Chapter 10
Ensuring Privacy and Confidentiality in Digital Video Surveillance Systems

Aniello Castiglione
Università degli Studi di Salerno, Italy

Alfredo De Santis
Università degli Studi di Salerno, Italy

Francesco Palmieri
Seconda Università degli Studi di Napoli, Italy

ABSTRACT

Both private and public organizations are considering the implementation of video surveillance technology for the purposes of general Law Enforcement and Public Safety programs. In several situations, such solutions, often characterized by high-speed network connections, plenty of storage capacity, and a high computational power, may be suitable in protecting public safety, detection or deterring, as well as assisting in the investigating of criminal activity. In this scenario, privacy protection, lawful evidence enforcement (through incontrovertible documentary proof), and content confidentiality are the most challenging security topics relating to several information society sectors (Finance, Homeland Security, Healthcare, etc.) that require interdisciplinary input from legal experts, technicians, privacy advocates, as well as security consultants.

Starting from these ideas and concepts, this chapter aims at presenting an innovative network-based digital video surveillance solution that meets all the aforementioned security and privacy requirements ensuring that the recorded data will be only accessible to a subset of authorities, trusting each other under precisely defined policies, agreements, and circumstances. This would aid the surveillance activities, when needed, without disrupting the privacy of individuals.

DOI: 10.4018/978-1-61350-501-4.ch010

INTRODUCTION

With the increasing demand for greater security, following the 9/11 terrorist attacks on the United States, video surveillance technologies are starting to be used in most of the critical locations in every country, such as airports, banks, public transport as well as busy city centers. These systems are being used for different tasks, ranging from object detection, vehicle tracking, analysis of human behavior, to people searching and counting, thus assuming a fundamental role for personal safety, traffic control, resources planning and Law Enforcement. The success of these tasks relies on the existence of specific hardware and software infrastructures that can guarantee the efficient capture and storage of visual data, while providing means that not only improve individual privacy protection but also secure the data against illegitimate activities. Visual data may be illegally intercepted for a use that is different to the originally intended one. It may also be maliciously manipulated in order to either hide and/or introduce fake evidence. For example, within a health-care context, the interception/use of images by anyone outside of the environment infringes patient privacy rights. While, in a banking, industrial or military context where either the replacement of a camera with a fake one or the falsification of its video output can be used to hide hostile activity.

In order to avoid the aforementioned problems, electronic means should be used in conjunction with robust ad hoc architectural features, introducing a reliable way to protect, possibly with lawful enforcement, the produced images and video streams originating from the source capture devices. Specifically, modern digital video surveillance systems need to use effective data authentication procedures to confirm the origin of the surveillance data and their credibility as investigation material in order to prevent and trace any illegal manipulation or falsification of the data as well as ensure their validity as legal proof with law-enforcement authorities (Welsh & Farrington, 2002). Furthermore, since video surveillance systems can be operated to collect personal information about identifiable individuals, to be processed only for specific, explicit and legitimate purposes, all the organizations accessing such data must have the authority to collect, view or use them fairly according to all the existing laws and rules. The European Union is one of the first places in the world that has adopted a specific set of rules and laws explicitly protecting privacy rights and regulating the handling of personal data (EU Parliament, 1995; Becker et al., 2008). In order to cope with all these issues, the primary security measure that can be employed by video surveillance systems is encryption, which can both provide the required degree of confidentiality as well as deny any third party access to their content. On the other hand, the application of robust asymmetric cryptosystems on visual data for real-time applications not only further aggravates the processing requirements but also introduces several impairment factors such as expansion of the packet size, ciphering latency and jitter, which adversely condition the overall video quality.

One possible solution to avoid these problems is the use of hybrid encryption technologies, providing asymmetrical key agreement schemes based on X.509 digital certificates, for initial end-to-end strong authentication between the involved entities, and high-performance symmetric stream encryption, in order to efficiently handle the ciphering of video streams. This hybrid approach relies on using an effective combination of both symmetric and asymmetric encryption schemes, exploiting their specific features and strengths in order to achieve an acceptable security level. In fact, there currently seems to be no systematic method capable of breaking this security scheme in realistic time. Some privileged entities, such as Government or police/law-enforcement agencies, also need to be able to access the data stored in the video surveillance archival systems. Nevertheless, it is not desirable that a single subject or organi-