Chapter 40
Optimization of Operational Large-Scale (Cyber) Attacks by a Combinational Approach

Éric Filiol
Operational Cryptology and Virology Laboratory, ESIEA, Laval, France

Cécilia Gallais
Operational Cryptology and Virology Laboratory, ESIEA, Laval, France

ABSTRACT

Recent attacks against critical infrastructures have shown that it is possible to take down an entire infrastructure by targeting only a few of its components. To prevent or minimize the effects of this kind of attacks, it is necessary to identify these critical components whose disruption, damage or destruction can lead to the paralysis of an infrastructure. This paper shows that the identification of critical components can be made thanks to a particular pattern of the graph theory: the vertex cover. To illustrate how the vertex cover can be useful for the identification of critical components, the electrical power transmission and distribution system of the United States is used as an example. It is shown how it is possible to build an attack scenario against an infrastructure with the results of a vertex cover algorithm.

INTRODUCTION

The recent attacks against power lines in Crimea (MacFarquhar, 2015) left three quarters of its population without electricity for several days – until three weeks in certain areas (BBC News, 2015) since some repair works were delayed due to the presence of demonstrators. These attacks required the destruction of four pylons only to leave most of the 1.8 million residents of the peninsula without electricity.

On the 25th of May 2005, 1.5 million to 2 million customers were deprived of electricity for several hours in Moscow and nearby regions due to a fire and explosion in a local south-eastern substation. The lead of a terrorist attack was ruled out here as the incident was in fact caused by aging equipment which

DOI: 10.4018/978-1-7998-2466-4.ch040

were overburdened by high demand (Arvedlund, 2005). The failure of this one substation led to a power outage in several areas thanks to a cascade effect (Hechtkopf, 2005).

In order to prevent or at least minimize the effects of this kind of attacks and failures, the components of an infrastructure whose disruption, damage or destruction can lead to its paralysis have to be greatly secured, but first of all, they have to be identified.

The trail which is studied to identify the critical components of an infrastructure is the vertex cover, a particular structure of the graph theory (Berge, 1976). An infrastructure is then modelled by a graph whose vertices represent the components of the infrastructure and whose arcs represent the links of dependency between two components. Every kind of components has to be taken into account to allow a more complex and global vision of the infrastructure security. Therefore, the notion of infrastructure is based on the definition of a critical infrastructure presented in (Filiol & Gallais, 2014) which does not define an infrastructure by its IT components only, as it is usually done (Brunner & Suter, 2008) (Commission of the European Communities, 2005) (Moteff & Parfomak, 2004). Indeed, most of the official definitions lack of some essential components, as the external components, the geographical components and most surprisingly, the human components; despite the fact that some experts consider that the humans are the weakest link in security (Mitnick & Simon, 2003). On the other hand, it also increases greatly the amount of the collected information on the targeted infrastructures, and so the size of the representing graph.

Others specific structures of the graph theory are also particularly useful to identify the vulnerabilities of an infrastructure. The path is one of them. The application of shortest path algorithm on the representing graph enables to build attack scenarios against the infrastructure (Filiol & Gallais, 2015). Then the study of these scenarios allows evaluating the security of the infrastructure. These structures are named attack patterns.

The attack trees had also been considered as they were already widely used to model infrastructures (Ten et al., 2007). An attack tree is an undirected graph with no cycle whose root represents the goal and the paths which link the root to the leaf nodes represent the different way to reach the goal. The attack trees were finally rejected, mostly as they can be seen as a particular form of graph whose structure has be considered too poor to represent precisely an infrastructure, which may have several critical assets to protect, because of the existence of a unique root.

After a presentation of the infrastructure model, it is explained how solving the minimum vertex cover problem allow the identification of the critical components whose disruption, damage or destruction can lead to the paralysis of the entire infrastructure. The electrical power transmission and distribution system of the United States – also named power grid – is used as an example to illustrate how the vertex cover enables the identification of the critical components of the infrastructure and then the evaluation of its security and its resilience.

A MODEL OF INFRASTRUCTURE BASED ON THE GRAPH THEORY

As said previously, the identification of critical components can be made thanks to a particular pattern of the graph theory: the vertex cover. In order to use this pattern, a model of infrastructure based on the graph theory has first to be defined.