Marius Iulian Mihailescu

Research Statement

My research interests are in *cryptography*, *computer security*, and *privacy* with applications in protocols designs, zero-knowledge proofs, multilinear maps cryptography, multi-party computation, searchable/homomorphic encryption, game theory, cryptanalysis, lattice-based cryptography, elliptic-curve cryptography, (ring) learning with errors, securing biometric data, steganography, and ethical hacking practices. Also, I am dealing with complex environments where a part of my work has been used, such as Internet-of-Things, Blockchain, Bitcoin applications, Smart City, BYOD, Big Data, and Cloud Computing.

One of my goal is designing and building secure systems. The leakage of confidential data plagues lead many computing systems today to a critical point. My Ph.D. work has focused on protecting biometrics data confidentiality against a powerful and common class of attackers - *attackers who can have full access to data stored on servers*. Such attackers take place in numerous settings. *Firstly*, due to the recent advanced towards cloud computing, an increasing number of companies and users are hosting data on external cloud storage, so their sensitive data becomes readily available to cloud administrators. Indeed, the most recent surveys show that security remains one of the most important concerns for customers of cloud computing and an impediment in adopting clouds for potential customers. *Secondly*, hackers are breaking the security of systems and are gaining access to a part or to entire data stored on a server. *Thirdly*, we know from recent news that due to many attacks, some of them, quite vital, the government has been accessing a large amount of private data even without a subpoena. Finally, even a local data center is exposed, because insider attackers are responsible for many data leaks.

The ideas behind my research directions started when I analyzed a set of vulnerabilities for which I built secure schemes and managed to secure the systems for the institutions where I worked (e.g. Chief Executive Officer at *Dapyx Solution Ltd.*, Head of Research Department at *Lumina - The University of South-East Europe*, Research Assistant at *Softwin Ltd.* part of BitDefender Ltd.). My work has been unfolded using three areas: *theoretical cryptography*, *applied cryptography* and *systems security*. In *theoretical cryptography*, I am building schemes or cryptographic algorithms and I am setting up their mathematical background that can be further implemented in real-life scenarios. In *applied cryptography*, I am analyzing different cryptographic schemes, comparing their results (resources performance, encryption/decryption time etc.) and find the suitable ones for the mentioned requirements, by building practical-yet-provably-secure systems. In *systems security*, I am exploring the fundamental security flaws in popular systems and build defense techniques for them, requiring no or minimal changes to the underlying systems. My contributions in these areas complement and reinforce each other.

Nowadays, most of the existing systems does not have any policy or security schemes to protect the confidentiality against these attackers. For systems that need to compute on sensitive data, the common approach has been to assume that a part of the server is trusted, either uncompromising or inaccessible for the adversary, such as the database or the operating system; then, the attacks to the application are prevented by using techniques such as static or dynamic analysis, language-based enforcement, or information flow control. Unfortunately, this assumption does not hold for the attackers we described, because they can have access to all server components and can simply read the data from the trusted component (e.g, from the database or main memory).

My work provides guarantees for confidentiality and modern approach against powerful and relevant class of attackers.

My Approach

A multidisciplinary approach to security research

Computer security is closely related to a wide range of other fields. Security problems exist in operating systems, networks, databases, distributed systems, and many other fields. My research approach is to understand the topic thoroughly, to identify new problems, and to apply the most suitable techniques from a broad range of sources. I have managed to successfully integrate applied techniques from fields such as game theory, steganography, biometry, applied cryptography with the goal to solve the security problems that I encountered.

Collaboration

My multidisciplinary approach works also very well, when it is applied in collaboration with experts in related fields. I have always enjoyed collaboration and I believe that interaction is important for the success of the research. The collaborations within the team can lead to great achievements, because the discussions refine ideas and provoke new insights. I look forward to the abundant collaboration opportunities afforded in an academic position.

Balance of theory and practice

In my research, I strive to find solutions that have a strong mathematical background and have applicability in real life scenarios. Furthermore, I strongly believe that formal analysis and practical experimentation are both necessary in building secure systems. Formal analysis is indispensable for designing security systems, while building systems and experimenting can provide invaluable feedback, especially on usability, which is critical for the practical security of systems.

Both cryptography and systems security are essential for a more secure and privacy-preserving world. My work in cryptography and systems security has significantly improved security and privacy, and shows the importance and impact of proposed techniques/methods. I believe that my vision for cryptography will enable a faster translation of cryptographic research into real applications. I have also invested considerable time in studying other crucial application areas, such as banking, e-learning, healthcare, and financial. I have in plan to foster synergies between cryptography (theoretical and practical), systems and application areas, such as biometrics, healthcare, financial, and ultimately make the world a safer, more secure place.

Research Projects and Directions

I am very enthusiastic to continue my work in cryptography and security of the systems, as well to create a bridge between real life systems and cryptography (theoretical cryptography and applied cryptography). Some of the *research proposals and directions* on which I am currently working are:

Blockchain and Provable Security. *My goal is to build a research program that will provide a provable security for emergent decentralized systems, especially by combining techniques from programming languages and cryptography.* In my research for blockchain and provable security I managed to connect the academic theory with practical security challenges by applying a generally two-phase process. My research is based on the connection between theory and challenges raised by practical security for blockchain and its applications, such as bitcoin. My approach is a research process done in two phases. First, I start with a critical analysis of the existing security protocols and their related assumptions. This is achieved by gathering user data and how the implementation process had been executed.

I managed to study the consensus in a closed environment, the blockchain technology raising new subjects and challenges for the consensus in an open environment in which the nodes can participate (join) and leave the network when they want. Blockchain technology represents an excellent combination between distributed systems, databases and cryptography, being a fascinating research area.

Based on an extensive survey in the field, in 2018 I have designed and implemented a tutorial entitled "Blockchain Database and Fundamentals of Distributing Computation". The tutorial has been presented at *SecITC Conference* in 2018, together with my fellow researchers from the University of Bucharest and Institute of Computers. The research has been based on one of the most recent academic workpapers, to reduce the size of the consensus group to a small subset of nodes that are participating in the blockchain. The tutorial has been focused on the blockchain lack of permission, my opinion being the technological advance of the blockchain.

I have designed several ideas of important research to be presented in theoretical and applied security information conferences, such as IEEE Security and Privacy, USENIX Security, CCS, and NDSS; scientific seminars and workshops that focused on specific areas such as Usable Privacy and Safety (SOUPS'2019, SOUPS'2018) and IEEE Security and Privacy Symposium (SP2020). Such conferences managed to attract an important interest and participation from the industry side; I believe that the researchers from applied security have to exceed the written part and to find the applicability of the theoretical models in practice. I managed to work closely with the industry, for example in the process of designing and implementing systems and blockchain prototypes with applicability on *eNotary* and *eHealth* area. The prototypes and systems have been done in a partnership framework with EagleVet Ltd. and Dapyx Solution Ltd. Open source projects have been started, such as *BlockDude* and *CryptoBlockSnake*. I have managed to participate and to take legal actions in standardization association, such as Technical Committee 208 – Blockchain and Distributed Ledger from Romanian Standardization Association, a very good part of the proposed ideas, have been implemented within the legal framework of the standards, such as ISO/TC 307 – Blockchain and distributed ledger technologies. A significant amount of work-related to Bitcoin and passwords had an important impact on the academic environment, a course being proposed as a pilot. The B.Sc. and M.Sc. students were getting a huge interest, projects and ideas started to evolve and Ph.D. students became more attracted to do their research in these directions. I have an active role in the public debates regarding the policies used for the implementation of the blockchain at the national level as Member TC208, regulations policies for cryptocurrencies and the restrictions of strong cryptography.

Provable Security for Cryptocurrencies. Cryptocurrencies don't fit within the theoretical framework for distributed computing and cryptography but rather is based on the weakness of the hypotheses. In my research, I have developed an *IceCube* model based on a network structure that is more appropriate for Bitcoin. The model includes the presence of the anonymous communication channels which don't have a predetermined PKI, as well as the hypotheses about the allocation of the computational resources, such as "hashing power" through participants. The IceCube model is useful for the exploration and validation of a new architecture of cryptocurrency. To demonstrate this, I have designed and set the foundations of new construction which proves to be secured in this model, also obtaining desirable effects. First, starting with a new scheme entitled *X-Coin*, I showed that the mining process of the bitcoin can be recycled to provide a global backup system for public data sets. Second, most of the miners are participating in large coalitions known as mining pools; in the last years, the influence over the network has been consolidated at a large scale with helpful coalitions which threaten the security hypothesis of Bitcoin. My research work managed to show that all these coalitions are possible as a consequence of Bitcoin puzzle construction. Therefore, I designed and developed a new approach, entitled "inadequate puzzles" which uses zero-knowledge proofs intending to allow the coalition members to defect, despite the encouragement of forming new coalitions.

Programming languages for modeling bitcoin applications using secure protocols. Cryptocurrencies provide a useful abstracting entitled "global database" which is accessible in public mode and provides consistency on a global level. The advantage of these systems is seen as a platform to attract a bigger community of developers and enthusiasts to implement a large area of application for money transfer. The success of these applications build as a top layer for these types of platforms requires a special composition of the cryptography primitives. These compositions are inclined towards implementation based on errors, often having a catastrophic impact, especially when the compositions and solutions are implemented by developers without the proper experience. One of the main goals of my research in this direction is to create a load balancer and to distribute the load of the cryptography security from programmer to the compiler, which generated "secure-by-construction" protocols, from normal specifications written by programmers with no proper experience.

Applied and Practical Computations over Encrypted Data. In many cases, cryptography algorithms run over sensitive data, but running them over encrypted data could protect data confidentiality. For example, a common class of computations for medical data involve matrix manipulations (e.g., approximations to linear regression). I am working on a software tool, which is implementing an algorithm that supports supports SQL-like operations over encrypted data and is not suitable for such operations. Also, another idea is to use fully homomorphic encryption (FHE) which is a better fit in our case than in the case of SQL queries. The matrix manipulations usually have a fixed access pattern, which does not depend on the data. The way in which a computation is mapped to FHE will result in the performance results, which are different by orders of magnitude. Overall, I would like to design and implement an easy-to-use language for interpretations of the matrix operations for FHE together with a compiler that has the possibility to map a computation at a certain moment of execution to an efficient FHE evaluation. The evaluation is done by performing different optimizations automatically.

Another very interesting discussion and topic, which worth to be discussed and to design a solution, is the possibility to run learning algorithms over the encrypted data in a different approach: let us imagine the following scenario: different parties own some data, the parties does not trust each other, but they are willing to disclose a computation result, which can be seen as global. Multi-party computation is too slow in this case, so what I am proposing in order to discover is a common way to compute the data that can be run in an efficient way. Currently, I am developing a machine learning classification technique over encrypted data. The results that I managed to obtain prove that we can have an efficient support for three major classifiers which are used in the most common machine learning algorithms.

Integrity of server results. A large part of my work has been focused on protecting data confidentiality. We have the following scenario: we have a malicious server, which will return incorrectly results to the queries made by a client. In this way, the functionality of client will be affected together with its data confidentiality. At this moment, I am working on designing a framework of algorithms and cryptography scheme/protocol, which will help the clients to check the correctness of the query results. Currently, there are some schemes, which are used for checking the computations, but it is not very clear how to integrate them into a real life system that has the capability to verify the result of any computation, which are proven also inefficient for databases.

Big Data - Securing the query process. In order to protect the confidentiality of big data, it would be great to encrypt the data and queries. Because we are facing with large size of data, big data systems are counting on effective compression. The computation over data does not have too many chances, because we can no longer have a simple mechanism of encrypting the compressed bulk data. My approach is to build a mechanism that is able to query the encrypted volumes of big data in an efficient way, and to enable compression in the same time. As a basic foundation, the deterministic encryption schemes give the possibility to have some certain forms of compression, and this will be able to create secure versions of existing algorithms, which are able to compute on compressed (unencrypted) data.

Improving client-side security. Most of my work so far removed the trust of the server by making the server to process the encrypted data. The client code will keep the access to the key for decryption and will have the possibility to decrypt the data, as well as it performs the control operations for gaining access, such as granting other users access to a set of private data. A very interesting part of my work has been done on developing techniques for improving client-side security. For example, let us consider the following scenario: I want to make sure that the client-side code does not have any leaks of data through a lack of distraction by making access control decisions based on data that has not been verified from a server that was compromised.

Future Research Directions

The increasing dependence of industry, government, and society on networked information systems means that access control in distributed systems is even more critical.

I would like to continue my research on searchable/homomorphic encryption, blockchain (bitcoin, proof-of-work, proof-of-stake, consensus), multi-party computation, (ring) learning with errors, lattice-based cryptography, blockchain, quantum cryptography, IoT, big data security, cloud computing security, visual secret sharing schemes, designing new protocols, improving privacy enhancing technologies and extend these directions to public key cryptosystems, particularly to new methods that would enable to automatically produce (or verify) security proofs of pairing-based cryptosystems.

Together with my colleague from Institute of Computers and University of Bucharest, I have also started a project in which we are attempting to use elliptic curve cryptography and searchable encryption (EuroCrypt'20). The techniques we develop will gain trust and open many other possibilities for verification of implementation of cryptography protocols.

A good part of my work focused on three different blockchain applications (cryptocurrencies, message encryption, and network authentication) for which I managed to write comprehensive papers that systemize the current technological advances and which offers an amazing source of knowledge and state-of-the-arts for practical application. The experience achieved in every case lead me straight to the second phase of my research: designing and implementation of advanced systems based on practical threat models.

I consider that installing the Bitcoin application and the transparency of the certificate to be landmarks registered in computer security infrastructure. Both systems, are build using the consensus and global history, to use a weak threat model which to be considered a priority in the academic research and to have at the same time an important impact. Not only these systems deserved to be studied literally, but also to demonstrate the potential based on the responsibility to make progress with the problems that frustrated for decades the field of computer security. In my research, I am interested in developing and deploying new systems using the following principles, including CONIKS and beacons based on blockchain. This will be done for verifying the lottery public system. New techniques and fundamentals are foreseen for developing security protocols that can be applied much better in a real context, such as:

- **Designing cryptography mechanisms focused on the user**. While the opacity of the PGP application has been an original problem that represented the base of launching the research in usable security, messaging security remains as being unsolved. In my research, I wish to reverse the approach of the research and to ask the question "how we can make the cryptography mechanisms to be adapted for the user interfaces which are already installed on the user computers?". For a problem such as a transcript consistency without any cryptography mechanism (or using a simulation from Human-Computer Interaction (HCI) entitled "Wizard-of-Oz"), we can evaluate the aspects which capture most of the users and then to determine the maximum level of security which can be provided. I consider that this approach will extend further to problems of discovering private contact and synchronization between multiple devices.

- **Game theory for multi-level systems**. The consensus protocols bitcoin-style gives the impression that new fundamental techniques for analyze game theory is necessary. Bitcoin includes multiple games, each of them with different players that operate at different time intervals. The software agents operate one with each other in real-time, while the mining operations are synchronized with the blockchain (for every 10 minutes or more) and human scanning changes the policy at a lower rate. Incentives and exchange rate requires more economical tools, such as the models oriented on active prices. Beyond the simple modeling of the consensus protocol in bitcoin, there are multiple fascinating questions related to the design mechanism of the agent algorithms (smart contracts) and the implementation process in the cryptocurrency system, such as Ethereum, including name systems, auctions, and financial exchanges.

- **Developing security characteristics of the security protocols**. While multiple studies explored how the end-users interact with the security of software applications, less effort has been done in evaluating the developers of the applications as important players in installing and configuring the protocol. We need a well-thought methodology for evaluation of how well the protocols can be applied for securing the software applications in a real environment. The evaluation needs to be focused as well on the developers which are undergoing to make mistakes (deliberated or unintentionally) and which further prove that are having a negative impact and with devastating repercussions for clients, company and as well as the developers involved in installing and configuring the protocol. This thing requires some techniques from usable security as well as the methodology of studying the productivity of the developers and their correctness for discovering the essential principles for designing future security protocols.

- **Languages for verifying and implementing smart contracts**. Ethereum and other cryptocurrencies allow the users to specify complex contracts that operate independently, being executed in collaborative mode by a group of miners which runs a "consensus computer". The previous experience showed that developing such contracts it is quite difficult and predisposed to error. We need new languages and tools which will help the developers, building new techniques for formal verification, to assure that the implementation of the protocols fulfills the expected logic. This represents the first application for developers, to study and to make proper comparisons between the security of different programming paradigms to be used to achieve high-level tasks, such as "implementation of sealed-bid auctions".

I would also be delighted to join any other research project for which my expertise in the topics mentioned above and not limited to would be an asset.

Marius Iulian Mihailescu, Ph.D.

November 27, 2020