International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:3, 2007

The Future of Electronic Money

Maria E. de Boyrie, Darlene Nelson, and James A. Nelson

***Abstract*—**The history of money is described in relationship to the history of computing. With the transformation and acceptance of money as information, major challenges to the security of money have involved engineering, computer science, and management. Research opportunities and challenges are described as money continues its transformation into information.

***Keywords*—**Electronic, information, money, risk.

I. Introduction

TRADITIONALLY, banks were like fortresses with thick stone walls, steel vaults, and metal cages surrounding the teller windows. This model of banking was necessary because in the past money had intrinsic value in the form of scarce metals such as gold and silver. Gold and silver meet the basic characteristics of money: a medium of exchange, unit of account, store of value, and more difficult in today's electronic world – be anonymous. Many economists and libertarians feel that money should not contain information about transactions, and more controversial, should be useable in an anonymous environment, including black markets [1].

II. The Walls of the Fort

Banks were meant to provide a safe and trusted storage site and a secure area for transactions. The use of paper to represent money was a move to the idea that a symbol could be used to represent gold or silver and could be "on-demand" converted to the precious metals. Paper currency was much easier to transport and use than heavy and bulky metals. The acceptance of the public of paper money depended on the public's trust or belief that the issuing authority was stable, reliable and available. The authorities that issued paper currency were typically private banks, states, and countries although other entities also issued their own currencies. Paper money was information about gold and silver that carriers could use to make commercial transactions without having to carry large amounts of metal. The public's acceptance of currency depended on their trust that the information contained in the paper would be exchangeable for the intrinsically valuable metals [2].

Without trust, paper money is just paper and therefore has about the same value as a leaf in the wind. When the public believes that paper money has value, banks stored the paper with the same fortress like protections as they used for precious metals. When customers deposited their paper money in a bank, that money was stored and treated as if it were gold.

Large amounts of cash (paper money) can be awkward to transport even with high denomination currency. The inconvenience of carrying large quantities of paper currency was mitigated by the introduction of checks that contained information identifying the writer's account. The account information is just an identifier that ties the customer to bookkeeping records of the paper or check transactions that the customer has completed. Checks are different than currency in that with currency the value is determined in the denomination printed by the issuer on the money. With checks the customer enters the value and the person that accepts the check for payment must trust that the information concerning the identity of the signer is valid. The acceptor must also trust that the signer's account actually contains the necessary funds (bookkeeping information) to complete the transaction by cashing the check or depositing the money into the acceptors account (transfer booking information from one account to another). Security focused on physical security by protecting money just as if it were gold. It was kept behind stone walls and locked vaults; often guarded by men with weapons.

As paper money and checks increased in popularity, criminals discovered that they could compromise the integrity of money by making copies (forgery) or spoofing identities by signing checks using someone else's identity. Technology to protect the information content of money focused on watermarks, special paper, complex colors and graphics, security threads, and other anti-counterfeiting technologies. Counterfeiting of paper money is just an extension of the old information integrity violation of taking a piece of lead and painting it gold. Checks complicate security in that the paper itself may be real or counterfeit and the signer may also be a valid signer just passing an insufficient funds check or a thief compromising the validity of the signature of the account owner. The use of checks increases the risk that the information about the account is not valid.

Checks and money are still secured behind steel cages and stone walls, but content integrity security has moved beyond metallurgical assay to information "assay". Testing the integrity of the information on money and checks also shifted beyond the walls of the bank to the transaction point where merchants became charged with inspecting the currency for

Manuscript received March 15, 2007.

M. E. de Boyrie is with the Department of Finance, New Mexico State University, Las Cruces, NM 88003 USA.

D. Nelson is with University Advancement, New Mexico State University, Las Cruces, NM 88003 USA.

J. A. Nelson is with the Department of Accounting & Information Systems, New Mexico State University, Las Cruces, NM 88003 USA (phone: 505-646-5678; e-mail jnelson@nmsu.edu).

integrity and to verify the identity of the signer. Merchants physically examine money to determine if it is counterfeit and also examine the personal credentials of the check signer to determine if identity information is valid. Today, merchants can instantly determine via electronic communications the validity of the information transaction amounts.

The evolution of money as information accelerated with the introduction of mainframe computers in the 1950s to process banking transactions and to store information about money. The physical US dollar, English pound, French frank, or other currency was no longer required to conduct monetary transactions. Money has become electronic information: no gold or paper is required. Money is just a coded series of binary digits: 1 and 0. The information was still stored in a secure central location in a mainframe computer behind stone walls and locked doors. Access to the computer was just as controlled as access to the steel vault.

Not only were the doors locked as the vault was locked, but access was controlled by possession of physical keys and possession of information. Information controls access to the vault through knowledge of a lock combination or access to the computer through knowledge of user ID and password. Protection of money stored electronically depended on protection of the computer through physical access controls to the computer room just like physical access to the vault. But electronic information stored in computers has a second layer of security: information about user IDs and passwords.

Security was relatively simple during the period as very few people had access to the vault or to the computer. Certainly customers were not allowed access to the computer. The decentralization of access to computers through the use of terminals complicated the security of the money information. Access to the computer is now outside of the controlled environment of the computer room and out in the lobby of the bank where tellers have terminals that have information (money) input and output from the computer. Security is complicated by the number of people with user IDs and passwords and the physical location of computer terminals.

Information integrity is compromised by human error at the access point (terminal). Tellers make errors and tellers may also intentionally attempt to violate the integrity of banking information and steal information (money).

III. The Walls of the Fort Fall Down

As money has transformed from gold and silver to paper currency, to checks, and today to electronic information, the walls of the bank have also transformed from stone and steel to electronic walls. Firewalls, intrusion detection systems, intrusion preventions systems, and access control lists are all designed to protect money as information [3], [4]. Their goal is to protect the confidentiality and integrity of banking information by limiting access to the electronic bits. Those ones (1) and zeros (0) store not only traditional money characteristics of being an exchange medium, account unit, and a store of value, but also store information that is anonymous with traditional money. Electronic money contains traditional information about value, but also holds information about the account numbers involved in the transaction. These account numbers are linked to personal, and by U.S. law, private information about the account holders.

The introduction of telecommunications allowed banks to facilitate the completion of remote transactions by transferring information about accounts through “wire transfers”. Wire transfers move information about accounts over distances outside of the physical walls of the bank without the transfer of paper. Money is now truly moving electronic information [5], [6], [7]. The introduction of personal computers and the Internet increased the number of access points to bank computer systems and the potential for information compromise. Anyone, almost anywhere, can try to turn the electronic keys to any bank in the world. Banks that had physical control of a very limited number of access points now allow access from millions of personal computers, PDA’s, and cell phones.

Anyone with the technical skills to take advantage of programming and electronic vulnerabilities can potentially access not only electronic money, but also information about accounts. Electronic walls attempt to prevent hackers from accessing information, but the biggest problem has not been hackers. Bank customers are the problem. Every customer with an Internet banking account has the electronic keys that allow them access to the bank. The customer’s user ID and password or credit card numbers are the keys to their accounts. If the customer does not protect those keys or voluntarily gives them to others through phishing or other social engineering schemes the customer’s identity and money can be compromised. Most data breeches where a laptop or tape is lost or stolen do not result in actual losses to the customer because most common thieves do not understand the value or how to use the information that they have acquired.

IV. Risk

Our job as IT auditors is to reduce the risk to the bank and to their customers. Risk management defines risk as a function:

$$\text{Risk} = \text{Asset} * \text{Threat Probability} * \text{Impact}$$

In the past the asset was physical; gold, paper money, or checks. Today the asset is information (usually electronic) and we should focus our efforts on protecting the information asset. The three major threat categories are: (1) hacking into bank computer systems through exploitation of technical vulnerabilities, (3) intentional or accidental data loss (laptop, tape or other data breeches), and (3) identity theft or unauthorized account access by gaining access keys through theft, phishing, or other means.

The first threat category, hacking and technical exploitation of vulnerabilities, is a constant battle between programmers of banking systems and the hacking community. This battle is waged through putting up electronic walls (firewalls, IDSs, and IPSs) and hacker's attempts to break into systems. This category will continue to provide employment and research opportunities for thousands of computer and information scientists.

The author has been advocating encryption of all banking information as a basic requirement of sound banking to mitigate the first threat and second categories of threats by hacking or data loss. If a hacker only gains access to encrypted data or a lost laptop is encrypted, then no information is compromised. Encryption makes these threats a non-issue. Banks have been slow to adopt universal encryption because of cost and time considerations. Encryption imposes an additional processing burden on computers that may significantly slow the performance of banking systems. However, those that refuse to encrypt do not fully appreciate the cost of not encrypting. Banks must consider the cost of monetary losses, customer notification costs, and the costs of reputation whenever banking information is compromised. Encryption places another wall between the information and the potential thief. Computer and information scientists have a challenging opportunity to develop encryption techniques that are safe, fast, and efficient.

Even with sound "walls" of encryption, the third threat category remains a very human problem. Whoever knows or has possession of the keys (account numbers, user IDs and passwords) has access to the information even if it is encrypted. Thieves will go to extraordinary lengths to exploit human weaknesses to get people to give them the keys to their accounts. Many people trust official appearing email or official looking websites and comply with phishers requests to provide account information. As long as humans are involved we risk the intentional or unintentional compromise of the keys and therefore access to the banking information. Procedures and policies can help to mitigate the threat of phishing, but people will always be human. Training and public information campaigns can help reduce the risk of phishing, but will never be sufficient. Technical solutions such as programs that scan websites for potential phishing sites can only reduce the risk. A good thief only needs to talk to a person to gain their trust and get them to give away the keys. Risk mitigation techniques that require transparent two-factor authentication such as biometrics or machine identifiers may help reduce the threat, but research into technologies, training and human behavior remains a major challenge.

V. The Future

The technical and human problems of money as information provide great opportunities for research and solutions to the unauthorized access to money as information. However, money as information contains information beyond value [7], [8], [9]. Information about the transaction, including links to the names and identities of those involved in the transaction, is part of today's electronic money. This is in direct conflict with the idea previously mentioned that money should be anonymous. When money is anonymous, users of the money cannot be identified through the money. Paper money can be used in black-markets, be used to avoid income and other taxes, and be moved to other countries. This is a social issue with social solutions. When citizens don't trust their own country's currency or banking system, they return to barter (as happened in Russia with the collapse of Ruble after the demise of the Soviet Union) or use anonymous alternatives such as the US dollar or gold. Economies that thrive on black-markets or those that have un-trusted currencies will not willingly accept money that has information other than value. Electronic money and banking will be difficult to impose as the standard for transactions in many parts of the world. Money as information is complicated by the attachment of transaction information to electronic money [10], [11], [12], [13]. Electronic money that contains non-monetary information is unacceptable in many countries, cultures, and to many individuals. The question for research is how to make electronic money acceptable for anonymous transactions.

References

[1] J. P. Barlow, "The economy of ideas," *Wired*, Issue 2.03, March, 1994.

[2] J. G. T. Salisbury and G. A. Barnett, *The world system of international monetary flows: A network analysis," vol. 15, no. 1, pp. 31-49, Feb. 1999.*

[3] M. Jakobsson and M. Yung, "Revokable and versatile electronic money," In *3rd ACM Conference on Computer and Communications Security*, pp. 76-87, New Delhi, Mar. 1996.

[4] G. Davies, "Monetary innovation in historical perspective: Why revolution always boils down to evolution," Keynote address at the *First Consult Hyperion Digital Money Forum 7th-8th October 1997,* London, 1997.

[5] K. Hart, "Heads or tails? Two sides of the coin," *Man*, New Series, pp. 637-656, Vol. 21, No. 4 Dec. 1986.

[6] P. Ludlow (ed.), "High noon on the electronic Frontier: Conceptual issues in cyberspace**,"** MIT Press, 1996**.**

[7] N. Kiyotaki and R. Wright, "A contribution to the pure theory of money," *Journal of Economic Theory, v*ol. 53, no. 2, pp. 215-235, Apr. 1991.

[8] M. R. Williams, *A History of Computing Technology*, 2nd Edition, Wiley-IEEE Computer Society Press, April 1997.

[9] J. van den Ende and W. Dolfsma, "Technology-push, demand-pull and the shaping of technological paradigms - Patterns in the development of computing technology," *Journal of Evolutionary Economics, vol. 15, no. 1, Mar. 2005.*

[10] J. A. N. Lee, ""Those who forget the lessons of history are doomed to repeat it: or, Why I study the history of computing," *IEEE Annals of the History of Computing*, vol. 18, no. 2, pp. 54-62, 1996.

[11] M. S. Mahoney, "The history of computing in the history of technology," *Annals of the History of Computing, vol.* 10, pp. 113-125, 1988.

[12] G. Bell, "History of personal workstations," *Proceedings of the ACM Conference on The history of personal workstations***,** pp. 1-17, 1986.

[13] M. C. McChesney, "Banking in cyberspace: an investment in itself," *Spectrum, IEEE,* vol. 34, no. 3, pp. 54-59, Feb. 1997.

.