this attack category involves a series of threats that aim to exploit security flaws that belong to different layers of the IoT protocol stack, as defined by the IETF working group. More analytically, these attack types are explained inside the scope of the second attack taxonomy dimension, next.

UNIT IV

Applications of public key and symmetric cryptography

Public key cryptography is typically used in **e-signatures**. An e-signature is a mathematical method to authenticate the identity of a user and maintain the integrity of a document, message, or software.

The main business applications for public-key cryptography are:

- **Digital signatures** − It is a message produced by user's private key used as authenticity of a user. The digital signature generated by the private key of a user and hash algorithm. First the message is encrypted by the private key of the user. The encrypted message creates a signature for user after using the hash algorithm on it.
- **Encryption** − It can transform the plaintext into unreadable format, and it can be used to connect message securely to receiver. Encryption is a procedure that scrambles information to protect it from being read by anyone but the intended receiver. An encryption device encrypts information before locating it on a network. A decryption device decrypts the information before passing it to an application.
- A router, server, end system, or dedicated tool can facilitate as an encryption or decryption device. Data that is encrypted is known as ciphered data (or simply encrypted data). Data that is not encrypted is known as plain text or clear text.
- **Authentication** − It can certify that the message or user is legal or not. Authentication represent that users are who they request to be. Availability describe that resources are accessible by authorized parties such as "denial of service" attacks, which are the sensitive matter of national information, are attacks against availability.
- **Non-repudiation** − The message sender does not decline the signature after communication. Non-repudiation defines that a person who sends a message cannot decline that sent it and, conversely, that a person who has received a message cannot decline that received it. Furthermore these technical elements, the conceptual reach of information security is broad and versatile.
- **Integrity** − The signature provides the received message is not modified. Integrity describe that that information is secured against unauthorized changes that are not distinguishable to authorized users; some incidents of hacking compromise the integrity of databases and several resources.
- **Confidentiality** − The communicated message is encrypted by the public key of receiver such that only the pre-determined user's private key can be used to decrypt the message.
- **Key generation** − Each user generates two keys including public key and private key. The private key is maintained at user side and public key is freely accessible in the network.
- **Signing** − Each user can implement signing operation using its private key.
- **Verification** − The signed signature is verified by the public key of concerned user.

Symmetric key cryptography relies on a shared key between two parties. Asymmetric key cryptography uses a public-private key pair where one key is used to encrypt and the other to decrypt. Symmetric cryptography is more efficient and therefore more suitable for encrypting/decrypting large volumes of data. Symmetric cryptography is used in Payment applications, such as card transactions where **Personal Identifiable Information (**PII) needs to be protected to prevent identity theft or fraudulent charges.

Public key Infrastructure (PKI)

There are three key components of PKI: digital certificates, certificate authority, and registration authority. By hosting these elements on a secure framework, a Public Key Infrastructure can protect the identities involved as well as the private information used in situations where digital security is necessary, such as smart card logins, SSL signatures, encrypted documents, and more. These elements are vital in securing and communicating digital information and electronic transactions. We go over these elements in more detail below.

1. Digital Certificates

PKI functions because of digital certificates. A digital certificate is like a drivers license—it's a form of electronic identification for websites and organizations. Secure connections between two communicating machines are made available through PKI because the identities of the two parties can be verified by way of certificates.

So how do devices get these certificates? You can create your own certificates for internal communications. If you would like certificates for a commercial site or something of a larger scale, you can obtain a PKI digital certificate through a trusted third-party issuer, called a Certificate Authority.

2. Certificate Authority

A Certificate Authority (CA) is used to authenticate the digital identities of the users, which can range from individuals to computer systems to servers. Certificate Authorities prevent falsified entities and manage the life cycle of any given number of digital certificates within the system.

Much like the state government issuing you a license, certificate authorities vet the organizations seeking certificates and issue one based on their findings. Just as someone trusts the validity of your license based on the authority of the government, devices trust digital certificates based on the authority of the issuing certificate authorities. This process is similar to how code signing works to verify programs and downloads.

3. Registration Authority

Registration Authority (RA), which is authorized by the Certificate Authority to provide digital certificates to users on a case-by-case basis. All of the certificates that are requested, received, and revoked by both the Certificate Authority and the Registration Authority are stored in an encrypted certificate database.

Certificate history and information is also kept on what is called a certificate store, which is usually grounded on a specific computer and acts as a storage space for all memory relevant to the certificate history, including issued certificates and private encryption keys. Google Wallet is a great example of this.

Security and vulnerability of cyber physical infrastructure networks

Security by design

- Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature. Some of the techniques in this approach include:
- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way, even if an attacker gains access to that part, they only have limited access to the whole system.
- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to "fail secure" rather than "fail insecure". Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
- Audit trails track system activity so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.

- Full disclosure of all vulnerabilities, to ensure that the window of vulnerability is kept as short as possible when bugs are discovered.

Security architecture

The Open Security Architecture organization defines IT security architecture as the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services. Techopedia defines security architecture as a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible.

The key attributes of security architecture are:

- the relationship of different components and how they depend on each other.
- determination of controls based on risk assessment, good practices, finances, and legal matters.
- the standardization of controls.
- Practicing security architecture provides the right foundation to systematically address business, IT and security concerns in an organization.

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware and software-based.

- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

"Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, the complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected. Today, computer security consists mainly of "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats.

However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As a result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets". The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

In order to ensure adequate security, the confidentiality, integrity and availability of a network, better known as the CIA triad, must be protected and is considered the foundation to information security. To achieve those objectives, administrative, physical and technical security measures should be employed. The amount of security afforded to an asset can only be determined when its value is known.

Vulnerability management

Vulnerability management is the cycle of identifying, remediating or mitigating vulnerabilities, especially in software and firmware. Vulnerability management is integral to computer security and network security. Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities, such as open ports, insecure software configuration, and susceptibility to malware. In order for these tools to be effective, they must be kept up to date with every new update the vendor release. Typically, these updates will scan for the new vulnerabilities that were introduced recently. Beyond vulnerability scanning, many organizations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors, this is a contractual requirement.

Reducing vulnerabilities

While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include seL4, and SYSGO's PikeOS – but these make up a very small percentage of the market. Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or another piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk, but even in highly disciplined environments (e.g., military organizations), social engineering attacks can still be difficult to foresee and prevent.

Inoculation, derived from inoculation theory, seeks to prevent social engineering and other fraudulent tricks or traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts.

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner and/or hiring people with expertise in security, though none of these guarantee the prevention of an attack. The effects of data loss/damage can be reduced by careful backing up and insurance.

Mobile and wireless network security in Cyber Physical Systems

Mobile cyber-physical systems are a prominent subcategory of cyber-physical systems. Examples of mobile physical systems include mobile robotics and electronics transported by humans or animals. The rise in popularity of smartphones has increased interest in the area of mobile cyber-physical systems. Smartphone platforms make ideal mobile cyber-physical systems for a number of reasons, including:

- Significant computational resources, such as processing capability, local storage
- Multiple sensory input/output devices, such as touch screens, cameras, GPS chips, speakers, microphone, light sensors, proximity sensors
- Multiple communication mechanisms, such as WiFi, 4G, EDGE, Bluetooth for interconnecting devices to either the Internet, or to other devices
- High-level programming languages that enable rapid development of mobile CPS node software, such as Java, C#, or JavaScript
- Readily available application distribution mechanisms, such as Google Play Store and Apple App Store
- End-user maintenance and upkeep, including frequent re-charging of the battery

For tasks that require more resources than are locally available, one common mechanism for rapid implementation of smartphone-based mobile cyber-physical system nodes utilizes the network connectivity to link the mobile system with either a server or a cloud environment, enabling complex processing tasks that are impossible under local resource constraints. Examples of mobile cyber-physical systems include applications to track and analyze

CO_2 emissions, detect traffic accidents, insurance telematics and provide situational awareness services to first responders, measure traffic, and monitor cardiac patients.

Mobile Security

With increasing number of mobile devices with 802.1X interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops, access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and PDA's (Personal Digital Assistant) with 802.1X interface.

Security within mobile devices fall under three categories:

1. Protecting against ad hoc networks
2. Connecting to rogue access points
3. Mutual authentication schemes such as WPA2 as described above

Wireless IPS solutions now offer wireless security for mobile devices.Mobile patient monitoring devices are becoming an integral part of healthcare industry and these devices will eventually become the method of choice for accessing and implementing health checks for patients located in remote areas. For these types of patient monitoring systems, security and reliability are critical, because they can influence the condition of patients, and could leave medical professionals in the dark about the condition of the patient if compromised.

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks.

There are a range of wireless security measures, of varying effectiveness and practicality.

SSID hiding

A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier. This provides very little protection against anything but the most casual intrusion efforts.

MAC ID filtering

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

Static IP addressing

Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.

802.11 security

IEEE 802.1X is the IEEE Standard authentication mechanisms to devices wishing to attach to a Wireless LAN.

Regular WEP

The Wired Equivalent Privacy (WEP) encryption standard was the original encryption standard for wireless, but since 2004 with the ratification WPA2 the IEEE has declared it "deprecated", and while often supported, it is seldom or never the default on modern equipment.

WPAv1

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes pre-shared key WPA virtually uncrackable.

PEAP

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Robust Wireless Infrastructure

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to the protection of the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an old IEEE 802.11 standard from 1997. It is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP was superseded in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.11X.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

Security settings panel for a DD-WRT router

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless access. Hacking has also become much easier and more accessible with easy-to-use Windows- or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather information from it through laptops and/or other devices, or even break in through this wireless card–equipped laptop and gain access to the wired network.

Cloud Computing and Data Security

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end-users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. Identity management systems can also provide practical solutions to privacy concerns in cloud computing. These systems distinguish between authorized and unauthorized users and determine the amount of data that is accessible to each entity. The systems work by creating and describing identities, recording activities, and getting rid of unused identities.

In a cloud provider platform being shared by different users, there may be a possibility that information belonging to different customers resides on the same data server. Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process called "hyperjacking". Some examples of this include the Dropbox security breach, and iCloud 2014 leak. Dropbox had been breached in October 2014, having over 7 million of its user's passwords stolen by hackers in an effort to get monetary value from it by Bitcoins (BTC). By having these passwords, they are able to read private data as well as have this data be indexed by search engines.

Physical control of the computer equipment (private cloud) is more secure than having the equipment off-site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud. There is the risk that end users do not understand the issues involved when signing on to a cloud service. This is important now that cloud computing is common and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or Google Assistant). Fundamentally, private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.

Limitations and Disadvantages

Cloud computing is cheaper because of economics of scale, and—like any outsourced task—you tend to get what you want. In cloud computing, the control of the back-end infrastructure is limited to the cloud vendor only. Cloud providers often decide on the management policies, which moderates what the cloud users are able to do with their deployment. Cloud users are also limited to the control and management of their applications, data and services. This includes data caps, which are placed on cloud users by the cloud vendor allocating a certain amount of bandwidth for each customer and are often shared among other cloud users. Privacy and confidentiality are big concerns in some activities. Due to the use of the internet, confidential information such as employee data and user data can be easily available to third-party organizations and people in Cloud Computing.

Cloud computing has some limitations for smaller business operations, particularly regarding security and downtime. Technical outages are inevitable and occur sometimes when cloud service providers (CSPs) become overwhelmed in the process of serving their clients. This may result in temporary business suspension. Since this technology's systems rely on the Internet, an individual cannot access their applications, server, or data from the cloud during an outage

Event awareness and system monitoring for cyber physical infrastructure

Security Event Monitoring provides real-time monitoring, correlation and expert analysis of activity in your environment, detecting and alerting on valid threats to your data and devices. The purpose of monitoring is to promote effective communication. In modern IT, monitoring tells the DevOps or Site Reliability Engineering (SRE) teams how well an observable system is doing its job.

Before implementing a monitoring process, you need to define the metrics you want to monitor. From there, you can collect that set of predefined metrics (and, potentially, logs) from the relevant monitored systems. Then, you'll need to aggregate the data, determine and highlight trends, and call out any disruptions, problems or other errors. There are multiple possibilities, that might cause a warning from the monitoring tools, but here are some examples:

Network latency

Poor application response time

Decreased I/O performance

Failed database operations

Modern web applications use two types of monitoring: synthetic and real user monitoring (RUM). Synthetic monitoring is generally used to monitor short-term trends, while RUM is better suited for long-term ones. Synthetic monitoring uses automation tools to measure a system's functionality. For example, it will use sample values to decide if a web application is performing as expected. RUM involves recording the user's actual interaction with the application and finding out if the application is performing or functioning as expected.

Monitoring isn't a new practice or concept. It has always been a part of the modern computing landscape, going back as far as the dawn of the personal computing era. One early example of monitoring was Norton Disk Doctor. The program would scan PC disk drives and report on problems it found.

In today's DevOps environment, SRE teams use monitoring to check the overall health of individual servers, networks, and data storage. Monitoring functions as a subset of an environment's overall observability goals.