Cross border Interbank Payment System (CIPS) Security Supplements; Tangible Radio Safety Box, Software as non-textual Password and Revolving Executable Code Modules

A. D. ZISOPOULOS[1], K. G. PANITSIDIS[2], G. K. BRONI[1], N. D. KARTALIS[1]
[1]Department of International and European Economic Studies,
University of Western Macedonia,
Kila University Campus, Kozani 50100,
GREECE

[2]Department of Management Science and Technology,
Faculty of Economics,
University of Western Macedonia,
Kila University Campus, Kozani 50100,
GREECE

Abstract: Our research started a long ago as additional security for the asset owner to facilitate CIPS (Cross-border Interbank Payment System) holistic security. Minor corrections were proposed, like an e-mail with a new domain for every transaction, Ping services in a VPN environment, and mirroring avoidance. Our primary approach was to fight internal fraud and hacking threats. Apart from these known vulnerabilities indemnification, we propose three specific security supplements. A shortwave activated latch inside a local safe box and Thales interconnector for a tangible bank security system. The asset owner unlocks his funds as digital money or tangible items like gold through radio communications SDR (Software Defined Radio). Second is the cornerstone of our civilization, the computer-executable avoiding all methods for non-textual passwords. Our last development is a GitHub antipode Software authoring anonymous system. According to our plan, the Internet-based banking system software has separated intercommunicating subroutines. All subroutines are assigned to various programmers for independent implementation, avoiding the internal hacker without the need to find him. For example, a system software written by splitting it into 12 subroutines assigned to 12 programmers working on subroutines has a probability of the thirteenth order of magnitude.

Key-Words: Internal Fraud, Inside hacking, Software authoring, Cross-border Interbank Payment System, Quantum Financial System, GitHub, Assembler code, Radio TeleType

Received: October 18, 2022. Revised: November 4, 2022. Accepted: November 17, 2022. Available online: December 14, 2022.

1 Introduction

The high level of digitalization in our times brought us to the point that all aspects of life must be based on an e-enabled system. All development plans, along with Humanitarian actions and monetary issues, are based on computer and network security in a strategic economic environment, [18], [21].

But passing through their midst, he went away. This Luke (4:30), Lemma describes essential operations' defense and security axiom: "Hide away your innermost thoughts and existence." The Bible lemma, although it started as military policy, it applies very adaptively to the current asymmetric war business environment, [14].

Internal Fraud-Hacking represents more than 90% of International Economic Fraud. The primary assignment during the 2008 international debt crisis for BIS (Bank of International Settlements) was the isolation of risk in the banking sector. We readjusted the same isolation to secure assets, gold, and money, [28]. Edward Snowden committed typical internal fraud by hacking the US government at the highest internal level. But, unfortunately, it seems that banking has higher standards. From internal fraud incidents, according to FED, the most relevant are: Forgery, Account take-over / impersonation, and Insider trading. Nothing from these concerns is internal hacking, but it lies inside there.

Introducing our research, we present a payment analysis of the first demo Quantum Financial System payment and three security solutions:

1. CIPS (Cross-border Interbank Payment System) is the first payment security aspect.
2. Tangible security protection for all bank systems
3. Executable subroutine as a non-textual password.

4. GitHub antipode Software authoring anonymous system

2 CIPS – QFS Online Security

Cross-border Interbank Payment System (CIPS) based on investment assets located at Quantum Financial System (QFS) is the most recent implementation of network-based payments and asset interchange, [5], [30], [32]. As a new system, it uses all existing advanced technologies. Therefore, it is ready for any advances over the following years like Exascale, [23] and StarLink, [16], long after the USA president started a similar initiative also older, [20] and fresh new, [4].

2.1 Procedures for Beneficiaries of QFS Funds

To transfer 5,000 USTN (United States Treasury Notes) via QFS, various authors have given similar descriptions, [25], [27]. All Procedures described here are for first-time Beneficiaries of QFS Funds. The analysis procedure is straightforward. First, we select the exact phrasing for money transfer procedures described in the operations manual. Then, the derived security issues are headlined, revealed, or even solved through our research.

Money Transfer and improvements. There are six Procedures for Beneficiaries of QFS security issues to be examined:

1. Receive e-Notice.
2. Connect to QFS.
3. Confirm Identity.
4. Create a Security ID.
5. Accept USD Transfer.
6. Transfer USN/USTN.

2.1.1 Receive e-Notice QFS SYS

Procedures to solve under the QFS system with a simple e-mail system are:

- You receive an e-mail notifying you that you have received
- a transfer of a USTN asset-backed currency
- fully available to you via the Quantum Financial System

2.1.2 Connect to QFS

Procedures to be solved with ping-web techniques:

- The QFS already knows who you are, as they have pinged
- your bank account
- based on the account details provided in the payment order.
- You connect to QFS based on a URL link in step 1 above.

2.1.3 Confirm Identity

There is a 3step process to confirm you are the legitimate beneficiary having ping and e-mail vulnerabilities:

1. Your bank account pinged;
2. You get a one-time code via e-mail
3. You confirm the code received. Successful Ping.

2.1.4 Create Security ID

These types of problems are solved with a non-textual password and TANGIBLE schema:

- Once the ”Ping” confirms your regular bank account has been.
- Successfully verified and authenticated
- you will prompt to enter your secret code
- to confirm the opening of a mirror QFS account.

2.1.5 Accept USD Transfer

These steps are internal to QFS; therefore, any security hole solved inside the system:

- Your newly opened SECRET, SECURE PERSONAL account
- credited with the amount of USN or USTNs received.
- Your account is now fully operational and available to you
- for transfers of funds to 3rd party beneficiaries.

2.1.6 6=Transfer USN/USTN

The last step is the linkage procedure, which is helpful for all customized software.

- From the ”Sending” Screen, you may transfer Transfers can be in any currency
- and instantly converted at pre-set rates of exchange
- and funds are immediately available to the beneficiary
- which uses the same process to receive funds [steps 01 to 06]

2.2 Security Improvement Headlines

The above six steps five thousand dollars demo transaction faces initially by design simple security issues like e-mail, ping, and mirroring

E- mail comes from the dawn of the computer age and has served us along many incidences all these years. Even in the simplest form, e-mail is vulnerable, [33]. In CIPS’s case, all these QFS-generated e-mails would represent a severe security hole. Since e-mail protocol is a rigid standard only minor frontend processing is possible. An indicative solution for such a severe problem is a new domain

for every mail. The automatization level of the business environment and ICANN's recent regulations released DNS from the monopolies, [19]. Solutions are:

- Every e-mail in the funds' transfer procedure (steps 1-3) is addressed with an instantly created domain name.
- Every e-mail embedded inside an FTP service.
- A new protocol email-liked, especially for funds transfer.

Ping is secured in a private network but in the open net, and suffers from all internal and external hacker threats, [9], [10]. We believe the word "ping" has nothing to do with the classic internet pinging application. Instead, it concerns a new and redesigned protocol and application without unnecessary information wandering around the global Internet, [11].

Mirroring is used heavily in the early days of land and cellphone spying. Secret services hear and record personal conversations through telephone mirroring. We keep much effort into keeping the main servers operational but mirroring adds unnecessary effort. For the sample transaction of 5000 USTN, three solutions serve the payment credibility:

1. A complete tangible solution for fund access
2. along with a physical gold repository long-distance latch.
3. An executable or object file provided by the asset owner as a non-textual password
4. An authoring system with programming modules from different programmers revolving during execution.

3 Tangible Security for Cross border Interbank Payment System (CIPS)

Last year's research, during the Covid-19 pandemic, previous year's study found all pathogenic of existing cryptocurrencies and CBDC (Central Bank Digital Currencies), [1], with public blockchain and various privacy and privacy security issues. Rule-based expert system is on one side of system security, [3], while in the exact opposite direction is our tangible methodology. However, we believe that with one step back and two ahead, we forward home-land primitive security in its roots and a step ahead of the attacker.

Our general approach is to access the funds or the safety boxes far away from internet fraud and insider hacking. Our conceptual method lies in figure 1. First, the owner of the assets activates, 12 thousand kilometers away, the gate of his treasure box from Los Angeles to Tel-Aviv through direct transmitting in short waves in our application. The steps for this operation are presented in figure 2:

Fig. 1: Safer banking order from LA to Israel, 12000 km without internet scam

1. Origination of computer system
2. Amateur radio USB interface, [17], [22].
3. Direct Sampling Shortwave Radio, [29].
4. Transmission Short wave aerial
5. Receiver Antenna
6. SDR for RATT (Software Defined Radio, Radio Automatic Teletype), [7].
7. Fanless mini pc industrial computer
8. (e latch safe box for gold repository), [30].
9. SafeNet eToken from Thales, [24].
10. Core Exascale data center, [15].

The interoperability of the system flows in sequential flow in short pathways. In a simple computer system,
(1) the funds or money owner keys in the order in "cold storage mode," which does not connect to anything. Encryption, in this case, is combined with the data. The computer data feed an Amateur radio USB interface (2) for preprocessing and a standard ICOMtype Direct Sampling Shortwave Radio (3). Finally, the signal is transmitted to any shortwave band (3) and reaches the Receiver Antenna.

A computer program dominates this process. This vents the RF signals in time and space in a procedure much better than the military super standard of Random Frequency Hopped Spread-Spectrum, [6]. Internet bottlenecks rarely appeared in the last few years. Our advantage is that mil-spec voice systems run in real-time while we can operate a simple or complex "time shift" along the frequency (band) shift. The shortwave channel bands are minimal; compared to the Internet, we have the advantage of non-synchronous operation.

For example, the actual even Baudot character stream transmits a character now in band 31, during the next in shortwave band 70 on a second later in an epic time-space shift.

Fig. 2: The hardware for RTTY secure banking over the air of short waves

The transmitted RF data, after perception, are converted to computer data. Then, the RF data guide through the SDR (6) to the destination industrial computer (7). Until today, no one has opened the electronic latch of a safe bank box without bank interception (8). In our application, the computer (7) drives the supercomputer data center (10) through a THALES additional security device(9).

A patent could ensure the whole system, but we prefer the rapid prototyping of a Research Magazine to the WIPO bureaucracy for reasons like:

- Three years until patent protection is much time, and the competition could easily violate our intellectual property.
- The immediate impact of a high-tech research magazine.
- Through the magazine, we are a step ahead to actualization outside industrial prototyping and product selling.

4 Object and Executable Files for Non-Textual Password Schema

The cornerstone of our civilization is the computer-executable file, containing appropriate CPU as running instructions. This file in assembler machine code generates after object linking the various ”semi-executable” files, like object files or shared library files. There are many options to create our password schemas, like runtime object-linking. Generally, this procedure is rare but not unique. Our research tries to prove that executing object files provided by the asset owner and embedded with authentication transactions is a more secure alternative to textual passwords. Network applications incorporate programming libraries in various operating environments:

- The Microsoft visual studio and Azure platform
- The Matlab Compiler shares programs as standalone applications and web apps.
- Python Standard Library.

Our approach is complementary to existing non-textual passwords techniques:

- Various biometric Authentication, fingerprint, face recognition, retina, and others do not solve the internal official hacker problem.
- Various biometric Authentication, fingerprint, face recognition, and retina do not solve the internal official hacker problem.
- the Negative Authentication Systems (NAS), [2], the approach lies more in goodwill than human criminality studies.
- Honeywords, Cracking-Resistant Passwords, Natural Language Encoders, Bloom Filter, and Graphical Passwords are primitive consumer, not banking-oriented solutions.
- Multi-factor Authentication adds an unnecessary step to the process. In the same sense, in the previous tangible chapter, very quickly, we can add a lead with a web camera reporting continuously ”24/7/365” the gate’s opening.
- various non-textual passwords issued by police authorities suffer from bureaucracy and acceptability from the owner of the funds. The operation starts when the fund owner prepares and verifies on his computer an object file with unlimited imagination alternative security options:
- Connect to various public or private URLs.
- Calculations based on universal tempo spatial data (like the sunrise exact astronomical time in a different city for every other day or during the day)
- written to confuse reverse-engineering with unlimited dissemination of deceitful information actions.

The file runs locally, and we keep all test data as a guide to accessing our funds in the bank. The file is sent to the bank, which saves it in cold storage. The remote Data Processing facility receives the file and incorporates it into its security system. The ”object” runs through the Internet in a variety of options. The procedure ends by giving full (or partial) access to digital assets.

4.1 The Hackers' Paradise

An executable file inside a server generates problems in any data center, representing a nightmare for the system administrator. Unfortunately, the security strategy is a lonesome task. So far, it has yet to be found any technical or scientific proposal or implementation for using executable code as a non-textual password. But this is not an academic exercise. This is an everyday undeclared war. So we investigated many solutions.
The ”object” file is linked and executed by the user in a separate ”consumable” pseudo server as the first stage of Multi-Factor Authentication. The functionality of such a semi-automatic procedure is as follows:

- Is uncrackable compared to limited 1028*28-bit textual security.
- The main army of malicious attacks covers the actual entry points.
- We avoid a whole stack of security services providers that, by definition, are a point of internal hacking actions.

4.2 Thales Authentication Tokens and FIDO Devices:

Thales is a defense giant with a range of electronics and communications. For example, the SafeNet eToken FIDO is a USB token adapted to the (different altogether) CIPS security systems, [24]. It is used as extra security to avoid internal hacking in radio-TTY latch and subroutine authentication. Its features need alteration:

- Physical token is the SDR latch and safe box.
- PIN is the RTTY output and the subroutine output.
- Touching is not helpful today, but a remote touching device is on the way for WIPO.

5 Object and Executable Files for Non-Textual Password Schema

The cornerstone of our civilization, the computer-executable file, is the only one recognized by the CPU as running instructions. This file is in assembler machine code and generated after linking various ”semi-executable” files like object files or shared library files. There are many options to develop our password schema, like runtime linking. Generally, this procedure is rare but not unique. Our research tries to prove that executing object files provided by the asset owner and embedded with authentication transactions is a more secure alternative to textual passwords. Network applications incorporate programming libraries in various operating environments:

- The Microsoft visual studio and Azure platform
- The Matlab Compiler shares programs as standalone applications and web apps.
- Python Standard Library.

Our approach is complementary to existing non-textual passwords techniques:

- Various biometric Authentication, fingerprint, face recognition, retina, and others do not solve the internal official hacker problem.
- Various biometric Authentication, fingerprint, face recognition, retina, and others do not solve the internal official hacker problem.
- the Negative Authentication Systems (NAS), [8], the approach lies more in goodwill than human criminality studies.
- Honeywords, Cracking-Resistant Passwords, Natural Language Encoders, Bloom Filter, and Graphical Passwords are primitive consumer, not banking-oriented solutions.
- Multi-factor Authentication adds an unnecessary step to the process. In the same sense, very quickly in the previous tangible chapter, we can add a lead with a web camera reporting continuously ”24/7/365” any gate opening.
- various non-textual passwords issued by police authorities suffer from bureaucracy and acceptability from the owner of the funds.

The operation starts when the fund owner prepares and verifies on his computer an object file with unlimited imagination alternative security options:

- Connect to various public or private URLs.
- Calculations based on universal tempo spatial data (like the sunrise exact astronomical time in a different city for every other day or during the day)
- written to confuse reverse-engineering with unlimited dissemination of deceitful information actions.

The executable file is verified locally for errors. All relevant test data are kept as a guide to access our funds in the bank. The file is sent to the bank, and we save it in cold storage. The remote Data Processing facility receives the file and incorporates

it into its security system. The ”object” runs through the Internet in a variety of options. Finally, the procedure ends by giving full (or partial) access to digital assets.

5.1 Hackers Paradise

An executable file inside a server generates problems in any data center, representing a nightmare for the system administrator. Unfortunately, the security strategy is a lonesome task, and so far, has yet to find any technical or scientific proposal or implementation for using executable code as a non-textual password. But this is not an academic exercise. This is an everyday undeclared war. So we investigated many solutions.

The ”object” file is linked and executed by the user in a separate ”consumable” pseudo server as the first stage of Multi-Factor Authentication. The functionality of such a semi-automatic procedure is as follows:

- is uncrackable compared to limited 1028*28-bit textual security.
- The actual entry point is covered by the main army of malicious attacks.
- We avoid a whole stack of security services providers that, by definition, are a point of internal hacking actions.

5.2 Thales Authentication Tokens and FIDO Devices

Thales is a defense giant with a range of electronics and communications. For example, the SafeNet eToken FIDO is a USB token adapted to the (different altogether) CIPS security systems, [24]. It is used as extra security to avoid internal hacking in radio-TTYlatch and subroutine authentication. Its features need alteration:

- Physical token is the SDR latch and safe box.
- PIN is the RTTY output and the subroutine output.
- Touching is not useful today, but a remote touching device is on the way for WIPO.

6 Secure Software Authoring with Anonymous Code Routing

The last presented method would apply to any critical software close to military standards. CIPS software protects severe world assets, and protection must be at the appropriate highest level, [30], [31]. The method with the acronym “SSAACR” is more of a software engineering tool with complex specifications and benefits not only in system security.

6.1 Software Internal Hacker

Authoring a complicated piece of software has various weak points and security holes concerning human behavior options concerning only personnel:

7. The upper management
8. The auditor team in the bank data center.
9. Various devices, cell phones, and Q-phones.
10. Huge data centers, Starlink satellites, and the main computer.
11. The software authoring team, unfortunately, has absolute control over program functionality.

World history teaches that Leonidas was once betrayed in Thermopylae by Ephialtes and Jesus Christ in Golgotha by Judas Iscariot. Therefore, we cannot avoid internal hackers. One method to minimize the internal fraud risk is to isolate the disinfected executable code without knowing its position in the code. The technique is simple. We split the executable code into interconnection modules and assigned every module to various programmers. The method originated from multiple sources, [12].

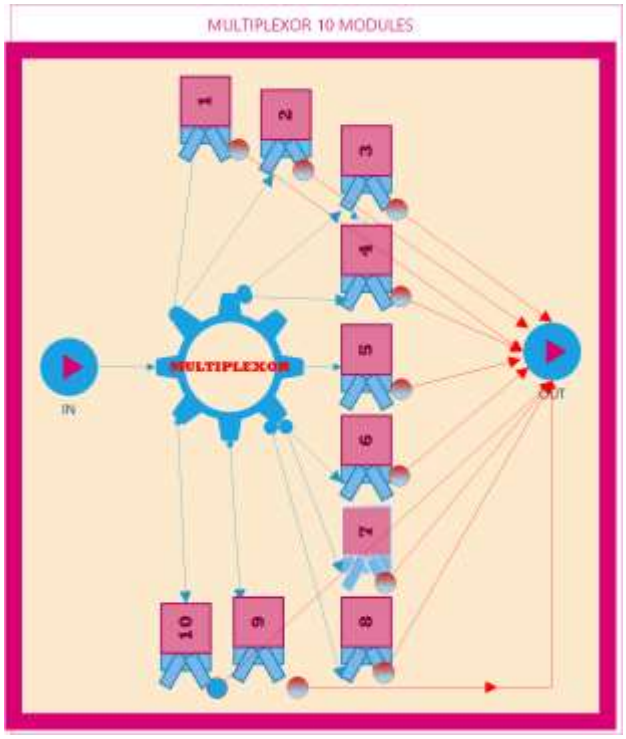

Fig. 3: Elemental multiplexor module with the same subroutine written by ten programmers

6.2 Authoring Multiplexor Elemental Module

Multiplexing is an advantageous technique in all types of engineering, [26]. Figure 3 is the heart of our methodology and has four types of elements:

12. An unique input point.
13. Rerouting logic to a random or specific

program module.

14. Programming entities with input and output data.
15. An unique output port

The input and unique output points are universal in programming until no pseudo-code Quantum languages benefit from Quantum Financial System and vice versa, [32]. According to a randomization algorithm, the ”eight teeth gear” in the center receives input data and passes them to one of the ten programming entities.

The boxes in figure 3 with in-out points are all together at the exact moment:

- Autonomous programming code in any computer language using object linking. Someone with more traditional skills could name it simply a subroutine).
- All ten subroutines share the same functionality, although in a very different programming implementation and own library usage. All ten functionalities concern only one task.
- Every box also represents an implementation team of analysts and programmers, either internal to the bank or an outsourcing company. In that sense, the single module is done ten times by ten teams.

Different programmers and companies write all the modules for security reasons. The method was criticized heavily by the industry at a conference. In an Academic environment, researchers do not accept that a subroutine passes only arguments and no other ”hacking info.” Hackers have different behavior than professional programmers. Indicatively a few ways to pass information hidden inside arguments could be:

1. After the insignificant fifth decimal point.
2. A hashing function based on various text operations.
3. Insignificant indirect addressing URL access.
4. Time-date-spatial combinations.

These are only the beginning. Suddenly, the whole dark web would start authoring ”money-order” routines, seeking a needle in a haystack.

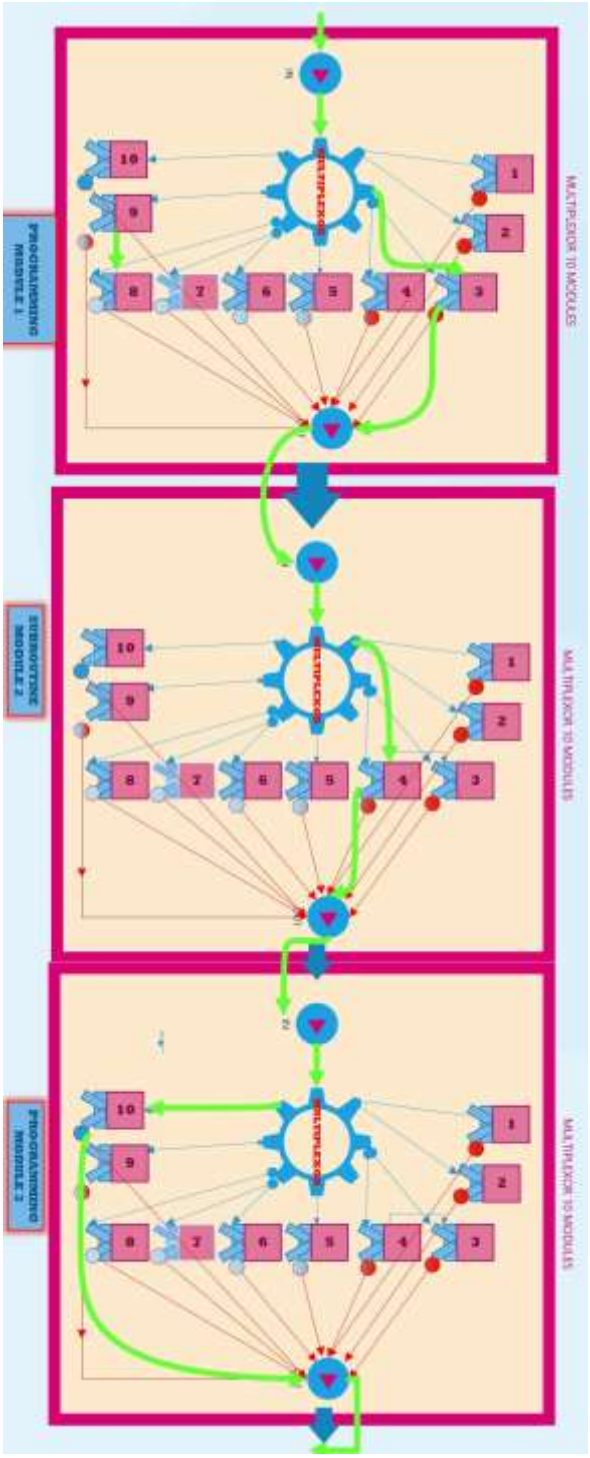

Fig. 4: A three-stage multiplexor for a program with three tasks, each written by ten different companies

6.3 Three-Stagetage Multiplexor Example

The beta test production system based on the Elemental Multiplexor (figure 3) connected in various multidimensional connection types expanding in space and time. To keep things in non-chaotic explanatory balance, a simple machine prepared with the following features:

16. The single starting point on top.
17. Elemental Module ONE.

18. Elemental Module TWO.
19. Elemental module THREE.
20. The final exit point on the bottom.

The machine has three functions. Ten different programming teams prepared all these. All interconnections are displayed in diagram 4.

6.4 Multiplexor Module Interoperatability Example

The story starts in the bank software department, QFS in this case, but the procedure adapts to any software authoring team. The bank defines three basic modules with functionality:

21. The e-bank authenticates the user through any known (or unknown above) methodology and passes the authenticated date to Module TWO.
22. The module reads from module ONE all data. Then, the current module passes the user a menu of actions along with input from the user and IBAN to the next module.
23. The last module, THREE, executes a traditional "Send-order()", [13], function to bank assets.

The running example in figure 4 shows the procedure flow. The steps are:

1. Main entry point.
2. The router algorithmically sends the control to programmer Three:
3. The code for module ONE, as written by the third programmers' team, is executed.
4. Flow goes to subroutine-module TWO
5. Router sends the control to programmer Four.
6. Module TWO, written by programmer Four is executed,
7. Flow goes to module THREE,
8. Router sends the control to programmer Ten,
9. Module THREE, written by programmer Ten, is executed finally,
10. Program terminates.

6.5 Methodology Mathematics and Statistics Analysis

Different mathematical methodologies prove that increasing the programming modules is several orders of magnitude better than increasing the number of programmers.

The modules in a System software cannot be unlimited due to design and practical obstacles. Also, the programming team has limits like cost and functionality arguments:

- The number of programmers (p1,1p2, p3.. p12)
- The number of programming modules (m1,m2, m3,.., m12)

6.5.1 Permutation Table

There are many ways to select implementation programmers or programming teams and modules.

Modules / Programmers	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	64	128	256	512	1024	2048	4096
3	3	9	27	81	243	729	2187	6561	19683	59049	177147	531441
4	4	16	64	256	1024	4096	16384	65536	262144	1048576	4194304	16777216
5	5	25	125	625	3125	15625	78125	390625	1953125	9765625	48828125	244140625
6	6	36	216	1296	7776	46656	279936	1679616	10077696	60466176	362797056	2176782336
7	7	49	343	2401	16807	117649	823543	5764801	40353607	282475249	1977326743	13841287201
8	8	64	512	4096	32768	262144	2097152	16777216	134217728	1073741824	8589934592	68719476736
9	9	81	729	6561	59049	531441	4782969	43046721	387420489	3486784401	31381059609	282429536481
10	10	100	1000	10000	100000	1000000	10000000	100000000	1000000000	10000000000	100000000000	1000000000000
11	11	121	1331	14641	161051	1771561	19487171	214358881	2357947691	25937424601	285311670611	3138428376721
12	12	144	1728	20736	248832	2985984	35831808	429981696	5159780352	61917364224	743008370688	8916100448256

Fig. 5: Probability Table

Figure 5 concerns a "Permutations Table" of 12 Programmers authoring the 12 different Modules subroutines of a complex computer program. The table is simple and presents the various options for the executable programming path. The number is moderate in mathematics (8,916,100,448,256) but impressive in linguistics "eight trillion nine hundred sixteen billion one hundred million four hundred forty-eight thousand two hundred fifty-six."

6.5.2 "SSAACR" Multidimensional Analysis and Visualization

The above simplification with 12 programmers writing twelve modules are only a presentation simplification. The "SSAACR" system is under beta testing with much more complexity expected. Differences in the production system are:

1. Every module could be split into another three, the basic, the first half, and the second half; implementing the principle, and nobody knows how many modules exist.
2. The 12 programmers writing 12 modules concepts for every programmer could have an integrated idea of the whole system.
3. Every successful bank transaction gives credits to programmers and modules.
4. Every night shift during idle system time repeats several times the daily load.

A mathematical solution to the above design is the multidimensional construction of module intercommunication. During analysis, there was the need to visualize the system to decide the desired security level. This visualization is the different module routing. We try to reduce features from 49 dimensions to one and two dimensions and

visualize them (maybe existing overfitting to our results and have to try other techniques like:

- Classification Dataset
- Principal Component Analysis (PCA)
- Singular Value Decomposition
- Linear Discriminant Analysis
- Isomap Embedding
- Locally Linear Embedding
- Modified Locally Linear Embedding
- SNE Plots
- Heatmaps
- Multidimensional Scaling (MDS).

Our goal was to find clusters among them. All preliminary work is presented in a dataset but exceeds and overrides the presentation purposes of this chapter. All three methods' scientific level override the basic concept of "Bank Transactions Security."

6.6 "SSAACR" Future and Problems

Security systems' priority is exactly confidence and silence. Nobody would know how the software wrote initially, possible patches, and failures. "SSAACR" prepared for big with a lot of "extra-Galactic" actualization problems:

- The software development cost is sky-rocketed, minimizing the benefit/cost ratio.
- The authoring software project must concern only banking and military applications.
- A perpetual repeat running on night's shift is not always possible or efficient
- There are more computer languages and systems than the software industry could ever accept.
- The simplicity of the methodology is a problem, but it also denotes a strong secrecy point.
- "SSAACR" needs further development through Data Science guidelines.

7 Discussion

One step backward, two steps ahead are necessary sometimes after physical sequence disruption. This one-century step back to "Baudot" teletypes is temporary only when internet security complies with human beings' standards. Primarily Baudot represents an engineering exaggeration for exceptional cases and security standards alteration.

Triggering through short waves but automation and teleoperation are only possible through the standard Internet. Semi-automatic and mixed technology systems are appropriate in high-end banking systems.

Insurance for law enforcement The three engineering solutions presented above are only sometimes the most efficient security solution. In typical cases, a small insurance premium covers any small-medium liabilities. The problem would be internal fraud from both sides, the bank and the beneficiary of the assets, since a third party, the reinsurance broker, pays the bill.

Legal expenses instead patent filing are used to bypass the hustle and cost of patent filing. As a general guideline until today, we acquired several invention patents through WIPO filing. Although this is crucial for the commercialization of our research today, we violated the general rule. The three specific developments here are eligible for invention patents.

1. Fast prototyping and market entry.
2. Penalties payment for violating another person's patent better due to long awaiting granting time.
3. Producing and distributing specialized products in an amateur base is more secure since no advertisement leakages or general information.

Intellectual Property exploitation is a complicated task in our patent troll days. Scientists and inventors have various alternatives to commercialize their work. New trends in intellectual property are:

1. The standard WIPO patent.
2. Implementation under secrecy and profit comes from personal or company consultancy.
3. In some countries, they only accept patents with three-dimensional nature.
4. Military Patents have no protection.

Serious Problematization started for realizing non-textual password authentication. The solution is to use the revolving module's schema as described in the next chapter. Also, the revolving modules authoring methodology could execute the crucial modules twice or more to achieve the highest security. In such programming, the probability is close to infinitive.

Payment repetition is repeated all over again during idle system periods. The action is necessary due to transaction differences—every module process the same data and outputs the same results. After the money transaction, the system reruns the whole procedure sometimes. This repetition is done in clones or backup systems and rolled back immediately. The possible discrepancies found are scored and evaluated by semi-automatic software.

Future Research on Internal Hacking would be interdisciplinary research. It starts from human behavior and psychology, continues with supercomputing and Intragalactic Networks, and reaches programming and investment banking. Research teams around the globe work on various subjects in the area like:

1. Frequency hopping analogy to Internet security and telephony.
2. Personalized unique non-de-posit security.
3. Non-money trading security.
4. Personal (even URL) recorder devices for trusted programmers and traders.
5. Counter and Counter-Counter Counter-Counter actions for holistic security.

8 Conclusion

Cross-border Interbank Payment System (CIPS) and one of its counterparts, the Quantum Financial System (QFS), will dominate investment banking in the following years, with security for all new services being a significant threat. Our preliminary research found that executable computer code redefinition for security reasons is still possible after all these years of complex computing. We reject software domination on network security and retract mixed-mode security, intermixing tangible and software elements. We also propose that every central installation adopt customized noncommercial applications.

USA radio amateurs association with 1 million members shows us the road to diversified personal security, although the SDR (Software defined Radio) is not a complete solution to avoid internal fraud. The missing link is not Thales Defense Systems Corporation's "SafeNet eToken." Possibly Thales from Miletus, the Greek philosopher, could explain himself in the famous phrase: "If there is a change, there must be something that changes, yet does not change."

References:

[1] Ashfaq Ahmed, Atta Muhammad, Muhammad Owais, Kifayat Ullah, and Muhammad Usman. Social, political, and psychological impacts of covid-19 digitalization of the currency and emerging world order. *WSEAS Transactions on Environment and Development*, 2202.

[2] Mona A Ahmed and Abdel-Badeeh M Salem. Intelligent technique for human Authentication using a fusion of finger and dorsal hand veins. *WSEAS Transactions on Information Science and Applications*, 18:91–101, 2021.

[3] Mohammad Arfizurrahmanl, Mohammad Shahadat Hossain Ahmad, Mohammad Shahadat Hossain, Mohammad Ahsanul Haque, and Karl Andersson. Real-time non-intrusive driver fatigue detection system using belief rule-based expert system. *J. Internet Serv. Inf. Security.*, 11(4):44–60, 2021.

[4] Joe Biden. Fact sheet: President Biden to sign an executive order on ensuring responsible development of the digital assets-the white house, 2022.

[5] Georgia Broni, Anastasia Metsiou, and Athanasios Zisopoulos. Economic life and its evolution: The case of Aristotle. In *XV. International Balkan and Near Eastern Congress Series on Economics, Business and Management, Plovdiv/Bulgaria May*, pages 29–30, 2021.

[6] MN Cankara and ME Cek. Covert digital communication using random frequency hopped spread-spectrum. In *2021 13th International Conference on Electrical and Electronics Engineering (ELECO)*, pages 490–493. IEEE, 2021.

[7] Sabrina Corpino, Lorenzo Gagliardini, and Galib Alili. Software-defined Radio-based communication subsystem for c3 ground control station. 2021.

[8] Dipankar Dasgupta, Abhijit Kumar Nag, Denise Ferebee, Sanjib Kumar Saha, Kul Prasad Subedi, Arunava Roy, Alvaro Madero, Abel Sanchez, and John R Williams. Design and implementation of a negative authentication system. *International Journal of Information Security*, 18(1):23–48, 2019.

[9] M Durairaj and A Manimaran. A study on securing cloud environment from DDoS attack to preserve data availability. *the international journal of science and technology*, 3(2):63, 2015.

[10] Saugata Dutta and Kavita Saini. Securing data: A study on different transform domain techniques. *WSEAS Transactions on Systems and Control*, 16:110–120, 2021.

[11] N Ch SN Iyengar, Arindam Banerjee, and Gopinath Ganapathy. A fuzzy logic-based defense mechanism against distributed denial of service attacks in the cloud computing environment. *International journal of communication networks and Information security*, 6(3):233, 2014.

[12] Han Jipeng and Lichen Zhihang. A constraint and object-oriented fifth generation programming language and its compiler and runtime system, 2022.

[13] S. Kovalyov. Order send-trade functions-mql4 reference, https://docs.mql4.com/trading/ordersend.

[14] Apostle Luke. *BIBLE 4:30*. King James.

[15] Satoshi Matsuoka. Fugaku and a64fx: the first exascale supercomputer and its innovative arm CPU. In *2021 Symposium on VLSI Circuits*, pages 1–3. IEEE, 2021.

[16] Jonathan C McDowell. The low earth orbit satellite population and impacts of the SpaceX StarLink constellation. *The Astrophysical Journal Letters*, 892(2): L36, 2020.

[17] microHAM, micro keyer iii https://www.microham.com/contents/en-us/d126-mkiii.html.

[18] Yevheniia Mishchuk, Svitlana Rebrova, Petro Krush, Dmytro Zinchenko, and Kateryna Astafieva. Digitalization security is a marker of modern mechanical engineering technology implementation. *WSEAS transactions on Business and Economics*, 2021.

[19] Nicola Palladino and Mauro Santaniello. IANA functions, ICANN, and the DNS war. In *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance*, pages 43–61. Springer, 2021.

[20] Michael G Raymer and Christopher Monroe. The US national quantum initiative. *Quantum Science and Technology*, 4(2):020504, Feb 2019.

[21] Ye M Rudnichenko, SI Melnyk, NI Havlovska, OLENA Illiashenko, and NV Nakonechna. Strategic interaction of state institutions and enterprises with economic security positions in the digital economy. *WSEAS Transactions on Business and Economics*, 2021.

[22] Chengzhi Sun, Jiyu Lu, and Yunqing Liu. Analysis and prevention of information security of USB. In *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, pages 25–32. IEEE, 2021.

[23] SWITCH incorporation, Data Center Sector, Switch LAS VEGAS 7 Data Center — The Core Campus, Las Vegas, Nevada | Nevada https://www.switch.com/las-vegas/ as retrieved 27/11/2022.

[24] THALES. Fido devices and fido2 devices have strong passwordless authentication https://cpl.thalesgroup.com/accessmanagement/authenticators/fido-devices, 13 6 2022.

[25] Aria Thomas. Quantum financial system: The basic overview, 3 2022.

[26] Robert R. Tucci. Quantum is compiled with an approximation of multiplexors, 2004.

[27] Volks Netzwerk Team. QFS Quanten Finanzsystem Internationales Wahrungs System. https://www.volksnetzwerk.de, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi0mrf42sD7AhWjS_EDHVzmAjoQFnoECAsQAQ&url=https%3A%2F%2F8000lichter.com%2Fget_file.php%3Fid%3D34876656%26vnr%3D461473&usg=AOvVaw1AB839ESeAKPShGl-yWzcs, as retrieved 27/11/2022.

[28] Webpage: Internal Fraud Open-Risk Manual https://www.openriskmanual.org/wiki/Internalfraud, as retrieved 27/11/2022.

[29] Huaji Zhou, Lifeng Yang, and Zilong Wu. Feasibility analysis of tactical radio station communication behaviors cognition. In *2021 AsiaPacific Conference on Communications Technology and Computer Science (ACCTCS)*, pages 160–166. IEEE, 2021.

[30] Athanasios Zisopoulos. Midas, repository with" under the pillow gold" using antipodal unique identification of golden coins for regional development and monetary applications. *Review of International Geographical Education Online*, 12(1):628–643, 2022.

[31] Athanasios Zisopoulos. Obi -WIPO invention patent 20210100177, "gold bullion origination and verification system with unique identification by embedding traceable ingredients". 2, 2022.

[32] Athanasios Zisopoulos and Georgia Broni. Quantum agriculture insurance model for productive precision farming enabled with original fishery, apicultural and cultivation patents. *International Journal Of Scientific And Technology Research*, 2021.

[33] Janko Zufic, Marko Pogarcic, and Ivan Pogarcic. E-mail fraud question of motive. *WSEAS Transactions on Computer Research*, 2018.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

-Athanasios Zisopoulos worked on QFS resourcing, Python programming, and all four methods of security (Chapters: 2,3,4,5,6).
-Konstadinos Panitsidis worked on programming items in non-textual passwords and secure authoring software with anonymous code routing.
-Georgia Broni worked on the realization of tangible security (chapter 3) along with partial support on overall authoring and chapter 7.
-Nikos Kartalis investigated internal fraud and bank payments in chapters 1 and 2 along with the overall support and chapter 7.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.