A Method of Warning About Unauthorized Access to a Room

Cristian-Ovidiu OPRIȘ
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
cristian.opris@upb.ro

Abstract

This paper is based on the study of cybercrime in the context of a world based on technology. Whether it is financial losses, data leaks or mental trauma resulting from harassment in the online environment, cybercrime is part of the reality of the modern world, where the multiple advantages of using the most advanced technologies bring with them disadvantages that cannot be ignored. We will treat the types of cyberattacks, but also the methods by which we can protect ourselves as much as possible. An example of increasing the degree of security in terms of physical access to a room containing sensitive information, achieved at low cost, is also provided. A "smart" entrance mat is used to provide access, a coconut fiber mat into which Linqstat (Velostat) tactile force sensors and the data processing electronics provided by them have been inserted.

Index terms: access security, cyberattacks, tactile sensor, Velostat

1. Introduction

Cybercrime is increasingly common, and current technical methods of combating cybercrime are often ineffective. Therefore, preventive strategies become necessary to reduce cybercrime. The following two aspects are important: the characteristics of criminals to understand the motivations behind the crime, but also the characteristics of users' computer systems to better understand how they are victims of cybercrime.

Cybercriminals are developing increasingly intelligent techniques for their victims in the online environment: individuals, companies or organizations. Cybercrimes are on the rise due to lack of cyber security. All types of computer crimes consist of both the computer and the person behind it as victims. A generalized definition of cybercrime may be “Unlawful acts wherein the computer is both a tool and target”. Cybercriminal is a person who commits an illegal act with a guilty intention or commits a crime in context of cybercrime [1]. Cybercriminal can also be the person who illegally enters a secure room containing classified data in digital form to steal it. In this context, a method for detecting the number and even the approximate weight of people who can illegally access a secure space is presented.

Cyber security is a term of security which is implicated through diversified disciplines, most of them focusing on technical or psychological problems such as computer science, criminology, economics, engineering, information systems, management, medicare, neurophysiology, psychology, sociology, etc. It affords the people with discussions about behaviors and motivations, benefits and consequences about cybercrime and security [2]. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. The latest

technologies like cloud computing, green computing, mobile computing, e-commerce, net banking are required high level of information security [2].

Measures aimed at mitigating cyber-attacks should be implemented through the replication of already existing approaches and methods established to curb conventional crimes in society. These measures should be in the form of government policies, enactment of legislative laws, education and awareness and cooperation between government agencies, private sectors, the public and relevant international bodies. Special committee of experts and stakeholders should be instituted to oversee the modification of conventional strategies and approaches in order to fine tune implemented policies to be cybercrime specific [3]. Some measures can be:

- *Reduce Opportunities*: elaborate system design so that hackers do not hack the computer.
- *Use Authentication Technology*: use password bio-metric devices, fingerprint or voice recognition technology and retinal imaging, greatly immense the difficulty of obtaining unauthorized access to information systems.
- Data Recovery: develop tools for data recovery and analysis.
- Reporting: always report the crime to cyber fraud complaint center in one's country as they maintain huge data and have better tools for controlling cybercrime.
- Install firewalls: as they block particular network traffic according to security policy.
- Attachments: Avoid opening attachments or e-mails which were not expected and have come from an unknown source or person [4].

2. Types of cybercrimes

Among the reasons behind the actions of cybercrime are fighting for a cause in which the criminal believes, financial gain, public recognition. Types of cyberattacks will be classified as follows (Table 1).

Table 1. Types of cybercrimes [1]

Cybercrime against individuals	**Cybercrime on property**	**Cybercrime within organisations**
E-mail Spoofing	Intellectual Property crime	Hacking
Phishing	Cyber squatting	Password
Spamming	Cyber vandalism	Denial attack
Cyber defamation	Hacking system	Virus attack
Cyber stalking	Alerting way of unauthorized	Mail bomb
Salami attack	Logic bomb	
Computer sabotage	Trojan horse	
Malware		

2.1. Cybercrime against individuals

E-mail is one of the most used applications for communication. Security from this point of view is defined as the ability to provide confidentiality. E-mail date and E-mail address spoofing are the two important forms of E-mail spoofing. E-mail date spoofing occurs when someone changes the sending date and e-mail address spoofing refers to sending mail which pretends to come from someone else [5]. The date and time of the email are particularly important in such cases bank statements, communications from the chief / chief in terms of terms, etc. Simple Mail Transfer Protocol (SMTP) is the largest and most important protocol for e-mail. Unfortunately, this does not include security policies.

Phishing uses a technique in which the attackers are trying to trick victims. These attacks start with an email from an attacker pretending be someone or something you know or trust (bank,

knowledge, shop). In the content of the email appears a redirecting to a link or a file attached, the purpose is to show everything as convincing as possible to get money from the victims.

With spam emails being around for more than 40 years, cybercriminals have always found new ways to us them to catch victims out, having gauged "click rates rising from 13.4% in the second half of 2017 to 14.2% in 2018," according to Adam Sheehan from MWR InfoSecurity [6].

Defamation is a false statement that harms the reputation of individual person, business, product, group, government, religion of nation. For a statement to constitute defamation a claim must generally be false and made to someone other than the person defamed, and result injures the reputation of a person who is defamed [7].

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware is not the same as defective software - software that has a legitimate purpose but contains harmful bugs (programming errors) [8].

2.2. Cybercrime within organisations

In 1997, the Group of Eight (G8) established a "Subcommittee986 on High-tech Crimes", dealing with the fight against cybercrime. During their meeting in Washington DC, United States, the G8 Justice and Home Affairs Ministers adopted ten Principles and a Ten-Point Action Plan to fight high-tech crimes.988 The Heads of the G8 subsequently endorsed these principles, which include [9]:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
- Law-enforcement personnel must be trained and equipped to address high-tech crimes.

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection. The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries [9].

Several EU legislative actions contribute to the fight against cybercrime. These include:

- 2013 - A Directive on attacks against information systems which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions. In 2017, the Commission has published a Report assessing the extent to which Member States have taken the necessary measures in order to comply with the Directive.
- 2011 - A Directive on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse).
- 2002 - ePrivacy Directive whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information. In 2017, the Commission proposed to repeal the Directive and replace it with a Regulation concerning the respect for private life and the protection of personal data in electronic communications.
- 2001 - Framework Decision on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviors that EU States need to consider as punishable criminal offences. On 13 September 2017, the Commission has proposed a new Directive aiming at updating the current legal framework, removing obstacles to

operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective [10].

According to Check Point (Figure 1), in 2021 education and research were the sectors with the highest volume of attacks, up 75% compared to 2020. On the next positions, "the government/military sector had 1,136 attacks per week (47% increase), and the communications industry had 1,079 attacks weekly per organization (51% increase)" [11].

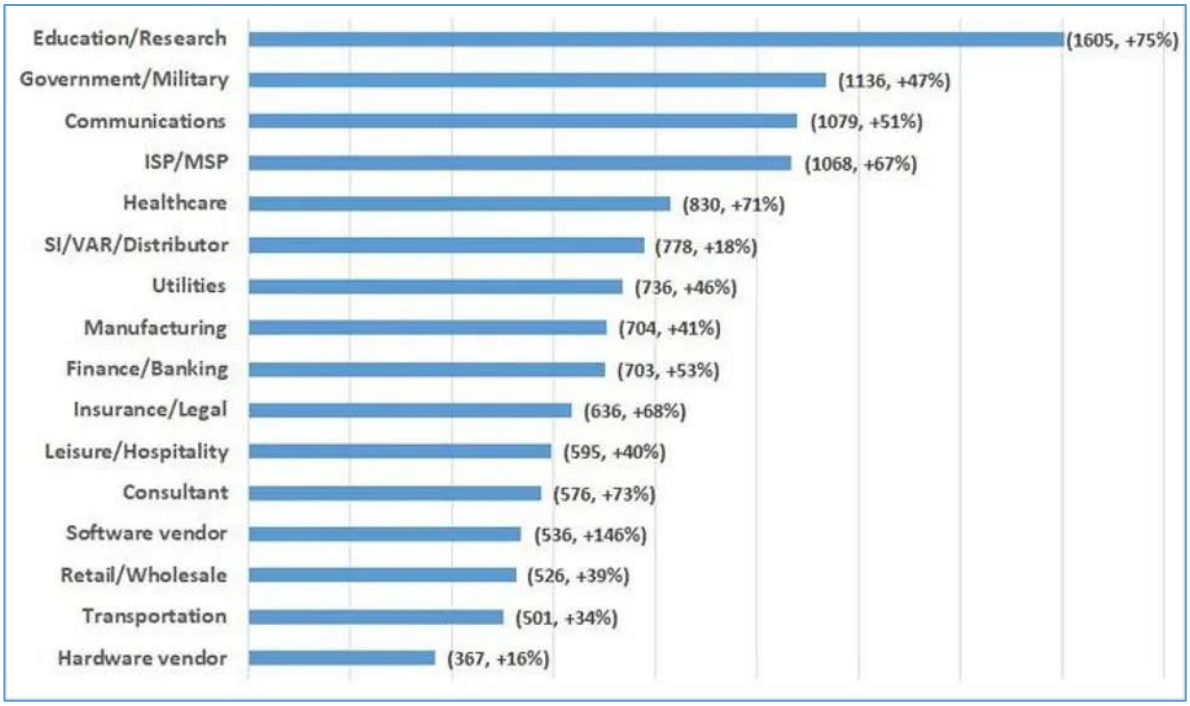

Fig. 1. Average weekly attacks per organisation by industry [11]

Possible reasons for these differences may be the types and frequencies of attacks experienced as well as the importance that each company places on the theft of information assets versus other consequences of the incident [12]. The following figure shows the types of cyberattacks for 60 companies.

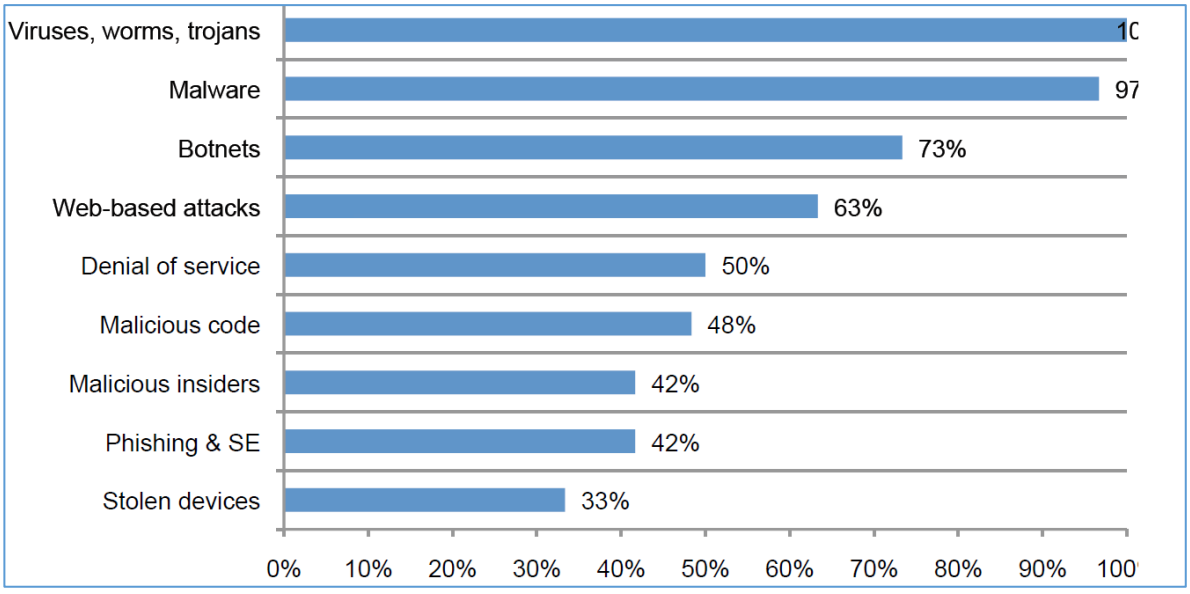

Fig. 2. Types of cyberattacks for 60 different companies [12]

3. The method of warning of unauthorized access to a room containing sensitive data

To obtain data about the approximate weight and number of people accessing a secure room, it was decided to use eight tactile force sensors [13] mounted in an entrance mat. The sensors will be placed so that the surface of the mat is distributed equally for each sensor (Figure 3).

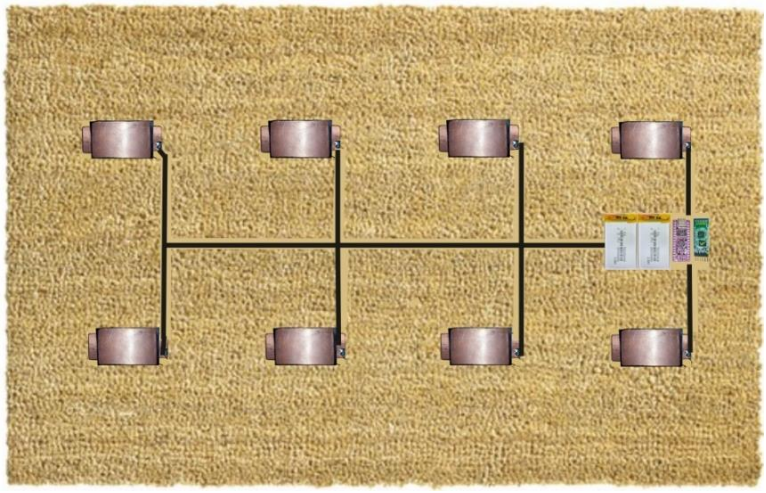

Fig. 3. "Smart" entrance mat

Two 40x60 cm entrance mats were used to make the "smart" entrance mat. In the first mat, eight cutouts were made in which eight tactile force sensors were placed, and on one side of the mat a cutout was made in which the electronic circuits were mounted. After commissioning, the entire surface is covered with a durable cloth for protection. The second mat is glued back-to-back with the first. This is the one that will be positioned normally, face up at the entrance to the secure room.

The block diagram of the electronic assembly is shown in Figure 4. Sensors are indicated by their resistance values (Rs1 to Rs8). The Velostat material is characterized by the phenomenon of piezo resistivity, i.e., it changes its electrical resistance because of its deformation [13].

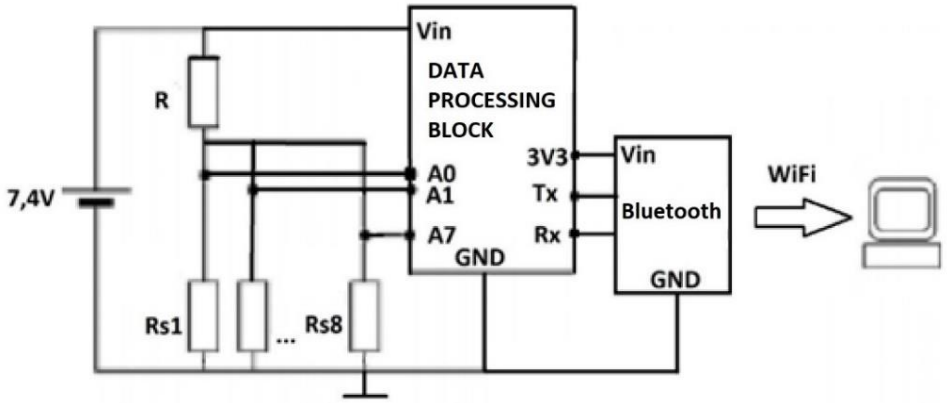

Fig. 4. The block diagram of the electronic assembly

The value of the resistor R is chosen so that we have optimal voltages at the input of the data processing block. The data processing block contains signal amplifiers and the Arduino Nano Board which contains 8 analog inputs. Warning decisions made by programming the Arduino board are transmitted via the Bluetooth Module to a computer or mobile phone via the Bluetooth Terminal application. The Arduino Nano Board and Bluetooth Module were chosen due to their small size and low power consumption. The entire electronic assembly is powered by 7.4 V lithium-polymer batteries.

4. Conclusion

In conclusion, the foundation of criminal justice system is to keep order and secure justice in the society. Safety is one of the basic needs of people according to Maslow's pyramid of hierarchical needs and crime prevention [14], in this respect, emerges as a necessity for development of a healthy and safe society. Therefore, the state has to be one step ahead the criminals in terms of the use of technology or the control/surveillance of the technology in order to prevent unlawful actions in cyberspace. As the uncontrolled power is not (a true and just) power, similarly, the uncontrolled technology is not (a helpful and good) technology for citizens. Without safety, which is one of their basic needs, the citizens will not feel like they are living in a free and happy world [15].

This paper presented a way to warn of a break-in (by forcibly removing a locking system) in a room containing sensitive data. The mode is also valuable if the classic alarm device is disabled. The Internet is a powerful tool and effective means of communication, but it is vulnerable just like anything else. To defend against cybercrimes, intrusion detection techniques should be designed, implemented, and administrated.

References

[1]. E. N. Kaur, "Introduction of Cyber Crime and its Types," International Research Journal of computer Science (IRJCS), 2018.
[2]. V. Kavitha, "Cyber Security issues and challenges - a review," International Journal of Computer Science and Mobile Computing, vol. 8, no. 11, 2019.
[3]. M.B. Owiso, Cyber Crime, https://www.academia.edu/12741661/Cyber_Crime.
[4]. M. Lakshmi Prasanthi, Tata A.S.K. Ishwarya, "Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 3, March 2015.
[5]. E.S. Pilli, "Forensic analysis of e-mail address spoofing," in 2012 Third International Conference on Computer and Communication Technology, 2014.
[6]. Spam still first choice for cyber crime, according to study. https://www.information-age.com/spam-still-first-choice-cyber-crime-according-study-123473840/#.
[7]. A.L. Ishabakaki, "Defamation in social media (cyber defamation) legal perspective in Tanzania," Victory Attorneys & Consultants.
[8]. http://cs.sru.edu/~mullins/cpsc100book/module05_SoftwareAndAdmin/module05-04_softwareAndAdmin.html. [Online].
[9]. I.T.D. Sector, "Understanding cybercrime: phenomena, challenges and legal response," Sept. 2012.
[10]. Cybercrime. European Commission. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en.
[11]. Check Point, Check Point Research: Cyber Attacks Increased 50% Year over Year, 2022. https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/.
[12]. P. Institute, "Cost of Cyber Crime Study: United States," HP Enterprise Security, 2013.
[13]. C.O. Opris, I.B. Bacis, L. Milea, A. Vasile, "Implementation of a Resistive Pressure Sensor Made With "Linqstat" for Automotive". ISSE 2023, Timișoara, Romania.
[14]. S. Mcleod, Maslow's Hierarchy of Needs, Simply Psychology, http://www.simply psychology.org/maslow.html. Accessed Apr. 20, 2023.
[15]. Z. Gul, R. Terkesli, "Crime of the Millennium: Cyber Crime," Humanity & Social Sciences Journal 7, 2012.