[Home] [Current Edition] [Compendium] [Forum] [Web Archive]
[Email Archive] [Guestbook] [Subscribe] [Advertising Rates]

JIBC

FC'97 Conference Papers

Rafael Hirschfeld (Ed.)

Financial Cryptography

First International Conference, FC '97
Anguilla, British West Indies, February 1997

Proceedings

Editor's note:

The following are abstracts of papers presented at the Financial Cryptography '97 conference held in Anguilla, BWI in February 1997. The full papers are published in proceedings form as Volume 1318 of Springer-Verlag's Lecture Notes in Computer Science (LNCS) series. The preface of the proceedings volume is also included. All material is copyright (c) 1997 by Springer-Verlag. All rights reserved.

The book has ISBN 3-540-63594-7. If you would like to obtain a copy of the book, it can be ordered from a bookstore or directly from Springer-Verlag. Orders from Springer can be placed via email to the address orders@springer.de or orders@springer-ny.com.

Preface

On the last week of February 1997 a group of cryptographers, security experts, computer hackers, lawyers, bankers, and journalists converged on the small Caribbean island of Anguilla for FC97, the first international conference on Financial Cryptography. The conference aimed to foster cooperation and exchange of ideas among this diverse group. Anguilla's status in the financial world (it's an offshore tax haven) made it an appropriate venue for a conference on this topic.

Financial cryptography is intended to cover all topics related to the security of financial transactions and to digital commerce in general. Thus the conference program runs the gamut from pure cryptosystems to the technology of electronic money to legal and regulatory policy issues. Although security of monetary transactions is an ancient concern, and the use of cryptography for this purpose is not new, the modern study of the area has its roots in the pioneering work of David Chaum in the 1980's on electronic cash, in which cryptographic techniques were developed expressly for payment applications. Chaum's primary concern was anonymity. Although anonymous payments are not popular among many banks and central banks, anonymity remains an important and active area of concern for researchers and privacy advocates. It is thus perhaps fitting that the conference opened with a session on anonymity.

The papers appear in the order in which they were presented at the conference. Although they were mostly grouped into sessions by topic, other scheduling constraints in some cases made this impossible. These are revised versions of the accepted submissions. Revisions were not checked on their scientific aspects, and the authors bear full responsibility for the contents of their papers.

The program also included invited talks by Simon Lelieveld, Ronald Rivest, and Peter Wayner, and a panel discussion on legal issues of digital signatures by Michael Froomkin, Charles Merrill, and Benjamin Wright. All of these speakers have provided summaries of their presentations. In addition to the regular conference program, a rump session chaired by Peter Wayner provided an opportunity for less formal presentations. One of the rump session presentations, by Ronald Rivest on lottery ticket micropayments, has been selected for inclusion in this volume.

Financial Cryptography '97 was the brainchild of Robert Hettinga, who also founded the Digital Commerce Society of Boston. Assembling a group of people most of whom had never or hardly met him, let alone each other, he turned his vision into a reality. Vincent Cate handled all of the local arrangements in Anguilla. Ian Goldberg led the pre-conference tutorial workshop. Julie Rackliffe was responsible for coordinating exhibits and sponsorship. All of them deserve thanks, as do the members of the program committee for their efforts in evaluating the submissions and selecting the program, and of course the authors, without whose submissions there could be no conference. (US president Bill Clinton also played a part in the success of FC97 by ordering a cooling off period, averting a strike at American Airlines that would have made it difficult or impossible for most attendees to reach Anguilla.)

Rafael Hirschfeld
FC97 Program Chair
August 1997

Financial Cryptography '97
Anguilla, BWI
24-28 February 1997

Program Committee:
Matthew Franklin, AT&T Laboratories--Research, Murray Hill, NJ, USA
Michael Froomkin, U. Miami School of Law, Coral Gables, FL, USA
Rafael Hirschfeld (Program Chair), CWI, Amsterdam, The Netherlands
Arjen Lenstra, Citibank, New York, NY, USA
Mark Manasse, Digital Equipment Corporation, Palo Alto, CA, USA
Kevin McCurley, Sandia Laboratories, Albuquerque, NM, USA
Charles Merrill, McCarter & English, Newark, NJ, USA
Clifford Neuman, Information Sciences Institute, Marina del Rey, CA, USA
Sholom Rosen, Citibank, New York, NY, USA
Israel Sendrovic, Federal Reserve Bank of New York, New York, NY, USA

General Chairs:
Robert Hettinga, Shipwright/e$, Boston, MA, USA
Vincent Cate, Offshore Information Services, Anguilla, BWI

Exhibits and Sponsorship Manager:
Julie Rackliffe, Boston, MA, USA

Workshop Leader:
Ian Goldberg, Berkeley, CA, USA

Financial Cryptography '97 was held in cooperation with the International Association for Cryptologic Research and was sponsored by The Journal of Internet Banking and Commerce, Offshore Information Services, e$, and C2NET.

Table of Contents

M6 The SPEED Cipher
Yuliang Zheng

T1 Evaluating the Security of Electronic Money
Simon L. Lelieveldt

T2 Electronic Cash---Technology Will Denationalise Money
David G.W. Birch, Neil A. McEvoy

T3 Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective
David P. Maher

T4 Some Critical Remarks on "Dynamic Data Authentication" as Specified in EMV '96
Louis Claude Guillou

T5 Single-chip Implementation of a Cryptosystem for Financial Applications
Nikolaus Lange

W1 Perspectives on Financial Cryptography
Ronald L. Rivest

W2 Auditable Metering with Lightweight Security
Matthew K. Franklin, Dahlia Malkhi

W3 SVP: a Flexible Micropayment Scheme
Jacques Stern, Serge Vaudenay

W4 An Efficient Micropayment System Based on Probabilistic Polling
Stanislaw Jarecki, Andrew Odlyzko

W5 On the Continuum Between On-line and Off-line E-cash Systems - I
Yacov Yacobi

R1 Towards Multiple-Payment Schemes for Digital Money
H. Pagnia, R. Jansen

R2 Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System
Markus Jakobsson, Moti Yung

R3 The Uses and Limits of Financial Cryptography: A Law Professor's Perspective
Peter P. Swire

R4 Legal Issues in Cryptography
Edward J. Radlo

R5 Digital Signatures Today
A. Michael Froomkin

R6 An Attorney's Roadmap to the Digital Signature Guidelines
Charles R. Merrill

R7 Alternative Visions for Legal Signatures and Evidence
Benjamin Wright

R8 Money Laundering: Past, Present, and Future
Peter C. Wayner

R9 Electronic Lottery Tickets as Micropayments
Ronald L. Rivest

F1 Strategic Tasks for Government in the Information Age
Paul Lampru

F2 Using Electronic Markets to Achieve Efficient Task Distribution
Ian Grigg, Christopher C. Petro

F3 The Gateway Security Model in the Java Electronic Commerce Framework
Theodore Goldstein

F4 Highly Scalable On-line Payments Via Task Decoupling
David W. Kravitz

F5 GUMP; Grand Unified Meta-Protocols
Recipes for Simple, Standards-based Financial Cryptography
Barbara Fox, Brian Beckman, Dan Simon

F6 Secure Network Communications and Secure Store \& Forward Mechanisms with the SAP R/3 system
Bernhard Esslinger, J\"urgen Schneider

Anonymity Control in E-Cash Systems

George Davida (University of Wisconsin-Milwaukee)
Yair Frankel (CertCo LLC)
Yiannis Tsiounis (GTE Laboratories Incorporated)
Moti Yung (CertCo LLC)

Electronic cash, and other cryptographic payment systems, offer a level of user anonymity during a purchase, in order to emulate electronically the properties of physical cash exchange. However, it has been noted that there are crime-prevention situations where anonymity of notes is undesirable; in addition there may be regulatory and legal constraints limiting anonymous transfer of funds. Thus pure anonymity of users may be, in certain settings, unacceptable and thus a hurdle to the progress of electronic commerce.

The conceptual contribution of this work is based on the claim that given the legal, social, technical and efficiency constraints that are imposed, anonymity should be treated as a Control Parameter facilitating flexibility of the level of privacy of note holders (determined by the dynamic conditions and constraints).

In light of this parameterization, we review recently developed technical tools for tracing and anonymity revocation (e.g., owner tracing and coin tracing). We elaborate on the differences in the various technologies with respect to security assumptions and we discuss practical considerations of computational, bandwidth and storage requirements for user, shop, bank and trustees as well as whether the trustees must be on-line or off-line. We also claim that while anonymity revocation can potentially reduce crime it can also produce instances where the severity of the crime is increased as criminals try to social engineer around tracing revocation. To prevent this we suggest the notion of ``distress cash.'' On the technical side, we provide efficiency improvements to a protocol for coin tracing and point at a technical solution for distress cash.

How to Make Personalized Web Browsing Simple, Secure, and Anonymous

Eran Gabber, Phillip B. Gibbons, Yossi Matias, Alain Mayer

An increasing number of web-sites require users to establish an account before they can access the information stored on that site (``personalized web browsing''). Typically, the user is required to provide at least a unique username, a secret password and an e-mail address. Establishing accounts at multiple web-sites is a tedious task. A security- and privacy-aware user may have to invent a distinct username and a secure password, both unrelated to his/her identity, for each web-site. The user may also desire mechanisms for anonymous e-mail. Besides the information that the user supplies voluntarily to the web-site, additional information about the user may flow (involuntarily) from the user's site to the web-site, due to the nature of the HTTP protocol and the cookie mechanism.

This paper describes the Janus Personalized Web Anonymizer, which makes personalized web browsing simple, secure and anonymous by providing convenient solutions to each of the above problems. Janus serves as an intermediary entity between a user and a web-site. Given a user and a web-site, Janus automatically generates an alias -- typically a username, a password and an e-mail address -- that can be used to establish an anonymous account at the web-site. Different aliases are generated for each user, web-site pair; however the same alias is presented whenever a particular user visits a particular web-site. Janus frees the user from the burden of inventing and memorizing distinct usernames and secure passwords for each web-site, and guarantees that an alias (including an e-mail address) does not reveal the true identity of the user. Janus also provides mechanisms to complete an anonymous e-mail exchange from a web-site to a user, and filters the information-flow of the HTTP protocol to preserve user privacy. Thus Janus provides simultaneous user identification and user privacy, as required for anonymous personalized web browsing.

Anonymous Networking and Virtual Intranets: Tools for Anonymous Corporations

Jim McCoy
Electric Communities

Providing a secure and scaleable architecture for anonymous and pseudonymous communications over the Internet is a difficult and challenging task which has previously been approached in a piecemeal fashion. The tools and protocols available to Internet users have not achieved the generality and transparency necessary to make this task of securing communications privacy worth the effort for most people. If the promises of geodesic networking and distributed communications are to be realized then the problems with existing tools must either be overcome or bypassed.

As user concerns over privacy and the amount of information regarding their habits and interests on-line grow the legal status of transactions and providing information on the Internet continues to become more and more unclear. Over the past few years the popularity of the Internet has grown exponentially and the eyes of government regulators around the world are beginning to turn to this new form of communication with questions of how to control and monitor the flow of information and services. It becoming increasingly important that computer users have the ability to conduct their affairs behind the protective cloak of anonymity and complete privacy. So far the tools and protocols available for such private communications have focused upon securing and authenticating simple transactions, but this is not enough.

The systems proposed in this paper attempt to go a step beyond such simple services and provide users the means by which they can establish persistent communications structures that provide for as much security and anonymity as desired while remaining transparent to the users in general operation. Through such mechanisms is possible for Internet users to create "virtual intranets", communications hierarchies and organizations which have no physical existence.

Unlinkable Serial Transactions

Paul F. Syverson, Stuart G. Stubblebine, and David M. Goldschlag

Abstract:

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. The protocol prevents the service from tracking the behavior of its customers while protecting the service vendor from abuse due to simultaneous or ``cloned'' usage from a single subscription. We present variants of the protocol supporting pay-per-use transactions within a subscription. We describe other applications including third-party subscription management, multivendor package sales, proof of group membership, and voter registration.

``Efficient Electronic Cash with Restricted Privacy''

by Cristian Radu, Ren\'{e} Govaerts and Joos Vandewalle

In this paper we propose a coin-based electronic payment system suitable for small payments. It is derived from Brands' scheme presented at Crypto'93, in the sense that the coins are built using the representation problem. The main contribution of our solution consists of the speedup of the withdrawal protocol. The gain of efficiency is achieved preserving the same level of integrity for user, shop and bank. A coin remains untraceable with respect to the user. This feature is fulfilled even if one assumes that the bank has unlimited computing power and colludes with shops in order to trace a coin to a specific user. However, a set of coins are linkable to a pseudonym of the user, restricting in this way his privacy. This drawback can be limited by ``rotating'' coins derived from different pseudonyms in a set of consecutive payment transactions.

The SPEED Cipher

Yuliang Zheng
School of Computing, Monash University

McMahons Road, Frankston, Melbourne, VIC 3199, Australia
Email: yzheng@fcit.monash.edu.au

ABSTRACT

SPEED is a private key block cipher. It supports three variable parameters:

(1) data length --- the length of a plaintext/ciphertext of SPEED can be 64, 128 or 256 bits.
(2) key length --- the length of an encryption/decryption key of SPEED can be any integer between 48 and 256 (inclusive) and divisible by 16.
(3) rounds --- the number of rounds involved in encryption/decryption can be any integer divisible by 4 but not smaller than 32.

SPEED is compact, which is indicated by the fact that the object code of a straightforward implementation of SPEED in the programming language C occupies less than 3 kilo-bytes. It makes full use of current, and more importantly, emerging CPU architectures which host a large number of high-speed hardware registers directly available to application programs. Another important feature of SPEED is that it is built on recent research results on highly nonlinear cryptographic functions, as well as other counter-measures against differential and linear cryptanalytic attacks.

It is hoped that the compactness, high throughput and adjustable parameters offered by SPEED, together with the fact that the cipher is in the public domain, would make it an attractive alternative cipher for security applications including electronic financial transactions.

The source code of SPEED implemented in the programming language C is located at the following URL:
http://pscit-www.fcit.monash.edu.au/~yuliang/

EVALUATING THE SECURITY OF ELECTRONIC MONEY
THE VIEW OF A EUROPEAN CENTRAL BANK

FC 97, Anguilla
February 25, 1997

Simon L. Lelieveldt
De Nederlandsche Bank

BIOGRAPHY OF THE SPEAKER

Simon Lelieveldt has joined the Nederlandsche Bank in October 1995 as a senior staff member of the Payment Systems Policy Department to assist in the policy formulation concerning pre-paid cards and payment systems on the Internet. He has been a member of the G-10 task force on security of electronic money. He is a member of the project team (within the central bank) responsible for the supervision of pre-paid schemes in the Netherlands.

He has previously worked as a project manager (1990-1992) and as a policy advisor (1992-1995) to the marketing payments department of the Postbank (market share of 50 % in payments in the Netherlands). As such he has been responsible for implementing commercial projects (large scale distribution of credit cards), commercial feasability studies on new payment systems and the development of the pre-paid chipcard (Chipknip) in the Netherlands.

ABSTRACT

After defining electronic money the presentation shortly touches upon regulatory aspects. It is shown that the goal of regulating electronic money is to establish the safety of deposits of the consumer as well as the means to transfer these deposits (payment products). The dutch implementation of this regulatory goal follows the concept (see also:http://www.systemics.com/docs/papers/EU_perspective.html) that issuing value is seen to be equivalent to deposit taking and therefore subject to supervision. As a result the dutch central bank (1) actively monitors developments with respect to electronic money and (2) reviews the schemes under the rules of the supervision law.

After summarizing the BIS report on the security of electronic money (see:http://www.bis.org/pub/cpss18.htm) the presentation focuses on the security issues that are considered during the review of electronic money schemes. These include the committment of top management, the content and implementation of security policy, the soundness of the designed protocol and the content of the risk analysis. In this context it is noted that central banks' requirements for a pilot or mass market exploitation may differ. Furthermore it is shown that the requirement that banks should issue the value, not necessarily implies that the scheme operator should be a credit institution. It does imply however, that any non-banks involved in the scheme, will have to comply with the relevant requirements (that will be passed on from the participating banks to these organizations).

Electronic Cash--
Technology will denationalise money

Financial Cryptography, Anguilla (February 1997)

by David G.W. Birch and Neil A. McEvoy

Abstract

Emerging technologies, particularly the synthesis of cryptographic software and tamper-resistant smart card hardware into the electronic purse, will make the cost of entry into the currency issuing 'market' quite small. Many organisations may then wish to enter this market, for example as a means of supplying credit (as envisaged by Frederick Hayek), of raising finance, or of encouraging customer loyalty (explored by Edward de Bono). Whereas the world's currencies are currently organised on territorial lines, we foresee a future in which currencies occupy (overlapping) niches according to the virtual, as well as geographic, communities to which people belong and a vigorous 'foreign' exchange market where people (or, more likely, their PCs) trade these currencies. Just a couple of years ago the concept of electronic cash was unknown in the mass market, but soon it will be taken for granted and will be as widespread as credit cards and chequebooks are today -- and the ramifications of such a widespread deployment deserve serious examination and debate.

Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective

David P. Maher, AT&T Labs, dpm@research.att.com

Abstract

We put many of the new fault induction and reverse engineering attacks on secure systems into the context of real device implementations and actual systems. We describe countermeasures that diminish the overall practical significance of these new results when considered in the context of a rational design process and an overall systems security strategy.

Some Critical Remarks on Dynamic Data Authentication as specified in EMV '96

Louis Claude Guillou
France Telecom, Branche Developpement, CNET / DSM
CCETT, 4 Rue du Clos Courtel, BP 59
F-35512 Cesson Sevigne cedex 9, France
Email: louis.guillou@ccett.fr

Abstract

Every banking card will soon include an electronic chip and, after a transitional period, the magnetic stripe will disappear. For ensuring a worldwide interchange, Europay International S.A., MasterCard International Incorporated and Visa International Service Association have been cooperating for the last three years in the production of the so-called EMV specifications; the latest release specifies a method for dynamic data authentication. We analyzed that method which requires a pair of RSA keys in every card; such a method is highly questionable. We propose an alternate method which eliminates the detected problems while offering significant benefits at system level.

Single-chip implementation of
a cryptosystem for financial applications

Nikolaus Lange
SICAN Braunschweig GmbH
Richard-Wagner-Str.1, D-38106 Braunschweig
nlange@sican-bs.de

Abstract

This article presents a hardware architecture called "GCD - General Crypto Device", realized as a single chip for system solutions in the EFT area. Special emphasis is put to this application area as the GCD supports all functions and security mechanisms commonly required by financial security systems (DES, RSA, key generation schemes).

The GCD mainly targets at the electronic financial area, like electronic funds transfer, Electronic Cash, Electronic Banking and Chipcard applications. Other typical applications of the GCD are network security (e.g. on ATM or ISDN), access control systems (ACS), or upcoming consumer cryptosystems like pay TV or pay radio.

Keyfeature of the devices new concept is an optimized processor containing instructions especially required by crpto functions. Additionally the single chip realisation reduces the required space and the accessibility of sensitive signals. Probing sensitive internal data like a generated session key or global master keys requires a very high level of technical skills (like microprobes) not to be expected to become commonly available in the near future

The ASIC is based on a 32-Bit RISC special processor with embedded high speed crypto functions. The major new achivement lies in the processor architecture, which includes a pipeline stage, designed for efficient long number arithmetic, like it is needed in the RSA cryptosystem [1]. The resulting overall performance of the device is significantly higher than that of existing realizations due to the used design concept, the performance is further enhanced due to the direct linking of the embedded components. The physical security combined with a high cryptographic flexibility at reasonable costs allows the usage of new cryptographic algorithms even in consumer market applications.

The paper is organized as follows: Section 1 gives an introduction. Section 2 pointes out the motiviation to design a device dedicated to the efficient realization of cryptosystems. Section 3 described the requirements and the architecture of typical cryptosystems used in the financial cryptography area. Section 4 presents the architecure of the General Crypto Device and its contents. While section 5 shows two examples, section 6 concludes the paper.

Perspectives on Financial Cryptography

Ronald L. Rivest
MIT Lab for Computer Science
(RSA / Security Dynamics)
rivest@theory.lcs.mit.edu

I present some debatable propositions about financial systems and financial cryptography. (Warning: the propositions expressed may or may not be believed by the author, and may be phrased in a deliberately provocative manner. They may contradict each other. This paper follows the author's slides closely, and does not have all of the ancillary comments of the author and the audience.)

Auditable Metering with Lightweight Security

Matthew K. Franklin and Dahlia Malkhi
AT&T Labs -- Research, Murray Hill, New Jersey, USA
{franklin,dalia}@research.att.com

abstract

In this work we suggest a new mechanism for metering the popularity of web-sites: The compact metering scheme. Our approach does not rely on client authentication or on a third party. Instead, we suggest the notion of a _timing scheme_, a computation that can be performed incrementally, whose output is compact, and whose result can be used to efficiently verify the effort spent with high degree of confidence. We use the difficulty of computing a timing scheme to leverage the security of a metering method by involving each client in computing the timing function (for some given input) upon visiting a web site, and recording the result of the computation along with the record of the visit. Thus, to forge client visits requires a known investment of computational resources, which grows proportionally to the amount of fraud, and is infeasible for visit counts commonly found in the World Wide Web. The incremental nature of the timing function is used to create a new measure of client accesses, namely their duration.

SVP: a Flexible Micropayment Scheme

Jacques Stern, Serge Vaudenay
Ecole Normale Sup\'erieure --- CNRS
{Jacques.Stern,Serge.Vaudenay}@ens.fr

We propose a cheap micropayment scheme based on reasonable requirements. It can be used for any payment which is online between the customer and the vendor and offline with the broker. It is flexible in the sense that many security options are possible depending on the policy of the involved participants. We avoid large data storage, heavy computations. The scheme is software based for the customer and hardware based for the vendor. Possibilities of having software-based solution for both are also presented.

An efficient micropayment system based on probabilistic polling

Stanislaw Jarecki
Laboratory for Computer Science
MIT
Cambridge, MA 02139, USA
(Work partly done during an internship at AT&T Labs - Research.
Partly supported by a DARPA grant.)

and

Andrew Odlyzko
AT&T Labs - Research
Florham Park, NJ 07932, USA

Abstract

Existing software proposals for electronic payments can be divided into ``on-line'' schemes that require participation of a trusted party (the bank) in every transaction and are secure against overspending, and the ``off-line'' schemes that do not require a third party and guarantee only that overspending is detected when vendors submit their transaction records to the bank (usually at the end of the day).

We propose a new hybrid scheme that combines the advantages of both of the above traditional design strategies. It allows for control of overspending at a cost of only a modest increase in communication compared to the off-line schemes. Our protocol is based on probabilistic polling. During each transaction, with some small probability, the vendor forwards information about this transaction to the bank. This enables the bank to maintain an accurate approximation of a customer's spending. The frequency of polling messages is related to the monetary value of transactions and the amount of overspending the bank is willing to risk.

The probabilistic polling model creates a natural spectrum bridging the existing on-line and off-line electronic commerce models. For transactions of high monetary value, the cost of polling approaches that of the on-line schemes, but for micropayments, the cost of polling is a small increase over the traffic incurred by the off-line schemes.

On The Continuum Between On-line and Off-line E-cash systems - I

Yacov Yacobi
Microsoft, Redmond, WA 98052

yacov@microsoft.com

March 11, 1997

Abstract.

Electronic cash systems for small transactions are discussed, with the functionality goal of minimizing involvement of third parties in transactions between users. To this end the potential role of randomized audit mechanisms is discussed. A continuum exists between the extremes of totally on-line and totally off-line payment systems, and there exist business motivations to establishing an intermediate ``working point.''

Our security goal is to protect the systems against economically motivated adversaries. Let the adversarial expenses (to interfere with normal operation of wallets) be C_b, and $1/d$ be the audit sampling rate, and for simplicity assume that each payment has a value of one unit. Then when the adversarial payer breaks even with her investment, C_b, the probability not to detect her is $O(exp(-C_b/d))$.

A curious observation on the so called ``after the fact double-spender exposure'' mechanisms unexpectedly falls from the analysis of randomized audit mechanisms.

Towards Multiple-payment Schemes for Digital Money

H. Pagnia and R. Jansen

Darmstadt University of Technology
D-64283 Darmstadt
Germany

Abstract

Recently, many payment schemes for digital money have been proposed. In most of these schemes money can be spent only once and must then immediately be returned to the bank.

In its first part the paper discusses the advantages of schemes which allow the recipient of the money to use it directly for further purchases. We explain why most existing schemes do not support such a payment scheme and make a proposal of how to efficiently overcome this drawback.

The design process of our scheme is shown in detail, starting with a simple scheme and applying additional features in a step-by-step manner. The resulting off-line payment scheme provides anonynimity as well as transferability.

Anonymity however is not unconditionally guaranteed but can be revoked by public authorities if necessary.

Additionally the scheme can easily be extended to support divisible money, a feature that is particularly important for multiple-payment schemes.

In the second part of the paper, we address the problem of achieving a fair exchange of money against service between the customer and the vendor.

Few solutions to this problem have been published and most of them involve a trusted third party which actively supports the exchange. Using such an active component has the disadvantage that - for high transaction rates - the trustee easily constitutes a bottleneck.

We present an alternative solution based on a `passive' trustee thereby avoiding the former disadvantage.

In the proposed protocol the trustee simply serves as a public blackboard to which vendor and customer can write information concerning the current state of their business.

In case of fraud these information can be used as a proof by both parties.

Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System

Markus Jakobsson
Moti Yung

ABSTRACT:

Due to business relationships, alliances, trust, and distribution of liability, ``distribution of power'' is an important issue in financial systems. At the same time as the security of the scheme is strengthened by this decentralization, the perception of the security is also strengthened, which is important from a business point of view. Furthermore, apart from increasing the security, client trust and availability of the system, distribution of power can also increase its functionality, as we demonstrate.

We suggest an anti-trust mechanism, namely, a method for distribution (potentially controlled by different entities), and apply it to a versatile electronic-money system. The method diffuses a task into distributed modules using recent cryptographic technology; doing so, it achieves increased security, privacy, availability and functionality without introducing any noticeable disadvantage. It uses ``Magic Ink Signatures'' of {JY-Eurocrypt.pl'97}, which are blind signatures that are distributedly generated using a threshold of signers, and where signatures can always be unblinded using (perhaps another) threshold of signers as well. Furthermore, we combine this with recent proactive technology, which enables a stronger adversarial setting. We also suggest techniques for reorganization of data stored and used by various functions, employing secure repository.

The result is an electronic money system that allows user anonymity and its revocation (a notion recently advocated by some works so as to prevent potential criminal actions.) The control over revoking anonymity is given to distributed modules that control a hidden alarm channel. As part of the task diffusion we find ways to simplify and reduce the overall complexity of the system. The revocation ability and distribution of the trust are efficient and allow a large degree of versatility in the functionality of the system (change mechanisms, numerous financial instruments: cash, charge, check, micro-payments, etc.).

"The Uses and Limits of Financial Cryptography: A Law Professor's Perspective"

Peter P. Swire
Ohio State University
College of Law
Columbus, Ohio, USA
swire.1@osu.edu
www.osu.edu/units/law/swire.htm

Abstract:

There is considerable support in the cryptography community for the "Cypherpunk Credo," defined as: "Privacy through technology, not legislation." Much discussion to date has assumed that the U.S. government's opposition to strong cryptography, such as its key escrow proposals, is the primary obstacle to widespread use of anonymous electronic cash. For purposes of this paper, I assume that strong cryptography is legal and readily available. Even in that event, I claim that strong cryptography will be used to preserve anonymity only in a highly restricted subset of financial transactions. Furthermore, because technology often will not assure privacy, legal rules can and should play an important supplementary role in the protection of privacy in financial transactions.

Legal Issues in Cryptography

by Edward J. Radlo
Partner, Fenwick & West LLP
Palo Alto California
March 1997

A company or individual interested in manufacturing and marketing products that implement cryptographic functions must be aware of several important legal and policy issues. The major of these issues are discussed in this paper. Some of these issues are highly controversial, and continue to generate much public attention, particularly the existence and construal of the export control laws of the United States and the promulgation of Federal Information Processing Standards (FIPS). International laws, regulations, and customs must be considered. Another issue briefly discussed in this paper is that of standards set by industry and non-U.S. groups. A fifth issue, patents, has also engendered controversy by virtue of the U.S. government's unusual attempts to shape cryptography policy via the patent laws, and by virtue of some important pieces of patent litigation.

Digital Signatures Today

A. Michael Froomkin
University of Miami School of Law
froomkin@law.miami.edu

To a lawyer, two issues stand out as critical impediments to the widespread acceptance of digital signatures in electronic commerce: the unresolved nature of liability issues and the looming uncertainty about the nature of the public key infrastructure. These issues are so closely related as to be almost intertwined.

An Attorney's Roadmap to the Digital Signature Guidelines

Summary of Remarks at Financial Cryptography '97
Anguilla, BWI, February 27, 1997

By Charles R. Merrill

ABSTRACT

The Digital Signature Guidelines, published August 1, 1996 by the American Bar Association's Information Security Committee, represent a pioneering collaboration of technologists and attorneys to fashion a system of legal non-repudiation can be based upon an a public key infrastructure, to provide secure electronic commerce in an open system such as the Internet. This paper, written and presented at FC97 by one of the Co-Reporters of the Digital Signature Guidelines, traces an authentication/non-repudiation hypothetical example through ten separate steps of technological and legal analysis under the Guidelines.

Once a digital signature has been created with an asymmetric cryptosystem, if it is verifiable with an appropriate certificate issued by a trusted third-party certification authority, a rebuttable presumption of the signer's identity arises, which reverses the normal burden of proof applicable to a signed pen-and-ink writing. The subscriber to the certificate has a number of ways to rebut the presumption, including a showing that the subscriber's private key was used without authority, and that the subscriber did not violate a duty of care to protect the private key from compromise.

The full text of the Digital Signature Guidelines may be downloaded at http://www.abanet.org/scitech/ec/isc/dsgfree.html, and a Tutorial from the Guidelines is at http://www.abanet.org/scitech/ec/isc/dsg-toc.html.

ALTERNATIVE VISIONS FOR LEGAL SIGNATURES AND EVIDENCE

Ben Wright

Abstract:

"I have two messages: (a) there is more than one way legally to sign an electronic transaction; and (b) the environment in which a transaction is effected and recorded can affect your ability to prove it to a judge and jury, perhaps more than could the strength of the cryptography used. Although it is popular to believe that public key digital signatures are the only good way to sign electronic business messages for legal purposes, digital signatures have some hurdles to overcome. The legal infrastructures set up for them in Utah and Washington state make them unattractive to members of the general public. Some biometric signing methods can be easier for people to understand and use."

Money Laundering: Past, Present and Future

Peter C. Wayner

Regulation aimed at combating money laundering is a serious challenge for designers of digital cash system. This talk sketches out some of the problems with tracking every transaction and tries to identify how the tension between regulators and designers is bound to grow. It is not meant to be comprehensive nor does it have any solutions to offer---it only diagnoses some of the problem so people can concentrate on solutions.

Electronic Lottery Tickets as Micropayments

Ronald L. Rivest
MIT Lab for Computer Science
(RSA / Security Dynamics)
rivest@theory.lcs.mit.edu

We present a new micropayment scheme based on the use of ``electronic lottery tickets.'' This scheme is exceptionally efficient since the bank handles only winning tickets, instead of handling each micropayment.

Strategic Tasks for Government in the Information Age

Paul Lampru (Paul_L2@verifone.com)
Strategic Marketing for Electronic Commerce and Security
Financial, Healthcare and Government Markets
U.S. Division, VeriFone, Inc.

Financial Cryptology Conference 1997
Anguilla, BWI
February 24-28, 1997

(The ideas expressed in this paper are those of the author and do not necessarily represent those of VeriFone, Inc.)

Introduction

Today we are participating in a sea-change that may equal or exceed the social and economic impact we experienced when we transitioned from an agrarian economy to an industrial economy over one hundred years ago. Clearly government officials recognize the enormous opportunity this transition offers to dramatically reduce the cost of government services while improving their quality. As companies rapidly switch to information-based businesses, government support, leadership, and vision are needed to accelerate and guide the development of a commercial/government infrastructure that will support a new economy.

We should carefully consider the answers to several important questions before applying government's influence to support and channel the construction of new global economic and social infrastructure so that it serves our national interests.

What is the driving technology force behind this paradigm shift to an Information-based economy?

What are the key elements that might facilitate this transition?

What are the dynamics of this shift?

Answering these questions could help shape government strategies to ensure that new "digital factors of production" are used to benefit national and global interests well into the next century. This paper proposes answers to these questions and presents ideas that might contribute to the development of an Electronic Commerce infrastructure in the United States.

Using Electronic Markets to Achieve Efficient Task Distribution

Ian Grigg   Christopher C. Petro

28 February 1997

Abstract: The Internet was built using the efforts of a worldwide team of programmers that coordinated and competed through laissez-faire methods. Much of the effort was freely provided, or paid for by entities in a process that did not conform to normal commercial revenue-seeking or government regulatory behaviour. This points to major inefficiencies in the market for software. One inhibitor is the large search costs undertaken by managers to acquire new programmers.

On the other hand, there are inherent inefficiencies in the way in which much of the free Internet software is developed. Specifically, there is no efficient way for users to direct the efforts of developers, other than by contracting for entire projects. This often results in a mismatch between development and requirement, as user communities and developer communities are sufficiently culturally different to make communication non-perfect.

We propose a market-based solution that allows many users to each contribute small amounts to projects, and for the sum effect of these contributions to influence and direct the activities of programmers towards tasks that users demand. A range of solutions is presented, from a web billboard bounty market to trading exchange markets for digital financial instruments. Reputational effects, intermediaries and differentiation are considered.

Relying on the existance of efficient electronic payment mechanisms and the efficiency promised by new electronic markets (both web billboard and digital financial instrument forms), we submit that the markets proposed could make small tasks more readily directable over the Internet, and could significantly enhance the efficiency of certain classes of software development.

The Gateway Security Model in the Java Electronic Commerce Framework

Theodore Goldstein
ted.goldstein@eng.sun.com

Abstract

This paper describes an extension to the current Java security model called the "Gateway" and why it was necessary to create it. This model allows secure applications, such as those used in electronic commerce, to safely exchange data and interoperate without compromising each individual application's security. The Gateway uses digital signatures to enable application programming interfaces to authenticate their caller. JavaSoft is using the Gateway to create a new integrated open platform for financial applications called Java Electronic Commerce Framework. The JECF will be the foundation for electronic wallets, point of sale terminals, electronic merchant servers and other financial software. The Gateway model can also be used for access control in many multiple application environments that require trusted interaction between applications from multiple vendors. These applications include browsers, servers, operating systems, medical systems and smartcards.

Highly Scalable On-line Payments Via Task Decoupling

David W. Kravitz
CertCo, LLC
kravitzd@certco.com

Several digital payment systems have been described which attempt to simulate or extend already existing payment mechanisms so as to make them suitable for electronic commerce. Such mechanisms or instruments include cash or coins (e.g., DigiCash, NetCash), checks (e.g., NetCheque), and credit cards (e.g., CyberCash). The anonymity, off-line, and peer-to-peer aspects of some of these systems can introduce security weaknesses and major scalability problems. One approach to security, as taken by the Millicent architecture, is to only allow very low cost transactions. True security, unlike the approach taken by First Virtual, requires clear delineation of the customer and merchant roles. The goal of this paper is to outline an approach which is inexpensive enough to allow for very low value transactions but secure enough to allow for intermediate value transactions, while providing true customer anonymity with respect to merchants and electronic handling of refund requests. Unlike NetBill and the GC Tech GlobeID system, under the default operation of the system the customer in no way authenticates or identifies itself to

the merchant, pseudonymously or otherwise. This is an example of the decoupling of tasks used as a basic design principle: Each system component deals directly with only those aspects in its narrowly defined scope of responsibilities, and within this asynchronous system time-consuming or time-varying issues not directly related to the payment flow, such as actual delivery of digital goods, are handled outside of the basic payment flow. After presenting a high-level comparison of our approach to those of two other instant debit systems, GlobeID and NetBill, we give a more detailed explanation of the design criteria and characteristics exhibited by this new approach to on-line payments.

GUMP
Grand Unified Meta-Protocols
Recipes for Simple, Standards-based Financial Cryptography

Barbara Fox
Brian Beckman
Appendix by Dan Simon

Microsoft Corporation
February 1997

Abstract. In this paper, we present a set of simple, all-parties-authenticated application protocol frameworks appropriate for a wide variety of financial applications running on the Internet. Collectively, we call these frameworks "GUMP", for Grand Unified Meta-Protocols. The driving goal of the design is simplicity, so as to reduce dramatically the cost of engineering and deployment of application protocols. The simplicity of GUMP follows directly from a number of business-level premises, chief of which is that the client must digitally sign all transactions.

One builds an application protocol from GUMP by "filling in the blanks" with custom business data types and logic. In that sense, GUMP is a set of frameworks, templates, or meta-protocols. The goal of this paper is not to engineer protocols, but to describe abstractly how they might be straightforwardly engineered, concentrating on the authentication phases common to most, if not all, financial protocols. The applications may include home banking, purchasing, bill payment, securities trading^×any application that requires client-server mutual authentication and integration with legacy systems.

While many of the points in this paper may seem embarrassingly simple and obvious, that is, in fact, the point. In the design of public-key protocols each design team inexorably ends up inventing nearly the same primitive notions. Since no team can afford the time to abstract general frameworks, these protocols end up being virtual collections of special cases. Furthermore, the written specifications, again due to time pressure, frequently do not carefully distinguish between requirements, high-level design, and deep details, mixing them all together in one, swirling description. The really hard problem then falls to the implementors whose job it becomes to translate complex protocol design into simple working and interoperable code.

GUMP is our attempt to provide a greatly simplified abstract toolkit for the protocol engineer. We present three application protocol prototypes^×Registration, Transaction, and Delegation^×based on the pending IETF TLS (Transport-Layer Security) Protocol, which is based on Netscape's widely deployed SSL (Secure Sockets Layer). The GUMP Registration meta-protocol assumes the password (shared-key) extensions to TLS as proposed to the IETF working group and documented in the Appendix. These extensions protect a GUMP one-time shared secret that the server uses to authenticate a certification request. The rest of the protocols make minimal usage of cryptography beyond digital signatures. All leverage the client-authentication feature of SSL version 3.

The contributions of this paper include:

Reduction of multiple financial account relationships to a single unsecret, which, when certified along with a public key, supports authentication without secrecy. A new class of Internet-safe transactions with delegation, where a member of an access group may give permission to an agent to initiate a transaction on his behalf.

Secure Network Communications and Secure Store & Forward Mechanisms within the SAP R/3 System

Bernhard Esslinger
SAP-AG
Bernhard.Esslinger@sap-ag.de

Jürgen Schneider
SAP-AG
J.Schneider@sap-ag.de

Abstract

Information security and data protection is gaining more and more importance with business[s1] software such as R/3 because:Business applications become "mission-critical" if companies carry out their most important business processes with them.Programs and data are subject to a greater danger of loss, change and espionage in client/server environments than in mainframe based systems.The danger increases even more as the systems become interconnected with publicly accessible LANs and WANs.R/3 processes highly sensitive data (for example, company-internal and person-related information). Therefore a number of security mechanisms are already active in R/3 since the beginning: authentication of all users by means of passwords, R/3 authorization concept, and protection of the communication between front-end and application server by compression. Now SAP enhances the security of R/3 by Securing online network communications (the SNC Project) and by Implementing secure store&forward mechanisms for electronic payment (the SSF Project).