

Security Issues in Customer Relationship Management Systems (CRM)

Huei Lee

Eastern Michigan University
Department of Computer Information Systems; Ypsilanti, MI 48197
734-487-4044
Huei.lee@emich.edu

Kuo Lane Chen

University of Southern Mississippi
School of Accountancy and Information Systems; Hattiesburg, MS 39406
601-266-5954
e-mail: chenku60@yahoo.com

Chen-Chi Shing

Radford University
Information Technology Department; Box 6933 Radford, VA 24142
cshing@radford.edu

Marn-Ling Shing

Taipei Municipal University of Education
Early Child Education Department and Institute of Child Development; 1 Ai-Kuo West Road, Taipei, Taiwan, R.O.C.,
shing@tmue.edu.tw

ABSTRACT

The purpose of this paper is to discuss the security issues in customer relationship management (CRM) systems and possible solutions to prevent attacks in CRM applications.

INTRODUCTION

The objective of customer relationship management (CRM) is to identify, acquire, and retain customers (Maurer, 2005). CRM software or systems include sales, services and customer support, call centers, sales force automation systems, and order management. In the last ten years, software companies attempts to consolidate some of these incongruent technologies into an integrated system (Lee & Chen, 2005). The sale of CRM applications is expected to reach more than 5 billion in 2005 (Lee & Chen, 2005; Nelson, Wecksell, & Frey, 2002; Buttle, 2003).

Because the CRM system is customer-centered, a multi-channel strategy is used by major CRM software. All kinds of machines such as handheld computers, fax machines, and cellular phones can be interface devices for accessing CRM systems. Among them, Internet access becomes a necessary requirement for most CRM systems. A major part of a CRM system can be classified as a B2C system. Convenience is a major characteristic for CRM systems; however, it also opens the doors for various security

attacks. These attacks range from denial of service (DOS), Mal-ware attacks, and identity theft. Methods to prevent these attacks in CRM systems become an emerging issue. The purpose of this paper is to discuss the security issues in CRM systems and possible methods to prevent security attacks (Panko, 2004).

MAJOR CRM SYSTEMS AND MAJOR COMPONENTS

Major CRM systems in the market today are Siebel, mySAP, and Oracle. Web-based software, such as Salesforce.com, is becoming very popular. Figure 1 shows a screen of the Salesforce.com. Major components of a CRM system include:

1. Sales
2. Call centers
3. Sales force automation systems
4. Order management
5. Customer support



Figure 1: Salesforce.com

POSSIBLE SECURITY ATTACKS TO A CRM SYSTEM

Possible security attacks in a CRM system are:

1. Denial of service. Denial of service (DOS) is to make the attacked system unavailable to customers. Possible attackers are angry customers, script kiddies, former employees, and the competitors.
2. Intrusion of sales automation systems and customer database. Sales Automation systems normally have numerous information about customers. Potential attackers can break into the systems and steal the customer information.
3. Identity theft. Identity theft happens when “someone uses your personal information without your permission to commit fraud or other crimes.”
4. Malware attacks. Malware includes viruses and worms; Malware attacks can cause the DOS, hardware damage, and data loss (Panko, 2004).

PROTECTION METHODS AND CONCLUSIONS

One of the problems with CRM systems is the tradeoff between security and convenience. These methods includes: using a good passwords, installing firewalls, installing anti-virus programs, and using virtual private network (VPN). Most common security method is to use user ID and passwords. However, simply using ID and passwords is not enough. Improved methods include use of a long password and the encryption of the passwords. Virtual Private Network (VPN) is the use of a secure channel in the Internet communications. Customer awareness is important in preventing the social engineering attack (Panko, 2004). This paper discussed possible attacks in a SCM system and possible methods to defend it. However, a survey must be done to find out what methods are effective and useful.

REFERENCES

- Buttle, F. (2003). Customer Relationship Management - Concept and Tools, Elsevier: Boston.
- Convery, S. (2004). Network Security Architectures, Cisco Press, Indianapolis, IN, 353-357.
- Fridahl, M. (April 8, 2004). Study: S.F. Area Has Most WiFi Hot Spots, <http://www.eweek.com>.
- Golvin, C. S. (2002) What Do Wi-Fi Consumers Look Like? Forrester Research.
- Henry, P. S. and Luo, H. (2002) Wi-Fi: What's Next? IEEE Communications Magazine, Dec, 40(12), 66-73.
- Holden, G. (2003). Guide to Network Defense and Countermeasures, Course Technology, Thomson Learning, Inc., Boston, MA.
- Kaneshige, T. (July 1, 2002). Wireless CRM Beckons, Line56, <http://line56.com/articles/?ArticleID=3806>, retrieved November 13, 2004.
- Kharif, O, (FEB, 18, 2004). Special Report: Wi-Fi's Growing Pains. Business Week Online.
- Lee, H. & Chen, K., “Secured Wireless Communications and the Customer Relationship Management (CRM) Applications”, Proceedings of IACIS Pacific 2005 Conference, Taipei, Taiwan, May 2005.

- S. Maurer. (Nov 4, 2005). "Identify, Acquire, And Retain Customers With CRM," <http://crmproductreview.com/crmproductreview-50-20051104IdentifyAcquireandRetainCustomerswithCRM.html>
- Nelson, S. Wechsell, J. and Frey, N. (2002). 2002 CRM Survey Points to solid Demand and Modest Growth. Strategic analysis Report, 24 May, Garner.
- Panko, R. R. (2004). Corporate Computer and Network Security, Prentice Hall, Upper Saddle River, NJ.
- Robb, D. (Feb 18 2004). 802.11g Not Necessarily Better, <http://www.wi-fiplanet.com>
- Siebel, <http://www.crmondemand.com/crm/what-is-crm.jsp>, retrieved, May 2005.
- Songini, M. (November 5, 2001). Wireless CRM: Strings Attached. Computerworld, <http://www.computerworld.com/softwaretopics/crm/story/0,10801,65277,00.html>.
Retrieve: November 13, 2004.
- Wildstrom, S. H. (February 19, 2004). How-To's of Wi-Fi, Business Week Online.
- Whitman, M.E., Mattord, H. J. (2003). Principle of Information Security, Course Technology, Thomson Learning, Inc., Boston, MA.
<http://www.consumer.gov/idtheft/>, retrieved, Oct 2005.