Chapter 15
A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions

Leila Benarous, Benamar Kadri, and Ahmed Bouridane

15.1 Introduction

It is the age of information; almost everything is digitalized and connected, thanks to the internet. What took hours a few decades ago now takes seconds, what was considered a mere science fiction is now a reality and most of what was impossible is now possible.

The massive use of internet and electronic devices greatly requires and depends on the security and privacy as people are becoming more active in the cyberworld, sharing massive information especially via social networks which are the newest type of addiction that people cannot live without, our privacy is being threatened.

Ordinary users believe that the internet is safe and that they are immune from threats and are not targeted by attackers maybe it is the human nature to be trusty and optimistic to feel safety and security but the truth is that this is just an illusion; the cybersecurity is being threatened every day, at least one million of new viruses and malware is released daily, and more than 100,000 cyberattacks every hour which costs over 100 billion dollar yearly [1].

Ensuring security is mandatory and is rather a difficult task because of many reasons:

L. Benarous (✉) • B. Kadri (✉)
Department of telecommunications, Faculty of Technology, University of Abou Bekr Belkaid, Tlemcen, Algeria
e-mail: leila.benarous@mail.univ-tlemcen.dz; benamarkadri@yahoo.fr

A. Bouridane
Department of Computer Science and Digital Technologies, Northumbria University, Newcastle upon Tyne, UK
e-mail: ahmed.bouridane@northumbria.ac.uk

R. Jiang et al. (eds.), *Biometric Security and Privacy*, Signal Processing for Security Technologies, DOI 10.1007/978-3-319-47301-7_15

- Firstly, the number of new malwares released everyday makes it difficult to keep the track. In addition, the new viruses rely on new techniques to avoid detection such as self-changing code on each infection or the use of cryptography.
- Secondly, the attacks may come from the inside of the networks making it more effective as the attacker might have higher access rights.
- Thirdly, the attacker is unknown (his/her level, techniques and motivation).
- Finally, attacks and malwares exploit the system and software vulnerabilities which may include the vulnerabilities of the security system itself.

Regardless of all the previously mentioned challenges, the security protectors keep developing new techniques and search for new solutions to keep the networks, systems and data safe.

The main focus of this chapter is to survey the cyberworld security and its evolution as the technologies of networks, systems and data saving are developing. The survey includes a historical overview, the security objectives, its issues and their classification, its solutions including the current solutions (authentication, steganography, ..., etc.) and future tendencies such as biometric solutions for authentication, its attackers and threat creators and their different classifications. Finally, as the cybersecurity crimes are spreading and governments are taking legal action against attackers, a brief description of forensic investigation process is included.

15.2 The CyberWorld

The cyberworld and virtual world are other words referring to the internet. The simplified definition of internet would be: "a set of computers or machines linked to huge servers that provide different services for the machines to use". This is not the technical definition, rather it is an easy way to define the concept and technology.

We, humans, are the users of the machine which can be a computer, smartphone, tablets, smart TVs or any other device that can connect us to the internet.

The services are the websites we use such as social media (Facebook, twitter, YouTube, ..., etc.), mailing websites (Yahoo, Gmail, Hotmail, ..., etc.), e-commerce websites (eBay, PayPal, Alibaba, Amazon, ..., etc.) or any other websites that we frequently use.

The server for a normal network user means nothing but a black box and is totally invisible, all what is clear for a normal user is that he/she contacts an internet service provider, pays a bill and he/she is connected to the cyberworld and enjoys its services.

15.3 Darknet or Deep Internet

The internet defined above is what most of the users know but there are other terms such as the darknet or deep internet; it is a part of the internet that is accessible via special tools such as Tor [2] or Riffle from MIT [3], and it contains websites that cannot be accessed directly from normal search engines like Google. One of the definitions of darknet is: "a class of networks that aim to guarantee anonymous and untraceable access to web content and anonymity for a site" [4]. This dark side of the internet is used by hackers and dangerous criminals because it ensures intractability.

Although cybercrimes occur in both the clearnet and the darknet, the crimes of darknet are out of this chapter's scope, instead more focus is forwarded to security threats to clearnet, the systems and information.

15.4 Internet Usage

This section includes some frequently used online services that make us so dependent on the internet in general with all its components and that put our privacy at stake. The mostly used internet services are regrouped by category from Alexa websites ranking.

- *Search engines and mailing services*, such as Google, Yahoo and MSN
- *Social media networks;* include video sharing websites (YouTube and Daily motion), online TV, social services (Facebook, Twitter, Instagram, Weibo, ..., etc.) and blogging websites (Tumbler, Blogger, ..., etc.)
- *E-commerce services*: all websites allowing transactions or establishing business, banking or simply buy-sell websites such as Alibaba, Amazon, eBay, PayPal
- *E-learning*: includes websites used for learning that present lectures, webinars or training, also encyclopaedias such as Wikipedia, ask/answer forums like Stack OverFlow or Ask, and it includes also scientific journals and academic websites
- *News and entertainment*: journals, magazines, health, sports, map and weather services are few examples
- *Cloud services, storage and file sharing*: include Google drive, drop box, media fire, ..., etc.
- *Gaming*: online gaming websites such as Twitch and Battle, ..., etc.
- *Advertising*: such as onclickads
- *Personal/organizations websites*: websites of corporation and individual personalities
- *Industrial monitoring and controlling*, which includes remote access services; controlling and monitoring industrial equipment such as robots [5]

15.5 History of Cybersecurity

> "The cyber issue is not new, but rather has taken a half-century to develop. Indeed, it was already decades old before the general public and many senior leaders recognized its salience in the mid-1990s." *Michael Warner*

Historians think that security issues appeared as early as 1960s. However, in theory it appeared much earlier, more precisely in 1949 when the mathematician John von Neumann defined the virus and worm as self-replicating automata [6].

Although the theoretical concept has existed for so long, it was only after the successful security attacks have occurred that the importance of cybersecurity was emphasized. The attacks cost fortunes, exposed secrets and endangered lives.

Historians observed that the cybersecurity concerns took different trends through decades and that it was influenced by political and sociological events. For example, during 1980s, the cybersecurity concern was foreign espionage. During the 1990s, the threat has been directed towards civilian critical infrastructures and later on, the terms cyberterrorism, organized crime and hacking were used to describe the attacks [7].

Based on their chronological order, the major security issues that occurred in the past five decades can be described as follows:

- In 1964, AT&T started monitoring Phone Freaks also known as Phreaks who were able to make free phone calls.
- In 1968, potentially the world's first case of computer espionage was carried out by a German spy in German subsidiary of IBM.
- In 1971, hackers made the viral *Creeper* worm which infected ARPANET.
- In 1981, *Elk Cloner* was made by 15 years old Richard Skrenta.
- In 1982, a group of teenagers hacked high-profile computers in the USA; the operation was called *414 s break-ins*. A similar operation named *Cuckoo's eggs* occurred from 1986 to 1988.
- In 1988, *Morris* worm was released and ARPANET recorded its first major network incident.
- In 1990, the first self-modifying viruses were created.
- In 1992, *Michelangelo* virus was released overwriting the first 100 sectors of the hard disk causing what was called the first digital mass hysteria.
- In 1994, two major hacking operations were recorded, the *RomeLab* incident and the *Citibank* incident.
- In 1995, the first Microsoft word-based virus was created.
- In 1998, *Back Orifice* was released to give remote system administration (Trojan Horse). Also the hacking incidents of *Solar Sunrise* and *Moonlight Maze* were recorded that year.
- In 1999, *Melissa* spread by infecting emails.
- In 2000, *I Love You* spread by sending itself to the first fifty people in windows address book. In the same year, the computers of California University were used by hackers to crash the websites of Amazon, eBay and Yahoo.

- In 2001, *Code Red* and *Nimda* worms were used to take over the control of computers and use them for DDoS. In the same year, the first cyber world war was recorded caused by a conflict between USA and China, where hackers from many countries in the world participated.
- In 2003, *Slammer* and *Blaster* were used to launch DDoS attacks. Also Titan Rain aimed to access high-profile computers in the USA.
- In 2004, *Sasser* caused systems to crush and internet to slow down.
- In 2007, *Zeus* was used to steal banking and other information.
- In 2008, *Conficker* worm was used to form botnets. Also K*oobface* virus spreads through email or social media service such as Facebook, causing fake buying operations and thus money theft.
- In 2009, *GhostNet* and *Operation Aurora* incidents were launched, the first was for cyberspying and the second was against Google and other high-tech companies to access and modify their codes.
- In 2010, *Stuxnet* was used for industrial espionage, and *WikiLeaks* launched an attack called *wikileaks* cable gate where confidential diplomatic cables were leaked.
- In 2011, *Duqu* was released (a modified copy of *Stuxnet*) also the *Ramnit* virus which steals Facebook accounts and passwords. The year recorded highly publicized hacking attacks such as: the attacks against Sony and other corporations, against governments and the theft of CO_2 emission allowance.
- In 2013 and 2014, many hacking operations were done, and most of the attacks focused on stealing Facebook and email credentials [6, 8–10].

15.6 Security Objectives

The objectives presented here are the requirements of the security solutions. Originally, there were three principles which are the availability, the confidentiality and the integrity but three other principles were added as the security needs required which are the authenticity, non-repudiation and auditability. The six objectives are explained in this section as follows:

- *Availability*: allows the authorized parties to access to the systems and required data resources, i.e. the system can always provide its services to the authorized requester and the resources can be used when needed by the authorized requester as well. One of the most dangerous threats to availability is the Denial of Service attack which prevents the authorized users to access a system (resource) and thus preventing them from using its services [6].
- *Confidentiality (privacy)*: ensures that an asset (personal data or resource) is accessed by the authorized person only [11, 12]. One of the major threats to privacy is the exposure of data.

– *Integrity*: ensures that the data is modified by the authorized person only. This means that the content is coherent and authentic and has not been altered by a third party [11].
– *Authenticity*: the ability of a system to confirm the identity of a sender where he is first identified then authorized (or denied) to access the system [11].
– *Non-repudiation*: it ensures that the sender (originator of the message) cannot deny sending the message [11]. This principle was added because the users would deny having sent the message if they are legally prosecuted especially in cases where the message contains illegal content, threats or in e-commerce the user's denial of purchase.
– *Auditability*: it was added by the US Department of Defence and it is "the ability of a system to trace all actions related to a given asset" [11]. The system records all important events such as sending and receiving messages, the IP addresses and any other relevant information to help detect security issues and bugs, trace the intruders, and resolve and document the issues.

15.7 Security Threats

After emphasizing above how dependable we have become on the cyberworld and the importance of security by stating some of the major security threats recorded, this section discusses the security threats which can be classified into two main types: *physical* and *logical*.

The *physical attacks* require the physical presence of the attacker and his/her direct interaction with the system of network components. This usually results in the loss of the device or equipment, its destruction or generating noise and interfering with wireless signals.

On the other hand, the *logical threats* can be divided into three classes depending on the target: the *information*, *networks* and *systems*. The attacks on the networks are depicted in the table below where different kind of networks (infrastructure-based and ad hoc) are presented along with major threats related to each type. In Fig. 15.1 and Table 15.1 the previously mentioned problems and their solutions are presented which will be further explained in the next section.

The following describes some of the attacks and security threats previously mentioned:

– *Denial of Service (DoS)*: it is an attack that aims to overtake a network or a machine and prevent it from providing services. This kind of attack can be done via flooding attacks or exploiting technical vulnerabilities of a system or a protocol. The Distributed Denial of Service (DDoS) attack is more dangerous since it uses multiple machines to launch the attack in order for the attacker(s) to overtake the machines (often these attacks are also called zombie or bot machine and they form a botnet to launch the DDoS attack). DoS attacks can be addressed by filtering the IP addresses and dropping the packets coming from the attacker's

IP. This can become very hard in DDoS since the attacker uses multiple machines each sending a certain amount of packets to cause the denial of service of the victim sever (it is a synchronized attack, sending multiple packets from different machines); in this case, filtering the IP addresses and detecting the attacking machine become hard [13].

- *Spoofing* or *Impersonation*: it is an attack where the attacker pretends to be another node which in most of the times is a trusted node. Among spoofing attacks there are:
  - *The IP spoofing attack* where a node changes its IP address to another address that is different from its real source address.
  - *ARP spoofing*, it aims to send fake replies to ARP queries, which results in mapping the IP address to a fake MAC address and thus poisoning the ARP cache.
  - *The DNS spoofing* which is similar to ARP spoofing and results in directing the requester to the wrong webpage or mailing service by mapping the pages to the wrong addresses in DNS cache, also known as Kaminsky attack where the attacker tries to poison the DNS cache by fabricating a reply to a specific request; the attacker mainly succeeds in the attack because he can guess the sequence number of the DNS reply known as the Query ID [14, 15].
- *Flooding*: it is an attack that aims to saturate the network or resources of targeted node by sending enormous amount of packets such as TCP SYN packets; or PING packets.
  - In the *SYN flooding*, the attacker sends SYN messages from different IP addresses to the victim server, the server reserves a memory space for the information related to the half opened connection, replies with ACK and waits for the ACK of the attacker or the expiry of the session, with many half opened requests the memory space allocated for storing connection information will reach its limit causing the denial of service.
  - In *Ping Flooding attack* also known as the *ping of death*, the attacker sends multiple ping requests to cause the absence of response of the victim.
  - There is another type of flooding which is the *UDP flooding*; it relies on sending a large number of UDP packets to the victim resulting in the Denial of Service [13, 16].
- *Jamming*: a physical layer attack which interferes with the radio frequency used for communication between nodes of the network. The noise generated disrupts the communication between the nodes causing collision and failure [17].
- *Man in the middle* (active interference): it is an attack where the eavesdropper generates, alters or drops packets. The attacker first intercepts the traffic, breaks the authentication chain and then impersonates the hacked endpoints seamlessly [18].
- *Node isolation*: partitioning the network by preventing a node or a set of nodes from communicating with the rest of the network [19].

- *Route disruption:* one of the routing problems where the routes are modified by faking the route replies so that routing loops are created, or packets are forwarded along erroneous, non-optimal or non-existing routes [19].
- *Resource consumption:* decreasing the network performance by consuming network bandwidth or node resources such as the memory or the energy [19].
- *Eavesdropping* also known as disclosure attacks, where the attacker intercepts and analyses the network traffic (broadcasted messages); it is a passive attack since the user does not alter, create or drop the packets [19].
- *Wormhole (Tunnelling)*: the wormhole attack is possible even if the attacker has not compromised any host and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records the packets (or bits) at one location in the network, tunnels them (selectively) to another location and retransmits them from there into the network [20].
- *Timing attacks*: the attacker pretends to be closer to the victim nodes than it really is. This can be done either by sending a fake route reply (rush attack) or by flooding the network with hello messages (hello flood attack) that are transmitted with high power, enough to make the victim node believe that the attacker is a neighbour node [19].
- *Stealthy attack*: it is similar to DoS attack but the attacker does not control the node instead he/she manipulates the routing table of the victims so as the routed packets cause disruption to the network. Another form of stealthy attack is also based on the manipulation of routing table and allows the attacker to eavesdrop nodes that are out of his range by using the victim node [21].
- *Black hole attack:* it is an attack launched by an insider which fails to propagate messages or packets and drops it instead [22].
- *Sinkhole attack*: the attacker or malicious node attracts network traffic and then does a selective forwarding [23].
- *Spamming*: hackers often use this technique to deliver the recipient unwanted emails such as advertisements, to spoof the user credentials (phishing) or to crash the mailing server by sending millions of spams, an attack known as mail bombing [24].
- *Position faking attack and GPS spoofing*: in this attack, the attacker generates a stronger localization signal than that of the GPS signal with a fake position so as the receiver node gets fake information [25].
- *Sybil attack*: the ability for the attacker node to have multiple identities which is dangerous because the node can use the multiple identities to generate additional votes in election algorithms, to route multiple paths through it (the malicious node) or to avoid traceability [25, 26].
- *Masquerading attack*: the attacker node poses as a legitimate node to conduct other attacks such as injecting false messages [22].
- *Replay attack*: attacker node records exchanged packets to retransmit them later [27].
- *Session hijacking*: the attacker forges unprotected session after it has been initialized by forging the IP address and computing the sequence number to launch DoS attacks [27].

- *Phishing*: an attack against computer users to convince them into performing an action that can cause them harm. It can be done by sending emails to the victim where they have to download an attachment or click a link. The attachment could contain malwares such as viruses, spyware or key logger that either steal the information of the user, slow the performance of the system or destroy it. The link would direct the user to a fake webpage where he could be asked to provide sensitive credentials [28].
- *Password cracking*: it can be done either by guessing the password, stealing the file containing the password (if stored as clear text), brute force or dictionary attacks or known through social engineering techniques. Noting that a password is generally not saved as clear text but as hash values and sometimes even salted hash values (a salt is a random value added to a password before it is hashed, and it ensures that two passwords would not have the same hash) [29].
- *Teardrop*: an attack that can be used to cause denial of service. It exploits the features of IP datagram which is that a single data unit can be of a variable length and can be fragmented into smaller pieces and transmitted; each piece will indicate its position in the original data unit and length so as the receiver reassembles the pieces to get the complete data sent. The attacker would use those features, but the position of the pieces will overlap causing the system to crash while trying to assemble them [30].
- *Social engineering*: the attacker deceives the users to give him/her confidential information such as password, system configuration or contact information. The social engineering uses psychological tricks, since human often tends to trust, sympathize and help each other. The hacker can use these characteristics to trick his/her victims. The hacker often does background research about the targeted company and collects useful information which he can use in gaining the trust of the victim. The attacker pretending to be an insider can contact the victim by phone, email or in person and request sensitive information. This attack is also known as human hacking [31].
- *Technical vulnerabilities*: it includes the system, network protocol and database vulnerabilities, for example: SQL injection, buffer overflow, ..., etc. [32].
- *Data mining*: it refers to a process of nontrivial extraction of implicit, previously unknown and potentially useful information from databases [33].
- *Dumpster diving* is also known as *trashing* and is one of social engineering techniques. The attacker collects the trash of companies to look for useful information such as contacts, password, old hard disk, printouts of code source, security system design, system configuration, ..., etc. The hacker can use the collected information to break-in the system or network [30, 34].
- *Fragmentation attacks*: fragmentation of a packet into tiny pieces sometimes overlapping pieces to create problems to the receiver if there is no minimum fragment size and offset [35].
- *Malware*: it is a portion of codes intended to cause harm. It includes:

- *Viruses*: "Fred Cohen defines the term computer virus as a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself" [36].
- *Ad ware*: tools for advertising; these software might install other tools without permission [37].
- *Spyware*: tools used to gather information about a user or organization without their knowledge [37].
- *Rootkit*: a malicious code that hides its presence in the system by intercepting and filtering commands of operating systems that might lead to its discovery, and when discovered and removed, it could re-establish itself. It is named rootkit because it operates as root [30].
- *Worm*: unlike the virus which requires the user taking action such as executing or copying the carrier program for it to propagate, worms are malicious programs that self-propagate across a network exploiting security flaws in used services [38].
- *Scripts*: also known as the cross-site scripting (XSS) vulnerabilities, allow the attacker to include malicious code typically written with JavaScript in the website sent to a victim's browser. The code can log the keyboard input, steal credentials or the session identifier and many other forms of attacks [39].
- *Trojans or Trojan horses*: a program with overt and covert functions, the overt function is what expected from the program, the covert is the unwanted and unexpected function that represents the threat to the user or a system. Examples of covert function: key logging, stealing credentials, . . . , etc.
  Remarque: unlike viruses, a Trojan does not replicate [40, 41].
- *Backdoor*: it is often used by hackers to control computers to create bot networks and launch DoS attacks; it is a method to access a system by bypassing authentication and security controls [42].

– *Right alteration*: if an attacker gets to access the system as an administrator or a root, he could change the rights of legitimate users giving them the least rights.
– *Repudiation and right violation:* a user can deny being the originator of data and this action is known as repudiation, while right violation is when someone tries to steal credits of a digital work pretending to be the real owner.
– *Destruction*: can either be physical attack such as smashing the electronic devices, magnetizing it, using chemical products or putting it in fire or it can also be logical such as tampering or damaging the files and data [43].
– *Fraud and theft*: fraud is altering the data integrity for gain such as falsifying transactions. Theft includes software and hardware theft and it is the act of trading information, secrets or the stolen hardware for profit [44].

15.8 Security Solutions

This section describes some of the security solutions and measures mentioned in Table 15.1 and Fig. 15.1, such as: the authentication, steganography, cryptography, anti-malware, intrusion detection and prevention systems, firewalls, freshness protection, virtualization, backup, patches and user education.

15.8.1 Triple A (AAA)

It is the first security measure against systems, networks and databases intruders as it identifies the authorized user, grants them with specific access rights and records what occurs in the system.

– *Authentication*: it is the process of identifying a user or a person, and its mechanisms can use three qualities:

  - *Knowledge-based authentication*: "*Something the user knows*" such as text passwords, schemes or image password, secret question, ..., etc. It is the most basic and common way of securing systems, information or networks. Providing the user's ID and password is the first mandatory step to get a secured access. The major problem with using password is that we can forget them, for that we often look for ways to memorize them such as writing them in a diary, using tools to organize and save passwords (password managers or password keepers) or the use of "Cookies" which stores the user ID and password (hashed) to access websites. Another problem with this technique is that passwords can be guessed or cracked [30, 41, 50].
  - *Possession-based authentication*: *"Something the user has"* like tokens, dongles, badges, smart card, ..., etc. It is commonly used in workplaces as workers often carry badges and smart cards also in hotels with electronic door locks (smart keys). It can exploit many technologies such as RFID (Radio frequency), Bluetooth or via USB. Yet, this method also has drawbacks, such as losing the hard key or forgetting it [50].
  - *Physiology-based authentication*: "*Something the user is*" also known as biometrics and is based on the physical characteristics of a person, such as: face, eyes (retina and iris), voice, veins, fingerprint and hand geometry [30] and also the behavioural characteristics such as the keystroke rate, signature, gait and handwriting. The biometric authentication relies on taking sample of the authorized persons and storing them in a database to compare them later during the verification process (to identify and authorize the persons to access) [14].

Table 15.1 Networks security threats

Network		Security threats (non-exhaustive list)	Solutions
Ad hoc networks	Mobile	Viruses and worms -Denial of Service (SYN flooding, jamming or hello flood) -Monitoring, traffic analysis and eavesdropping -Active interference -Route disruption -Node isolation -Wormhole -Resource consumption -Fabrication, modification and dropping attacks -Timing attacks [19]	-Secure routing: authentication and cryptography -Intrusion detection techniques [19]
	Vehicular	-Malware -Spamming -Denial of service -Black hole attack -Broadcast tampering -Replay attack -Position faking -Global positioning system spoofing -Masquerading -Sybil attack -Certificate/key replication -Message tampering/manipulation -Tunnelling [45]	-Redundancy provides resilience to black holes -Authentication -Cryptography -Encrypted precise positioning system to avoid GPS spoofing -Rogue repudiation basing on reputation model [22]
	Sensor	-Spoofing -Modification -Replay attack -Eavesdropping -Replication attack -Camouflage -Jamming -Tampering -Collision -Resource exhaustion -Unfairness in location -Selective forwarding -Sinkhole -Sybil -Wormhole -Flooding (hello, SYN, ACK) -De-synchronization -Stealthy attack [26]	-Authentication -Cryptography algorithms and software -Crypto-processors (against physical tampering) -Jammed area isolation -Spread spectrum techniques to prevent jamming -Randomness multiple paths in routing, using probabilistic routing and the introduction of fake messages in the network as a solution against traffic analysis -Radio source testing, random key distribution, central registration of node and position verification as a solution again Sybil attack [26, 46]

(continued)

Table 15.1 (continued)

Network		Security threats (non-exhaustive list)	Solutions
	Body	-Denial of service -Eavesdropping -Replay attack -False data injection -Unauthorized access -Selective reporting -Data alteration -Impersonation [47, 48]	-Encryption -Authentication and authorization -Intrusion detection and prevention -Freshness protection [47, 48]
Infrastructure based	Internet	-DNS cache poisoning -Spamming -DNS spoofing -Denial of Service, Distributed Denial of Service -Session hijacking -Malwares (worms, viruses, spyware, adware, scripts and Trojans) -Hacking and social engineering -Password cracking -Exploiting technical vulnerabilities of the protocols and systems (SQL injection, buffer overflow, ..., etc.) -IP spoofing -ARP spoofing -Phishing and web spoofing -Flooding -Teardrop attack [14]	-Anti-malware (antivirus, anti-spyware, etc.) -Firewall (hardware and software) -Intrusion detection and prevention -Encryption -Authentication and authorisation -Securing internet explorers and disabling scripts -Educating the users -Backups -Applying patches -Detecting vulnerabilities in protocols and systems and disabling unnecessary services -Check configurations [14]
	Internet of things	-Denial of service -Physical attacks -Privacy attacks: eavesdrop-ping, traffic analysis and data mining [49]	-Authentication and authorization -Identity management -Trust management -Key exchange and management -End to end security: applying cryptography and hashing (IPsec, TLS) [49]
	Cloud computing	-Eavesdropping -Sabotage (denial of service) -Theft -Fraud -External attacks (scanning vulnerabilities, and malware) -Fragmentation attacks -Intrusion and session hijacking -Backdoor -Spoofing -Man in the middle -Replay attack -Dumpster diving -Social engineering and password guessing [44]	-Intrusion detection -Firewalls and layered defence mechanisms -Virtualization -Authentication and authorization -Backup -Encryption -Network security protocols (for example: VPN) [44]

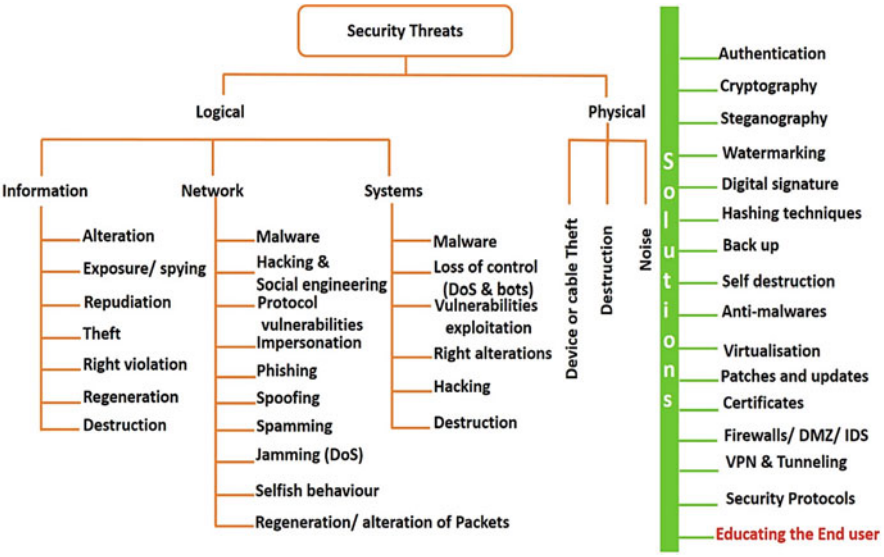

Fig. 15.1 Classification of security threats

An efficient biometric solution has the following five characteristics:

- *Robustness* which means that it remains unchanged overtime,
- *Distinctiveness* which means that it is unique for each individual,
- *Availability* which means that all individuals have it,
- *Accessibility* which means that it is easy to scan and capture its features using sensors,
- And *acceptability* which means that people do not object taking the measurement [51].

Biometrics offer a secured authentication since it is not easy to fake, steal or fabricate biometrics characteristics and it holds a very bright future. However, it is not as reliable as it was predicted to be as it became possible to fake fingerprint per example, although other physiological characteristics are still considered secure such as retina, iris, . . . , etc. That is why more researches are being conducted in this field [14]. Further details of the biometric solutions are explained in the case study surveying them (see Sect. 15.10).

– *Authorization*: it enables determining the user who, once identified, is permitted to have the resources. It is implemented through the use of access control mechanisms by granting or denying the access to a resource according to a set of criteria. It differentiates the users by granting different set of rights and privileges [49].
– *Accounting or Auditing*: Monitoring and tracking the activity related to the use of a resource gives the security administrator the ability to know what actually

occurs in the system and the network. This allows him/her to have a clear view of what is supposed to happen, thus giving him/her a higher chance of detecting the vulnerabilities and correcting them [14].

15.8.2 Cryptography

Cryptography is the science of securing messages by scrambling the content so it will not be understood by a third party. One of the earliest uses of cryptography is credited to Julius Caesar. The cryptography continued to develop over the year. It has two types: the symmetric cryptography and the asymmetric cryptography. Chronologically, the secret key cryptography came first, but since the secured distribution and management of these keys were the drawbacks of this method, the asymmetric cryptography came to resolve this problem by relying on the use of a pair of keys one is public used for encryption and the other is private used for decryption [52, 53].

The cryptography is the key technique for many security solutions such as: IPsec, VPN, SSL and TLS.

15.8.3 Steganography

The concept was first given by Johannes Trithemius (1462–1516) in his book "steganographia" and is created from the combination of two word "stegano" which means hidden and "graphia" which means writing. It is the art and science of securing message exchange by hiding it with innocent object.

Digital steganography includes hiding data of digital format into another innocent cover such as images, videos, audio files, documents (word, PDF, web pages, etc.), compressed files (rar, zip, etc.), virtual machine disk file, network protocols (headers) or operating system files, ..., etc.

For each type of cover file used, the concept aims to embed the message in such a way to make the alteration undetectable visually. The alteration might cause the stego file (the resulting file with the embedded data) to be larger in size, with lower quality or include noise that can be perceptible by human eye or ear (images, videos and audio files) [54–56].

The steganography techniques can be dangerous if misused; many hackers and cybersecurity attackers are using it to launch attacks or seal deals secretly, per example your computer can be hacked as soon as you open an image in your browser [57] and data exfiltration can be successfully undetected using steganography [58].

In the following, a brief overview of some of the existing steganography techniques is given:

– *Steganography in images*: images represent a perfect steganography cover file as it is easily exchanged, can hold a fairly high size of secret data and is innocent and does not draw suspicions. Many methods are developed to embed the data such

as hiding data in the least significant bit of the pixel which is one of the most used methods that hides the message by changing the least significant bit from a byte, thus making the changes undetectable especially in images since the changed byte (pixel) will give an approximately the same colour (shades of the same colour), in the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), in the colour pallet or at the end of the file. Note that the JPEG images are the mostly used cover files as they have a small size (compressed) and are widely used thus non-suspicious [54].

- *Steganography in audio*: steganography can be applied to audio files by hiding the secret data within the audio signal in an imperceptible way, i.e. the resulting signal has the same characteristics and the changes made to the audio file will likely not be detected by the human ear [59].
- *Steganography in videos*: videos have a larger size than images and can store more secret data, and they are innocent and easily exchanged. Steganography techniques in videos can exploit the fact that a video is composed of a set of images where the DCT, DFT, LSB and DWT techniques can be used, other techniques embed the data in the motion vector and some techniques rely on embedding data by exploiting the encoding/decoding process or by embedding data in the audio and images of the video. Steganography techniques can be extended to work on streaming videos [54].
- *Steganography in protocols*: the steganography techniques can use protocols headers to embed data, per example the sequence number field in TCP protocol, the TTL (Time To Live) in IP protocol or the VoIP protocol which generates a great number of small packets that can be used to embed small amounts of secret data [54].
- *Text and linguistic steganography*: some steganography methods rely on the semantic of the words or its spelling to hide data, per example some methods hide data within English text by altering the spelling of the words between the US and UK [60], or by changing the dots, punctuation or the stressing of the words in Arabic language [61]. Steganography can also be applied to the spoken language and the way the words are pronounced and stressed or by replacing words with synonyms and metonymy [62].

15.8.4 Anti-Malware

Anti-malware relates to a set of tools to detect and remove malwares (viruses, worms, adware, spyware, rootkit, ..., etc.). Searching for malware can be done by two techniques:

- *Heuristic methods* which enable the detection of new threats based on the behaviour of malware and the effects left on the system.
- *Signature methods*, by searching for malware signature from the anti-malware database which is updated regularly every time a malware is detected and analysed. This method is fast but it detects known threats only.

Anti-malware detects a set of malware of different types; there are specific tools for each type of malwares such as: antivirus which detects viruses, worms and Trojans, ..., etc.; anti-spyware which removes spying software left by hackers and adware removers which remove the adware from the system. It is important to note that sometimes a malware can be an adware, spyware or a Trojan and a rootkit blended together to be more discrete and destructive [63].

Recent anti-malwares use combined methods (signature and heuristic) to provide security and efficiency in terms of scanning time. An example of such an anti-malware is presented in the patent *US 7725941 B1* [64], where an executable file is scanned for malware presence following these steps:

- Detecting, an attempt to execute a file on the computer;
- For a known file, a signature malware check is performed;
- For an unknown file (encountered for the first time), a risk analysis based on a plurality of risk factors is performed;
- Based on the risk analysis, identifying which malware detection algorithm is to be used for the file, in addition to signature detection;
- If no malware is detected using the malware detection algorithms, the execution of the file is permitted [64].

The risk analysis is based on: file source, file origin, file path, file size, whether the file is digitally signed, whether the file is a download utility, whether the file is packed, and whether the file was received from a CD, as a file downloaded from the internet is more suspicious than the one copied from a CD, also the files downloaded from the internet can be rejected by the anti-malware if its origin URL is blacklisted (even before scanning it); files that are not digitally signed, have small size, launch other processes, create copies, download other files or are saved in root directory are more suspicious than other files and potentially are (infected by) a malware [64].

The malware detection algorithms include: heuristic detection algorithms, statistical analysis (frequency and pattern of instructions), instruction-based emulation and environment-based emulation [64].

15.8.5 Intrusion Detection and Intrusion Prevention Systems

Intrusion Detection System (IDS) monitors the events occurring within a system or a network and analyses them to detect security problems. The system is passive which means that it saves the security problems details in log files and alerts the security administrator but it does not try to stop or prevent the attack. Intrusion prevention system (IPS) detects the intrusion and attempts to stop it. The key functions that an IDS/IPS (IDPS) system performs are: logging and reporting security events, alerting the security administrator and preventing the attacks [65].

There are different types of IDPS based on its used method and its spatial distribution:

- *Signature based*: this type of IDPS detects the known threats by comparing their unique pattern known as a signature to the database of known threats. It is the simplest detection method and it is ineffective at detecting unknown threats [66, 67].

- *Anomaly based* (behaviour based): the IDPS compares the normal behaviour to the observed events to detect threats. The IDPS creates normal profiles based on the typical observed activity of users, hosts, network connections, or applications, and compares it using statistical methods with the observed activities such as sudden high consumption of bandwidth or processors to detect and eliminate the threat. It is effective at detecting unknown threats [67, 68].
- *Stateful protocol analysis*: the IDPS tracks the state of network, transport and application protocols that have a notion of state, i.e. it can link requests to responses and identify unexpected sequence of commands. However this type of IDPS cannot detect threats that do not violate the proprieties of known protocols such as creating many TCP sessions to cause denial of service [67].
- *Host based*: the IDPS monitors the host which can be a machine or a server, by tracking network traffic, running processes, file/directory access and modification (edit/delete) and system logs to detect suspicious activity that can potentially be a local threat [67, 68].
- *Network based*: the IDPS monitors network traffic and analyses the network and application protocol activity to identify and eliminate suspicious activity [67, 68].
- *Hybrid IDPS* (host/network based): the IDPS has two parts, an interface that monitors the network and an interface that monitors the local host [67, 69].

Some recent researches focus at building an IDPS inspired by the human immune system known as Artificial Immune System (AIS), a new branch of artificial intelligence, basically working like our immune system which is able to distinguish self- and non-self-cells and protect the body against non-self-cells. In computer science, a non-self-cell is the intrusion. Further details can be found in Farhaoui [70].

15.8.6 Firewalls

It is very common to find a local network which enables the exchange of file and sharing resources such as the printer. The enterprise can extend its network by using the internet to provide services and information to its users. That can cause an open port that can be exploited to launch attacks and other related security problems. Firewall aims to secure the local network and isolate it from the threats, and it detects the intrusion to the system, controls the access to the resources and analyses the coming traffic. There are different categories of firewalls:

- *Stateless firewall*: the oldest and the basic method where each packet is controlled independently basing on the administrator's predefined rules. It filters the packet basing on their IP addresses and Port number

- *Stateful firewall*: a memory-based firewall; the packets are not only controlled basing on the administrator rules (IP, Port number) but also on the session state; this allows to detect and prevent some DoS attacks such as SYN flooding
- *Applicative firewall (proxy)*: this firewall must know all the protocols and rules of the application, each application, has a special process in the proxy that is responsible for the filtering
- *Authentication firewall*: the filtering is not based on the Machine addresses (IP) only but on the users as well
- *Personal firewall*: anti-malware and anti-spyware tools that are installed on the host machines [71]

15.8.7 Freshness Protection

A security measure that can be used to prevent the attacker from replaying the eavesdropped packets or data (it allows the detection of replayed data). It is a technique used in networks. It can be applied by the use of timestamp (Kerberos), nonce (Needham–Schroeder protocol) or the use of sequence numbers [72–74].

15.8.8 Virtualization

Virtualization allows having multiple operating systems on the same server or host system. It can be used for security purposes such as testing un-trusted software because virtual systems occupy specific partitions. Therefore, if the system is compromised, the infected partition(s) can be isolated and the access to resources such as the disk or networks can be severed and the system can be halted. It is recommended to back up the virtual system to restore it in case of severe security problems. Also, because the virtual system is independent from the physical architecture, virtualization is considered as one of the security solutions [75].

15.8.9 Backup, Patches and Users Education

In many cases, the security problem is due to wrong configuration, such as leaving open port or wrong firewall configuration, which is the mistake of the security administrator. Training the security administrator to do backups, monitor the network traffic and applying patches to detected vulnerabilities is mandatory to maintain the security of a system or a network. Sometimes the security system is correctly configured and relies on the combination of recent technologies such as biometry, the use of tokens, smart cards, firewalls, IDPS, and anti-malware known as the layered security system, making it hard to be attacked externally. Yet, because

of the user it can be broken because they fall for social engineering attacks which rely on the authentic (insider) users to gain an authorized access. Thus, users must be aware of this attack and taught not to fall for it.

15.9 Attackers and Security Breakers

After explaining security threats and solutions, it is important to introduce and classify threat makers also known as the security attackers, breakers or hackers, which will be the content of this section.

There are many ways to classify an attacker or a security breaker. M, Raya et al. [76] classified attackers of VANETs in three dimensions which can be applied to any network attacker.

The first criterion is whether or not the attacker belongs to the networks:

- The *insider attacker* who belongs to the network
- The *outsider attacker* who does not and may be considered as an intruder

The second criterion is concerned with the intention/purpose of the attack which results in two classes as well:

- The *malicious attacker* who aims for a full destruction
- The *rational attacker* who unlike the malicious attacker has a personal reason for the attack to gain profits and thus has a specific target

The last criterion relates to the type of attack, and this also gives two classes:

- The *passive attacker* who eavesdrops the networks but does not alter or generate packets
- The *active attacker* may alter, drop or generate packets

We can consider other criteria such as the types of security threat, and the technical level of an intruder.

Considering the criterion of the technical level, we would have two categories of attackers:

- *Script kiddies* also known as *click kiddies* or the amateur hackers, who create threats by using pre-made hacking tools or copying scripts made by other skilled hackers and often available on the internet [14].
- *Expert* or professional hackers: they have high-level programming skills, write their own hacking tools, make malwares, exploit system vulnerabilities and are more dangerous.

If we consider the type of security threats, four main categories of attackers can be distinguished:

- *Hackers*: the word hacker originally was used to describe a person who is expert at writing and modifying computer programs, learning the details of a computer

and stretching its capabilities. Now it is used to describe the malicious intruder. A hacker can be motivated by profit, psychological reasons such as: greed, revenge, self-satisfaction or mental illness; or governmental such as political activists (hacktivists) or spies [34].

There are three types of hackers:

- *The white hat hackers*: also known as the ethical hackers, who have the permission to access a system, and their skill level is the same as that of the black hackers but white hackers are hired by organization to evaluate their security system [77]. The ethical hackers are considered to be experts and have an advanced level of skills in network and computing technologies. Ethical hackers have their community and they organize and attend conferences and workshops to exchange knowledge. They are trained and certified hackers (for example: the EC-Council CEH certificate) [78].
- *The grey hat hackers*: they are hybrid between the black and white; sometimes they act legally and sometimes not [77].
- *The black hat hackers*: they are malicious hackers who intrude the systems illegally to cause harm [79]. Black hackers have a high level of skills, and they can detect systems and network flows and vulnerabilities and exploit them to take over the control or cause harm. They can develop their own hacking tools and methods, create malwares, use cryptography or steganography techniques or even rely on social engineering techniques. In most of the times, they succeed at launching their attacks in anonymous and untraceable ways, thus they may be considered as a real threat to corporations and states and they present a challenge to cybersecurity protectors and investigators.

– *Malware makers* are the virus, Trojan, adware, spyware, rootkit and other malware writers who are considered skilled programmers with good theory background. They develop harmful codes that can be used to exploit vulnerabilities, collect and steal data, create a backdoor and control the system or cause complete destruction. Most importantly, they develop it to avoid detection and in most of the cases it has more than one function and it uses advanced techniques such as steganography (Trojans), cryptography or rootkit to keep being hidden and undetected.
– *Phreaks* are hackers who are specialized in breaking phone networks. They are one of the earliest types or attackers, and they hack phone networks to make free calls.
– *Crackers* originally used to describe the security systems breaker (cracker), now used for describing password crackers [14].
– The above-mentioned types of attackers are not the only existing as some are specified at hacking bank cards (carders), smartphone system and applications, games and software, networks, ..., etc.

Figure 15.2 gives the classification of security attackers basing on the previously explained criteria.

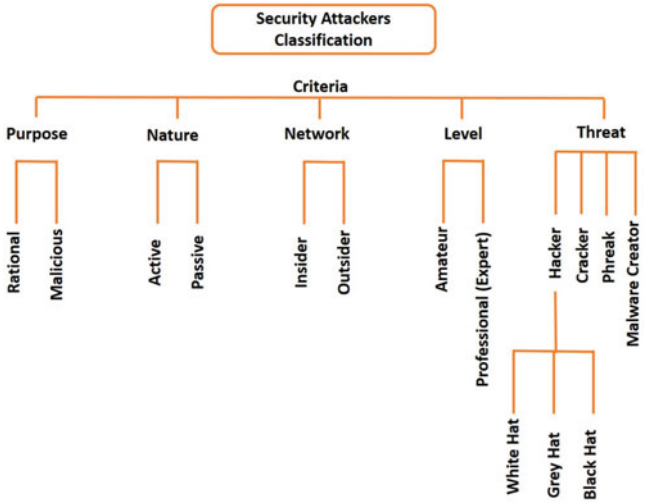

Fig. 15.2 Classification of security attackers

15.10 Forensic Investigation of Cybercrime

Cybercrime is defined as "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network". In its general meaning, it can be any crime that considers the cyberspace (computers and internet) as a tool, or as a target.

Some cybercrime examples include:

- Damage to computer data or programs
- Computer sabotage
- Computer espionage
- Public switched telephone network (PSTN) intrusions
- Major computer network intrusions
- Network integrity violations
- Privacy violations
- Industrial/corporate espionage
- Software piracy

Cybercrime can be categorized into three categories:

- *Violent cybercrimes* (cyberterrorism, assault by threat, cyber talking, child pornography, . . . , etc.)

– *Non-violent cybercrimes* (cyber trespass, cybertheft, cyber fraud, ..., etc.)
– *Destructive cybercrimes* (hacking into a network or a system; introducing viruses, worms and malwares; mounting DoS attacks, ..., etc.)

We will discuss in this chapter the cybercrimes that aim to take down systems and networks (non-violent and destructive cybercrimes), and the investigation process done by forensic investigators.

The investigation process can be divided into three main steps:

– The first step in the investigation is to detect the cybercrime (while it is still happening or after it ends with success or failure).
– The next step is to secure the evidences.
– The last step is to analyse the evidences and extract the crime proofs.

All the three phases involve using specific tools and require skilled IT experts and investigators who are trained to preserve the evidences.

15.10.1 Detecting the Cybercrime

Cybercrimes can be detected by intrusion detection tools, firewalls or anti-malwares. It can also be detected by the network or the security administrator by checking the network state regularly, verifying the system state, studying security logs or by noticing systems slow down or non-response. In case of spams, email headers can indicate the spammers IP. Although, malicious attackers rarely leave traces and in most of the times they use bots (victims) to launch attacks such as spams and DDoS, ..., etc. Their IP address will be hidden and tracking them for their crimes would be difficult; some solutions used by forensic investigators involve using "Honey Pots" and "Honey Net" (also known as cyber stings) to lure the attackers and capture them. The honey pots and honey net are computers and networks deliberately exposed to the public. Usually, they contain data that is not harmful to be exposed, and security systems and firewalls that contain vulnerabilities that can be exploited by the attackers.

15.10.2 Securing Evidences

This phase include defining the crime scene, and it is also required to do the disk imaging either by using tools such as Encase or using a standalone disk imager so as to make a bit stream copy and create an exact image of the disk (logically and physically identical) which is important to keep the original evidence intact. Volatile data in the memory must be saved using proper commands and tools before

shutting down the system where it is preferable to unplug the wires instead of using the command "shut down" to avoid self-destruction scenario. If the computer screen displays messages or executes certain programs, it is important to note that either by recording it with a camera or by memorizing the commands in a text format. It is mandatory for the IT expert to know how to save the evidence regardless of the operating system running on the machine or the type of electronic device in use (tablet, computer, smartphone, cloud, . . . , etc.). Every evidence must be tagged and logged and the transfer operation must be safe to keep the evidences as found.

15.10.3 Analysing the Evidence

The IT experts in forensic labs use the images of disk to extract files and analyse them. They can extract log files, trace the security reports, check history of visited websites, temporary files, email, social media network activity and their chat log, or even the history of downloaded software to look for malicious software that can be used to cause harm. They also analyse every file that can lead them to a clue related to the crime committed.

An attacker can use cryptography and steganography to hide or encrypt the files, and thus the help of cryptanalysts and steganalysis expert could be required in the investigation.

The next part is to provide the analysed evidence as an acceptable, non-repudiated proof in the courtroom against the criminals.

It is worth noting that if the attacker physically destroys the evidence (computer used for the attack) either by smashing it, magnetizing it, putting it in fire or exposing it to chemicals, there would be no way of proving anything against him unless a witness speaks against him, other kind of evidence is found or he admits his crimes on his own [14].

15.11 Case Study: Biometric Authentication Solutions

There are many unique features that can be used to identify a person and are used as biometric security solution; in what follows we will mention some of these solutions:

15.11.1 Eyes

- *IRIS recognition*: iris (Fig. 15.3) represents a great biometrics solution for authentication; because it is small (11 mm), the identification also known as the search for a match from the database is fast, it is distinguishable, stable over time,

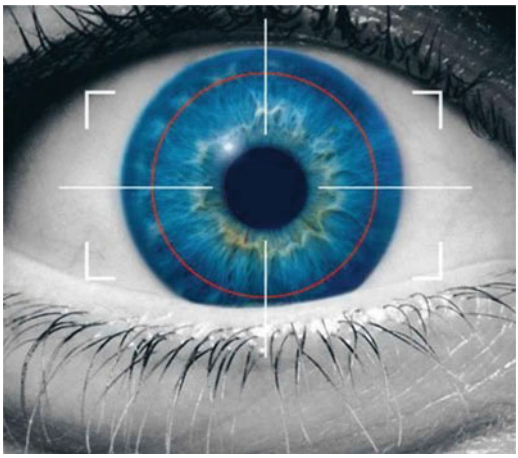

Fig. 15.3 Eye iris [80]

insensitive to angle of illumination and its distinctive annular shape facilitates reliable and precise isolation of this feature. The main steps for iris recognition system are:

1- Using a camera, the eye is captured
2- The image is then processed so as to isolate the iris by detecting its boundaries (pupil, limbus and eyelids)
3- Demodulation of iris code
4- XOR comparison of two iris codes

For more detailed explanation, we refer the reader to read this paper [81].

- *Retina authentication*: the authentication is based on the blood vessels in the retina of the eye which have unique patterns that can be used to identify a person. Since the blood vessels are at the back of the eye, the retina scan requires the use of a low intensity light before photographing and analysing it [82].

15.11.2 Ears

Ear authentication has more advantages than the face recognition as it degrades little with time and thus is considered more stable than the face. The authentication process in general is done in five stages:

1- *Ear detection*: it involves localizing the position of the ear in an image.
2- *Ear normalization and enhancement*: the detected segment (ear) is enhanced in terms of fidelity and may be subject to geometric or photometric correction.
3- *Feature extraction*: the segmented ear is reduced to a mathematical model (e.g. a feature vector) that summarizes the discriminatory information.

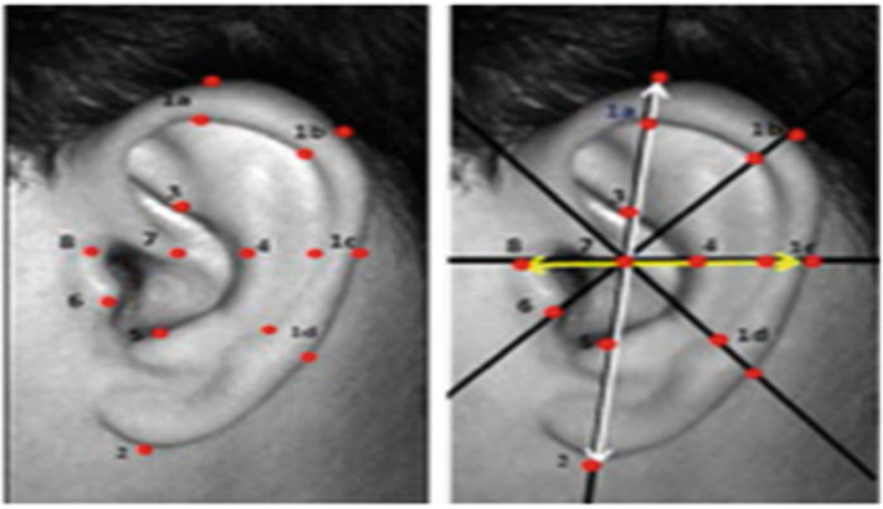

Fig. 15.4 Ear biometric, geometry-based authentication [83]

4- *Matching*: the features extracted must be compared to the features saved in the database.
5- *The decision*: after the matching, the decision is established as a (yes) or a (no).

This method of authentication relies on the geography of the ear, and the imaging can either be 2D (Fig. 15.4) or 3D [83].

Another type of ear authentication, which is based on the use of acoustic waves to distinguish the unique cavity shape of the ear, has been developed by NEC Corporation, Japan. The technology uses earphones with built-in microphone to send and receive wave sounds and extract features from the received signals which are unique to each individual basing on the unique structure of the ear (see Fig. 15.5). The earphone is used to eliminate the noise and to ensure a natural authentication even when moving or working [84].

15.11.3 Face Recognition

Face authentication is still very challenging problem. This is due to the variability of human faces under different operational scenario conditions such as illumination, rotations, expressions, camera viewpoint, aging, makeup and eyeglasses.

Face recognition method is classified into two methods:

- Feature-based methods
- Appearance-based methods

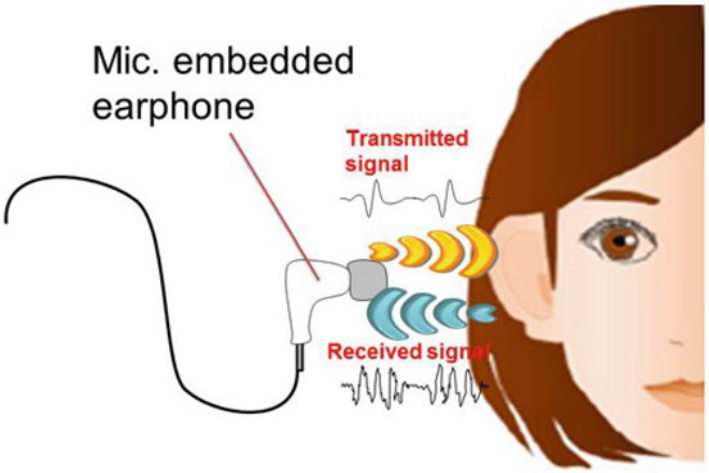

Fig. 15.5 Ear biometric, acoustic waves-based authentication [84]

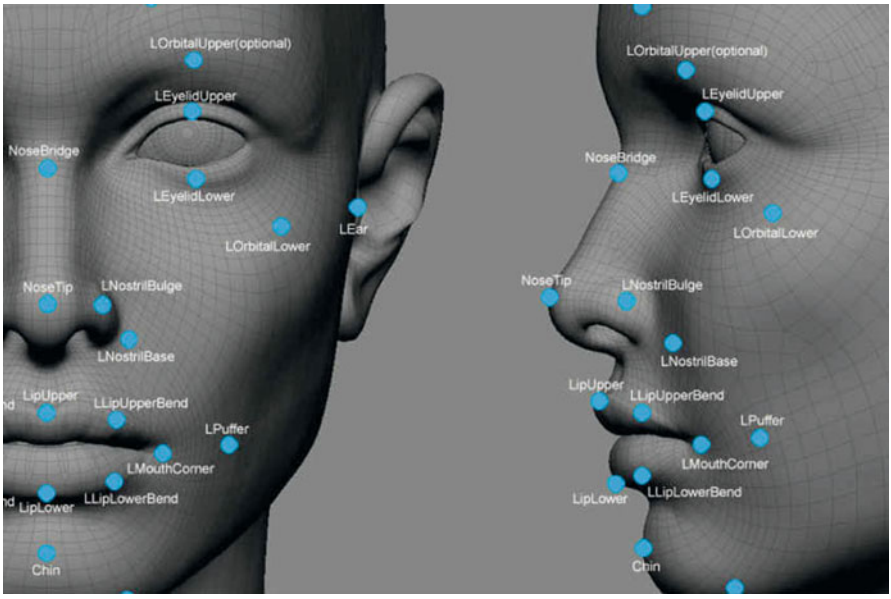

Fig. 15.6 Face biometric authentication [85]

Face recognition techniques can be either 2D (Fig. 15.6) or 3D and it uses properties and geometric relations such as the areas, distances and angles between the facial feature points such as the eyes, nose and mouth [86].

Fig. 15.7 Facial thermograms authentication [87]

15.11.4 Facial Thermograms

Visual face authentication faces the problem of lightening, changing pose and orientation. Those are the reasons why new techniques are developed for face recognition known as facial thermograms (Fig. 15.7) which are formed by the heat radiated by the face and are less affected by facial growth, pose and expressions. The images are captured using infrared camera and used to extract the authentication features [88].

15.11.5 Lip Biometrics

The lip print varies from a person to another, thus it can be used to identify a person, with its unique features formed by the lines, wrinkles, fissures, grooves, colour and shape (see Fig. 15.8) [90, 91].

15.11.6 Fingerprint

Each individual has a unique fingerprint, thus the use of fingerprint for authentication is widely adapted now. The fingerprint has three patterns loop, delta, and whorl, others features such as the valleys, the ridges, and the minutia which

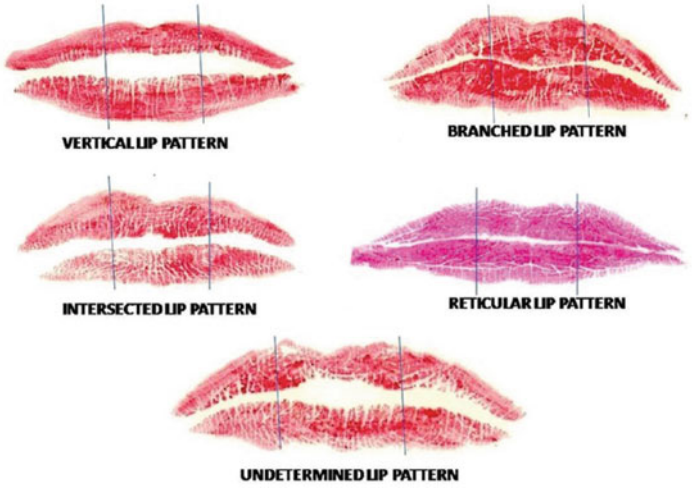

Fig. 15.8 Lip patterns [89]

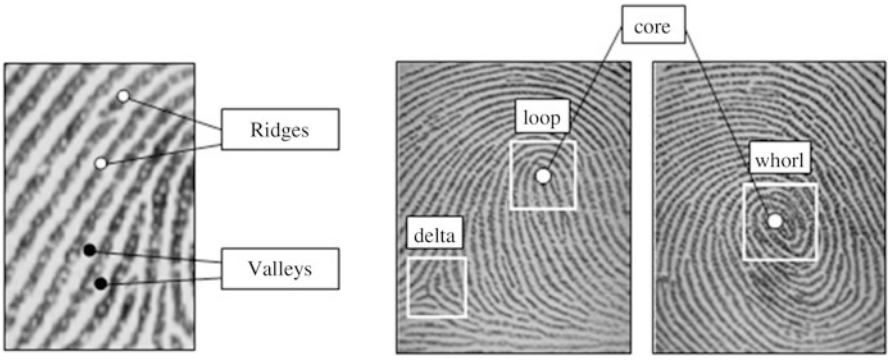

Fig. 15.9 Fingerprint [92]

refer to the various ways in which the ridges can be discontinuous (termination and bifurcation). The minutia is a key feature in identifying (authenticating) the individuals (Fig. 15.9) [92].

15.11.7 Fingernail

Some applications require secured short-term authentication and the use of biometric solutions is recommended. However, biometric characteristics such as retina, iris or fingerprint are considered as permanent characteristics of an individual, also because people would likely object having their biometric parameters saved for

non-crucial applications that they use temporarily; the transient biometric solution was created which involves the use of biometric characteristics that would change naturally after a period of time such as the fingernails that would change in 3–6 months. The unique nail bed, shape, colour, boundaries, scratches, white dots and texture of the fingernails are used to create a unique signature that can be used for the authentication [93].

15.11.8 Skull

Skull authentication can be done either by imaging (2D, 3D) where a set of points are selected and compared to identify a person or by using sound waves as in the most recent research SkullConduct (Fig. 15.10) which sends sound waves (vibration) with a specific frequency to the skull and records the echoed waves to identify a person [95, 96].

15.11.9 Brain Wave Authentication

Studies have shown that individuals exhibit unique brain patterns for similar tasks, and these unique patterns can be used as signatures for biometric authentication; the patterns are electrical activities generated by brain structures and measured by electroencephalogram (EEG). The authentication is done when the person does a certain mental task (the same he did when he got his identity from the system) and

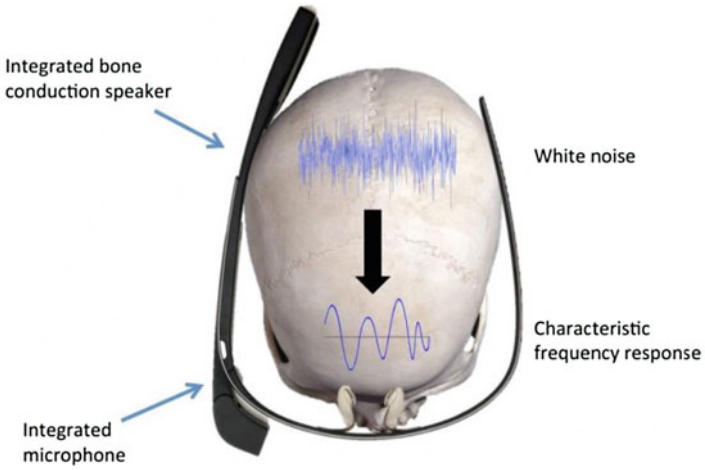

Fig. 15.10 SkullConduct, a skull authentication solution [94]

this task can be reading, multiplication, relaxing, ..., etc., and the EEG measures the electrical activity of the brain and compares it with the saved signature to accept or reject the individual.

This type of authentication is new and presents many advantages:

- Confidentiality (mental tasks)
- Difficult to mimic (each individual has a unique pattern)
- Impossible to steal (individuals emit different brain patterns when under stress, threat or mood change) [97]

15.11.10 Body Odour

Body odours can be classified into three layers or types: the first contains constituents that are stable over time regardless of diet or environmental factors, the second contains constituents that are present due to diet and environmental factors and the third contains constituents that are present because of the influence of outside sources such as perfumes. The first type of odour is unique to each individual and it is used in the authentication which uses e-noise to identify odour and individuals [98].

15.11.11 Palm Print

Palm print authentication is hand-based biometric technology. The palm is covered by the same skin as the finger tips and is used to uniquely identify a person. The palm has a set of unique features (see Fig. 15.11) that can be used to authenticate a person, such as:

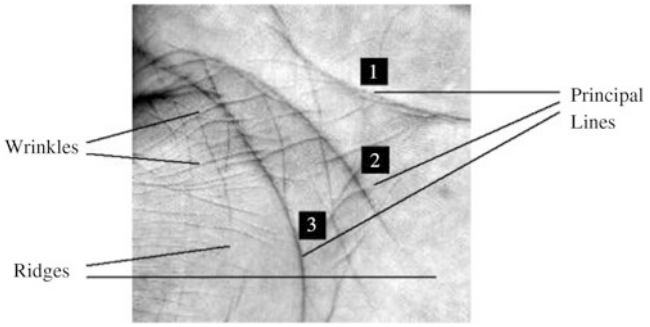

Fig. 15.11 Palm print-based biometric authentication [99]

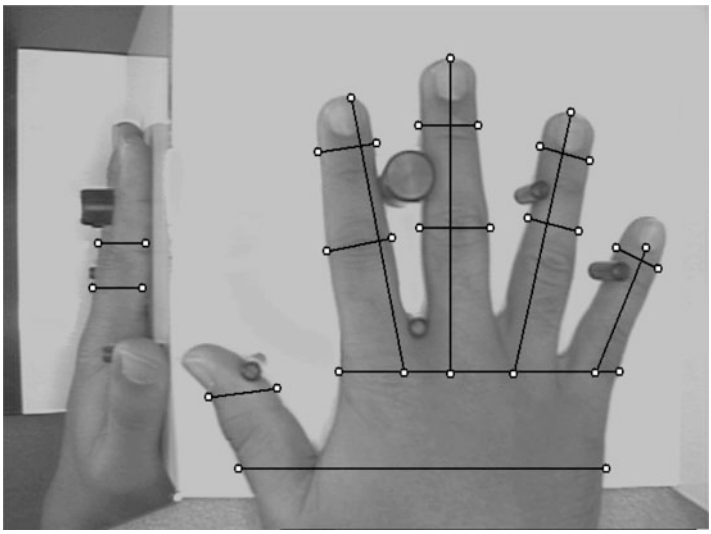

Fig. 15.12 Hand geometry-based solution [101]

- Palm shape (geometry feature)
- Form and location of principle lines (line feature)
- Wrinkles which are the thinner irregular lines (wrinkle feature)
- Delta point features at the root of fingers
- Minutiae features [100]

15.11.12 Hand Geometry

This technique measures the palm surface, length, width and shape, the fingers size and shape, and calculates the distances between a set of points in order to extract the unique features of the hand (see Fig. 15.12). This method is insensitive to changes in surface features such as tattoos, hair, cuts, scrapes, burns or dirt. However, it does not perform well if there are large bandages or casts on fingers, when the hand is deformed significantly or when a finger is missing [102].

It is also possible to use the foot geometry and print or the toes prints to authenticate a user.

15.11.13 Veins

Veins or the vascular pattern (see Fig. 15.13) can be used to authenticate a person as it is unique for each individual; this type of authentication can rely either on the veins in the face of the hand or on the fingers [104, 105].

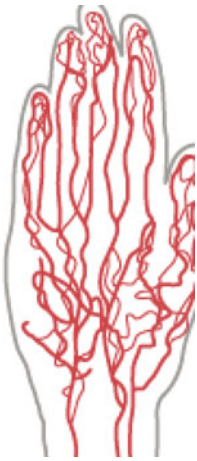

Fig. 15.13 Vein-based biometric authentication [103]

15.11.14 Keystroke and Mouse Moves

Although some researchers are against the use of keystroke as an authentication method by arguing that it is not unique all the time, other researchers are still interested in developing a keystroke based authentication systems, and they rely on some characteristics such as: the speed of typing, time between two key strokes, frequency of typing errors, the time a key is pressed, ..., etc.

Mouse dynamics is also a behaviour-based authentication method where the researchers record the mouse moves and clicks (right, middle and left buttons; drag and drop; stillness; single or double clicks) to create the user template which will be used later for the authentication [106].

15.11.15 Gait

Human way of walking is unique to each individual and it is used to authenticate living person to the system. The authentication can be done through three ways:

- *Machine vision*: relies on the use of cameras to record the person's walk and identify him. There are two approaches for machine vision, the model based (see Fig. 15.14) and the silhouette based.
- *Wearable sensors*: a set of non-intrusive wearable sensors can be attached to the person to identify his gait such as smartphones, smartwatches or shoes with sensors.
- *Floor sensor approach*: the gait of a person is saved and identified as he walks on a sensor-monitored floor as signals are generated from the stepped-on sensors [108].

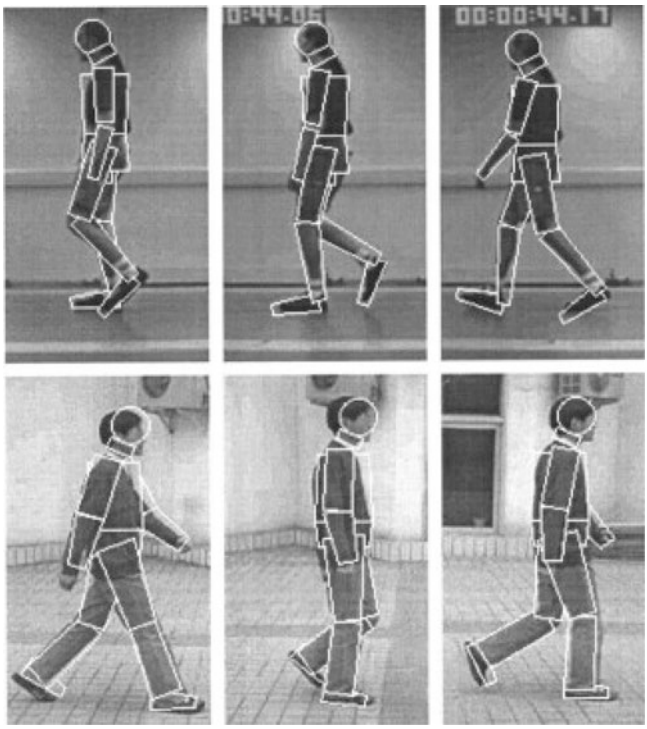

Fig. 15.14 Model-based gait authentication [107]

15.11.16 Speaker Recognition

Human voice is a unique identifier of a person and it differs from a person to another because of the different anatomy (throat shape) and the learned behaviour patterns. The user would provide a vocal passphrase to identify himself to the system. However, since the user's voice can change due to illnesses such as cold, and some individuals are expert in imitating voices, this system might not perform well in these cases, and it would be advisable to use it in a layered biometric security system instead of using it alone [91].

15.11.17 Heart beat

The heartbeat pattern (Fig. 15.15) is unique for each individual, and it represents a robust biometric security solution. One of the authentication approaches uses the electrocardiogram (ECG) which describes the electrical activity of the heart over

Fig. 15.15 Heartbeat authentication [109]

Fig. 15.16 Signature-based authentication [111]

time to identify the person. The ECG can be captured by external sensors attached to the wrist or from the fingers to provide easiness and acceptance so as this solution gets used in smartphones and other devices [110].

15.11.18 Signature and Handwriting

Handwriting and signatures (Fig. 15.16) are one of the oldest and most common behavioural biometric solutions where the idea of signing and authorizing papers is adopted as a method of authentication. This solution is done either online where the sensor compares not only the written passphrase but also the speed, acceleration and the pressure applied to the pen or offline where the passphrase image is compared to the one stored. The major problem of this approach is the forgers who can imitate the handwritings [112].

15.12 Conclusion

In the age we are living, being ignorant and illiterate does not refer to being unable to read or write but refers to the lack of ability to use computer and other digital devices. Kids since a very young age now use computers, tablets, smartphones, smartwatches, smart TVs, ..., etc. All those devices are connected to the internet almost all the time. Users are asked to provide credentials (ID, password, credit card number, ..., etc.) or they provide voluntarily other information related to their daily life routines, pictures, voice recording, videos, ..., etc., through social networks, and the data can be collected through spywares or the intrusions to the system unknowingly and without the permission of the user which creates privacy issues and other security threats which were explained in this chapter.

The security threats were not studied only for the internet, but also to the internet of things where any electronic device can be connected to the internet, in the cloud computing, and even too ad hoc networks such as sensors, vehicles, mobile and body networks.

To resolve the security problems, many solutions were proposed and developed such as the use of layered security solutions which include the use of firewalls, IDPS, anti-malware, authentication and access control where we focused more on surveying biometric solutions. Other security solutions were created to secure communication such as steganography. Each solution is a research field where improvements and evolution are always in progress and what boost this improvement is the fact the threat creator always tries to break the security; this challenge between the security protectors and breakers is what makes both sides work harder to outperform the other party.

The chapter included the presentation and the classification of the security breakers, their different targets, motivations, level and techniques as well as how cyber forensic investigator tries to catch them and what are the relevant steps in the investigation process.

In nutshell, the security issues and solutions will continue their evolution and development as new technologies, systems and protocols are invented and improved.

References

1. Cyber attack (2016) [Online], http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/
2. Tor, [Online], https://www.torproject.org/. Accessed 26 July 2016
3. A. Kwon, D. Lazar, S. Devadas, B. Ford, Riffle an efficient communication system with strong anonymity, in *Proceedings on Privacy Enhancing Technologies*, vol. 1, no. 20, 2016
4. G.I. Rathod, D.A. Nikam, Darknet: a class of networks to share anonymous digital content. Int. J. Innov. Res. Comput. Commun. Eng. **3**(7), 8 (2015)
5. Top 500 websites, ALEXA [Online], http://www.alexa.com/topsites. Accessed 25 Mar 2016
6. K. Geers, *Strategic Cyber Security* (CCD COE, Tallinn, 2011)

7. S. Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History* (Mercatus Center at George Mason University, 2011), p. 38
8. R. Brown, Computer security threats: a brief history (2014) [Online], https://powermore.dell.com/technology/computer-security-threats-brief-history/. Accessed 01 Mar 2016
9. M. Warner, Cybersecurity: a pre-history. Intell. Natl. Secur. **27**(5), 19 (2012)
10. M.D. Cavelty, *Cyber Security* (Oxford University Press, Oxford, 2012)
11. C.P. Pfleeger, S.L. Pfleeger, J. Margulies, *Security in Computing*, 5th edn. (Prentice Hall, Upper Saddle River, NJ, 2015)
12. K.M. Lord, T. Sharp, *America's Cyber Future Security and Prosperity in the Information Age volume II, Washington, DC : Center of New American Security*, 2011
13. Q. Gu, P. Liu, *Denial of Service Attacks*. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, 454–468, 2007
14. D.L. Shinder, E. Tittel, Tittel, *Cybercrime Scene of the Computer Forensics Handbook* (Syngress, Rockland, USA, 2002)
15. S. Friedl's, An Illustrated Guide to the Kaminsky DNS Vulnerability, Unixwiz.net Tech Tips [Online], http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html. Accessed 27 July 2016
16. S. Fontaine, Attaque DOS (Deny of service), authsecu [Online], http://www.authsecu.com/dos-attaque-deny-of-service/dos-attaque-deny-of-service.php#Attaque_SynFlood. Accessed 19 Mar 2016
17. Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials **8**(2), 23 (2006)
18. "Man in the middle attack," valency networks (2008) [Online], http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html. Accessed 31 July 2016
19. S. Şen, J.A. Clark, J.E. Tapiador, Security threats in mobile ad hoc networks, in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, Auerbach Publications, 2011
20. Y.-C. Hu, A. Perrig, D.B. Johnson, Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 11 (2006)
21. M. Jakobsson, S. Wetzel, B. Yener, Stealth attacks on ad-hoc wireless networks, in *Vehicular Technology Conference, IEEE 58th*, p. 9, 2003
22. C. Laurendeau, M. Barbeau, *Threats to Security in DSRC/WAVE* (Springer, Heidelberg, 2006), pp. 266–279
23. S.M.K.R. Raazi, Z. Pervez, S. Lee, Key management schemes of wireless sensor networks a survey, in *Security of Self-Organizing Networks MANET, WSN, WMN, VANET*, Auerbach Publications, 2011
24. J. Chirillo, *Hack Attacks Revealed, a Complete Reference with Custom Security Hacking Toolkit* (John Wiley & Sons, New York, NY, 2001)
25. M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
26. J. Sen, *A Survey on Wireless Sensor Network Security*, 2010
27. Z.M. Fadlullah, T. Taleb, M. Schöller, Combating against security attacks against mobile ad hoc networks (MANETs), in *Security of Self-Organizing Networks MANET, WSN, WMN, VANE*, Auerbach Publications, 2011
28. S. Piper, *Intrusion Prevention Systems for Dummies* (Wiley Publishing, Inc., 2011)
29. S. Martin, M. Tokutomi, *Password Cracking*, researchers report, Arizona University, USA (2012)
30. C.P. Pfleeger, S.L.R. Pfleeger, *Security in Computing*, 4th edn. (Prentice Hall, 2006)
31. K.D. Mitnick, W.L. Simon, *The Art of Deception Controlling the Human Element of Security* (Wiley Publishing, Indiana, USA and simultaneously in Canada 2002)
32. P.A.H. Peterson, P. Reiher, Exploits: buffer overflows, pathname attacks, and SQL injections, mathcs [Online], http://mathcs.slu.edu/~chambers/spring11/security/assignments/lab05.html. Accessed 26 Mar 2016
33. S. Noel, D. Wijesekera, C. Youman, *Modern Intrusion Detection, Data Mining, and Degrees of Attack Guilt* (Springer, 2002)

34. J.M. Kizza, *A Guide to Computer Network Security* (Springer, 2009)
35. R.L. Krutz, R.D. *Vines, Cloud Security A Comprehensive Guide to Secure Cloud Computing* (Wiley Publishing, 2010)
36. W. Apolinarski, *Cohen and the First Computer Virus, Seminar "Malware" Prof. Dr. Joachim von zur Gathen, Daniel Loebenberger WS* (2007–2008)
37. G. White, S. Black, *Malware, Spyware, Adware, Viruses*, Information Technology Services (Clark College), 2011
38. N. Weaver, V. Paxson, S. Staniford, R. Cunningham, A taxonomy of computer worms, in *ACM Workshop on Rapid Malcode*, 2003
39. M. Madou, E. Lee, J. West, B. Chess, Watch what you write: preventing cross-site scripting by observing program output, in *OWASP AppSec Conference*, 2008
40. M. Bishop, *Introduction to Computer Viruses* (Pearson Education India, 2006)
41. M. Egan, T. Mather, *The Executive Guide to Information Security Threats, Challenges, and Solutions* (Addison Wesley Professional, 2004)
42. C. Wysopal, C. Eng, T. Shields, *Static Detection of Application Backdoors* (Black Hat, USA, 2007)
43. E. Casey, *Digital Evidence and Computer Crime* 3rd edn. (Academic Press, 2011)
44. T. Roosta, S. Shieh, S. Sastry, Taxonomy of security attacks in sensor networks and countermeasures, in *The First IEEE International Conference on System Integration and Reliability Improvements*, 2006, p. 25
45. P. Seuwou, D. Patel, G. Ubakanma, Vehicular ad hoc network applications and security: a study into the economic and the legal implications. Int. J. Electron. Secur. Digit. Forensics **6**(2), 115–129 (2014)
46. T. Roosta, Taxonomy of security attacks in sensor networks and countermeasures, in *The first IEEE International Conference on System Integration and Reliability Improvements,* vol. 25, 2006
47. M. Mana, M. Feham, B.A. Bensaber, SEKEBAN (secure and efficient key exchange for wireless body area network). Int. J. Adv. Sci. Technol. **12**, 15 (2009)
48. M.A. Ameen, J. Liu, K. Kwak, Security and privacy issues in wireless sensor networks for healthcare applications. J. Med. Syst. **36**(1), 8 (2012)
49. M. Abomhara, G.M. Koien, Security and privacy in the internet of things: current status and open issues, in *Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE*, 2014
50. S.J. Stolfo, S.M. Bellovin, S. Hershkop, A.D. Keromytis, *Insider Attack and Cyber Security Beyond the Hacker* (Springer, 2008)
51. J. Wayman, A. Jain, D. Maltoni, D. Maio, *An Introduction to Biometric Authentication Systems* (Springer, London, 2005)
52. I. Curry, *An Introduction to Cryptography and Digital Signatures*, Version 2.0 (Entrust 2001)
53. S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, 2011)
54. L. Benarous, M. Djoudi, A. Bouridane, *Etudes Comparatives d'outils de stéganographie et d'outils de stéganalyse: Application aux images et aux vidéos* (Amar Telidji University, Laghouat, Algeria, 2015)
55. Y. Miche, Developing fast machine learning techniques with applications to steganalysis problems, Thèse de doctorat., Institut National Polytechnique de Grenoble-INPG, 2010
56. T. Sereyvathana, Discriminative algorithms for large-scale image steganalysis and their limitation, Electronic Theses, Treatises and Dissertations, The Florida State University, Florida, 2012
57. Stegosploit, the hack news [Online], http://thehackernews.com/2015/06/Stegosploit-malware.html. Accessed 25 July 2016
58. Hackers exfiltrating data with video steganography, tripwire [Online], http://www.tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/. Accessed 25 July 2016
59. S.K.J. Pooja, P. Balgurgi, Audio steganography used for secure data transmission, in *Proceedings of International Conference on Advances in Computing*, Springer, India, 2012

60. M. Shirali-Shahreza, Text Steganography by changing words spelling, in *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, Volume: 3*, Gangwon-do, 2008
61. M.L. Bensaad, Steganography and digital watermarking, Ph.D. Thesis, University of Laghouat (Amar Telidji), Laghouat, Algeria, 2014
62. R. Bergmair, *Towards Linguistic Steganography: A Systematic Investigation of Approaches Systems, and Issues*, Final year thesis, B. Sc.(Hons.) in Computer Studies, The University of Derby, UK, 2004
63. A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey, T. Williams, *Gray Hat Hacking the Ethical Hacker's Handbook*, 3rd edn. (McGraw-Hill, 2011)
64. M.A. Pavlyushchik, Method and system for antimalware scanning with variable scan settings. Patent U.S. 7725941 B1, 25 May 2010
65. J. Alexander, *Intrusion Detection and Prevention Systems (IDS/IPS) Good Practice Guide Jason Alexander* (NHS Connecting for Health, 2009)
66. S. Dinesh, Intrusion Prevention Systems: security's silver bullet? Bus. Commun. Rev. **33**(3), 36–41 (2003)
67. K. Scarfone, P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST special publication, 800, 94, 2007
68. C. Martin, Intrusion detection and prevention systems in the industrial automation and control systems environment, in *Process Control Systems Industry Conference*, Industrial Defender Inc. 2008.
69. I. Mukhopadhyay, M. Chakraborty, S. Chakrabarti, A comparative study of related technologies of intrusion detection & prevention systems. J. Inf. Secur. **2**, 11 (2011)
70. Y. Farhaoui, Intrusion prevention system inspired immune systems. Indones. J. Electr. Eng. Comput. Sci. **2**(1), 168–179 (2016)
71. Masquelier, Mottier, Pronzato, Les Firewalls, Institut d'électronique et d'informatique Gaspard-Monge (IGM), France, 2000
72. M.A. Ameen, J. Liu, K. Kwak, *Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications* (Springer, 2010), p. 9
73. Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on cyber security for smart grid communications. IEEE Commun. Surv. Tutorials **14**(4), 998–1010 (2012)
74. S. Goldwasser, M. Bellare, *Lecture Notes on Cryptography* (MIT, 2008)
75. J. Hoopes, *Virtualization for Security Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting, Syngress*, Burlington, USA, 2008
76. M. Raya, J. P. Hubaux, The security of vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
77. A. Cecil, A summary of hacking organizations, conferences, publications, and effects on society. [online], http://www.cse.wustl.edu/~jain/cse571-07/ftp/hacking_orgs/. Accessed 25 July 2016
78. Certified Ethical Hacker, Eccouncil [Online], https://www.eccouncil.org/Certification/certified-ethical-hacker. Accessed 09 June 2016
79. L.A. Long, *Profiling Hackers* (The SANS Institut, 2012)
80. Eye Scaning 2012, [Online], http://www.messagetoeagle.com/images/eyescanning.jpg. Accessed 25 July 2016
81. D. John, How iris recognition works. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 21–30 (2004)
82. D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi, Biometric authentication: a review. Int. J. u–e-Serv. Sci. Technol. **2**(3), 13–28 (2009)
83. A. Abaza, A. Ross, C. Hebert, M.A.F. Harrison, M.S. Nixon, A survey on ear biometrics. ACM Comput. Surv. **45**(2), 35 (2013)
84. NEC biometrics technology uses sound to distinguish individually unique ear shape. NEC, 7 Mar 2016 [Online], http://www.nec.com/en/press/201603/global_20160307_01.html. Accessed 30 Apr 2016

85. Face recognition, 2016 [Online], http://reconocimientofacial.site/wp-content/uploads/2016/01/reconocimiento-facial-orna-innovations.jpg Accessed 07 October 2016
86. M. Savvides, J. Heo, S.W. Park, Face Recognition, in *Handbook of Biometrics*, ed. by A.K. Jain, P. Flynn, A.A. Ross (Springer Science & Business Media, New York, 2007), p. 43
87. human facial recognition, 2002, [Online]. http://www.nationalinfrared.com/images/Human_facial_imaging_recognition.jpg. Accessed 25 July 2016
88. S. Vasikarla, H. Madasu, Online biometric authentication using facial thermograms, in *Applied Imagery Pattern Recognition Workshop (AIPR), IEEE*, 2012
89. Lip print 2013, [Online], http://www.jfds.org/articles/2013/5/2/images/JForensicDentSci_2013_5_2_110_ 119777_f7.jpg. Accessed 25 July 2016
90. M. Chora, *The Lip as a Biometric* (Springer, 2009)
91. O.S. Adeoye, A survey of emerging biometric technologies. Int. J. Comput. Appl. **9**(10), 0975–8887 (2010)
92. D. Maltoni, R. Cappelli, Handbook of biometrics, in *Fingerprint Recognition*, ed. by A.K. Jain, P. Flynn, A.A. Ross (Springer, New York, 2008), pp. 23–42
93. I.B. Barbosa, T. Theoharis, A.E. Abdallah, On the use of fingernail images as transient biometric identifiers Biometric recognition using fingernail images. Mach. Vis. Appl. **27**(1), 65–76 (2016)
94. SkullConduct, 2016, [Online], http://s.newsweek.com/sites/www.newsweek.com/files/styles/embed-lg/public/2016/04/25/biometrics-skull-skullconduct-password-security.jpg. Accessed 25 July 2016
95. S. Schneegass, Y. Oualil, A. Bulling, SkullConduct: biometric user identification on eyewear computers using bone conduction through the skull, in *Proceedings of the 34th ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2016)*, 2016
96. H.O. Alanazi, B.B Zaidan, A.A Zaidan, 3D Skull recognition using 3D matching technique. J. Comput. **2**(1) (2010), p121–126
97. C.R. Hema, M.P. Paulraj, H. Kaur, Brain signatures: a modality for biometric authentication, in *International Conference on Electronic Design*, Penang, Malaysia, 2008
98. P. Inbavalli, G. Nandhini, Body odor as a biometric authentication. Int. J. Comput. Sci. Inform. Technol. **5**(5), 6270–6274 (2014)
99. Intech, 2011, [Online], http://www.intechopen.com/source/html/17745/media/image2.png. Accessed 01 Aug 2016
100. G. Lu, D. Zhang, W.K. Kong, M. Wong, A palmprint authentication system, in *Handbook of Biometrics*, ed. by A.K. Jain, P. Flynn, A.A. Ross (Springer, New York, 2008), p. 171–187
101. [Online], http://www.360biometrics.com/img/hand_features.gif. Accessed 25 July 2016
102. S.T. David, P. Sidlauskas, in Hand Geometry Recognition. *Handbook of Biometrics* (Springer, 2008), p. 91–107
103. Palm Veins, 2012, [Online], https://crisisboom.files.wordpress.com/2012/01/how-palm-vein-works.gif. Accessed 25 July 2016
104. D. Mulyono, H.S. Jinn, A study of finger vein biometric for personal identification, in *Biometrics and Security Technologies, IEEE*, pp. 1–8, 2008
105. K. Wang, Z. Yuan, D. Zhuang, Hand vein recognition based on multi supplemental features of multi-classifier fusion decision, in *Mechatronics and Automation, Proceedings of the 2006 IEEE International Conference* (Luoyang, Henan: IEEE, 2006)
106. G. Ioan Buciu, Biometrics systems and technologies: a survey. Int. J. Comput. Commun. Control **11**(3), 315–330 (2016)
107. L. Wang, H. Ning, T. Tan, W. Hu, Fusion of static and dynamic body biometrics for gait recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(2), 149–158 (2004)
108. J.E. Mason, I. Traoré, I. Woungang, Gait (Canada) biometric recognition, in *Machine Learning Techniques for Gait Biometric Recognition*, ed. by J.E. Mason, I. Traoré, I. Woungang (Springer International Publishing, Switzerland), 9–35, 2016.
109. Pulse,2012, [Online], http://www.homelandsecuritynewswire.com/sites/default/files/imagecache/stand ard/pulse_biometrics-1.jpg. Accessed 25 July 2016

110. F. Agrafioti, D. Hatzinakos, J. Gao, *Heart Biometrics: Theory, Methods and Applications* (INTECH Open Access Publisher, 2011)
111. Hand signature, [Online], http://www.b2bedocuments.com/images/signaturepad08.jpg. Accessed 25 July 2016
112. R. Das, S. Dhar, S. Das, S. Dutta, S. Mukherjee, A comparative study of biometric authentication based on handwritten signature. Int. J. Res. Eng. Technol. **02**(12), 2321–7308 (2013)