Security Issues in e-Contracting

Praveen Gauravaram and Ernest Foo

Information Security Institute (ISI)
Queensland University of Technology (QUT)
Brisbane, Australia

Abstract. Information security requirements and goals of e-contracting systems have not been closely examined in the open literature. This paper identifies key security goals and the services to be considered when designing e-contracting systems. Security of some online collaborative platforms that are currently in use for project management and that could be used for e-contracting is examined closely in this paper.

1 Introduction

Modern Architecture, Engineering and Construction (AEC) enterprises conduct business under a contract which constitutes a legally binding agreement enforced by the law between the enterprise and its customers or suppliers [19]. The automation of the contracting process, especially with the advent of the Internet in the past decade, has benefited the AEC industry with an improved productivity and security, effective aggregated contract information, efficient contract life-cycle process, reduction in the contractual errors and risk, profit optimization and better compliance effort [21].

An e-contracting system is a web-based software application used to conduct contracting between or among the business parties. The e-contracting system works as a representation of paper contracts. Online collaborative platforms such as Aconex [3], Constructware [9], Causeway [10], to name a few, are emerging as the principal systems for document management in the AEC sector. Such systems could potentially be used for e-contracting as well. However, we have not come across Internet based tools specifically meant for e-contracting. Added to that, the increasing use of the Internet as an effective business tool for e-contracting has motivated us to investigate the information security consequences that may occur when the Internet is used as a medium to form the contractual relationships. Considering

that the security of e-contracting system is paramount for the economic well being of the AEC indusrty, this paper addresses this issue and explores the security requirements and services of e-contracting systems.

In a related work, Knorr and Röhrig [20] have presented an open framework for the analysis of security requirements of business processes in electronic commerce. They have identified confidentiality, integrity, availability and accountability as the security objectives to suit the legal needs of a business process. Meier and Röhrig [22] have used a goal-oriented approach to derive appropriate security safeguards for the different contract types and discuss the implementation issues for electronic agent-based contracting systems.

The following are the contributions of this paper: This paper identifies the security requirements or goals that need to be considered for the e-contracting systems from a technical perspective. The paper provides the essential information security services that can provide the identified security requirements. In addition, the paper presents results of a survey on the security aspects of some AEC collaborative platforms that could be used for e-contracting.

The paper is organised as follows: Section 2 of the paper addresses the fundamentals of e-contracting. Section 3 of the paper explains e-contracting systems. Section 4 of the paper notes the e-contracting security requirements. Section 5 provides the security services essential for e-contracting. Section 6 provides the results of our survey on the security aspects of the AEC collaborative platforms used for e-contracting. Finally Section 7 concludes the paper.

2 E-contracting Basics

An electronic contract (e-contract) is an agreement created and signed in electronic form without using any paper or other hard copies [28]. It is a contractual agreement, represented as digital information and signed with the electronic or digital signatures of the participating parties [6]. An e-contracting process or life cycle consists of a number of phases where each phase constitutes activities confined to that phase. At a broad level, we classify e-contracting process into three phases:

- E-contract formation: The following steps take place during the formation of e-contracts.
  1. Informational: General contract preparations are made, information for a request or offer of services is provided and parties or collaborating partners are identified.
  2. Pre-contractual: Preparatory contracting process is performed where several contract negotiations are administered and managed.
  3. Contracting: Contract negotiations are performed, preliminary agreements are made regulating the steps on the proceedings of negotiations and a draft agreement serving as an example of the final contract is established.
  4. Enactment: Contract is executed with signatures of all the parties.
- E-contract management: Most of the time, it happens that enterprises might have to apply changes to the established contracts during its enactment [1]. The e-contracting management system incorporates any variations (updates) of the e-contracts formed between or among the contracting parties.
- E-contract archiving: The finalised e-contracts along with other related contractual communications between or among the business parties are archived for future evidential purposes.

3 E-contracting Systems

Some of the different methods that may be used to execute the e-contracting process include:

1. E-contract is formed by the exchange of text documents via electronic communications such as email where a party which issues the contract, writes the contract on his/her computer and emails it to the second party by typing the name and the second party emails it back to the first party with the name indicating the acceptance of the contract. A name typed in the e-mail is considered an electronic signature [14]. While electronic signatures describe signatures incorporated in a document by cryptographic or non-cryptographic means, digital signatures specifically describe signatures using cryptography.

2. The text documents that form the basis of an e-contract may be written in XML, a mark-up language for documents containing structured information [31]. Structured information contains both content and some indication of what role that content plays. One advantage of forming contracts using XML is that contracts can be processed using machines and contracts can be imported into contract management and negotiation tools and achieving better specifications of the contract using industry specific XML vocabularies.
3. An e-contract may be in the form of a "click to agree" contract. The terms and conditions of the contract are displayed on one party's website and the other party agrees to the contract by clicking an 'I agree' button on the website accepting the relevant terms and conditions.
4. Conceptual system architectures support either part of or the complete e-contracting life cycle process. For example, the multiple signing using digital signatures and dynamic update conceptual architectures described by Angelov *et al* [1] are used to manage the e-contract updates.

Generally, when contracting parties decide upon a particular method to execute e-contracting, their decision is influenced by the nature and importance of the relevant contract. For e-contracts of strategic importance or of high economic value, parties may wish to utilize appropriate mechanisms to achieve the security of relevant documentation.

4 E-contracting Security Requirements

Any system used to carry out the contracting process must make sure that the whole e-contracting process is secure. An e-contracting system must incorporate mechanisms to ensure that contractual evidence is securely gathered and stored in the case of disputes between or among the contracting parties. These mechanisms are the security services that may provide the security goals. The security requirements specifically meant for the e-contracting process have not been closely examined in the literature to date though the security requirements of other business processes such as e-commerce

and e-business have been explored [20, 26]. There is no strict rule which can be used to compile a list of security requirements for e-contracting systems. Our listing is based on the study performed on the different methods used to execute the e-contracting process as explained in Section 3 and the security analysis performed on some AEC collaborative platforms explained in Section 6.

We note that if the information and communications technology (ICT) used in the e-contracting process is secure, the e-contracting process itself is partially secured. There may be some unknown vulnerabilities in the e-contracting system that do not depend on the ICT but might affect the security of the contracting process.

We note that any e-contracting system should achieve the following security goals:

1. Confidentiality: It ensures protection of e-contracts and other communications from unauthorized disclosure in the e-contracting system. The contracting parties may not want to disclose the documents in every stage of the e-contracting life cycle to unauthorised parties. This condition depends on the agreement undertaken between or among the contracting parties before the start of the e-contracting process and on the type of business undertaken by the parties.
2. Integrity: It ensures that contractual documents exchanged between the contracting parties or stored in the e-contracting system at any point of time are not duplicated, modified or deleted. The contracting parties aim for secure storage or transmission of all contracting and related documents in every stage of the e-contracting life cycle.
3. Authenticity: It ensures that the parties involved in e-contracting are exactly who they claim to be. The contracting partners must authenticate themselves to the e-contracting system and their credentials need to be recorded and maintained throughout the period of e-contracting.
4. Non-repudiation: It ensures that contracting parties are prevented from denying having performed actions such as denying an established contract and denial of sending or receiving any messages.
5. Availability: It ensures that e-contracting systems and contractual data are available to the authorized personnel during the period of contract life cycle.

6. Proof of agreement: Every action of the contracting parties in the e-contracting system throughout the period of its usage is considered as a proof to which they have agreed.
7. Proof of existence: It assures the existence of contractual documents in the e-contracting system or documents communicated via the Internet at a point of time.

5 Security Services of E-contracting Systems

We have found that any e-contracting system may need to provide at least the following services to achieve the security goals to execute the contract life cycle described in Section 4.

5.1 Secure Access Control

To alleviate concerns about the security of e-contracts and the messages communicated, e-contracting systems must be designed so that users have limited access to the e-contracts, depending on their role within the enterprise or business which deals e-contracts. For example, in a collaborative platform used for e-contracting only a subcontractor may be allowed to access drawings and communications relating to a particular project while other project information is shared with other parties involved with the enterprise [4].

The rights to access, view, modify or delete contractual data in an e-contracting system are controlled by an access control system which the e-contracting system supports. The components of an access control system are:

1. User identification: This is a process by which the user identifies himself/herself to the e-contracting system. If a third party vendor licenses the e-contracting system to an enterprise to carry business, then, in the first step, the enterprise has to identify itself to the e-contracting system by registering with the third party vendor for a period of time. In the second step, the individual users in the enterprise identify themselves to the e-contracting system with a unique username.
2. User authentication: User authentication to the e-contracting system is a process of verifying the identity of the user to the system where the user confirms to the system who he or she is.

E-contracting systems with only password based authentication provide sufficient level of security. While user authentication verifies the user identity to a system, the user identification process just identifies the user to the system.

3. Authorization: Authorisation refers to the permissions or rights of the user to read, write (for example, add, create, delete or rename the e-contract files in the system) and execute contractual data in the e-contracting system. A security policy determines who will have access to different types of contractual information and whether or not they have a right to alter the data. The method by which the security policy is implemented is referred to as a security model [16].

5.2 Secure Communication

The collaborating parties participating in e-contracting need to address the effect of the risk involved in the exchange of electronic communications of e-contracts on their confidentiality and integrity in transmission. The personnel who use e-contracting systems need to make sure that these systems use secure Internet protocols such as secure sockets layer (SSL) [15] or Transport Layer Security (TLS) [11] to provide confidentiality, integrity and authenticity to the data in transmission.

5.3 Secure Archiving

Upon the completion of e-contracting, all the contractual documents processed in different stages of the e-contracting life cycle need to be archived for future evidential purposes. In this case, the e-contracting system such a collaborative platform would also need to be updated regularly so that the contracting parties need not be concerned with the continued readability and availability of the documents [32]. Alternatively, the data can be stored in an off-line archive. In this case it may also be possible to produce a copy of the project for project participants on CD ROM or DVD [32]. The parties should agree contractually before contracting, how the contracting data will be archived and what data will remain available to each project participant [4]. Secure archiving of contractual information requires durability of the storage media and readability of contractual documents.

Generally, contracting parties will not be found to have satisfied their obligation to preserve contractual documents if the mechanism on which they are stored has broken down or if the documents are saved in a format that is no longer able to be read by contemporary computer systems.

5.4 Digital Signatures

Digital signatures [25] based on the combination of public key cryptography (PKC) and cryptographic hash functions ensure data origin authentication, integrity of the signed contract, non-repudiation and proof of agreement. Digital signatures do not bind contracts to a particular time of origin. Usage of secure hash functions and the secure use of PKC ensure secure digital signature generation and verification processes. In some cases, digital signature schemes are linked to a particular hash function (for example digital signature algorithm (DSA) with SHA-1 hash function).

Security properties of hash functions:

The following are the fundamental security properties of hash functions [23].

1. Collision resistance: For a hash function H, it should be computationally infeasible to find two messages M_1 and M_2 such that $M_1 \neq M_2$ and $H(M_1) = H(M_2)$.
2. Preimage resistance: Given the digest $H(M)$ for a hash function H, it must be computationally infeasible to find M using only $H(M)$.
3. 2^{nd}-preimage resistance: Given a message M_1, it must be computationally infeasible to find another message M_2 such that $H(M_1) = H(M_2)$.

5.5 Digital Time-stamping

Time-stamping of digital signatures by a time-stamping authority (TSA) on contractual documents and archived documents provides proof of existence of those documents at a given point of time [27]. It can later be undoubtedly demonstrated that if digital signatures of that contract have been valid at the time of time-stamping.

The accuracy of a time stamp depends on the accuracy of the timeserver that allows the TSA to synchronise its system clock over the Internet. The time information provided by the timeserver to a TSA is directly traceable to the Universal Time Code. Accuracies, for example, of 1-50 milliseconds can be achieved using Network Time Protocol (NTP version 3) depending on the characteristics of the synchronisation source [24]. The following are the security properties of the digital time stamp issued by a TSA.

Security properties of the TSA:

1. It must be infeasible for a time stamping authority to time stamp a document with a date and time that is different from the correct one.
2. It must be infeasible to change even a single bit of a time stamped document without the change being apparent.
3. Relative temporal authentication [5, 18, 17] intuitively combines message authentication with the notion of timeliness of messages. The TSA is said to provide this property if one is able to decide which stamp has been issued first for each pair of time stamp. This is achieved by applying a collision resistant hash function to the earlier stamps which is then incorporated in the later time stamp.
4. The TSA must be reliable and available when needed [2].

6 E-contracting Collaborative Platforms

We have identified that web-based AEC collaborative platforms designed for project collaboration between two or more companies can be used "as they are" to conduct e-contracting. The on-line collaboration platforms provided in Table 1 have been reviewed based on the vendor claims and the review of the content in the documentation available in their websites but not from the analysis of the real collaboration platforms. Hence the analysis of these platforms given in Table 1 has been based on our insights and is provided without any implied warranty on its accuracy.

It seems that many of these platforms achieve our security requirements for e-contracting without the need of all the security mechanisms described in section 5. Most of them facilitate secure

e-contracting by providing user authentication, access control, document integrity and confidentiality mechanisms, logging and audit mechanisms for non-repudiation, proof of agreement and proof of existence. Note that in the Table 1, "Y" stands for Yes, "Trans." for Transmission and "?" for Unsure highlights that all of the reviewed construction collaboration platforms provide user authentication through a username and password mechanism. Every platform provides role-based access control to restrict the availability of documents to only the authorised personnel. Most platforms provide document integrity and confidentiality during the transmission and uploading of the documents, but very few appear to provide document integrity and confidentiality once a project is finished, when documents are archived or backed up. Most of the reviewed applications log user actions and have a file version control mechanism where a new file version is created for every update to a contract document.

Table 1. Security Features of Reviewed Collaborative Platforms

Platform	Authentication	Access Control	Integrity	Confidentiality	Log & Auditing
Aconex [3]	Y	Y	Y	Trans.	Y
Citadon CW [7, 8]	Y	Y	Trans.	Y	Y
Constructware [9]	Y	Y	Trans.	Trans.	Y
TeamBinder [13]	Y	Y	Trans.	Trans.	?
ECM [10]	Y	Y	?	?	Y
E-Builder [12]	Y	Y	?	?	Y
Evoco [30]	Y	Y	?	?	Y
Information Channel [29]	Y	Y	?	?	Y

7 Conclusion

In this paper, we have identified seven security requirements for e-contracts and the mechanisms of an e-contracting system to achieve those security requirements. We have commented on the security of several AEC collaborative platforms used for e-contracting stating how these platforms possess the mechanisms to achieve the security requirements identified for e-contracting.

References

1. Samuil Angelov, Sven Till, and Paul Grefen. Dynamic and Secure B2B E-contract Update Management. In *EC'05: Proceedings of the 6th ACM conference on Electronic commerce*, pages 19–28. ACM Press, 2005.
2. Arne Ansper, Ahto Buldas, Märt Saarepera, and Jan Willemson. Improving the availability of time-stamping services. In Y. Mu V. Varadharajan, editor, *Information Security and Privacy : 6th Australasian Conference (ACISP)*, Lecture Notes in Computer Science, pages 360–375. Springer, 2001.
3. Aconex Australasia. Aconex australasia - online information management solutions. The link is available at `http://www.aconex.com/index.php?selectedSite=au`. Last access date: 25th of October 2006.
4. Paul Berning and Shaye Diveley-Coyne. E-commerce and the construction industry: The revolution is here, 2000. This paper is available at `http://www.constructionweblinks.com/Resources/Industry_Reports_Newsletters/Oct_2_2000/e-commerce.htm`. Last access date: 25th of October 2006.
5. Ahto Buldas, Helger Lipmaa, and Berry Schoenmakers. Optimally efficient accountable time-stamping. In Hideki Imai and Yuliang Zheng, editors, *PKC: International Workshop on Practice and Theory in Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pages 293–305. Springer, 2000.
6. Daniel Burgwinkel. Managing contractual relationships in virtual organizations with electronic contracting. In Luis M. Camarinha-Matos, editor, *Collaborative Business Ecosystems and Virtual Enterprises*, volume 213 of *IFIP International Federation for Information Processing*, chapter 12, pages 101–108. Springer, 1 edition, 2005.
7. Citadon. Citadon Collaborative Workspaces. The link is available at `http://citadoncw.citadon.com/support/CitadonCW/`. Last access date: 31st of July 2006.
8. Citadon. Security-Network Operations Security Policy. This document is obtained through a personal communication from the Director, Corporate Sales of Citadon.
9. Autodesk Constructware. Autodesk Constructware - Features & Benefits. The link is available at `http://usa.autodesk.com/adsk/servlet/index?siteID=123112&id=7104129`. Last access date: 26th of July 2006.
10. Autodesk Constructware. Causeway Behind the Profitability of the Construction Industry. The link is available at `http://www.causeway.com`. Last access date: 1st of August 2006.
11. Tim Dierks and Christopher Allen. The TLS protocol version 1.0. Internet Request for Comment RFC 2246, Internet Engineering Task Force, January 1999. Proposed Standard.
12. E-Builder. e-Builder - Construction Project Management. The link is available at `http://www.e-builder.net`. Last access date: 3rd of August 2006.
13. E-Builder. TeamBinder Project Collaboration Software. The link is available at `http://www.teambinder.com/teambinder/Home/`. Last access date: 31st of July 2006.
14. Kendall Freeman. Concluding Contracts by E-mail and the Use of Electronic Signatures. *In-House Lawyer, Issue 132*, July/August 2005. This article is available at the link `http://www.kendallfreeman.com/publications/in-houselawyer.asp`. Last Access date: 5th of May 2006.
15. Alan Freier, Philip Karlton, and Paul Kocher. The SSL protocol version 3.0- internet draft, 1996. This Internet Draft is available at the link `http://wp.netscape.com/eng/ssl3/ssl-toc.html`.Last date of access: 22nd of October 2006.

16. Dieter Gollmann. *Computer Security*, chapter Security Models. John Wiley & Sons, 1999.
17. Mike Just. *On the Temporal Authentication of Digital Data*. PhD thesis, Carleton University, 1998.
18. Mike Just. Some timestamping protocol failures. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98)*. Internet Society, March 1998. The paper is available at the link http://www.isoc.org/isoc/conferences/ndss/98/just.pdf. Last access date:6th of April 2006.
19. J.W.Carter and D.J.Harland. *Contract Law in Australia*. Butterworths, Sydney, 3rd edition, 1996.
20. Konstantin Knorr and Susanne Röhrig. Security Requirements of E-business Processes. In *I3E*, pages 73–86, 2001.
21. William McGovern and Lary Lawrence. *Contracts and Sales: Cases and Problems*. Matthew Bender, Sydney, 1st edition, 1986.
22. Arion Meier and Susanne Röhrig. Security Levels for Contracting Agents. In *SEC*, pages 495–506, 2002.
23. Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*, chapter Hash Functions and Data Integrity, pages 321–383. The CRC Press series on discrete mathematics and its applications. CRC Press, 1997.
24. David L. Mills. Network time protocol (version 3) — specification, implementation and analysis. Internet draft standard RFC 1305, March 1992.
25. National Institute of Standards and Technology. *Federal Information Processing Standards (FIPS) PUB 186-2: Digital Signature Standard (DSS)*. pub-NIST, January 2000. The document is available at `http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf`. Last Access date: 3rd of April 2006.
26. Susanne Röhrig and Konstantin Knorr. Security Analysis of Electronic Business Processes. *Electronic Commerce Research*, 4(1-2):59–81, 2004.
27. Security Technology Competence Centre (SETCCE). Trusted Electronic Archive. White Paper, September 2005. This document is available at `http://www.setcce.si/eng/download/Trusted_Electronic_Archives_-_White_Paper.pdf`.
28. Richard Stim. *License Your Invention: Sell Your Idea and Protect Your Rights with a Solid Contract "With CD"*, chapter Sample Agreement, pages 11–27. 2004.
29. BIW Technologies. BIW Technologies Ltd - Services / Information Channel. The link is available at `http://www.biwtech.com/services/ic.asp`. Last access date: 2nd of August 2006.
30. BIW Technologies. Web Based Collaboration Software & Online Document Management from Evoco - Specializing in Construction Project Management. The link is available at `http://www.evoco.com`. Last access date: 1st of August 2006.
31. Norman Walsh. A Technical Introduction to XML, 1998. The document is available at `http://www.xml.com/pub/a/98/10/guide0.html`. Last access date: 30th of October 2006.
32. Paul Wilkison. *Construction Collaboration Technologies- The extranet evolution*. Taylor & Francis, 1st edition edition, 2005.