Trust Issues and Solutions in Multimedia Content Distribution

Shiguo Lian, France Telecom R&D (Orange Labs) Beijing, China

ABSTRACT

Multimedia content distribution is a key technique for multimedia services, which transmits multimedia content from a sender to certain receiver(s). With the popularity of multimedia services, the trust issues in content distribution becomes urgent, including the authorized access, privacy protection, trusted payment, piracy surveillance, and so forth. This chapter introduces the trust issues in multimedia content distribution (e.g., authorization, authentication, privacy, payment, ownership, illegal distribution, forgery, etc.), reviews the latest research progress of the solutions, and presents some open issues and promising research topics. It is expected to provide valuable information to researchers or engineers in this field.

INTRODUCTION

Trust (Trust, 2009) is a complicated term which has different explanations in different fields, including social science, law, digital information, finance, etc. For example, in social science, trust (Misztal, 1996) is a relationship of reliance. A trusted party is presumed to seek to fulfill policies, ethical codes, law and their previous promises. Trust does not need to involve belief in the good character, vices, or morals of the other party. Persons engaged in a criminal activity usually trust each other to some extent. Also, trust does not need to include an action that you and the other party are mutually engaged in. Trust is a prediction of reliance on an action, based on what a party knows about the other party. In sociology, the degree to which one party trusts another is a measure of belief in the honesty, benevolence and competence of the other party.

In common law legal systems, trust is an arrangement whereby property is managed by one person for the benefit of another (Hudson, 2003). A trust is created by a settlor, who entrusts some or all of his or her property to people of his choice, i.e., the trustees. The trustees hold legal title to the trust property, but they are obliged to hold the property for the benefit of one or more individuals or organizations, usually specified by the settlor, who hold equitable title. The trustees owe a fiduciary duty to the beneficiaries, who are the beneficial owners of the trust property. The trust is governed by the terms of the trust document, which is usually written and occasionally set out in deed form. The trustee is obliged to administer the trust in accordance with both the terms of the trust document and the governing law.

With the wide applications of digital information, trust in digital information is becoming

DOI: 10.4018/978-1-61520-682-7.ch005
an important topic (Kelton, et al., 2008). And, many discussions of trust in this environment focus on issues like security or technical reliability. Specially, in security engineering, a trusted system is a system that is relied upon to a specified extent to enforce a specified security policy (Taipale, 2005). As such, a trusted system is one whose failure may break a specified security policy. It is often defined from four aspects, i.e., classified information, trusted computing, policy analysis and information theory. In classified information, trusted systems are used for the processing, storage and retrieval of sensitive or classified information. In trusted computing, trust is used by the Trusted Computing Group (TCG, 2009) mainly in the sense of authorization that defines whether a user is authorized to do something. In policy analysis, trusted systems in the context of national or homeland security, law enforcement, or social control policy are systems in which some conditional prediction about the behavior of people or objects within the system has been determined prior to authorizing access to system resources. In information theory, a trusted system is based on the definition of ‘Trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel’ (Gerck, 1998). This chapter will focus on the trust in security engineering.

Multimedia content distribution (e.g., digital TV, mobile TV, IPTV, online music, etc.) is a kind of digital information system (Lian & Zhang, 2009), which becomes more and more popular with the rapid development of network technology and multimedia technology. Thus, the trust in multimedia content distribution is urgent, especially the security aspects. Generally, a multimedia distribution system, composed of the sender (and device), receiver (and device), transmission channel, storage device, etc., distributes the multimedia content from the sender(s) to receiver(s) through various communication manners. Multimedia content’s properties, such as large volumes, worthy commerce value, real time interaction, etc., make multimedia distribution systems different from traditional information systems. Till now, some means to confirm the trust in multimedia distribution have been proposed (Lian, 2009). However, few works has been done to show the progress of trust issues and solutions in this field. This chapter aims to review the latest research results in trust issues and solutions for multimedia distribution, and provide valuable information to researchers or engineers.

The rest of the chapter is organized as follows. Section 2 reviews related work. A number of trust issues in multimedia content distribution are discussed in Section 3. In Section 4, solutions to ensure trust are introduced in detail. Furthermore, we propose some open issues and hot topics in Section 5. Finally, conclusions are drawn in the last section.

RELATED WORK

In digital information systems, the following trust issues have been deeply studied, including trusted computing, web of trust, and trust in electronic commerce. Considering that multimedia distribution often needs the hardware-based devices, web access or electronic transactions, the trust issues and solutions in these topics may provide valuable information for trusted multimedia distribution. In the following content, these topics will be reviewed.

Trusted Computing

Trusted Computing (TC) is a technology promoted by the Trusted Computing Group (TCG, 2009). The term has a specialized meaning. With Trusted Computing, the computer will consistently behave in specific ways, and those behaviors will be enforced by hardware and software. Enforcing this trusted behavior is achieved by loading the hardware with a unique ID and unique master key. And, Trusted Computing is extremely controversial as the hardware is not merely secured for the owner, and it is secured against the owner as well.

Chip manufacturers, hardware manufacturers and operating system providers all plan to include Trusted Computing into coming genera-
How Trust and Reputation-Based Collaboration Impact Wireless Sensor Network Security
www.igi-global.com/chapter/trust-reputation-based-collaboration-impact/39386?camid=4v1a