Chapter XXI
Trust in the Value–Creation Chain of Multimedia Goods

Andreas U. Schmidt
CREATE-NET Research Centre, Italy

Nicolai Kuntze
Fraunhofer Institute for Secure Information Technology, Germany

ABSTRACT

Security in the value creation chain hinges on many single components and their interrelations. Trusted Platforms open ways to fulfil the pertinent requirements. This chapter gives a systematic approach to the utilisation of trusted computing platforms over the whole lifecycle of multimedia products. This spans production, aggregation, (re)distribution, consumption, and charging. Trusted Computing technology as specified by the Trusted Computing Group provides modular building blocks which can be utilized at many points in the multimedia lifecycle. We propose an according research roadmap beyond the conventional Digital Rights Management use case. Selected technical concepts illustrate the principles of Trusted Computing applications in the multimedia context.

INTRODUCTION

Major scientific efforts have gone into security issues of the value creation chain and lifecycle of digital multimedia products, see the Proceedings of the IFIP TC-6 TC-11 Conferences on Communications and Multimedia Security (1999-2007), and (Zeng, et al., 2006). Thus far these developments have been a rather traditional application of information security to the life-cycle of multimedia data. In particular, authorisation policies and metadata for Digital Rights Management have reached a high degree of maturity (Kosch, et al., 2005). All proposed architectures for multi-media production and distribution have the common characteristic of a few-to-many association between
media sources and consumers. This asymmetry is currently gradually changing. The distinction between media consumers and producers becomes less sharp in Web 2.0 communities like Flickr, YouTube and Facebook. Citizen journalism is a new buzzword. And although the mainstream of media production and distribution will still for a long time be largely resting on centralised business models, information and communication technology exhibit a trend toward convergence which treats user devices on the same technical footing as media servers, for instance.

Likewise the traditional security architectures supporting the life cycle of multimedia content are centralistic and focused on the enforcement of Digital Rights Management (DRM) policies throughout the processes. This approach has its own technical, as well as economical and societal problems (Becker, et al., 2003; Drahos, & Maher, 2004; Mulligan, et al., 2003). On the other hand, the trend toward decentralised distribution structures calls for radically new security foundations. Merabti, & Llewellyn-Jones (2006) suggest approaches to DRM which are rooted in cellular automata to establish trust between consuming and distributing nodes. The authors also mention Trusted Computing as a potential underlying technology.

The purport of this chapter is to show that Trusted Computing is a viable technology option for the security fundamentals of old and new multimedia production and distribution models alike. The standardisation efforts of the Trusted Computing Group have produced what has the potential to become a universal security fundament for the information society. The distinct feature of the new technology is its inherently decentralised organisation. The consequences of this change of paradigms must not be underestimated. Though classical security systems, e.g. for access control and Public-Key Infrastructures (PKI), can easily be modelled using TC, the underlying trust models leave ample space for alternatives – already known or yet to be envisaged.

The chapter is organised as follows. Section 1.1 presents fundamental notions of Trusted Platforms which are essential for the understanding of the concepts outlined in Section 2, which structures the life-cycle of multimedia according to security requirements. Key usages of TC are highlighted in Section 2.2. Section 3 introduces TC on a more technical level, providing prerequisites for the architectural ideas sketched in Section 4. The latter presents two key concepts for TC application in multimedia content distribution, the first centred on mobile devices, the second on traditional Digital Video Broadcast (DVB) architectures. Section 5 contains a concluding discussion focused on security assessments and practical implications of this novel combination of technologies.

1.1 The Notion of Trusted Platforms

The idea of building security into open, connected systems by using computing platforms enhanced by security-relevant functionality in protected places has a long history, rooted in the often-cited study by the Rand Corporation, (1970), see also (Gasser, et al. 1989). These platforms are characterized by a few key properties.

A hardware security anchor is the key to the protection of the system behaviour and acts as a root of trust for its secure operation. Secondly, functional building blocks in a system that are assumed to be trusted, i.e., to behave in a well-defined manner for the intended purpose, form the Trusted Computing Base (TCB) of the system. The TCB comprises such components of a system which cannot be examined for trustworthiness during operation, but only by out-of-band processes like compliance and conformance testing, validation, and certification.

The TCB together with the hardware security anchor can be used to turn a system into a trusted platform (TP), which is a very ambitious, and still today theoretical, concept. The key concept is the extension of trust in an open system from