Secure E-commerce Protection Profile

Anil Kumar Venkataiahgari
Department of Computer Science
and Software Engineering
Concordia Univeristy
Montreal, Quebec, Canada

Mourad Debbabi
Concordia Institute for
Information Systems Engineering
Concordia University
Montreal, Quebec, Canada

J. William Atwood
Department of Computer Science
and Software Engineering
Concordia Univeristy
Montreal, Quebec, Canada

Abstract

We present a Secure E-commerce Protection Profile (SEPP) that captures security requirements for securing sessions in the e-commerce operational environment. The SEPP is prepared in accordance with the Common Criteria (CC), Version 2.1, as specified by the ISO 15408 standard. The SEPP states the requirements that sessions must satisfy in order to respond to the needs of e-commerce. The Target of Evaluation (TOE) security environment, which is composed of threat agents, vulnerabilities, attacks and threats, is described in detail. It is followed by describing the administrative security policies that are necessary to safeguard the TOE or its operating environment. The risks to the TOE are identified. The security objectives for the TOE are stated.

Keywords: Security, e-commerce, Protection Profile (PP), unicast, multicast, Common Criteria (CC)

1. Introduction

Security is a significant concern for e-commerce, whether it is for unicast, multicast or broadcast services. Also, liability is a significant issue because the subscriber has to share his sensitive credentials, such as credit card information, with unknown principals, while merchants have to make sure that they are providing the services only to the authenticated and authorized customers. There are several unicast e-payment platforms and protocols such as credit card based, e-Cash based, e-Cheque based, Smartcard based and Micropayments based e-payment platforms [10, 27] and e-payment protocols, such as Secure Socket Layer/ Transport Layer Security (SSL/TLS) [23], Secure Electronic Transactions (SET) [24], i-Keyed Protocol (iKP) [25], which enable a merchant to conduct a one-to-one exchange with its customers. However, these platforms and protocols cannot be directly applied in the context of e-payments in multicast and broadcast scenarios as the infrastructure would not scale to wider population and would suffer a limitation on scalability.

Several researchers have discussed and proposed e-commerce protocols for securing e-commerce transactions. D. Gollmann [30] has described the e-commerce security issues by outlining the role of cryptography, digital signatures and non-repudiation, public key infrastructure, etc. Randy and Joseph [4] discuss the security issues and countermeasures by describing the threats to e-commerce, privacy issues, and Distributed Denial of Service (DDoS) attacks. In [31], C. Yang and C. N. Zhang have proposed an efficient method for managing security policies using XML and role based access control. They claim that their role based access control model for web-based applications simplifies security policy administration for web-based applications. In [32], S. W. Tak et al. proposed a design and evaluation of an adaptive security protocol to support secure e-commerce transactions. Although these papers shed some insight into the security issues of e-commerce environments, they concentrate on implementation, without addressing formal security requirements of the e-commerce environment.

To our knowledge, no one has formally captured the security requirements of e-commerce sessions. A basis for such a formal review is provided by the Common Criteria (CC), Version 2.1, as specified in the ISO 15408 standard [33].

Principal parties would have many questions for which they seek an answer such as the following:

- Who will conduct the authentication process?
- How to verify the identity of the subscriber, and legitimacy of the merchant?
- What kinds of information must be verified?
- What authority and access privileges should be enforced?
- What kinds of audits are required, if an error or session compromise occurs?

- What is the liability and risk involved in the transaction processes?
- What are the technical and non-technical issues and performance tradeoffs to consider when applying security and key management techniques in support of unicast, multicast or broadcast environments?

These security issues are of even more concern in multicast/broadcast networks, as the risk in compromising a session is far greater in such environments compared to unicast due to the fact that the data are now open to a much wider population.

This paper introduces the Secure E-commerce Protection Profile (SEPP), by presenting the security issues, both technical and non-technical, that are relevant to the Target of Evaluation (TOE), i.e., e-commerce environment. We discuss the security issues of any session (i.e., unicast, multicast or broadcast) such as: membership dynamics (especially in the multicast case [2, 6]); authentication (identification of principals) [12]; authorization (providing the session keying material only to the authorized subscriber(s)); resource accounting (which has implications on the network support for non-repudiation of principal parties); group management (dealing with key management [1] and the 1-affects-N problem [3]); scalability [3, 7, 9]; robustness (ability to continue functioning under load).

2. Target of Evaluation

This section provides context for the Target of Evaluation (TOE) by stating the features that are outside the scope of TOE discussion and the security features of the TOE that must be considered for securing sessions. The TOE aims to outline e-commerce security features such as authentication and authorization of e-commerce parties, protection of data confidentiality, data integrity, non-repudiation of parties and accountability.

2.1. Features outside of scope

There are several requirements of securing sessions in an e-commerce environment. However, addressing each requirement requires a lot of insight into several research areas. Therefore, we separate the features that this Protection Profile (PP) addresses from those that are outside the defined TOE. The TOE features that are outside the scope of the defined TOE are stated as follows:

- *Physical security:* Protection of the components at the physical layer.
- *Multicast group management:* The technical and non-technical complexity involved in managing the multicast groups [3].
- *Multicast session Key management:* Multicast session key distribution that relates to the multicast key management [1].
- *External environment:* Threats, risks, and security objectives evolving from outside the defined TOE.
- *Ad hoc networks attacks:* Attacks specific to the wireless networks such as wormhole attack [28], blackhole attack [29], rushing attack [26], etc.
- *Certified delivery:* The issues related with the guaranteed goods/service delivery for the subscriber's e-payment.

2.2. Security features of the TOE

The security features of the TOE are the properties that govern the security infrastructure of the e-commerce interaction. The following security features are identified as essential features that the TOE is intended to provide to e-commerce sessions.

- *Authentication:* Authenticate subscribers, merchant's content providers, messages in transit and principals [11].
- *Confidentiality:* Prevent or detect leakage of sensitive data.
- *Integrity:* Prevent or detect corruption of sensitive data.
- *Authorization:* Authorize subscribers and their e-payments.
- *Non-repudiation:* Collect a non-refutable proof of a principal's involvement in e-transactions such as identifying and time stamping who communicated with whom, how much and how often.
- *Accountability:* Define revenue collecting method (revenue collection at the sender or receiver side).
- *Money atomicity:* Guarantee that the e-commerce protocols neither create nor destroy money [19].
- *Goods atomicity:* Guarantee that the merchant receives e-payments only if the subscriber receives the goods/service.
- *Anonymity:* Provide support to allow anonymous events such as anonymity of transaction, subscriber and description of goods.

3. TOE security environment

The TOE security environment classifies the nature of security problems the TOE is intended to address. It describes the assumptions, threat agents, vulnerability sources, sources of attack, and threats to the TOE or its security environment. It concludes by stating the organizational security policies with which the TOE is intended to be operational.

3.1. Assumptions

The TOEs usage assumptions state the assumptions that are made in the TOE security environment. We outline below the assumptions that dictate the operating environment of the TOE.

- *Privileged user:* Authorized administrators or the Trusted Third Persons (TTPs) (e.g., registration authority and certification authority) are implicitly assumed to be trustworthy; however, they can act unfairly if they have flaws in their governance.
- *Outside threat:* The TOE operating environment is assumed to have the necessary protocols to resolve any security threat that emerges from outside the defined TOE such as a natural calamity like an earthquake, fire, flood, etc.

3.2. Threats to security

This section identifies the threat agents that are responsible for causing damage to the TOE security. This is followed by identifying the sources of vulnerability and attack that could possibly threaten the security of the TOE or its environment. The intended organizational security policies are described in the last section to counter these security threats.

3.2.1. Threat agents. A threat agent is a computing or communicating principal that is identified as instigating a specific class of threats to the TOE security environment. We classify threat agents based on the principal party's expertise requirement, resource usage, and the motivation of their threat. These threat agents arise due to both the dynamic nature of the host groups and due to the interference of privileged and unprivileged principal parties with the customer, merchant and the communicating network. The threat agents relevant to the TOE or its operating environment are described in Table 1 as follows:

Table 1: Threat Agents for the TOE

Threat Agent Label	Threat Agent	Resources	Expertise	Motivation
TA.GOOD_INSIDER	TTPs, policy server, service provider, merchant	Moderate/ Substantial	Low/ High	Non-malicious
TA.BAD_INSIDER	Malicious service provider, malicious merchant, malicious subscribed customer	Moderate/ Substantial	Low/ High	Malicious
TA.LEGAL_HOST	Subscribed customer	Moderate/ Substantial	Low/ High	Malicious
TA.PREV_NEW_HOST	Former subscribed customer, new subscriber	Moderate	Low/ High	Malicious
TA.INVADER	Unprivileged external sources	Minimal/ Moderate	High	Malicious

3.2.2. Sources of vulnerability. Several sources of vulnerability could appear due to improper system design, improper application of security protocols, improper or unclear service parameters, underlying protocol weaknesses, single point of failure, etc. The sources of vulnerability that are applicable to the TOE or its operating environment are stated as follows.

- *V.ARCH_DES*
  - *Vulnerability:* Improper system architecture and design supporting e-commerce
  - *Description:* Poor system architecture and design leading to disputes by the subscribers, merchants, payment systems over the service charges; overall resulting in unreliable e-commerce with security holes and breaches
- *V.AUTH_PROT*
  - *Vulnerability:* Use of clear text authentication protocols
  - *Description:* Weak remote user authentication and authorization techniques leading to severe security breaches in the framework
- *V.PAY_PROT*
  - *Vulnerability:* Poor development of e-payment systems
  - *Description:* Inefficient payment platforms or protocols application to e-commerce without proper quality testing will jeopardize security features such as confidentiality, integrity, availability and money atomicity
- *V.MIDDLEWARE*
  - *Vulnerability:* Poor middleware design and development
  - *Description:* Improper middleware application to e-commerce leading to inefficient data access and/or security breaches in the framework
- *V.SERV_PARAM*
  - *Vulnerability:* Not clearly defined service policies, service parameters
  - *Description:* Merchants trust relation with the subscriber at risk due to unclear specifications of the service policies, unclear session parameters jeopardizing availability of the services
- *V.POLICIES*
  - *Vulnerability:* Insufficient and unclear plans, procedures and policies
  - *Description:* Overstated or undermined plans, procedures and policies with no formal

validation or justification will result in substantial loss of resources and time

- *V.SPOF*
  - *Vulnerability:* Single Points of Failure
  - *Description:* Inefficient routing protocols usage or improper design layout resulting in points of failure at a source of data transfer resulting in service disruption

3.2.3. Sources of attack. The sources of attack arise not only due to the operating environment of the TOE but also due to the weaknesses in the underlying protocols that dictate the TOE operating environment. It is possible that there exist several kinds of sources of attack on different operating environments. We define below the possible attack sources that are specific to the TOE or its operating environment.

- *A.REPLAY:* It is a type of man-in-the-middle (MITM) attack that exploits the weaknesses in the system design and implementation of the protocols to launch an attack such as replay attacks [14].
- *A.DOS:* Denial of Service (DoS) and DDoS attacks are also a type of MITM attack that mostly involves either resource exhaustion or corruption of the OS runtime environment such as UDP bombing, ICMP or Smurf attacks or memory overflow attacks, TCP SYN flooding, CGI bin attacks [4, 5, 13].
- *A.SNIFF:* Sniffing captures data packets on the network and favors analysis of the network protocol to launch further attacks. There are many free tools available on Internet such as DSniff, AirSnort, etc [15].
- *A.SPOOF:* Spoofing exploits weaknesses in the user authentication protocols [16].
- *A.BRUTE:* Attack exploits weaknesses in the underlying cryptographic building blocks used in the payment system such as cryptanalysis [10] or Brute force attacks [17].
- *A.SOCIAL_ENGG:* Compromising network security by counterfeiting a legitimate principal to give away hints enough to break into system and launch malicious attacks such as virus attacks, data modification [18].
- *A.MALCODE:* Compromised network may lead to spreading virus or worms (malicious codes) to the service provider, its subscribers or other interacting principals. A good insight into popular viruses, Trojan horses and worms in the Internet can be found in [20].
- *A.BUFFER_FLOW:* Attacker places malicious script/code in the buffer's overflowing area that may pose as an attack at the time of program execution [21].
- *A.SQL_INJECT:* The attacker injects a code that does not filter input that is being entered directly into a form. This injected code poses as an attack once the attacker gets access to protected data [22].
- *A.FORMAT_STR:* The attack is due to the use of unfiltered user input as the format string parameter in programming language functions that perform formatting. For example, in C language, the printf() function can be exploited by a user to crash the program or execute malicious code [8].
- *A.ERROR:* A privileged user accidentally issues a bad command, which results in disputes among principals.

Now, we would describe the types of threat in terms of the threat agents that cause the respective attacks. A threat in an operating environment could arise due to its trusted staff and dishonest staff, authorized user and unauthorized user, virus or worm spreading, etc. The threat description would also provide a statement of the assets that will be prone to a threat. We describe in Table 2 the threats that are intended to be addressed by the TOE, based on the sources of threats possibly from threat agents and sources of attacks that were captured in the previous sections.

Table 2: Threats to the TOE

Threat Label	Threat Agent	Attack
T.MAL_ANALYSIS	TA.BAD_INSIDER, TA.PREV_NEW_HOST, TA.INVADER	A.SNIFF, A.SOCIAL_ENGG
T.MAL_MODIFY	TA.BAD_INSIDER, TA.PREV_NEW_HOST, T.INVADER	A.SNIFF, A.SPOOF, A.MALCODE, A.BUFFER_OVER, A.SQL_INJECT, A.FORMAT_STR
T.CONFIDENTIAL	TA.BAD_INSIDER, TA.LEGAL_HOST, TA.PREV_NEW_HOST, TA.INVADER	A.SPOOF, A.SOCIAL_ENGG, A.SQL_INJECT, A.FORMAT_STR
T.COVERT_CHANNEL	TA.BAD_INSIDER, TA.LEGAL_HOST, TA.PREV_NEW_HOST, TA.INVADER)	A.SOCIAL_ENGG, A.MALCODE, A.SQL_INJECT, A.FORMAT_STR
T.BAD_COMMAND	TA.GOOD_INSIDER	A.ERROR
T.SPOOF	TA.BAD_INSIDER, TA.LEGAL_HOST, TA.PREV_NEW_HOST, TA.INVADER	A.SPOOF, A.SOCIAL_ENGG
T.REPUDIATE	TA.GOOD_INSIDER, TA.LEGAL_HOST	A.REPLAY, A.DOS, A.SNIFF, A.SPOOF, A.SOCIAL_ENGG, A.MALCODE
T.DOS	TA.BAD_INSIDER, TA.PREV_NEW_HOST, TA.INVADER	A.DOS
T.ERROR_RECORD	TA.GOOD_INSIDER	A.BUFFER_FLOW, A.ERROR
T.VIRUS	TA.GOOD_INSIDER, TA.BAD_INSIDER, TA.LEGAL_HOST, TA.PREV_NEW_HOST, TA.INVADER	A.MALCODE

Each of the above threat labels is explained as follows. T.MAL_ANALYSIS occurs as malicious users analyze sensitive information in host machines, in servers or data in transit. MAL_MODIFY occurs as malicious users modify sensitive information. T.CONFIDENTIAL occurs as malicious and non-malicious principal parties impersonate others. T.COVERT_CHANNEL occurs as malicious and non-malicious principal parties encapsulate a malicious protocol within a given protocol that (normally) bypasses the protected network's firewall. The receiving program in the protected network would then accept this malicious protocol. BAD_COMMAND occurs as trusted principal parties accidentally issue a bad command that may pose as an attack. T.SPOOF occurs as malicious and non-malicious principal parties attack to obtain sensitive information. T.REPUDIATE occurs as authorized and trusted principal parties deny their participation in a session due to an attack that result in disputes with the suspected principals. T.DOS occurs as malicious principal parties attack to temporarily halt the service to the legitimate subscribers. T.ERROR_RECORD occurs as a trusted principal party's attack was ignored or undetected, and therefore the threat remains unaddressed. T.VIRUS occurs as principal parties spread a virus/worm to the principal machines causing data corruption.

3.3. Administrative security policies

This section gives very brief keywords for the administrative security policies that define the organizational support and governance that is required to maintain the safety/security of the TOE or its operating environment. More details in [33].

- *P.MONITOR:* Monitoring of security events.
- *P.CONFIG:* Proper configuration of protocols.
- *P.AWARE:* Personnel know their role in maintaining security.
- *P.ACCOUNT:* Precisely how is revenue collected?
- *P.DOCUMENT:* Security goals and protocols should be well documented.
- *P.RISK:* Risks should be carefully managed.

4. Risk categories for the TOE

Each risk to a principal party or any computing device could be categorized by assessing sources of threat and sources of vulnerability that we have discussed in previous sections. The categories of security risks that are relevant to the TOE are defined as in Table 3. We have provided a non-exhaustive list of risks that are associated with existing and potential subscribers, merchants, content providers, security policies, unavailability of service resources, e-payment principles, services, privacy, confidentiality, and trusted protocols and components.

Table 3: Risk categories for the TOE

Risk Category Label	Threat	Vulnerability
R.FAIR_HOST (Risks associated with the subscribed user)	T.CONFIDENTIAL, T.BAD_COMMAND, T.REPUDIATE, T.VIRUS, T.ERROR_RECORD	V.ARCH_DES, V.AUTH_PROT, V.PAY_PROT, V.POLICIES
R.OUTSIDER (Risks associated with new subscribers or unsubscribed users)	T.MAL_ANALYSIS, T.MAL_MODIFY, T.CONFIDENTIAL, T.SPOOF, T.DOS, T.VIRUS	V.ARCH_DES, V.AUTH_PROT, V.PAY_PROT, V.MIDDLEWARE, V.SERV_PARAM, V.POLICIES
R.SELLER (Risks associated with the merchant or merchant's content provider)	T.MAL_ANALYSIS, T.MAL_MODIFY, T.CONFIDENTIAL, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.ERROR_RECORD, T.VIRUS	V.ARCH_DES, V.AUTH_PROT, V.PAY_PROT, V.MIDDLEWARE, V.SERV_PARAM, V.POLICIES, V.SPOF
R.SECPOLICY (Risks associated with the security policies in place and with the new ones as they evolve by appending, replacing or modifying existing policies)	T.CONFIDENTIAL, T.BAD_COMMAND, T.REPUDIATE, T.ERROR_RECORD, T.VIRUS	V.ARCH_DES, V.PAY_PROT, V.MIDDLEWARE, V.SERV_PARAM, V.POLICIES, V.SPOF
R.UNAVAILABLE (Risks associated with unavailability of service resources)	T.CONFIDENTIAL, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.ERROR_RECORD, T.VIRUS	V.ARCH_DES, V.AUTH_PROT, V.PAY_PROT, V.MIDDLEWARE, V.SERV-_PARAM, V.POLICIES, V.SPOF
R.UNFAIR_CHARGE (Risks associated with the payment principles for the subscribed sessions such as collection of revenue for un-available service)	T.MAL_ANALYSIS, T.MAL_MODIFY, T.CONFIDENTIAL, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.ERROR_RECORD, T.VIRUS	V.ARCH_DES, V.PAY_PROT, V.SERV_PARAM, V.POLICIES, V.SPOF
R.MAL_SERV (Risks associated with the illegal use, modification or destruction of service provider's service)	T.MAL_ANALYSIS, T.MAL_MODIFY, T.CONFIDENTIAL, T.BAD_COMMAND, T.SPOOF, T.ERROR_RECORD, T.VIRUS	V.AUTH_PROT, V.PAY_PROT, V.MIDDLEWARE, V.SERV_PARAM, V.POLICIES, V.SPOF

R.PRIVACY (Risks associated with the threat to privacy, message confidentiality)	T.MAL_ANALYSIS, T.SPOOF, T.CONFIDENTIAL	V.ARCH_DES, V.AUTH_PROT, V.MIDDLEWARE, V.SERV_PARAM, V.POLICIES, V.SPOF
R.COMPONENTS (Risks associated with the trusted protocols or components misbehavior in the framework)	T.CONFIDENTIAL, T.REPUDIATE	V.ARCH_DES, V.AUTH_PROT, V.PAY_PROT, V.SERV_PARAM, V.POLICIES

5. Security objectives for the TOE

The security objectives are intended to provide shielding against the security threats, attacks, and vulnerabilities that arise due to breaches in the TOE or its operational environment. The security objectives for the TOE are described as follows:

- *O.PHYSICAL:* The access to and from the trusted devices must be bounded and shall be free of unauthorized logins.
- *O.BACKUP:* The TOE must include provisions for session's data and control signals to possess the capabilities for timely recovery to an operating state if the session is compromised or damaged in transactions.
- *O.RISK_ANALYSIS:* The TOE shall perform session's security risk analysis for random transactions to evaluate the future continuity of e-commerce.
- *O.AUTHENTICITY:* The TOE shall authenticate the principal parties and devices that are essential for continuity of e-commerce.
- *O.CONFIDENTIALITY:* The TOE protocols shall protect the confidentiality of information of subscriber, merchant, or any other principal's asset.
- *O.PRIVACY:* The TOE protocols shall protect the privacy of information of subscriber, merchant, or any other principal's asset.
- *O.COMPLY:* The administrating body, underlying protocols and computing systems shall comply with the International regulations, governing mandates, policies and controls that govern the deployment of the designed framework and its underlying protocols. This will ensure the safety of the system and its operators.
- *O.AUTHORIZE:* The TOE shall have the policies in-place to authorize all the principal parties involved in the e-commerce transactions as well as it must have flexibility to authorize new components as they evolve (due to change in administrative policies).
- *O.AVAILABILITY:* The TOE shall have the necessary protocols that ensure that the concerned principal parties have received the session keys that dictate the access to the services.
- *O.INTEGRITY:* The TOE shall have the necessary protocols that ensure the protection or detect the corruption of the distributed key(s) that dictate the success or failure of an e-commerce transaction.
- *O.ACCOUTABILITY:* The TOE shall have necessary protocols to make sure that the subscriber is charged only if he receives the service.
- *O.UPGRADE:* Mechanism to anticipate the network growth and plan upgrades to increase the service components such as number of routing devices, ports.
- *O.SCALABILITY:* The TOE shall have the necessary infrastructure and protocols for reducing the signaling overhead among various principals in an e-commerce transaction.

6. Conclusion

The SEPP is prepared in accordance with CC Version 2.1 as specified by ISO 15408. The whole idea of documenting SEPP is to give the reader a clear understanding of the security requirement specifications and operational controls that are needed to secure sessions in the e-commerce operational environment. The follow-up of SEPP specifications would facilitate any protocol developer to cross check the applicability of the developed protocol with SEPP to perceive if it meets the security requirements of e-commerce operational environment for any network. The developer or administrators can also know the constraints with which TOE security environment works. TOE security environment clearly states the threat agents, sources of vulnerabilities and possible attacks, and administrative security policies that must be in place to secure the operational environment. SEPP also identifies and categorizes the risks to TOE and provides its direct implication with the associated threats and vulnerabilities. The SEPP concludes by stating the security objectives that are intended to provide shielding to the security threats, attacks, vulnerabilities that arise due to breaches in TOE or its operational environment. Thus, SEPP security specs reveal that it is not possible for just one reliable protocol to fit each and every application.

Acknowledgements

J.W. Atwood and M. Debbabi acknowledge the support of the Natural Sciences and Engineering Research Council of Canada, through its Discovery Grants program.

References

[1] S. Rafaeli, D. Hutchison, "Survey of key management for secure group communication", *ACM Computing Surveys*, 2003, vol. 35, no. 3, pp. 309-329.

[2] G. Caronni, K. Waldvogel, D. Sun, B. Plattner, "Efficient Security for Large and Dynamic Multicast Groups", *In IEEE 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'98)*, Los Alamitos CA: IEEE Computer Society, 1998, pp. 376-383.

[3] S. Mittra, "The Iolus framework for scalable secure multicasting," *In proceedings of ACM SIGCOMM'97*, 1997, pp. 277-288.

[4] Randy C. Marchany and Joseph G. Tront, "E-Commerce Security Issues", *35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)*, 0-7695-1435-9/02 IEEE, 2002.

[5] S. Xu, R. Sandhu, "Authenticated Multicast Immune to Denial-of-Service Attacks", *ACM SAC*, 2002.

[6] P. Judge, M. Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey", *IEEE Network*, January-February 2003.

[7] D. M. J. Moyer, J. R. Rao, P. Rohatgi, "A Survey of Security Issues in Multicast Communications", *IEEE Network Magazine*, November-December 1999.

[8] T. Newsham, "Format String Attacks", *Guardent, Inc.*, September 2000.

[9] T. Hardjono, G. Tsudik, "IP Multicast Security: Issues and Directions", *Annales de Telecom*, July-August 2000, pp. 324-340.

[10] N. Asokan et. al., "State of the Art in Electronic Payment Systems", *Advances in Computers*, Academic press, Vol. 43, March 2000, pp. 425-449.

[11] A. Basu, S. Muylle, "Authentication in e-commerce", *Communications of the ACM*, December 2003, vol. 46, no. 12, pp. 159-166.

[12] A. Perrig, R. Canetti, D. Song, J. D. Tygar, "Efficient and secure source authentication for multicast", *Network and Distributed System Security Symposium*, NDSS '01, February 2001, pp. 35- 46.

[13] A. Habib, M. Hefeeda, B. K. Bhargava, "Detecting Service Violations and DoS Attacks", *NDSS* 2003.

[14] S. Keung, K. Y. Siu, "Efficient protocols secure against guessing and replay attacks", *In Proceedings of the 4th International Conference on Computer Communications and Networks (ICCN)*, 1995, pp. 105-112.

[15] Sniffing frequently asked questions: http://cs.ecs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm

[16] E. W. Felten, D. Balfanz, D. Dean, D. S. Wallach, "Web Spoofing: An Internet Con Game", *20th National Information Systems Security Conference*, October 1997.

[17] J. T. Trostle, "Timing attacks against trusted path", *Proceedings of 1998 IEEE Symposium on Security and Privacy*, May 1998, pp. 125-134.

[18] L. Orgill, W. Romney, G. Bailey, M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems", *In Proceedings of the 5th conference on Information technology education*, U.T, U.S.A, 2004, pp. 177-181.

[19] J. D. Tygar. "Atomicity in Electronic Commerce", *In Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing*, 1996, pp. 8-26.

[20] Randy C. Marchany and Joseph G. Tront, "E-Commerce Security Issues", *35th Annual Hawaii International Conference on System Sciences (HICSS)*, January 2002, pp. 2500-2508.

[21] J. McGregor et. al., "A Processor Architecture Defense Against Buffer Overflow Attacks", *In Proc. of the IEEE International Conference on Information Technology: Research and Education (ITRE)*, August 2003, pp. 243-250.

[22] Stephen Kost, "An Introduction to SQL Injection Attacks for Oracle Developers", HelpNet-Security, January 2004.

[23] L. C. Paulson, "Inductive analysis of the internet protocol TLS", *ACM Transactions on Information and System Security*, vol. 2, no. 3, August 1999, pp. 332-351.

[24] SET business description, programmer's guide, formal protocol definition, and protocol description: http://www.cl.cam.ac.uk/Research/Security/resources/SET/

[25] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Henreweghen, M. Waidner., "Design, implementation and deployment of the iKP secure electronic payment system", *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, April 2000, pp. 611-627.

[26] Yih-Chun Hu et. al., "Rushing attacks and defense in wireless ad hoc network routing protocols", *2003 ACM Workshop on Wireless Security*, ACM Press, pp. 30–40, 2003.

[27] M. Sirbu, "Credits and Debits on the Internet", *IEEE Spectrum*, vol. 34, no. 2, February 1997, pp. 23-39.

[28] Yih-Chun Hu et. al., "A defense against wormhole attacks in wireless ad hoc networks", In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03)*, April 2003.

[29] Yih-Chun Hu et. al., "A secure on-demand routing protocol for ad hoc networks", *8th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '02)*, September 2002.

[30] Dieter Gollmann, "*E-commerce security"*, *Computing & Control Engineering Journal*, Vol.11, No.3, pp. 115-118, 2000.

[31] Cungang Yang, Chang N. Zhang, "Designing Secure E-Commerce with Role-based Access Control," *2003 IEEE International Conference on E-Commerce Technology* (CEC'03), p. 313, 2003.

[32] S. W. Tak, Y. Lee, E. K. Park, J. Stach, "Design and Evaluation of Adaptive Secure Protocol for E-Commerce", *IEEE International Conference on Computer Communications and Networks* (ICCCN-2001), pp. 32-39, 2001.

[33] Anil Kumar Vankataiahgari, "Secure E-commerce Transactions for Multicast Services", Master of Computer Science Thesis, Department of Computer Science and Software Engineering, Concordia University, December 2005.