

Chapter 1

Introduction

Agusti Solanas and Antoni Martínez-Ballesté

UNESCO Chair in Data Privacy

Department of Computer Engineering and Mathematics.

Rovira i Virgili University

Av. Països Catalans 26, 43007 Tarragona, Catalonia, Spain

{agusti.solanas,antoni.martinez}@urv.cat

“If self-regulation and self-restraint are not exercised by all concerned with automatic data processing [...] the computer will become the villain of our society. It is potentially one of the greatest resources of our civilization, and the tragedy of slowing its development is unthinkable.”

Lance J. Hoffmann. 1969

This excerpt from an article by Lance J. Hoffmann published in *Computing Surveys* in 1969 points out the importance of taking into account the security and privacy aspects related to the use of computers. In this book, we recognize the importance of those topics and seek to collect a number of recent advances for the protection of privacy and security by means of artificial intelligence techniques, namely evolutionary computation, clustering, computer vision, etc. This book considers the security and privacy problems, and focuses on the relation between them and the field of artificial intelligence from a modern point of view. Notwithstanding, we should not forget that privacy and security have been important issues long before the age of computers.

From the very beginning, humans have tried to protect their privacy and enhance their security. Probably, the first attempt of ancient humans to gain some privacy and security was the use of caves. The size of the caves and the size of the entrances were important, for example the entrance would be smaller if the caves were to be used for secret activities.^{1,2}

As time passed ancient humans evolved and their intelligence and capabilities increased. The smarter they were the more sophisticated their privacy and security methods became. Among these sophistications, writing was an outstanding step forward for many ancient societies (*e.g.* Egyptians, Sumerians, Chinese, Assyrians, Greeks, Mayas, etc.) and it changed their view on many areas such as commerce, diplomacy and war. The way messages were transmitted from strategists to commanders in the battlefield evolved. It was no longer secure to send plain messages because if they were intercepted by the enemy vital operations could be endangered. As a result, cryptography, the art of secret writing, became essential to guarantee the confidentiality of communications. In recent decades, cryptography has expanded beyond confidentiality to include more sophisticated properties such as integrity, non-repudiation, authentication, etc (See³ for a comprehensive study of the history of cryptography).

Nowadays, many security and privacy problems cannot be optimally solved due to their complexity. In these situations, heuristic approaches should be used and artificial intelligence has proven to be extremely useful and well-fitted to solve these problems. Artificial neural networks, evolutionary computation, clustering, fuzzy sets, multi-agent systems, data-mining and pattern recognition are just a few examples of artificial intelligence techniques that can be successfully used to solve some relevant privacy and security problems.

Our main aim has been to gather high quality scientific articles that address privacy and security problems by using artificial intelligence techniques. It can be believed that privacy, security and artificial intelligence are like water and oil, and cannot be mixed. However, this book shows that security and privacy can extraordinarily benefit from artificial intelligence.

We hope that the book will spark the interest of researchers from both worlds (security and privacy, and artificial intelligence) in the investigation of future ways of collaboration that lead to a better understanding of the problems and their solutions.

1.1. Organization of the book

The book you are about to read has been structured in three main parts:

The first part “A brief introduction to privacy and security” comprises Chapter 2 and 3. The aim of this first part is to introduce the main problems related to the many aspects of security and privacy. In Chapter 2, Martínez and Solanas summarize some of the most relevant privacy threats

related to the use of information and communication technologies, namely the Internet, ubiquitous computing and large databases. Similarly, Ribargorda et al. provide the reader with an overview of information security in Chapter 3.

The second part, which includes Chapters 4 to 8, is devoted to several artificial intelligence techniques used to protect privacy in different areas. In Chapter 4, Schmid considers the problem of finding the right balance between societal benefit and individual privacy. He introduces some basic concepts such as anonymity, data perturbation and microaggregation, which are later used in other chapters. In Chapter 5, Pont-Tuset et al. follow the line of the previous chapter and study how data can be *desemantized* using, for example, neural networks. Taking the problem from a different point of view, Dewri et al. propose the use of multi-objective evolutionary computation for statistical disclosure control in Chapter 6. Chapter 7 is devoted to the study of cluster-specific information loss measures. Torra reviews and compares some of them emphasizing the importance of clustering and fuzzy sets. The second part of the book concludes with Chapter 8, where Gibert et al. show how multi-agent systems can be used to preserve the privacy of medical records in health-care applications.

The third part, which comprises Chapters 9 to 14, tackles the security problem from a broad point of view that includes physical security, national security and intelligence, and network security. In Chapter 9, Lu et al. propose the use of acoustic signal recognition and nonlinear Hebbian learning to detect vehicles that may be loaded with explosives approaching restricted areas. In Chapter 10, Puig et al. propose the use of textures in autonomous surveillance vehicles. This chapter compares different state-of-the-art texture classifiers and proposes an efficient solution to the problem of per-pixel classification of textured images with multichannel Gabor wavelet filters. Chapter 11 is devoted to the detection of aggressions in train compartments. Yang et al. present an efficient aggression detection system that integrates several aggression detection systems, including recognition of face patterns and one of the best detectors *i.e.* human beings. In Chapter 12, Decherchi et al. consider the problem of text-mining for homeland security. They present a system for clustering documents that combines pattern-recognition grouping algorithms with semantic-driven processing. In Chapter 13, Zarza et al. address the problem of defining network security protocols for sensor or mobile ad-hoc networks where thousands of nodes can be involved by means of genetic algorithms. Finally, Chapter 14 focuses on the problem of securing mobile ad-hoc networks against selfish

behaviors. Seredynski et al. propose a method that uses concepts concerning co-operation developed in evolutionary biology and tools like genetic algorithms and evolutionary game theory.

References

1. H. Holderness, G. Davies, A. Chamberlain, and R. Donahue. A conservation audit of archaeological cave resources in the peak district and yorkshire dales. Technical Report 7, CAPRA, (2006). URL <http://capra.group.shef.ac.uk/7/743Research.pdf>.
2. P. Arosio and D. Meozzi. The home-hunting habits of prehistoric britons. <http://www.stonepages.com/news/archives/002329.html>.
3. D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. (Scribner, December 1996).