Pervasive and Mobile Computing 24 (2015) 77–90

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

A survey on energy-aware security mechanisms

Alessio Merlo [a,*], Mauro Migliardi [b], Luca Caviglione [c]

[a] Computer Security Lab (CSecLab), DIBRIS - University of Genoa, Via all'Opera Pia, 13, 16145, Genoa, Italy
[b] DEI - University of Padua, Italy
[c] ISSIA - CNR, Genoa, Italy

ARTICLE INFO

Article history:
Available online 14 May 2015

Keywords:
Security
Energy-aware security
Green networking
Mobile devices

ABSTRACT

The increasing adoption of mobile devices as the preferred tool to access the Internet imposes to deepen the investigation of security aspects. In parallel, their power constrained nature must be explicitly considered in order to analyze security in an effective and comprehensive manner. This aspect, which is often neglected in the literature, allows investigating two important behaviors of mobile devices: (i) evaluate if all the layers accounting for privacy and security can be re-engineered or optimized to save power, and (ii) understand the effectiveness of draining energy to conduct attacks.

In this perspective, this paper surveys and highlights the most recent work on energy-awareness and security. Also, it summarizes the current state of the art on general techniques to save energy, as well as tools to perform measurements. The major contributions of this survey are, thus, a review of past work aimed at minimizing the energy footprint of security mechanisms, and the identification of promising research trends, such as detecting attacks via anomalous power consumption.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

According to [1], the power required to run the most popular ICT infrastructures leads to high economical costs and severe environmental footprints, especially in terms of Green House Gases (GHG) and emissions of CO_2. Therefore, developing some form of energy-awareness has been part of the research agenda on computing [2,3] and networking [4,5] for more than a decade. Such efforts have been defined as *green computing* and *green networking*, respectively. However, they often neglect the security aspect. While it could be acceptable in the past, the actual panorama imposes its explicit consideration, at least for two different aspects: the ubiquitous diffusion of battery-operated devices to access and store a variety of sensitive data [6], and the huge population of Internet users resulting into large-scale hardware deployments.

As a consequence, investigating techniques or solutions dedicated to making security more energy-efficient is a mandatory aspect, even more since in the past there has not been a systematic review of these efforts, while, on the contrary, they have been partially addressed separately in different fields, e.g., networking, computing and hardware/software design. Furthermore, previous surveys dealing with greening aspects were not mentioning security or privacy. For instance, [7,8] review the research done in the field of networks, with emphasis on methodologies ranging from silicon efficiency to dynamic management of the whole network infrastructure (e.g., by shutting down some routes to achieve power savings). Despite the fact that improving the performances of hardware or protocols would also enhance the efficiency of security

* Corresponding author. Tel.: +39 010 353 2344.
E-mail address: alessio.merlo@unige.it (A. Merlo).

http://dx.doi.org/10.1016/j.pmcj.2015.05.005
1574-1192/© 2015 Elsevier B.V. All rights reserved.

frameworks using such facilities, this is never explicitly discussed or evaluated. Ref. [9] deals with cloud computing without mentioning possible improvements by pursuing a more efficient security management, while [10] focuses on general attacks to increase power consumption of large-scale datacenters but without considering countermeasures. Lastly, similar considerations apply to Ref. [11], which analyzes recent data management techniques to reduce energy consumption.

In this perspective, this survey reviews the past work investigating relationships among security and energy. In detail, we considered papers meeting at least one of the following requirements: (i) they offer advancements in understanding the impacts of energy-saving practices and techniques on security; (ii) they introduce novel algorithms, architectures and protocols to reduce the energy consumption; (iii) they consider energy itself as an entity to protect (e.g., against malicious battery drain attacks); (iv) they consider energy as an indicator to reveal threats with a high degree of stealthiness [12].

To summarize, the contributions of this paper are:

1. to review the most recent and effective works on the optimization related to energy costs of security techniques deployed in mobile devices, network nodes and Wireless Sensors Networks (WSN);
2. to analyze studies quantifying the requirements in terms of power and/or energy of the most popular algorithms and protocols used to enforce security in the Internet;
3. to showcase innovative attacks or detection techniques leveraging energy consumption;
4. to evaluate the effectiveness and the accuracy of the most popular tools used to quantify the power used within real-world mobile devices, with emphasis on smartphones.

With regard to the authors' best knowledge, this is the first work surveying energy optimizations and security implications, and it thoroughly extends our previous investigation [13]. In more detail, this paper increases the amount of papers analyzed, enhances the discussion of the background, and also considers practical aspects of tools employed to measure the energy consumption in mobile appliances.

The remainder of the paper is structured as follows: Section 2 portraits the overall architecture of the survey. Section 3 discusses the energy management and the optimization techniques, which can be successfully adopted to optimize security aspects. Section 4 deals with the reduction of energy costs related to security, Section 5 discusses the case of WSN, Section 6 discusses the concept of energy as an asset to be defended and energy as an asset to be leveraged to enhance security. Section 7 reviews the most popular tools to measure consumptions, and, finally, Section 8 concludes the paper by discussing future directions on energy-aware security [14].

2. Survey architecture

To properly discuss related papers, group techniques and possible advancements, we designed the survey in the following manner:

- Section 3 briefly introduces fundamentals of energy management, with emphasis on possible relationships with security mechanisms;
- Section 4 provides an analysis on reduction of energy cost of security aspects. Specifically, it addresses two different kind of entities populating the Internet:
  - end nodes: due to the presence of batteries, mobile nodes are the most important playground where optimizing the impact of security algorithms in terms of energy consumption. Hence, proposals aimed at reducing the footprint of security aspects in end nodes belong to this category;
  - network nodes: modern telecommunication infrastructures must have sophisticated mechanisms to enforce security. Yet, the huge amount of served users requires making optimizations in different layers of the ISO/OSI protocol stack. Thus, here we review papers presenting optimizations/enhancements of network-centric security solutions.
- Section 5 discusses WSN. As energy-awareness is already a mainstream topic in this context, since it has always been considered as a design constraint, here we will only focus on studies explicitly dealing with energy-aware security aspects;
- Section 6 considers energy as an asset to protect, as it already happens for hardware or machineries. Especially, we separately address two different facets:
  - an asset to be protected: limited power availability makes mobile appliances fragile. Hence, many attacks aim at draining power to reduce the lifetime of a device (e.g., via traffic stimulation or by preventing sleep states);
  - an asset for detection: we consider here studies dealing with energy as a metric to detect malicious activities.
- Section 7 analyzes measurement tools. In fact the precise quantification of the energy consumption of algorithms and hardware components is still an open research problem. Besides, without exact measurements, it is difficult to understand what is to be optimized and to fully assess the achieved gains. Accordingly, here we review the most popular tools used to measure consumption with emphasis on solutions used in the surveyed literature.

3. A general overview of energy management and security

This section discusses the general methodologies for energy-efficient computing and networking, with emphasis on solutions that can be used in the perspective of reducing the energy consumption of security protocols or frameworks.

Download English Version:

https://daneshyari.com/en/article/465918

Download Persian Version:

https://daneshyari.com/article/465918

Daneshyari.com