

Preface

Mathematical discoveries, small or great, are never born of spontaneous generation. They always presuppose a soil seeded with preliminary knowledge and well prepared by labour, both conscious and subconscious.

Henri Poincaré

There is a fuzzy place where theoretical computer science, computer security, and applied mathematics are mixed. We can say that theoretical computer science is a mathematical discipline that often abstracts its problems from the (hardware and software) technology of “real” computer science. A part of these problems come up from computer security. Many applicable theoretical results appear in numerous guises since the explosive growth of computer science makes it impossible for anyone to stay up to date in all areas of the field.

This book has been written in response to our perception of such need in the area of cybersecurity. It is meant to serve as both: a resource for researchers and a text on the subject for graduate students.

The modeling of networks requires some mathematical background, but we have made the book as self-contained as possible. We do not presume any knowledge beyond some familiarity with linear algebra (vector and matrices), calculus, and probability and statistics. A chapter devoted to the basic concepts on networks is presented after a specific introduction on intentional risk. This is due to the need to find a conceptual framework where the relationships among individual entities or systems can be described and then measured in a meaningful way. Networks address these requirements very well: a network describes a collection of nodes and links between them.

The concept of a network addresses these requirements nicely: a network describes a collection of *nodes* and the links (*edges*) between them. The notion of nodes is fairly general: they may be individuals, computers, countries, or even groups of such entities. A link between two nodes signifies a direct relation between them. For instance, in a social context a link could be a friendship tie, while in the context of computer science, a link may be, for example, a physical connection between two computers.

Furthermore, in many practical situations, a real-life dataset can be represented as a network (or graph) because this structure can be easily understood and visualized. Such representation has applications everywhere, from the World Wide Web, where nodes represent web pages and edges correspond to the links between pages, to biology, the Internet, and a huge variety of technological systems. In fact, the last two decades have seen the birth of a movement in science, nowadays very well known under the name of complex networks theory. It involved the interdisciplinary effort of some of our best scientists in the aim of exploiting the current availability of big data in order to extract the ultimate and optimal representation of the underlying complex systems and mechanisms.

Specifically, network models also naturally abstract a large variety of computational situations. In addition, numerous specific computational problems, say involving decomposition of problem domains, can fruitfully be formulated as problems of manipulating and/or partitioning networks in various ways, including myriad of problems that employ the well-known divide-and-conquer paradigm.

In the model we are presenting, a complex network is used to represent the system where the nodes are the different components of the system, while the edges represent links between them. The *attacker* surfs on the complex network in order to get the valuable information contained in the system, but each *jump* from one node to another has its own cost depending on the characteristics of the target node and the corresponding link.

Following the paradigm given by Game Theory, the focus is put on the motivating elements for the attacker. We have considered the following: *Anonymity* (how easily the identity of the attacker is determined), *Accessibility* (how easily the attack is carried out), and *Value* (how profitable the attack is). All these elements will be introduced and studied in depth throughout the different chapters of this book. So, Chap. 1 is devoted to give an introduction to *Intentional Risk* and *Cybersecurity*. The basic concepts on networks are presented in Chap. 2. Chapter 3 is devoted to random walkers on a network. In this chapter we will review the main subjects related to random walkers we will need to introduce the concept of *Accessibility* of an element within the network, and Chap. 4 is devoted to the description, computation and applications of this concept in our models of intentional risk. In this sense, two different types of risk are identified related to Intentional Risk: *Static Risk*, studied and developed in Chap. 5, and *Dynamic Risk* which is analyzed in Chap. 6. Roughly speaking, Static Risk is the opportunistic risk, for instance, the risk concerning identity theft, while Dynamic Risk is the type of directed intentional risk that attempts to follow unauthorized paths. The paradigm for this type of risk is represented by the use of a vulnerability in the system to gain technical or administrative accesses based on affinities. In other words, Dynamic Risk is directly linked to the use of potentially existing paths (but not authorized) in the network when it is based on the potential affinity access layer. Finally, Chap. 7 is devoted to present a proof of concept software application using real data to model real-world computer networks and different types of known risks.

It has to be said that although the table of contents represents a categorization of the chapters by subject, the relationship between the chapters is not entirely linear.

There is a progression in the book, with some of the more technically demanding chapters coming later, as well as those that draw on concepts from earlier chapters, even though some chapters are cross-referenced.

This volume has not been designed to be a thorough reference. We refer the reader interested in additional information to the references at the end of the text.

We hope this book will encourage research on the field of cybersecurity.

Palo Alto, CA, USA
Móstoles, Madrid, Spain
Tres Cantos, Madrid, Spain
Móstoles, Madrid, Spain
May 2015

Victor Chapela
Regino Criado
Santiago Moral
Miguel Romance

Intentional Risk Management through Complex
Networks Analysis

Chapela, V.; Criado, R.; Moral, S.; Romance, M.

2015, XV, 126 p. 34 illus. in color., Softcover

ISBN: 978-3-319-26421-9