Information & Security: An International Journal

George Sharkov, vol.37, 2017, 5-7 https://doi.org/10.11610/isij.3700

FROM CRYPTOLOGY TO CYBER RESILIENCE – BRIDGING THEORY AND PRACTICE

George SHARKOV

The field of cryptology, based on cryptography and cryptanalysis, is a field of vast history and traditions. It has become an integral part and driver of the general evolution and development of information security.

It all starts with Eve (E) – the adversarial eavesdropper who wishes to learn the secrets that Alice (A) and Bob (B) exchange between themselves. "A," however, has something confidential to share, and she wants to share it with "B" and "B" only. This makes the information that "A" holds even more valuable. Does "A" know about "E" – perhaps yes, or perhaps not? However, "A" renders her message comprehensible to incomprehensible and gives "B" a secret key, with which he can render the message comprehensible again. This way, even if "E" sees the message, she will not be able to read it.

After Alice and Bob, it was Julius Caesar who used an alphabet shift cipher, now known as the Caesar Cipher, to communicate with his generals. We know about the Atbash cipher, used to encrypt the Hebrew alphabet, and the scytale transposition cipher, which some documents show, has been used by the Spartan military. Fast forward to the two world wars, cryptography has evolved along with the other sciences and has

Nowadays, cryptography is so much more – from a mechanism to ensure integrity and confidentiality to authenticate identities and provide proofing methods. Cryptography has evolved beyond privacy to a means to ensure access to fundamental human rights in a digital society. Now the torch is passed to young researchers, such as those featured in the current issue of the Information & Security Journal, who advance the field of cryptography and carry on the legacy of the past.

Inside this issue, you will find articles by participants in the 10th edition of CryptoBG – an International Summer School in Cryptography and Cyber Resilience, CryptoBG

2017 - the first edition of the CryptoBG series of summer schools to hold an International Scientific Symposium. The CryptoBG Summer School is a unique series of events, the first of which was organized in 2007. All summer school editions were organized in the National Institute of Education in Oriahovitza, a small village nested cozily at the foot of the beautiful Sredna Gora mountain near Stara Zagora, Bulgaria.

The National Institute of Education was established by Prof. Minko Balkanski, a famous Bulgarian physicist and supporter of CryptoBG, at the place that was, back in 1927, his father's house. Born on 24 July 1927 in the village of Oryahovitsa, Stara Zagora, Minko Balkanski graduated from high school at the fragile age of 15. After two more years at Sofia University, he left Bulgaria for France to continue his studies. Professor Balkanski saw his first home again in 1992, a few years after the fall of the Soviet regime in Bulgaria. Yet, strongly connected to his roots, Prof. Balkanski decided to renovate his father's house and create an education center, to preserve Bulgarian traditions, and enrich them with scientific innovation to support the local community.

This issue of the Information & Security Journal is dedicated precisely to this intersection between traditions and innovations, between theory and practice and between mathematics and cyber-resilience.

Split into two thematic sections, namely 1) *Advances in Cryptography and Implementation Guidelines* and 2) *Cyber Resilience Policies, Models, and Implementation*, this volume will present seven contributions in total by selected speakers at the International Scientific Symposium as part of CryptoBG*2017.

In *Advances in Cryptography and Implementation Guidelines*, you will find four articles, beginning with a review of the *optimizations of garbled circuits*, from point-and-permute to half-gates, going through garbled row reduction, oblivious transfer extensions and free XOR, to finally present several projects that implement garbled circuits with some of these optimizations, starting from Fairplay to the more recent approaches of OblivC and ObliVM.

Then, we continue with a contribution dedicated to *ASR, an automatic posteriori cryptanalysis tool for public keys generated with RSA*. This instrument links best practice recommendations for public key hardening with existing attacks, giving the other side of the communication channel a tool to detect unsafely (including weakened by purpose) generated keys.

The third contribution presents a *set of practical guidelines for preparing and implementing demonstrations of common security issues and shortcomings that affect mobile phones*' confidentiality, integrity and availability.

Next is a paper dedicated to *attacking leakage-resilient authenticated encryption schemes without leakage***.** The first published "leakage resilient" AE scheme is the RCB block cipher mode. RCB turns out to be insecure, even if there is no side channel for the adversary. The current paper presents several attacks on RCB.

In the *Cyber Resilience Policies, Models, and Implementation* section, you will find three papers that tie the advances in cryptography presented in the previous section into the broader policymaking context to secure our privacy and fundamental human rights.

The first paper of this section discusses the current national cybersecurity strategy of France, emphasizing training and international cooperation, and *discusses the need to continue the reform of the French intelligence services and to enhance the cooperation and the speed of innovation in the field of cybersecurity* – a general challenge for Western Europe.

The second paper presents *a methodological approach towards cybersecurity and resilience of complex and interconnected systems (known as systems-of-systems).* This systems-of-systems approach corresponds to the complexity of the digitized ecosystem and provides guidelines for implementing holistic cybersecurity policies, strategies, and models.

The third paper of the section describes a gamified approach toward practical aspects of cryptography applications and cybersecurity skills and competencies development. An untraditional kind of *CTF (Capture the Flag)* cyber exercise is presented with challenges of the type of *cryptographic puzzles* and stimulated *collaborative problem-solving* by mixed teams of researchers and technical professionals. Such exercises have been piloted at CryptoBG for years as a real example of bridging theory and practice.

We hope that with this issue of the Information & Security Journal, we inspire young scientists in the field of cryptography to continue the vast traditions of this field with a responsible, human-centered mindset towards innovation.

And last but not least, with this volume of the Information & Security Journal, we would like to express our utmost gratitude to Prof. Minko Balkanski, whose scientific research and humanitarian contributions, along with his kindness, wittiness, patience, and generosity, continue to inspire generations of Bulgarian researchers, innovators, creators, and dreamers, including ourselves.

About the Author

See p. 94 of this volume, https://doi.org/10.11610/isij.3706