Secure IT Evolution Short Analysis

Mircea-Constantin ȘCHEAU[1]*, Călin Mihail RANGU [2], Cătălin UDROIU [3]

[1]University of Craiova, [2]Financial Supervisory Authority, [3]Integrisoft Solutions
mircea.scheau@edu.ucv.ro, calin@rangu.ro, udroiu_catalin@yahoo.com

***Corresponding author:**

Mircea-Constantin ȘCHEAU
mircea.scheau@edu.ucv.ro

Abstract: Miliarde de persoane au acces la mediul online prin intermediul căruia se efectuează transferuri financiare sau de date cu caracter personal. Granițele criminalității informatice sunt deosebit de elastice. Domeniile critice sunt în atenția infractorilor. Balanța de profit și pierderi poate fi serios dezechilibrată în condițiile ignorării recomandărilor organismelor internaționale și a lipsei investițiilor. Sistemele defensive pot să devină victime la rândul lor, ca urmare a unui management defectuos. Fenomenul poate fi combătut numai printr-o abordare matură, profesională și plină de responsabilitate. Articolul încearcă să scoată în evidență rolul infrastructurii IT în lumina evoluției tehnologice și câteva dintre efectele ce se pot înregistra. Metodele de protecție propuse își doresc să răspundă așteptărilor cititorilor.

Cuvinte cheie: conexiune, vulnerabilitate, atac, malware, criptografie.

Abstract: Billions of people have access to the online environment through which runs financial transfers or personal data. The boundaries of cybercrime are particularly diffuse. The critical areas are in the focus of the offenders. The balance of profits and losses can be seriously prejudiced if the directions of international bodies are ignored. Defensive systems can become casualties due to poor management or lack of investment. The phenomenon can be overcome only by a mature approach, one that is professional and that takes full responsibility. The article attempts to underline the role of the IT infrastructure in the light of technological evolution and some of the effects that can arise. The proposed defence strategies have as objective fulfilling the readers expectations.

Keywords: connection, vulnerability, attack, malware, cryptography.

1. Introduction

The accessibility of the information systems, particularly in the area of development is becoming increasingly exposed in terms of security. The administration of servers, applications, computer networks and virtual domains implies an increase in the number of credentials, directly proportional to the extension of the operational risk degree in the absence of services, among others, for managing usernames and passwords. Within computer networks or for connection between workstations and applications, there are protocols and commands such as File Transfer Protocol (FTP) or Remote Copy Protocol (RCP) used to transfer files between a client and a server or between remote servers, Telecommunication Network (Telnet) or Remote login (Rlogin) for remote connection (Barrett, Silverman, & Byrnes, 2009), and authentication, two-way communication and Remote Shell Protocol (RSH) or Remote Execution Protocol (Rexec) for remote execution of SHELL commands. Unfortunately, penetrability is one of the major problems of these programs, as any file can be intercepted by an attacker that escalates and obtains administrator privileges. The username and password can be recorded by exploiting data packet monitoring programs (e.g. wireshark (Zhang, 2008)), Common Vulnerabilities and Exposures (CVE), or Zero-Day ones, and launching attacks (e.g. Denial of Service / Distributed Denial of Service - DoS / DDoS) may cause temporary or permanent equipment malfunctions. We are looking for solutions to prevent and deal with these issues as efficiently as possible encryption programs and installation firewall devices with the role of traffic monitoring and security, which can vary depending on the cost and complexity, further supporting the resolution efforts.

The exchange of information between national crime investigation organisations and the participation in joint teams to thwart/counteract the criminal phenomenon, come to complement the actions carried out by the international bodies. Collaboration takes place on the basis of clearly defined protocols, governmentally endorsed. On the other hand, however, the circulation of

https://doi.org/10.33436/v30i2y202008

computer weapons and the recording of similar effects in different parts of the globe entitle us to believe in the existence of platforms around which satellites of organized crime gravitate. The attack tools are borrowed or sold together with user manuals. It is provided support for users and participation in common actions is negotiated by suppliers.

This article is addressing to both system administrator specialists and end-users without advanced technical knowledge of security or server management, aiming to provide a clearer picture of some of the most useful security tools in the current activity. Business environments are constantly changing and companies are striving to protect their information behind the Virtual Private Network (VPN) or firewall devices with the role of traffic monitoring and security, but the costs can significantly affect accounts and stability.

2. Hash, SSH and Cryptography

In 1995, Tatu Ylönen, a researcher at the University of Technology in Helsinki, Finland, together with several colleagues, developed a cryptographic protocol called Secure Shell (SSH), which allows data to be transferred using a secure channel between network devices (Ylonen et al., 2015). SSH allows remote connection to one or more devices, executing commands inside that host and transferring data using a secure channel, the process described in figure 1. The first version, SSH1, was designed in 1995 to replace UNIX commands (Barrett, Silverman, & Byrnes, 2009) rlogin, rsh, rexec and rcp, considered unsafe. Version 2 of the Secure Shell package, SSH2, adopted in a revised version of the Internet Engineering Task Force (IETF) standard in 2006, was launched in 1997, the software being included and used as a mechanism for remote administration, integration or security for operating automation of operating systems or devices like Linux, Unix, firewalls, network equipment, etc. SSH allows authentication, encryption and data integrity checking.

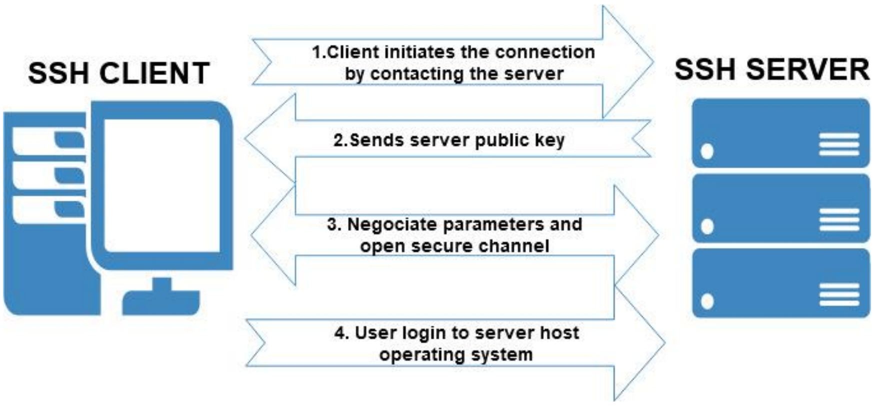

SSH CLIENT
1.Client initiates the connection by contacting the server
SSH SERVER
2.Sends server public key
3. Negociate parameters and open secure channel
4. User login to server host operating system

Figure 1. SSH connection **(**SSH Academy, 2020)

Based on a client/server architecture, as a way of working, Host X, using an SSH client application, sends a request to connect to a Host Y SSH server. The two hosts establish a secure cryptographic connection, authenticating on each server through public and private key pairs (Ylonen et al., 2015). Once the connection is established, symmetric (Young, Lecture 44) or asymmetricencryption and digital signatures based on another algorithm (e.g. hash (Grah, 2008)) are used, depending on the level of security intended to be provided. The most used in the last three decades were: Message Digest - developed on 128 bits (MD4, MD5), Secure Hash Algorithm - designed by the National Security Agency (NSA) of the United States of America (SHA-2, SHA256), Whirlpool - adopted as part of the joint International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 10118-3 international standard, Tiger – designed on 64-bits platform etc.

Hash allows unidirectional encryption, reducing a message from different margins, in a short, unique and irreversible representation (CGI Group Inc., 2004), the process described in figure 2. For example, by applying the SHA-256 function, the algorithm will generate a unique hash value of 256 bits. Some of the advantages of using the algorithm are:

- message integrity, any modification of the message is easily detectable;

- higher speed, a faster processing than in the case of other algorithms;
- compact size, digital signature being applied to the resulting message, ”digest”, which is considerably smaller than the original message.

However, it is possible for two different messages to produce the same "unique" hash value, incident known as `collision`, which makes the algorithm essentially futile (Hamilton, module course). Therefore, some of the hash algorithms have been abandoned over time due to the demonstrated vulnerabilities they induce. As an example, in 2017, a team of specialists from Google and National Research Institute for Mathematics and Computer Science (Centrum Wiskunde & Informatica – CWI) from Amsterdam, discovered a SHA-1 vulnerability by creating a collision (Stevens et al., 2017).

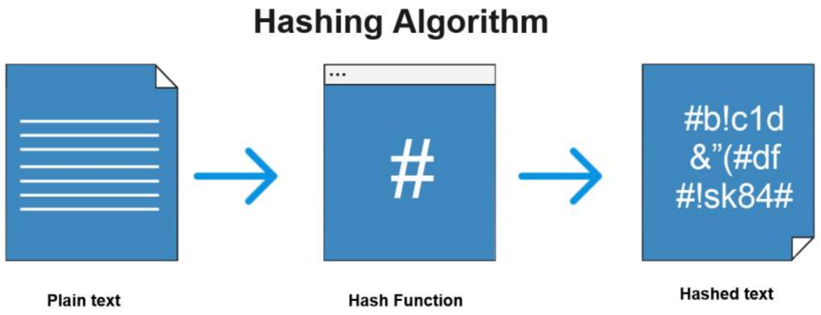


Figure 2. Conversion from Plain to Hash text (Stefanovskyi, 2019)

Although attention was drawn to the potential dangers of SHA-1, it was not completely abandoned and, in January 2020, the matter had to be reevaluated due to strong attacks, the new collision giving the aggressors more flexibility and options. Pretty Good Privacy (PGP) encryption keys were created, allowing the target to be depersonalized when they were digitally signed with SHA-1. More specifically, attackers created the same hash for two or more entries, by adding additional data to each other (Goodin, 2020).

Questions about the differences and similarities between hash and encryption functions are quite common and that is why we present some of them in table 1. The main objective of the Hashing is to validate the integrity of the content and, possibly, the identity of the sender (digital signature), the objective of encryption being to increase the security level. Either of them are necessary in the handling of sensitive data, classified messages/information and both change their form or even their format. Specifically, encryption is a two-way function that naturally involves decryption, the hashing being unidirectional, with the role of changing an original text into one with a short, unique and irreversible value.

Table 1. Differences - Hash functions, Symmetric, and Asymmetric algorithms (Mehmood, 2017)

Characteristics	Hash	Symmetric	Asymmetric
No. Of keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used Key	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of compromised Key	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-256, SHA-384 or SHA-512	AES, Blowfish, Twofish, 3DES, RC4	RSA, DSA, Diffie-Hellman

As stated by Microsoft, symmetric encryption is the most popular and the oldest encryption technique used. A secret key can be a number, a word, or just a string of random letters applied to a message to change the form of the content in the case of encryption, or reconstitution, in the case of decryption (Microsoft, 2018).

Depending on the algorithm, the encryption strength can be directly proportional to complexity of the used key, as in table 2, but one of the reamining problems is the safety of a key transmission in a network or through a transfer environment, a priori considered to be insecure.

The cryptographic algorithms, a classification being available in figure 3, use strong or weak keys, some relevant examples (PSSG, 2017) being: Ron's Code 2 (RC2) - symmetric cipher key of 64-bit blocks, Triple Data Encryption Algorithm (3DES) - 56-bit block digit formed based on DES, by applying it three times, Rivest cipher 6 (RC6) - symmetric key block code derived from RC5, designed to meet the Advanced Encryption Standard (AES) requirements, Blowfish - symmetric encryption algorithm developed by Bruce Schneier in 1993, Data Encryption Standard (DES), globally accepted data encryption standard and Advanced Encryption Standard (AES), adopted as standard by the National Institute of Standards and Technology (NIST) in 2001, becoming landmarks in this context.

Table 2. Key lengths and initialization vectors (Riman, C. & Abi-Char, 2015)

Cryptographic function	Key length		Vector lengths	
	bytes	bits	bytes	bits
AES	16, 24, 32	128, 192 or 256	16	128
DES	from 1 to 8 bytes	from 8 to 64 bits	16	128
3DES	from 1 to 24 bytes	from 8 to 192 bits	16	128
BLOWFISH	from 1 to 56 bytes	from 8 to 448 bits	16	128
RIJNDAEL-256	from 1 to 32 bytes	from 8 to 256 bits	64	512
R4	from 1 to 256 bytes	from 8 to 2048 bits	--	--
TWOFISH	from 1 to 32 bytes	from 8 to 256 bits	32	256

Symmetric encryption can work either in block ciphers mode or stream ciphers mode, with some algorithms running only in block mode or stream mode, while others can run in both manners. In block mode, the cryptographic algorithm divides the input message into a structure of small, fixed blocks, that it encrypts or decrypts successively. In stream mode, each digit (sometimes just a bit) of the input message is encrypted separately. Basically, the block mode delivers a collection of text as a single block, the stream mode directly converting a text character into an encrypted text character (Saxena et al., 2018).

Simplicity is one of the characteristics of symmetric encryption and can be considered as an advantage, in the context of aiming for a higher processing speed, or as a vulnerability in front of attackers, which is one of the critiques brought to the procedure.

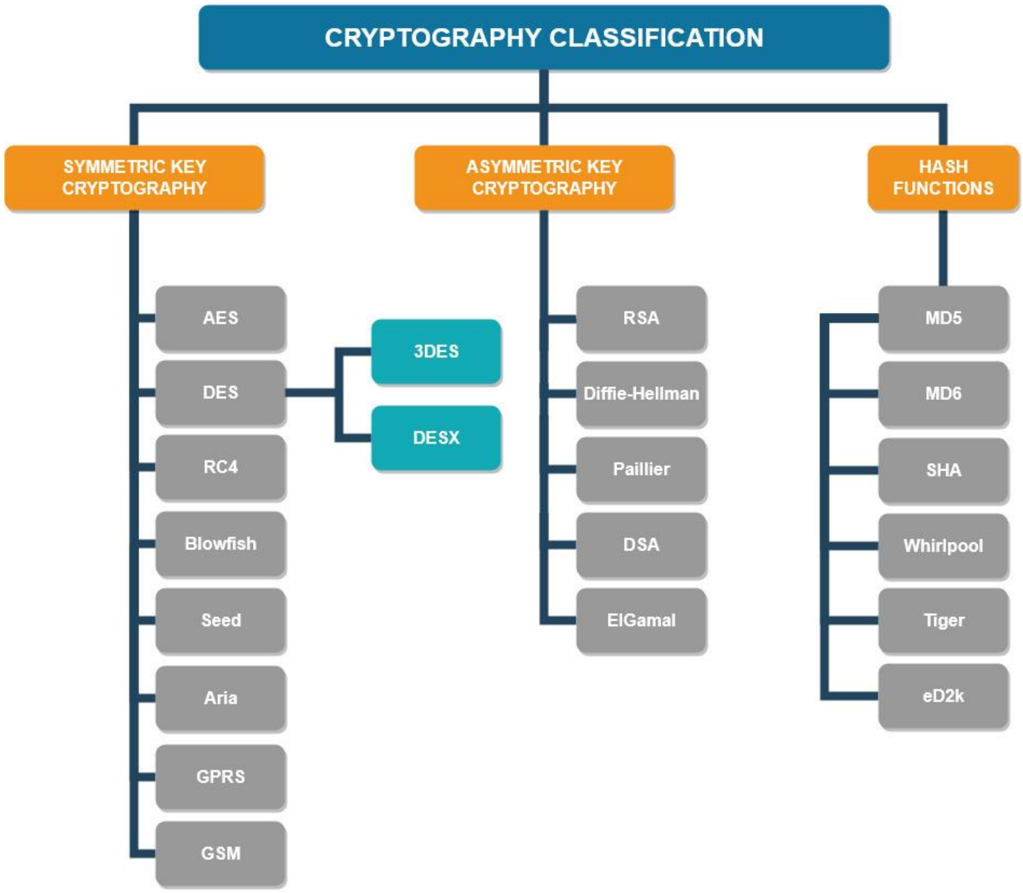
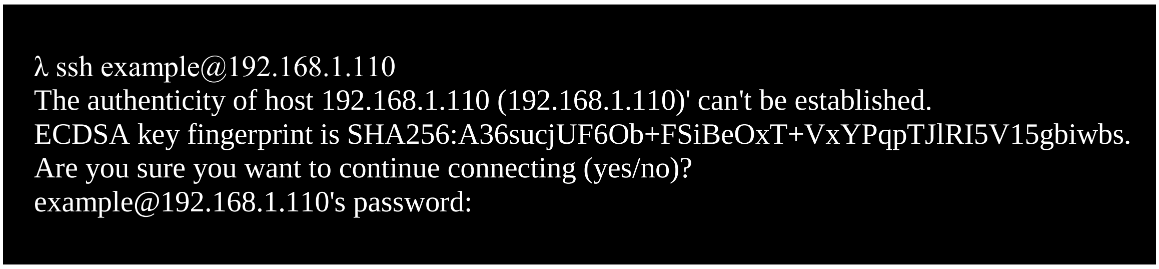


Figure 3. Algorithms with symmetric, asymmetric keys and hash functions (Sindhu & Sindhu, 2017)

Part of the disadvantages of symmetric encryption are eliminated by asymmetric encryption, which use a public key for encryption and a private key for decryption. As examples we can mention Rivest – Shamir – Adleman (RSA) algorithm used for encryption and decryption (Milanov, 2009) or Digital Signature Algorithm (DSA), algorithm used to detect unauthorized changes of the transmitted data and to authenticate the signer's identity. Sometimes it is based on complex mathematical functions, therefore, for efficiency, it is recommended to use devices with suitable configuration (Hardjono, Dondeti, 2005). Asymmetrical encryption techniques are usually slower than symmetrical techniques because they require additional processing power. hence a higher consumption of resources and algorithms may behave differently depending on the application area. As an example, the cryptographic power of the two algorithms, RSA and DSA, is about the same, but the performances are different. On the one hand, RSA offers a higher encryption speed being created for encryption and approximately simultaneous signing, and, on the other hand, DSA offers more security and produces the key immediately, taking into account the key generation technology and the fact that it was originally designed for digital signatures (NIST, 2013).

We want to highlight the connection mode and, practically, distinguish between two stages.

As first step, in order to establish the communication from the client side we issue a request for SSH connection with the server. The server listens for port 22, by default for SSH connections, and checks for the identity. With the development of the SSH1 protocol, port 22 was designed to replace the less secure telnet (23) and ftp (21) ports. If necessary, as an additional security measure, port 22 can be changed procedurally at each connection request. Except for the first access, when manual authentication is required, after checking the key, the server is added to the known_hosts file in the directory ~/.ssh directory on the client device, file that contains information about all the client-verified servers. The known_hosts file contains a list of known host keys, used to verify the identity of the remote host, thus preventing impersonation or interception. To emphasize the process as best as possible, we performed a test and captured in figure 4 the real exchange of messages, as they appear when we initiate the connection commands.



```
λ ssh example@192.168.1.110
The authenticity of host 192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:A36sucjUF6Ob+FSiBeOxT+VxYPqpTJlRI5V15gbiwbs.
Are you sure you want to continue connecting (yes/no)?
example@192.168.1.110's password:
```

Figure 4. SSH connection to a new server (authors study)

As the second step required to authenticate the access, after verifying the server, both client sides can negotiate a session key using, for example, the Diffie-Hellman mathematical algorithm **(**Baker, 1999) or another algorithm designed so that both parties can equally contribute to generating the session key. The session key generated in this case is symmetrically shared, i.e. the same key is used for both encryption and decryption.

The Diffie-Hellman algorithm **(**Revuelto & Socha, 2016*)*, mainly used for websites that use Secure Hyper Text Transfer Protocol (https), Secure Socket Layers/Transport Layer Security (SSL/TLS) protocols (Rescorla, 2001), and which ensures the confidentiality and integrity of the transmitted data, emails, VPNs (etc.), allows two PCs to use a common code, despite the fact that the two have never communicated with each other. The code is required to securely change a cryptographic key. For example, the algorithm is used by VPNs at the beginning of Internet Protocol Security (IPSec) - a sequence of cryptographic protocols used to protect data traffic through Internet networks, to negotiate the session key used by the block of symmetrical digits throughout the connection.

The easiest and most common way of validation is to use the password requested by the server when trying to establish the connection with it. Even if the password is encrypted, this method is not recommended due to the limitations imposed by the complexity of the password itself. The advised alternative is to use SSH key pairs. The associated SSH key pairs are asymmetric keys and serve different functions. The public key is used for data encryption, which can only be decrypted with the private key. Once the authentication is established, the SSH protocol uses powerful symmetric and hash encryption algorithms to ensure the integrity and confidentiality of the information.

3. Encryption & Financial transfers

Financial transactions involve data transfers that can be intercepted, hijacked or manipulated, depending on the objective of fraudulent grouping. Protecting the IT domain, viewed as a vital infrastructure or computerized sub-domains - components of other critical configurations, is essential in ensuring the security of each nation.

Consequently, the protection of end-users, natural persons or legal persons, represents the declared purpose of government policies. Crime is a term generally associated with illegal activities and the combination with the notion of computer or cyber results in a phrase that becomes one of the most problematic/delicate global problems. The US Department of Justice extends the definition of cybercrime by including any illegal activity involving a computer used to store information (Farion & Panasyuk, (2018)).

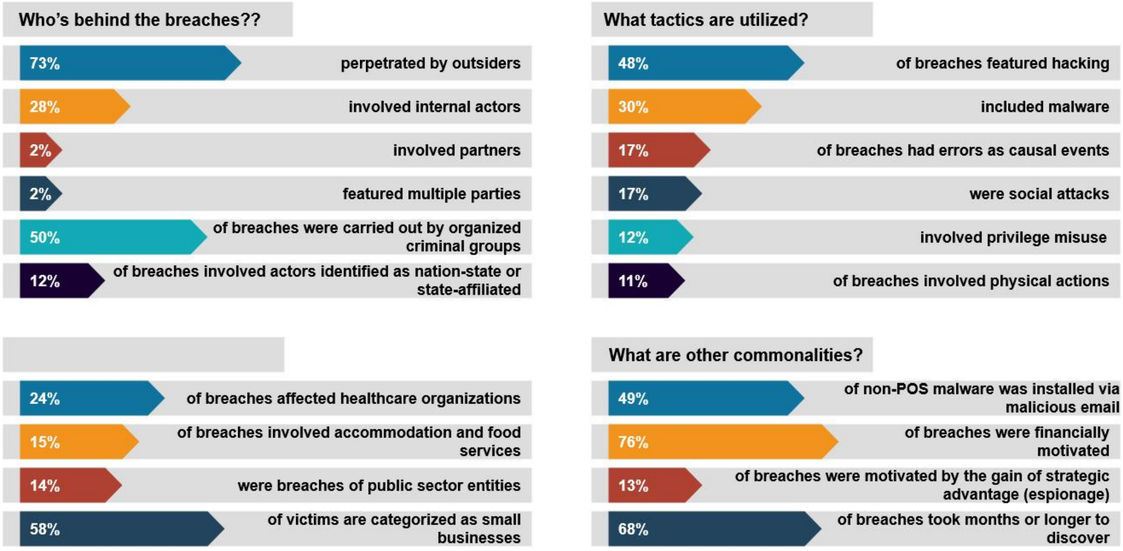


Figure 5. Summary of findings 2018 (Verizon, 2018)

The securing of information involves, inter alia, the provision of:

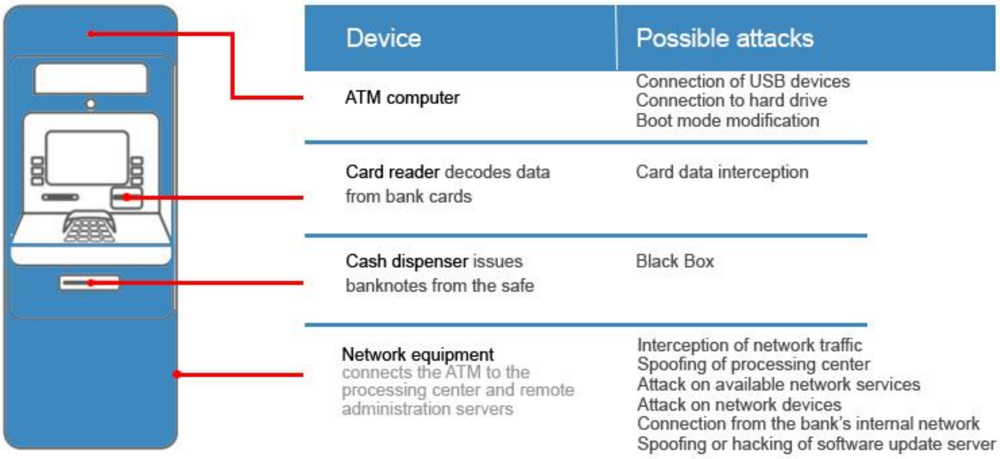
- Availability: authorized users must have access to information and associated resources when needed;
- Confidentiality: the information must be accessible only to authorized persons;
- Integrity: the information must be complete and correct/exact (Traxcom Technologies LLC., 2019).

According to a Verizon report regarding the investigation of security breaches for the year 2018, there were more than 53,000 incidents and 2,216 data leaks, the summary in figure 5 trying to bring to the fore the common actors, tactics and characteristics. The report is not comprehensive and may present inaccuracies, but it provides a fairly clear perspective on the phenomenon.

Encryption techniques have long been used in the banking financial industry to ensure the security of transactions; nowadays, they have to be adapted to new products and services offered to customers: secure card transactions in the online environment or ATM/PoS, secure currency exchanges, transfers of high value or clearing operations, securitization of derivative transactions on primary or secondary markets etc.

3.1. ATM / PoS Attacks

After 2012, there was a significant increase in non-cash transactions, to the detriment of cash transactions, determined in particular by the increase in the number of credit cards and the automation of payment processes via electronic channels. The services offered by an ATM include, among others, the connection of the card holders with the unit owning the machine. The exploitation of the ATM has evolved from exclusively cash release operations to more complex operations of depositing cash into own account or into a third party's account, transfers between accounts, currency exchanges, payment of invoices, etc. The network of devices has always been in the focus of criminals and, due to the technological evolution, as well as the software capabilities of the fraudulent persons, we are witnessing a reorientation from the brute force towards malware attacks. Fraudulent techniques have evolved very quickly and international specialized organizations are working together with technology providers to mitigate this phenomenon and reduce the losses incurred by financial institutions and their clients. In order to be able to run the commands for which it was designed, in addition to safe-deposit box, as can be seen in figure 6, the operation of the ATM requires a computer system with peripherals, operating system, user interface etc.



Device	Possible attacks
ATM computer	Connection of USB devices Connection to hard drive Boot mode modification
Card reader decodes data from bank cards	Card data interception
Cash dispenser issues banknotes from the safe	Black Box
Network equipment connects the ATM to the processing center and remote administration servers	Interception of network traffic Spoofing of processing center Attack on available network services Attack on network devices Connection from the bank's internal network Spoofing or hacking of software update server

Figure 6. ATM attacks (Positive Technologies. 2018)

The first step for an attack to be successful is to understand the operation and communication of the concerned/respective devices, the connectivity chain being presented in figure 7.

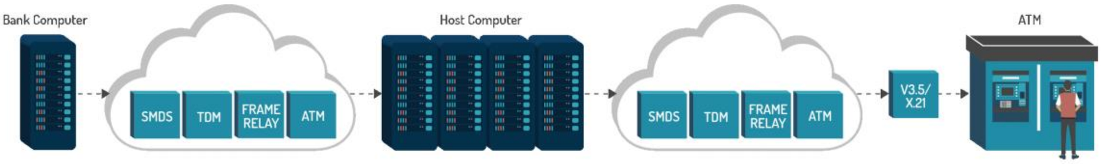


Figure 7. Banking – ATM Connectivity (Net2Edge, 2020)

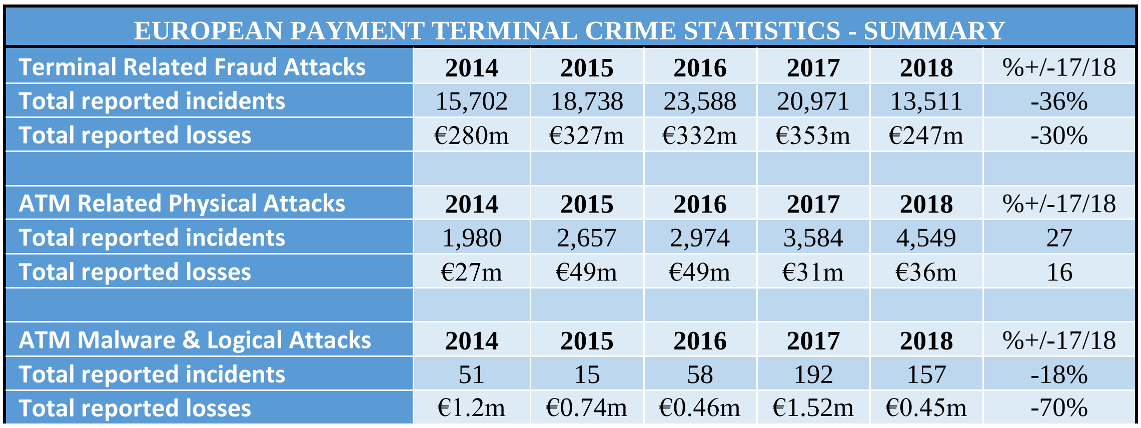
For some of the ATMs, analogue communications or V.35, data encryption is still in operation by using the 3DES algorithm, at a speed between 256 kb/s and 512kb / s. The Wireless ATM Network (WATM) can be viewed as a wireless extension (Xinri, 1997) of the Integrated Services Digital Network (B-ISDN) initially designed to provide simultaneous transmission over physical media, which supports integrated data transmission (data, voice, video) with QoS guaranteed, data encryption is done using the AES algorithm or other accepted algorithms. QoS stands for Quality of Service and represents the ability of a network to provide quality services using Frame Relay, Asynchronous Transfer Mode, Ethernet or 802.1, SONET or IP routed technologies. Compliance with ISO 8583, eXtensions for Financial Services (CEN / XFS), standard promoted by the European Committee for Standardization for client-server architectures and other international standards for financial transactions, depending on manufacturers, technology used or support available from transmission of information, network connection and communication system of ATMs supports TCP / IP, Asymmetric Digital Subscriber Line (ADSL) - asymmetric DSL communication technology that allows, depending on transmission or reception, transfer rate between 16 Kbps – 9 Mbps, Systems Network Architecture (SNA) - protocol created by IBM for interconnection and Synchronous Data Link Control (SDLC) - communication protocol created for SNA and that supports multipoint connections, Tunneling Async Protocol Diebold TC500 that requires an IBM or Enterprise IOS feature set, X.25 - standard protocol package defined by International Telegraph and Telephone Consultative Committee (ITU-T) etc. Some of the dedicated service providers are NYCE, PULSE, PLUS, Cirrus, AFFN, Interac, STAR, LINK, MegaLink, BancNet (etc.), the models proposed by them being adopted by smaller providers.

The next step taken by criminals is identifying the vulnerabilities that can be exploited in the processing modules, on the communication path, etc. The experts who analyzed the viruses attacks against ATMs classified them in two mainly categories:

- attacks (with malware) on the physical level of the ATM;
- ATM network malware attacks.

The first category involves the manual installation of a malware via a USB device, CD / DVD or a Raspberry Pi connected to the ATM network cable, local or remote running of the virus, access to the special control menu, followed by issuing cash delivery orders to the ATM, which accordingly releases the cash through the cash dispenser, as can be seen in figure 8. The equipment generally referred to as "black box" is used to send orders directly to the cash dispenser.

Table 3. ATM Attacks in Europe (EAST, 2019)



EUROPEAN PAYMENT TERMINAL CRIME STATISTICS - SUMMARY						
Terminal Related Fraud Attacks	**2014**	**2015**	**2016**	**2017**	**2018**	%+/-17/18
Total reported incidents	15,702	18,738	23,588	20,971	13,511	-36%
Total reported losses	€280m	€327m	€332m	€353m	€247m	-30%
ATM Related Physical Attacks	**2014**	**2015**	**2016**	**2017**	**2018**	%+/-17/18
Total reported incidents	1,980	2,657	2,974	3,584	4,549	27
Total reported losses	€27m	€49m	€49m	€31m	€36m	16
ATM Malware & Logical Attacks	**2014**	**2015**	**2016**	**2017**	**2018**	%+/-17/18
Total reported incidents	51	15	58	192	157	-18%
Total reported losses	€1.2m	€0.74m	€0.46m	€1.52m	€0.45m	-70%

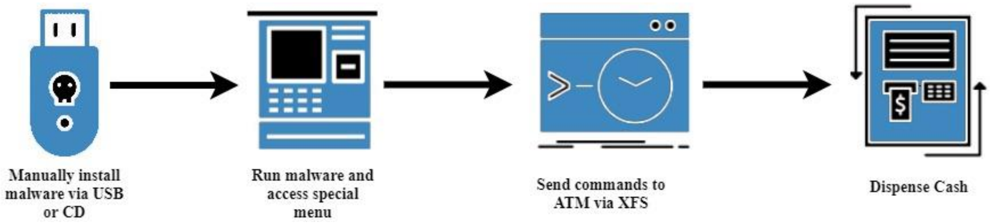

Manually install malware via USB or CD
Run malware and access special menu
Send commands to ATM via XFS
Dispense Cash

Figure 8. Physical ATM malware attack (Trend Micro & EC3, 2017)

One of the 2018 reports of the European Association for Secure Transactions (EAST) highlighted that during 2014–2018, the attacks at the physical level of the ATMs increased steadily. The report presented in table 3 reveals not only malware attacks, but also brute force attacks, explosive gas attacks or solid explosives attacks which reprsesent a serious concern. The figures did not take into account any collateral damage, which may in some cases exceed the value of cash. As with the Verizon report presented in figure 5, there should be considered several inadvertences generated by non-reporting of all registered losses by the banking institutions.

The second category involves, among others, infiltrating the network of the financial institution, a common method of phishing type exploiting the infection vectors through the emails sent to bank employees. Once infiltrated into the bank's network the attackers try to move laterally, identify the network to which the ATMs are connected, monitor their activity and initiate the cash release orders when the safe is fed near maximum capacity, process presented in figure 9. The operation may target only one ATM or sub-network, which allows simultaneous debit from multiple devices. Normally, ATM networks should be completely isolated from other networks, with separate routing/firewalls and specific protection systems. The degree of exposure when using a common network is directly proportional to the degree of accessibility on the part of the hackers, registering losses that can be neglected. Advanced Persistent Threat (APT) attacks are defined as strong attacks sustained by companies with special resources or even by states. APT-type Anunak/ Carbanak attacks against financial institutions, but not limited to them, attacks carried out by the group known as Cobalt and aimed targets in the European Union and Asia, Ripper or ATMitch attacks, named after the type of malware identified, have been carried out for several years and have proven that the position of administrator can be assumed and exploited for illegal purpose. Malware strains created in Eastern Europe were exported to Latin America. Some of them have been customized to hide the source code and disturb / distort the traceability.

Although, in theory it may seem easier for the attackers to intercept the ATM's communication with the financial institution and to manipulate the operation of the ATM from that access point, in practice the procedure is quite difficult, the communication being encrypted. Therefore, criminals prefer to launch direct attacks on devices or take control of the administration centers, as mentioned above.

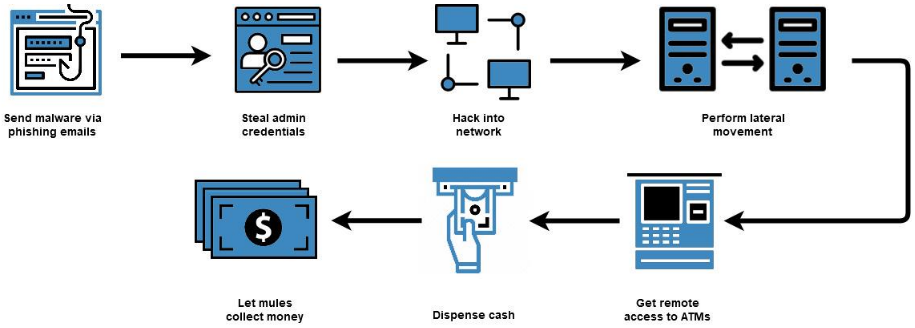


Figure 9. Network ATM malware attack (Trend Micro & EC3, 2017)

In a similar manner, attacks against PoS networks are being carried out. Malware infection (e.g. RAT Trojan) is facilitated by outdated technology, patch updates, non-implementation of recommended security solutions (e.g. Tokenization, EMV Chip, QRcode, Point-to-Point Encryption etc.) and especially non-compliance with the Payment Card Industry Data Security Standard (PCI DSS), created as a set of rules for protecting card holders and payment transactions insurances. Card data collected as a result of website infection (e-commerce), malware injection and web skimming (etc.), can be processed and used later for cash withdrawals from ATMs or payments to PoS- hate. Similarly, data collected as a result of infecting PoS networks can be further processed and used in fraudulent online transactions. Millions of records, hundreds of terabytes are collected annually, processed, exploited or sold on the dark market/dark web. Concentrated attacks are becoming particularly complex and difficult to counteract by national/international organisations in a timely manner without recording material losses, in the absence of the support provided by private companies specialized in the field. In the newly created context, reporting of Indicators of Compromise (ICO) and compliance with issuer recommendations become essential (VISA, 2019).

3.2. Ransomware Attacks

In-depth specialized studies have been published containing detailed explanations of how different malware classes are performing and the specific countermeasures to be taken, but the cyber-attacks draw attention to the need of implementing security policies that include a chapter of encryption for stored data and for the information transported through media transfer operations. The means of transmitting satellite information can become a casualty with the same ease as those commonly used in the event that the information transmitted is not strongly encrypted. Taking over the traffic control can lead to disruptions in the functioning of some national/international infrastructures, stopping or completely destroying them (NCSC, 2018).

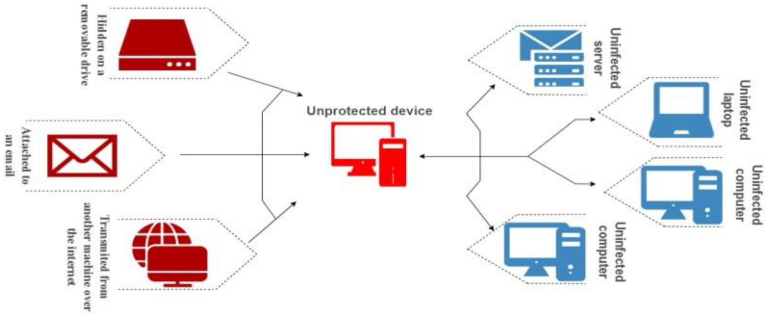


Figure 10. Ransomware penetration (Backup Assist, 2020)

By the end of 2019, millions of different strains of malware have been identified and their number is increasing compared to previous years, even though some of them were isolated, analyzed, blocked and the criminal groups arrested. A particular filiation is represented by ransomware, with varying structures in terms of complexity, and using advanced tactics to circumvent security policies. Depending on the design, it disables the restore function of the operating system (e.g. delete or encrypt the backups) thus preventing the restore to an earlier unencrypted version, the virus may be present even after the devices are restarted. Some of the propagation modes are relatively common, through spam files, infected USB drives or unsecured Internet connections, as seen in figure 10, with the same result of unavailability of data, files and blocking access to (how much) more resources.

The ransomware that uses symmetrical encryption will generate a key on the subject's computer and send it to the attacker before starting file encryption. The advantage of symmetric encryption is supported by a much higher speed than the asymmetric one, usually using unique keys with the length of 256 bits. The level of performance is imposed by each attacker and becomes essential in achieving the goal. Even if it is considered to be weaker, symmetric encryption allows more files to be encrypted than asymmetric encryption at the same time, but the likelihood that the information can be retrieved under certain conditions, with the support of specialized companies, is higher. In contrast, asymmetric encryption is much more demanding and makes it almost impossible to restore data in the absence of the encryption/decryption key or algorithm identification.

4. Conclusions and Proposals

Confidentiality and security become synonymous, overlapping or inclusive. In the case of banking institutions, the financial losses can be directly proportional to those in the image, the relationship being biunique. Sessions hijacking, identity or credentials theft, just to name a few of the vulnerabilities, have a long-term impact on the trust of customers and investors.

The specialized literature abounds in well-constructed guides with applicability for different fields (e.g. NIST 800-40 (Souppaya & Scarfone, 2013), NIST 800-61 (Cichonski, et al., 2012) etc.). Without limiting to these, we also recommend some common sense measures that can prevent computer attacks, actions in accordance with international standards: education and information, implementation of a zero-trust policy, updating software and software systems,operation, installation of a consecrated/licensed antimalware/antivirus version, regular backup, network segmentation, network traffic monitoring, use of search engines with warning items related to the level of trust of the accessed sites, updating indicators of compromise, reporting (without abusing) all incidents / suspicions relevant to the ability organizations (in the case of Romania: CERT-RO, Cyberint etc.), in order to be able to take preventive measures or to limit the losses. Each institution must adapt its general plans to its own needs. Like other organizations, the Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security, offers a model on which the operating framework can be built on and customized (FEMA, 2014). Regular saving and making copies, encryption of stored information and those transmitted in the media are conditions required for a correct management of the data. Ensuring an adequate degree of resilience involves a plan for saving and restoring sensitive data, which always begins with risk assessment and business impact, and in addition to the back-up and post-disaster procedures, the set of documents must include communication procedures, guides on response strategies, etc. Each plan must be reviewed, as new vulnerabilities arise and must be addressed.

Acknowledgements

Mircea Constantin Șcheau, Călin Mihail Rangu and Cătălin Udroiu have equally contributed to this research. Authors discussed the results and contributed to the final version of the manuscript. The study expresses the opinions of the authors and does not reflect the official position or opinions of their institutions, University of Craiova, Financial Supervisory Authority or Integrisoft Solutions. The authors declare no conflict of interest.

This work is supported by the grant POCU 380/6/13/123990, co-financed by the European Social Fund within the Sectorial Operational Program Human Capital 2014-2020.

BIBLIOGRAPHY

1. Baker, K.A. (1999). Diffie-Hellman key exchange, <https://www.math.ucla.edu/~baker/40/handouts/rev_DH/node1.html#SECTION00100000000000000000>.
2. Backup Assist. (2020). <https://www.backupassist.com/blog/ransomware-protection-guide>.
3. Barrett, D. J., Silverman, R. E., Byrnes, R. G. (2009). *SSH, The Secure Shell: The Definitive Guide*, ISBN - 10: 0596008953, ISBN-13: 978-0596008956, O'Reilly Media, Inc., 2nd Edition.
4. CGI Group Inc. (2004). *Public Key Encryption and Digital Signature: How do they work?*, White paper, <https://www.yumpu.com/en/document/read/11531495/public-key-encryption-and-digital-signature-how-do-they-work-cgi>.
5. Cichonski, P., Millar, T., Grance, T., Scarfone, M. (2012). *Computer Security Incident Handling Guide,* NIST: National Institute of Standards and Technology, Special Publication 800-61, Revision 3, US Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
6. Computer Security Resource Center (2013). *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, <https://csrc.nist.gov/publications/detail/fips/186/4/final>.
7. European Association for Secure Transactions. (2019). *ATM Physical Attacks in Europe on the increase*, European Payment Terminal Crime Report, <https://www.association-secure-transactions.eu/atm-physical-attacks-in-europe-on-the-increase/>.
8. Farion, A., Panasyuk, V. (2018). *Cybercrimes, Cyber Law and Computer Programs for Security*, Advanced Computer Information Technologies, <http://ceur-ws.org/Vol-2300/Paper64.pdf>.
9. Federal Emergency Management Agency (2014). *FEMA Cadre Management Guide*, Department of Homeland Security, <https://www.fema.gov/media-library/assets/documents/185855 and https://www.fema.gov/media-library-data/1581102210880-fdf5972a71d36e1b0b9a5fabad7c7bd7/FEMA_Cadre_Management_ Guide1.pdf>.
10. Goodin, D. (2020). *PGP keys, software security, and much more threatened by new SHA1 exploit*, Ars Technica, Wired Media Group, <https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/information-technology/2020/01/pgp-keys-software-security-and-much-more-threatened-by-new-sha1-exploit/?amp=1>.
11. Grah, J.S. (2008). *Hash Functions in Cryptography*, University of Bergen.
12. Hamilton, G. CA642: *Cryptography and Number Theory*, modul course, School of Computing, Dublin City University.
13. Hardjono, T., Dondeti, L.R. (2005). *Security In Wireless Lans and Mans*, Volume, ISBN 10: 1580537553, ISBN 13: 9781580537551, Artech House Publishers.
14. Mehmood, A. (2017). *Differences between Hash functions, Symmetric & Asymmetric Algorithms*, Cryptomathic, <https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms>.
15. Microsoft Support (2018). *Description of Symmetric and Asymmetric Encryption*, Microsoft, <https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption>.
16. Milanov, E. (2009). *The RSA Algorithm*, pp. 1-11.
17. National Cyber Security Center (2018). *Turla group malware*, TLP White, N<https://www.ncsc.gov.uk/news/turla-group-malware>.
18. Net2Edge (2020). *Banking – ATM*, <https://net2edge.com/solutions/banking-atm/>.

19. Payment Security Support Group (2017). *Guidelines on cryptographic algorithms usage and key management - EPC342-08*, Version 7.0, European Payments Council.

20. Positive Technologies (2018). *ATM Logic Attacks: Scenarios*, <https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ATM-Vulnerabilities-2018-eng.pdf>.

21. Rescorla, E. (2001). *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley.

22. Revuelto, V., Socha, K. (2016). *Weaknesses in Diffie-Hellman Key Exchange Protocol*, CERT-EU, Security Whitepaper 16-002, <https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_16-002_Weaknesses%20in%20Diffie-Hellman%20Key%20v1_0.pdf>.

23. Riman, C., Abi-Char, P. E. (2015). *Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey*. Information Security and Computer Fraud, 3(1), 1-7.

24. Saxena A. K., Bhandari V., Hasan A., Sinha S. K., Shukla P. (2018). *Design and Development of Symmetric Cipher*, Proceedings of International Conference on Recent Advancement on Computer and Communication. Vol. 34. Print ISBN 978-981-10-8197-2, Online ISBN 978-981-10-8198-9. Springer, Singapore. DOI <https://doi.org/10.1007/978-981-10-8198-9_6>.

25. Sindhu, S., Sindhu, D. (2017). *Cryptographic Algorithms: Applications in Network Security*, International Journal of New Innovations in Engineering and Technology, ISSN: 2319-6319, Volume 7 Issue 1, <https://pdfs.semanticscholar.org/86be/e1b8479a695e390f7b50f91c26ec72c33d81.pdf?_ga=2.163359036.1668002088.1581074390-1689420595.1581074390>.

26. Souppaya, M., Scarfone, K. (2013). *Creating a Patch and Vulnerability Management Program*, NIST: National Institute of Standards and Technology, Special Publication 800-40, Revision 3, US Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>.

27. SSH Academy (2020). *SSH Protocol*, SSH Communications Security, Inc. <https://www.ssh.com/ssh/protocol>.

28. Stefanovskyi, O. (2019). *How to keep passwords safe using PBKDF2 hashing algorithm in Java*, Medium Corporation, https://medium.com/@stefanovskyi/how-to-keep-passwords-safe-using-pbkdf2-f23700710ec3.

29. Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y., Bianco, A.P., Baisse, C. (2017). *Announcing the first SHA1 collision, Google Security Blog*, <https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>.

30. Traxcom Technologies LLC (2019). *The Basics of SSL for IP Financial Transactions*, P/N: SSLWhitePaper-2010-500, <http://download1.newnet.com/docs/1467.pdf>.

31. Trend Micro Forward-Looking Threat Research (FTR) Team and Europol's European Cybercrime Centre (EC3) (2017). *Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types*, A TrendLabs Research Paper and Europol Report, <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf> and <https://www.europol.europa.eu/publications-documents/cashing-in-atm-malware>.

32. Verizon (2018). *2018 Data Breach Investigations Report*, 11th edition, Research report, <https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf>.

33. VISA (2019). *What To Do If Compromised, Visa Supplemental Requirements, Version 6.0*, <https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>.

34. Xinri, C. (1997). *Wireless ATM - An Overview*, Computer Science & Engineering, Mckelvey School of engineering, Washington University in St. Louis, <https://www.cse.wustl.edu/~jain/cis788-97/ftp/wireless_atm/index.html>.

35. Ylonen, T., Turner, P., Scarfone, K., Souppaya, M. (2015). *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*, National Institute of Standards and Technology Internal Report 7966, U.S. Department of Commerce, <http://dx.doi.org/10.6028/NIST.IR.7966>.

36. Young, B. *Lecture 44: Symmetric vs. Asymmetric Encryption*, Foundations of Computer Security, University of Texas at Austin.

37. Zhang, F. (2008). CSC 5991 Cyber Security Practice, Wayne State University.

Mircea-Constantin ȘCHEAU is PhD in Public Order and National Security with a theme of interest for the economic and security domains *"Cybercrime regarding Financial Transfers"*. Author and coauthor of three books, more than twenty scientific articles in the fields of management, economy, law enforcement, defense, critical infrastructures, information technology and lector for many international conferences.

Călin Mihail RANGU is acting as Director in Romanian Financial Supervision Authority (FSA). He is President of the Institute of Financial Studies, Vice-president of EIOPA InsurTech Task Force, President of FSA Shareholder Group in Consumer Protection, Board Member of EFICERT, Coordinator of Fintech HUB of FSA. He has a broad experience in management, banking, operational risks, IT security, consumer experience, IT and financial services, products and technologies. Călin is double licensed in economics and engineering, PhD in neural networks applied in financial series processing, MBA graduate in banking and finance, University Lector, MBA Lector. He acted over 13 years as director in National Bank of Romania and Raiffeisen Bank, and general director of Romanian subsidiary of Raiffeisen Informatik Austria Group. He published over 150 articles, and two books, being organizer or speaker in major Romanian conferences related to financial and banking sectors, consumer protection, ADR, IT, cyber-fares, operational risk management, or management and processes.

Cătălin UDROIU is a DevOps and Security Specialist, with a Master's degree in Business Information Systems. In the past 10 years had worked on multi-level support for various clients around the world, with expertise on Windows and Linux field, assisted teams, and implemented different continuous integration workflows of the organization.