

INFORMATION SECURITY AND DIGITAL RIGHTS MANAGEMENT: A BRIEF LITERATURE REVIEW

L. Whisenant

University of North Texas (UNITED STATES)

Abstract

This review aims to provide a comprehensive understanding of the closely related nature of Information Security (IS) and Digital Rights Management (DRM). Advances in our technological landscape and the ability of the user to self-generate content while being socially connected to a network of peers created a new level of IS awareness that Shaw et al. [1] expounded on by stating that “users with low-security awareness are one of the weakest security loopholes” [1, p. 93]. A feature handcuffed to IS, and one that is harder to find within our interconnected world, is that of privacy. Our ability to educate, protect, and conceal data at the forefront of our socially connected world led to a new decade in how we viewed our privacy and the steps needed to ensure intellectual ownership (especially in the mobile environment). In recent years an interesting and potentially useful technology has emerged that could shift the centralized nature of repositories. This technology coupled with the idea of peer-to-peer (P2P) networking revolves around the notion of a dispersed digital ledger to record transactions in a safe environment. In reviewing similar literature, information security as it pertains to the Internet of Things (IoT) has garnered much attention due to the amount of data these systems gather. Be it video surveillance, wireless sensor devices, home automation, or medical machines, all of these “things” track, gather, and store personal data and potentially (or eventually) intellectual property.

Keywords: information security, digital rights management, privacy, blockchain, ICT.

1 INTRODUCTION

The purpose of this review is to provide a comprehensive understanding of the closely related nature of Information Security (IS) and Digital Rights Management (DRM). We will cover 18 years of information to allow the reader to see the growth of the movement, as well as to highlight the various security solutions available for the data owner. Lastly, we will cover the latest research pertaining to IS and DRM with the goal of providing a sense of the future implications. Each section or selection of articles will be grouped based on the year in which the literature was published, as this will allow the reader to purposively examine the history of IS and DRM.

2 LITERATURE REVIEW

To begin, we will start with an article by Abie et al. [2] in which the authors describe an information distribution system built on six building blocks that emphasize a trust-incorporation scheme. These blocks (user, authentication/authorization, enforceable rights, privacy, tracking, and security) create a Distributed Digital Rights Management (DRM) solution that was applied to an e-learning program in Norway. Of particular interest to the current literature review was the researcher's goal of making multimedia content available to the students in a productive learning environment while supporting “an object-distribution system that allows streaming and the use of media-rich content over the network, while at the same time ensuring the protection of Intellectual Property Rights (IPR)” [2, p. 115]. IPR, as well as the inherent security that necessitates their purpose, was a key point that Anderson and Moore [3] were interested in when discussing the economics of vulnerability and privacy that exist within various companies and/or systems. They pointed out that many of the design flaws that exist in an application could easily be prevented if not for lack of consistent measures that disincentivize the developers (fast and cheap, rush to market, etc.), thus potentially avoiding the necessary rights attributable to the owner [3, p. 611-612].

2.1 The Art of Concealment

Moving ahead a few years, advances in our technological landscape and the ability of the user to self-generate content while being socially connected to a network of peers created a new level of IS awareness that Shaw et al. [1] expounded on by stating that “users with low security awareness are one

of the weakest security loopholes” [1, p. 93]. This statement coupled with the advances in wireless network systems created a need for a more robust authentication process to allow safe data transmission between endpoints and users. Zhou et al. [4] proposed a solution to this problem by focusing on the security component in the transmission process and thus created a graph-based approach that allowed packets to be organized into groups, thus “the main task at the sender is to sign and protect the code stream by joint authentication and coding before transmission” [4, p. 7]. The in-depth knowledge and algorithms used to create this approach are beyond the scope of this review, yet the researcher’s aim of protecting information leads us to important advances in how we protect and identify our data.

Steganography is the process of hiding information that is undetectable to anyone but the sender and receiver of the transmission [5, p. 20]. This idea is related to copyright infringement (piracy) and DRM. “Generally, a DRM system takes into consideration the following aspects: data to be protected, communication scenarios to be protected, access rights to be protected, the supported business model, and core techniques” [5, p. 6]. This concept of protecting information, attributing ownership rights, and hiding communication means “no such detection method should exist that would be able to tell carriers with hidden messages from innocent ones with a significant reliability” [6, p. 1].

A feature handcuffed to IS and harder to find in our interconnected world is that of privacy. Various technologies (sensors, cameras, biometric systems, etc.) have developed and thrived to the point that Cheung et al. [7] stated “the particular challenges include but are not limited to the difficulties in extracting semantic information for protection, the ability to apply cryptographic primitives to high data-rate multimedia streams, basic signal processing algorithms for protecting privacy without destroying the perceptual quality of the signal, and privacy models for governing and handling privacy rights in multimedia systems” [7, p. 1]. In short, our ability to educate, protect, and conceal data was at the forefront of our socially connected world and led to a new decade in how we viewed our privacy and the steps needed to ensure intellectual ownership (especially in the mobile environment).

2.2 Digital Rights Management (Enhanced)

According to Sachan and Emmanuel [8], our traditional view of a Digital Rights Management system (two-tiered; owner and consumers) “may not provide sufficient business scalability to the owner” [8, p. 1]. The researchers propose a multi-tiered platform that effectively inserts middle suppliers that could potentially affect company strategy in terms of untapped market potential. For our purposes, we will focus on the “meat” of their publication in that they suggested a license validation method using bit-vector transform to increase and improve the validation time needed to verify the data. This finding coincides with Yang et al. [9] in that they were also interested in intellectual property rights and how certain encryption technologies (namely Zang et al.’s DRM authentication scheme) could be improved to withstand an insider or stolen smart card attack. The mutual authentication and efficiency evaluation comparison showed that the researchers had “enhanced the Zhang et al. scheme to efficiently prevent various known attacks” [p. 194], and as such had enhanced the security needed to protect a user’s intellectual property.

Similar to Sachan and Emmanuel [8], Das et al. [10], sought to understand the security concerns of an organization by addressing a flaw common to Enterprise Digital Rights Management (E-DRM) in that of identity theft. The researchers were interested in improving prior research conducted by Chang et al. [11] through improvements to the authorization phase via “content key distribution... which also (sic) offers low communication and computation overheads and user’s anonymity” [10, p. 3383]. This notion was central to the work done by Yang et al. [12] in determining the E-DRM scheme needed to protect the digital contents of mobile users. Through prior exploration, the researchers determined that using a digital signature and certificate would not offer the level of protection needed. Instead, they focused on using a “one-way hash function and exclusive-or (XOR) operations to accomplish the user authentication so the computation costs can be greatly reduced” [12, p. 308]. This finding coupled with the global demand and use of mobile devices created a demand for more robust security while maintaining the user’s privacy in terms of biometric identification and personal information collection.

2.3 Privacy Rights and Future Implications

As shown in the prior literature, advances in IS and DRM have led to an increase in sophisticated methods of protecting personal information and intellectual property. Coupled with advances in technology is the potential for privacy rights to be infringed on by unsuspecting users. De-identification as defined by Ribaric et al. [13] is “the process of concealing or removing personal identifiers or replacing them with surrogate

personal identifiers in multimedia content, in order to prevent the disclosure and use of data for purposes unrelated to the purpose for which the information was originally obtained” [p. 134]. This process is similar to information hiding, in which the sender uses various deception techniques (watermarking, steganography, steganalysis, etc.) to conceal the contents of the data package. As it relates to de-identification, the researchers point out that this method is still in its nascent phase, yet their work highlights an issue that has far-reaching effects for the field of IS (social, legal, and political).

One of the purposes of the aforementioned deception techniques is potentially to thwart information leakage accidents or corporate hacking. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Virtual Private Networks (VPNs) are common methods to secure a network, yet Kim et al. [14] found a gap in terms of the research being conducted and concluded that the “reason why information leakage incidents and accidents occur despite the advancement of IS technology is because protective measures needed for the subject of IS and business trend were not considered” [p. 14804]. They also found that a lack of management was of potential concern and that “follow-up research should be conducted on IS management area of understanding company and people” [14, p. 14804]. In short, the authors suggest user education and specific leadership directions are key factors in data loss prevention (DLP).

However, with many companies streamlining their on-boarding process, the task of educating employees presents a daunting feat. To create an environment that is user-friendly, Frattolillo [15] suggested “interoperability among different DRM systems, since they enable web users provided with last generation internet browsers to access multimedia digital content protected by a proprietary DRM system by employing a different DRM system” [p. 283]. This browser-based approach to managing and implementing a DRM system, is especially important in the era of streaming services where users can “click and get” their desired content. According to Ma [16], “the video content such as films, digital network content is very popular in current times, especially films will pay much more cost to make, to produce and manufacture, thus it needs to protect the content from being shared or transfer to internet or being recorded and redistributed for illegal business trade” [p. 162].

This idea is convincing in theory, yet the practical truth is that many techniques (as described in the prior literature) can be utilized to steal intellectual property. Qin et al. [17] acknowledged it best when they said, “For a country or organization, information hiding techniques can be utilized to transmit confidential messages using steganographic techniques, protect copyright of a software or digital publication using watermarking techniques, etc. However, above techniques may also be used by the terrorists or illegal guys to endanger national security and destroy social stabilization” [p. 13421]. Simply stated, anything the good guys can accomplish, the opposite holds true.

2.4 The Present State of IS & DRM

In reviewing the prior literature, the researchers have shown the exponential growth data scientists have made in securing and protecting users’ information. In recent years, an interesting and potentially useful technology has emerged that could shift the centralized nature of repositories. This technology coupled with the idea of peer-to-peer (P2P) networking revolves around the notion of a dispersed digital ledger to record transactions in a safe environment.

According to Ma et al. [18], blockchain technology “provides distributed ledger technology (DLT) that store(s) the completed blocks in chronological order with tamper-resistance and security, (and) it allows participants to keep track of digital transactions without central recordkeeping. Each node holds a copy of the blockchain downloaded automatically, (and) the record’s authenticity can be verified by the entire community using the blockchain instead of a single centralized system” [p. 747]. The underlying algorithms of this technology are beyond the scope of this review, yet the scattered approach to information preservation provides an opportunity for researchers to apply specific security measures to ensure confidentiality in the exchange process. Gao et al. [19] proposed a Multiauthority Ciphertext-Policy Attribute-based Encryption (MA-CPABE) scheme that guarantees confidentiality, provides flexibility, allows granular access control, reduces the single point of failure, and can resist collusion attacks [p. 5234]. In testing their theory, the researchers provided examples in that their system could “reduce the time cost and management by artists when ensuring fairness of interest between them, agents and fans in the purchase of music copyright transactions, and the members’ privacy will be protected meanwhile they enjoy the sharing rights of broadcast of popular TV series” [19, p. 5235].

In reviewing similar literature, information security as it pertains to the Internet of Things (IoT) has garnered much attention due to the amount of data these systems gather. Be it video surveillance, wireless sensor devices, home automation, or medical machines, all of these “things” track, gather, and store personal

data and potentially (or eventually) intellectual property. Due to the sensitive nature of the information being collected, Yang et al. [20] suggests that to protect and verify the confidentiality and integrity of the data, encryption algorithms, hash functions, and digital signatures are all needed to ensure data reliability from point to point [p. 1-2]. Likewise, Heo and Jeong [21] stated that “the demand for encryption techniques such as MPEG-DASH for transmitting streams over networks is increasing. These video stream security methods guarantee stream confidentiality... therefore, it is necessary to secure information by deceiving methods that prevent other people from inferring the contents through a wide range of network scan” [p. 1]. Both sets of researchers emphasize the need for information security systems and the importance that stream confidentiality plays when transmitting data between devices.

3 DISCUSSION

In discussing the various methods used to protect privacy, thwart suspicious activity, and preserve the digital rights of authors, it is the researcher’s opinion that much innovation has been conducted in the realm of IS and DRM. Due to the constant threat of bad actors attempting to exploit zero-day threats and manipulate the end user, it is imperative that, like the prior authors have noted, we continue to research and find ways to improve our digital maturity as well as our digital environment. To this point, Bouchaala et al. [22] states that “cloud computing is the most promising paradigm in recent years. It contributes in the appearance and the evolution of new concepts and technologies. It offers on demand a fragrance of measured services accessible through heterogeneous platform and devices. Cloud users outsource their assets to remote cloud servers. Preserving privacy and fine-grained access are important concerns in security fields” [p. 498]. In this regard, the shift to a cloud environment will require secure access for those who choose to migrate their data at the behest of digital transformation, and according to Rubóczki and Rajnai [23], “managing cloud security so that policies and compliance standards enforced within an internal network are extended to the cloud remains a challenge for many organizations” [p. 11].

Lastly, as it relates to DRM, Ned Averill-Snell posed several interesting questions in his short article titled: *For Cloud Security Design, Don’t Ignore DRM*. He acknowledges that while most organizations are moving forward with adopting cloud infrastructure, they are still worried about the security of their data. He asks, “Who should be permitted to annotate or redact a document, and who should be allowed only to read, but not touch? When should reading and text copying be permitted, but not printing? And when a document requires a signature, how do you make digital signing available only to approvers while enabling others to read but preventing them from signing off?” [24, p. 1]. These questions further illustrate the need for secure practices when trying to maintain the authenticity of an article, while also preserving the rights awarded to the writer.

4 CONCLUSION

In closing, this review has encompassed nearly two decades of IS and DRM literature with the goal of highlighting the development and application of a technology vital to our intellectual and knowledge security. It is the opinion of the researcher that blockchain technology, coupled with the advent of the IoT, that our future will consist of a data structure that is distributed, synchronized, and accessible for all to participate.

REFERENCES

- [1] R.S. Shaw, C.C Chen, A.L Harris & H.J. Huang, “The impact of information richness on information security awareness training effectiveness,” *Computers and Education*, vol. 52, no. 1, pp. 92–100, 2009.
- [2] H. Abie, P. Spilling, B. Foyn, “A distributed digital rights management model for secure information-distribution systems,” *International Journal of Information Security*, vol. 3, no. 2, pp. 113–128, 2004.
- [3] R. Anderson, T. Moore, “The economics of information security,” *New Series*, vol. 314, no. 5799, pp. 610–613, 2006.
- [4] L. Zhou, B. Zheng, A. Wei, B.Geller, & J. Cui, “A scalable information security technique: Joint authentication-coding mechanism for multimedia over heterogeneous wireless networks,” *Wireless Personal Communications*, vol. 51, no. 1, pp. 5-16, 2009.

- [5] S.R. Lian, D. Kanellopoulos, G. Ruffo, "Recent advances in multimedia information system security," *Informatica*, vol. 33, 3-24, 2009.
- [6] M. Golian, A. Westfield, "Secure steganography in multimedia content," *Eurasip Journal on Information Security*, 2009.
- [7] S.C.S. Cheung, D. Kundur, A. Senior, "Enhancing privacy protection in multimedia systems," *Eurasip Journal on Information Security*, 2009.
- [8] A. Sachan & S. Emmanuel, "Enhanced digital rights management authentication scheme based on smart card," *Computers and Security*, vol. 30, no. 6, pp. 498-513, 2011.
- [9] H.W. Yang, C.C Yang, W. Lin, "An enterprise digital right management scheme with anonymous trust for mobile devices," *Informatica*, vol. 37, no. 3, pp. 307-313, 2013.
- [10] A.K. Das, D. Mishra, & S. Mukhopadhyay, "An anonymous and secure biometric-based enterprise digital rights management system for mobile environment," *Security and Communication Networks*, vol. 8, no. 18, pp. 3383-3404, 2015.
- [11] C.C. Chang, J.H. Yang, & D.W. Wang, "An efficient and reliable E-DRM scheme for mobile environments," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6176-6181, 2010.
- [12] J. Yang, H. Sun, P. Chen, "An enterprise digital right management scheme with anonymous trust for mobile devices," *Informatica*, vol. 37, no. 3, pp. 307-313, 2013.
- [13] S. Ribaric, A. Ariyaeinia, N. Pavesic, "De-identification for privacy protection in multimedia content: A survey," *Signal Processing: Image Communications*, vol. 47, pp. 131-151, 2016.
- [14] H. Kim, S. Park, H. Chang, "Information security research classification for future multimedia environment," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14795-14806, 2016.
- [15] F. Frattolillo, "Digital Copyright Protection: Focus on Some Relevant Solutions," *International Journal of Communication Networks and Information Security*, vol. 9, no. 2, pp. 282-293, 2017.
- [16] Z. Ma, "Digital rights management: Model, technology, and application," *China Communications*, vol. 14, no. 6, pp. 156-167, 2017.
- [17] C. Qin, D. Ye, X. Luo, "Information hiding and forensics for multimedia security," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13421-13429, 2016.
- [18] Z. Ma, M. Jiang, H. Gao, Z. Whang, "Blockchain for digital rights management," *Future Generation Computer Systems*, vol. 89, pp. 746-764, 2018.
- [19] J. Gao, H.Yu, X. Zhu, & X. Li, "Blockchain-based digital rights management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption," *IEEE Systems Journal*, vol. 15, no. 4. Pp. 5233-5244, 2021.
- [20] X. Yang, Y. Hou, J. Ma, H. He, "CDSP: A solution for privacy and security of multimedia information processing in industrial big data and internet of things," *Sensors*, vol. 19, no. 3, pp. 1-16, 2019.
- [21] J. Heo, & J. Jeong, "Deceptive techniques to hide a compressed video stream for information security," *Sensors*, vol. 21, no. 7200, pp. 1-14, 2021.
- [22] M. Bouchaala, C. Ghazel, & L.A. Saidane, "Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card," *Journal of Supercomputing*, vol. 78, no. 1, pp. 497-522, 2022.
- [23] E.S. Rubóćzki, & Z. Rajnai, "Moving towards cloud security," *Interdisciplinary Description of Complex Systems*, vol. 13, no. 1, pp. 9-14, 2015.
- [24] N. Averill-Snell, "For cloud security, don't ignore drm," *KM World*, vol. 24, no. 4, pp. 1, 2015.