SECURING CYBERSPACE

Advances in information and communications technologies are transforming our economies and societies. They have formed the basis for global economic growth and an increase in the standard of living. Profound changes can be seen in industry, government and trade, in work, education and leisure. In all aspects of our life we rely on information technology.

At the same time, the information and communications infrastructures have become a critical part of national economies. The other critical infrastructures—those assets, systems, and functions vital to national security, economic need, or public health and safety—encompass a number of sectors, including many basic necessities, such as food, water, public health, emergency services, energy, transportation, banking and finance, and postal services and shipping. All of them increasingly rely on information and communications infrastructures for their operation. Many of the infrastructures' networks are also connected to the Internet.

Unfortunately, the information and communications infrastructures have their own vulnerabilities and offer new opportunities for criminal activity and indeed new forms of crime. The criminal activities may take a large variety of forms and may cross many borders. Criminals, terrorists, and malicious users have exploited the anonymity and global reach of the Internet to launch attacks on the information infrastructure; put harmful and illegal content on the Internet; perform reconnaissance for physical attack; steal money, identities, and secrets; conduct hostile information operations; etc.

The information infrastructure is unique among the critical infrastructures because it is owned primarily by the private sector, it changes rapidly with the fast changes in the information technology area, and, as already mentioned, it is the backbone for many other critical infrastructures. The increasing reliance of critical infrastructures on networks and the Internet has increased the risk of cyber attacks that could harm the infrastructures. In many respects the threat of cyber attacks is escalating due to the increased availability of automated tools for malicious actions, the complexity of the technical environment, and the increased dependence of our society on interconnected systems. Therefore, protection of the information and communications infrastructures is vitally important.

Cybersecurity refers to the defense against attacks on information infrastructure. Cybersecurity has been a major concern of both governments and private sector for many years already. Worldwide, agencies such as the European Network and Information Security Agency, the US Department of Homeland Security, the Council of European Cybercrime Convention, Australia's Critical Infrastructure Protection Group, and the Asia-Pacific Economic Cooperation have set forth policies and initiatives to enhance the information security within their regions. Despite their continuous efforts, the new information and communications technologies has given rise even to more forms of computer-related crime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. The same technologies that enabled this unusual growth and now underpin our economy and way of life also increase the vulnerability of the information and communications infrastructure.

Certainly, there is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act. With the annual costs of digital attacks and financial losses rising to billions of dollars, what measures should be taken to minimize the impact these cyber breaches will have on the global economy? What practices should be implemented to address the daily occurrences of spam, spyware, DOS attacks, online extortion, IP theft, viruses, worms, and physical and cyber data breaches?

With the intention to highlight the importance of cybersecurity and the fight against cybercrime, the Editorial Board of *Information & Security: An International Journal* (I&S) decided to prepare a special I&S issue on vulnerabilities of modern information and communications infrastructures and the search for higher levels of cybersecurity. The objective was to promote research and development to understand and reduce vulnerabilities and to stimulate the dissemination of know-how.

The first article in this volume tries to provide a theoretical foundation for the subsequent discussion. Based on the relativity of the concept of cybersecurity, Xingan Li analyzes the economic impact of cybersecurity breaches. The author then argues that cybersecurity is a private good and should be provided mainly by the private sector. Regarding cybersecurity as a public good would discourage the private sector to invest in security provision, comments the author. However, in terms of prevention of security breaches, law enforcement can play an important role in establishing and enforcing liability mechanisms. Although it is still controversial whether and how cybersecurity players should be held liable for their activities, every step made in this direction will bring benefits, Xingan Li concludes.

Any payment system is characterized by a high level of risk in its different domains caused by great volume and number of operations, a lot of complex relations between clients and increasing speed of data transmission. Nowadays, one of the most important and challenging problems for the financial institutions becomes credit card fraud. Fraudulent electronic transactions have already been a significant problem that grows in importance with the expansion of modern information and communications technologies and the growth of the Internet into a global economic force. Fraud prevention and detection methods are being continuously improved; however, banks are losing billions of dollars worldwide each year.

Not only banks lose money because of credit card fraud. Cardholders also pay for the loss through higher interest rates, higher membership fees, and reduced benefits. Hence, it is in the interest both of the banks and cardholders to reduce illegitimate use of credit cards. And to the financial cost to cardholders one should also add the personal cost in time, inconvenience and frustration while an incident is investigated.

Credit card fraud continues to be a growing problem for Internet businesses. It is in a company and card issuer's interest to prevent fraud or, failing this, to detect fraud as soon as possible. Otherwise consumer trust in both the card and the company decreases and revenue is lost, in addition to the direct losses made through fraudulent sales.

Further, fraud on credit and debit cards has also a high cost to society as the proceeds are often used to fund serious organized crime such as drug trafficking and terrorism.

Considering the importance of the problem, the next group of articles discusses the nature of fraud and mechanisms for its detection.

The aim of Krzysztof Woda's article is to analyze the possible modern techniques for money laundering and terrorism financing, which can be carried out with electronic payment systems. The article identifies the most important characteristics of the particular payment systems, which predetermine such systems as especially suitable for illicit activities. Finally, Krzysztof Woda presents solutions to reduce the risk of illicit money transfers with electronic payment systems and puts a special emphasis on the development of reliable methods for detecting illegal money operations and financial computer crime.

Although introducing techniques for prevention is the most efficient way to reduce fraud, fraudsters are adaptive and, given time, will typically find ways to circumvent such measures. Methodologies for the detection of fraud are of great importance once fraud prevention has failed.

The artificial intelligence community constantly provides new technologies and solutions for fraud detection that have been already applied successfully to detect illegal

activities. Fraud detection, however, requires a tool that is intelligent enough to adapt to criminals' strategies and ever changing tactics to commit fraud. To address this need, the second article in this group proposes a new approach to transaction monitoring and credit card fraud detection. Vladimir Zaslavsky and Anna Strizhak attempt to develop a framework for unsupervised fraud detection based on the neural network technology. The authors apply the Self-Organizing Map algorithm to create a model of typical cardholder's behavior and to analyze the deviation of transactions, thus finding suspicious transactions. It enables automated creation of transaction monitoring rules in a learning process and makes possible their continuous improvement in an environment of dynamically changing information in an automated system.

In the ongoing quest for cybersecurity, cryptography plays an increasingly important role. Given this truth, the following two articles in this special issue of *Information and Security* address various security challenges, proposing novel efficient techniques.

With the rapid development of communications and information technologies, Oblivious Transfer (OT) has been widely applied in numerous applications and has become an important cryptography tool. The mechanism of the t-out-of-n OT protocol is a novel and significant version of the general OT protocol. In 2004, researchers proposed a new secure t-out-of-n OT protocol, which after a thorough analysis has shown to lack efficiency. In their article, Jung-San Lee and Chin-Chen Chang propose a novel t-out-of-n OT protocol based on the Generalized Chinese Remainder Theorem. As demonstrated by the authors, the proposed OT protocol not only satisfies the three essential properties of the general OT protocols, but also has better performance than related protocols. The authors further claim that the proposed t-out-of-n OT protocol is secure and efficient enough to be applied in real-world applications.

Advances in networking technologies and the continued growth of the Internet have also triggered another trend – towards outsourcing data management and information technology needs to external service providers. As a recent manifestation of this trend, there has been growing interest in outsourcing database services in both the commercial world and the research community. However, this introduces numerous security research challenges. Despite a large number of research activities done for securing outsourced databases and removing unencrypted data from exposure to the external server and other intruders, no work has been able to radically secure outsourced databases with associated indexes during the query execution. By exploiting such indexes and with relevant available knowledge, attackers can infer confidential information from the outsourced encrypted data. The article by Tran Khanh Dang discusses potential attacks in such situations and introduces two security protocols for outsourcing database services. The main contributions focus on solutions to the

problem of data privacy/confidentiality and user privacy. The theoretical analyses show that the proposed protocols can effectively protect outsourced data and its associated indexes as well as the clients against various sophisticated attacks.

Nowadays, we can transfer money electronically and shop using e-commerce applications. It could be predicted that, with network support, more activities will be performed without the need for a face to face contact. Hence, authentication has become one of the most significant and challenging issues in Internet applications. The following two articles provide a comprehensive treatment of this very important subject – remote authentication.

Password-based remote authentication is one of the most commonly used authentication techniques due to its simplicity and effectiveness. Authentication schemes generally use a password/ verification table stored at the server side. This stored-table system can easily suffer from verifier-stolen or modification attacks. Clearly, a more secure way to verify user legitimacy is required. Therefore, ID-based authentication schemes have been proposed to remove the requirement of having a password/ verification table stored on the server.

Among numerous schemes for protection, the remote password authentication schemes using smart cards are regarded as very efficient. As a result, smart-card based authentication schemes has become a popular research topic in recent years. In 2000, Hwang and Li proposed a new remote authentication scheme using smart cards based on ElGamal's cryptosystem. The main advantage is that a password table is not required to verify a user's legitimacy. Unfortunately, several security flaws have been identified in their method.

As cryptanalysis has evolved, however, a series of modifications that improve the known security flaws have been made subsequently. The article by Tzung-Her Chen, Du-Shiau Tsai, and Gwoboa Horng deals with a security problem found in a latest modification and improves it in order to construct a more secure version. The article also highlights a feature, mutual authentication, between a server and users found in many authentication protocols but seldom found in the considered series of modifications. Compared with other related schemes, the proposed schemes provide higher security. The authors have demonstrated that the proposed schemes are reliable and secure.

The next article by Chin-Chen Chang and Jung-San Lee proposes a novel practical and secure remote password authentication scheme that also overcomes the security weaknesses of Hwang-Li's scheme. The proposed scheme provides mutual authentication between the remote system and the user such that the server spoofing attack cannot have an effect. Mutual authentication is an essential requirement in remote password authentication schemes. Besides, the scheme allows the user to choose and

change passwords at will and can resist the replay attack without sophisticated concurrent mechanisms. Since the computational load of both the smart card and the whole system is quite low, the remote authentication scheme proposed by Chin-Chen Chang and Jung-San Lee is efficient, secure, and user-friendly to be applied in practice; moreover it could be employed on imbalanced networks as well.

Finally, this special issue provides also a comprehensive, up-to-date list with on-line resources on cybersecurity related forums, organizations, research groups, events, as well as some important publications.

The reader will not find answers to all related questions in this issue. We believe, though, that this I&S issue will stimulate the useful analysis and discussion on how to better address the issues of corporate, individual, and national cybersecurity between all the interested parties (law enforcement agencies, Internet Service Providers, telecommunications operators, software vendors, individual and organizational users, consumer representatives, data protection authorities, etc.), with the objective to enhance mutual understanding and cooperation. This issue attempts to raise the awareness of the risks posed by criminals on the Internet, to stimulate the research on cybersecurity, to identify effective counter-crime tools and procedures to fight cybercrime and to encourage further development of early warning and crisis management systems and mechanisms.

Petya Ivanova