Lecture Notes in Computer Science 1729

Masahiro Mambo Yuliang Zheng (Eds.)

Information Security

Second International Workshop, ISW'99
Kuala Lumpur, Malaysia, November 1999
Proceedings

Springer

Lecture Notes in Computer Science

This series reports new developments in computer science research and teaching, quickly, informally, and at a high level. The timeliness of a manuscript is more important than its form, which may be unfinished or tentative. The type of material considered for publication includes

- drafts of original papers or monographs,
- technical reports of high quality and broad interest,
- advanced-level lectures,
- reports of meetings, provided they are of exceptional interest and focused on a single topic.

Publication of Lecture Notes is intended as a service to the computer science community in that the publisher Springer-Verlag offers global distribution of documents which would otherwise have a restricted readership. Once published and copyrighted they can be cited in the scientific literature.

Manuscripts

Lecture Notes are printed by photo-offset from the master copy delivered in camera-ready form. Manuscripts should consist of no fewer than 100 and preferably no more than 500 pages of text. Authors of monographs and editors of proceedings volumes receive 50 free copies of their book. Manuscripts should be printed with a laser or other high-resolution printer onto white paper of reasonable quality. To ensure that the final photo-reduced pages are easily readable, please use one of the following formats:

Font size (points)	Printing area (cm)	(inches)	Final size %
10	12.2 x 19.3	4.8 x 7.6	100
12	15.3 x 24.2	6.0 x 9.5	80

On request the publisher will supply a leaflet with more detailed technical instructions or a TEX macro package for the preparation of manuscripts.

Manuscripts should be sent to one of the series editors or directly to:

Springer-Verlag, Computer Science Editorial III, Tiergartenstr.17,
D-69121 Heidelberg, Germany

ISBN 3-540-66695-8

9 783540 666950

ISSN 0302-9743

http://www.springer.de

LNCS 1729 Mambo Zheng (Eds.) ISW'99 Information Security

Masahiro Mambo Yuliang Zheng (Eds.)

Information Security

Second International Workshop, ISW'99
Kuala Lumpur, Malaysia, November 6-7, 1999
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Masahiro Mambo
Tohoku University, Education Center for Information Processing
Kawauchi Aoba Sendai, 980-8576, Japan
E-mail: mambo@ecip.tohoku.ac.jp

Yuliang Zheng
Monash University, School of Computer and Information Technology
MacMahons Road, Frankston, Melbourne, Victoria 3199, Australia
E-mail: yuliang.zheng@infotech.monash.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security : second international workshop ; proceedings / ISW '99, Kuala Lumpur, Malaysia, November 6 - 7, 1999. Masahiro Mambo ; Yuliang Zheng (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1729)
ISBN 3-540-66695-8

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-66695-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10703333 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Lecture Notes in Computer Science 1729
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Preface

The 1999 International Information Security Workshop, ISW'99, was held on Monash University's Malaysia Campus, which is about 20km to the south west of downtown Kuala Lumpur, November 6-7, 1999.

ISW'99 sought a different goal from its predecessor, ISW'97, held in Ishikawa, Japan, whose proceedings were published as Volume 1396 of Springer Verlag's LNCS series. The focus of ISW'99 was on the following emerging areas of importance in information security: multimedia watermarking, electronic cash, secure software components and mobile agents, and protection of software.

The program committee received 38 full submissions from 12 countries and regions: Australia, China, France, Germany, Hong Kong, Japan, Korea, Malaysia, Singapore, Spain, Taiwan, and USA, and selected 23 of them for presentation. Among the 23 presentations, 19 were regular talks and the remaining 4 were short talks. Each submission was reviewed by at least two expert referees.

We are grateful to the members of the program committee for reviewing and selecting papers in a very short period of time. Their comments helped the authors improve the final version of their papers. Our thanks also go to Patrick McDaniel, Masaji Kawahara, and Yasuhiro Ohtaki who assisted in reviewing papers. In addition, we would like to thank all the authors, including those whose submissions were not accepted, for their contribution to the success of this workshop.

The workshop was organized with the help of local committee members, including Cheang Kok Soon, Hiew Pang Leang, Lily Leong, and Robin Pollard. We appreciate their patience and professionalism. Robin Pollard led the committee as a general co-chair. We owe the success of the workshop to him as well as general co-chair Eiji Okamoto.

November 1999

Masahiro Mambo
Yuliang Zheng

Information Security Workshop (ISW'99)

Organizing Committee

Eiji Okamoto (**Co-chair**, Univ. of Wisconsin, Milwaukee, USA)
Robin Pollard (**Co-chair**, Monash University, Malaysia)
Hiew Pang Leang (Monash University, Malaysia)
Lily Leong (Monash University, Malaysia)
Cheang Kok Soon (Monash University, Malaysia)

Program Committee

Masahiro Mambo, (**Co-chair**, Tohoku University, Japan)
Yuliang Zheng, (**Co-chair**, Monash University, Australia)
David Aucsmith (Intel, USA)
George Davida (University of Wisconsin-Milwaukee, USA)
Robert H. Deng (Kent Ridge Digital Labs, Singapore)
Steven J. Greenwald (Independent Consultant, USA)
Ryoichi Mori (Superdistribution Laboratory, Japan)
Kazuo Ohta (NTT, Japan)
Aviel Rubin (AT&T Labs - Research, USA)
Andrew Z Tirkel (Monash University, Australia)
Moti Yung (CertCo, USA)

Contents

Electronic Money

Spending Programs: A Tool for Flexible Micropayments 1
Josep Domingo-Ferrer and Jordi Herrera-Joancomartí (Uni Rovira i Virgili, Spain)

Money Conservation via Atomicity in Fair Off-Line E-Cash 14
Shouhuai Xu (Fudan Univ., P. R. China), Moti Yung (CertCo, USA), Gendu Zhang, and Hong Zhu (Fudan Univ., P. R. China)

Engineering an eCash System..... 32
Tim Ebringer and Peter Thorne (Univ. of Melbourne, Australia)

Electronic Payment and Unlinkability

Unlinkable Electronic Coupon Protocol with Anonymity Control 37
Toru Nakanishi, Nobuaki Haruna, and Yuji Sugiyama (Okayama Univ., Japan)

On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives 47
Marc Joye (Gemplus, France), Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.), and Tzonelih Hwang (Cheng-Kung Univ., Taiwan, R.O.C.)

Secure Software Components, Mobile Agents, and Authentication

Security Properties of Software Components 52
Khaled Khan, Jun Han, and Yuliang Zheng (Monash Univ., Australia)

Methods for Protecting a Mobile Agent's Route 57
Dirk Westhoff, Markus Schneider, Claus Unger, and Firoz Kaderali (Fern Uni. Hagen, Germany)

Non-interactive Cryptosystem for Entity Authentication 72
Hyung-Woo Lee(Chonan Univ., Korea), Jung-Eun Kim, and Tai-Yun Kim (Korea Univ., Korea)

Network Security

Implementation of Virtual Private Networks at the Transport Layer 85
Jorge Davila (Uni Politecnica de Madrid, Spain), Javier Lopez (Uni de Malaga, Spain), and Rene Peralta (Univ. of Wisconsin-Milwaukee, USA)

Performance Evaluation of Certificate Revocation Using k-Valued Hash Tree 103
Hiroaki Kikuchi, Kensuke Abe, and Shohachiro Nakanishi (Tokai Univ., Japan)

Active Rebooting Method for Proactivized System: How to Enhance the Security against Latent Virus Attacks 118
Yuji Watanabe and Hideki Imai (Univ. of Tokyo, Japan)

Digital Watermarking

Highly Robust Image Watermarking Using Complementary Modulations .. 136
Chun-Shien Lu, Hong-Yuan Mark Liao, Shih-Kun Huang, and Chwen-Jye Sze (Academia Sinica, Taiwan, R.O.C.)

Region-Based Watermarking for Images 154
Gareth Brisbane, Rei Safavi-Naini (Wollongong, Australia), and Philip Ogunbona (Motorola Australian Research Center, Australia)

Digital Watermarking Robust Against JPEG Compression 167
Hye-Joo Lee, Ji-Hwan Park (PuKyong Nat'l Univ., Korea), and Yuliang Zheng (Monash Univ., Australia)

Protection of Software and Data

Fingerprints for Copyright Software Protection 178
Josef Pieprzyk (Univ. of Wollongong, Australia)

A Secrecy Scheme for MPEG Video Data Using the Joint of Compression and Encryption 191
Sang Uk Shin, Kyeong Seop Sim, and Kyung Hyune Rhee (PuKyong Nat'l Univ., Korea)

Electronic Money, Key Recovery, and Electronic Voting

On Anonymous Electronic Cash and Crime 202
Tomas Sander and Amnon Ta-Shma (Int'l Computer Science Inst., USA)

On the Difficulty of Key Recovery Systems 207
Seungjoo Kim, Insoo Lee (KISA, Korea), Masahiro Mambo (Tohoku Univ., Japan), and Sungjun Park (KISA, Korea)

An Improvement on a Practical Secret Voting Scheme 225
Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto (NTT Inf. Sharing Platform Lab., Japan)

Digital Signatures

Undeniable Confirmer Signature 235
Khanh Nguyen, Yi Mu, and Vijay Varadharajan (Univ. of Western Sydney, Australia)

Extended Proxy Signatures for Smart Cards 247
Takeshi Okamoto, Mitsuru Tada (JAIST, Japan), and Eiji Okamoto (Univ. of Wisconsin-Milwaukee, USA)

A New Digital Signature Scheme on ID-Based Key-Sharing Infrastructures 259
Tsuyoshi Nishioka (Mitsubishi Electric Corp., Japan), Goichiro Hanaoka, and Hideki Imai (Univ. of Tokyo, Japan)

Cryptanalysis of Two Group Signature Schemes 271
Marc Joye (Gemplus, France), Seungjoo Kim (KISA, Korea), and Narn-Yih Lee (Nan-Tai Inst. of Tech., Taiwan, R.O.C.)

Author Index 277

Spending Programs: A Tool for Flexible Micropayments*

Josep Domingo-Ferrer and Jordi Herrera-Joancomartí

Universitat Rovira i Virgili, Department of Computer Science and Mathematics, Autovia de Salou s/n, E-43006 Tarragona, Catalonia, Spain,
{jdomingo,jherrera}@etse.urv.es

Abstract. Micropayments are electronic payments of small amount. Given their low value, the cost of the corresponding electronic transactions should also be kept low. Current micropayment schemes allow a regular amount of money withdrawn from a bank to be split into fixed-value coupons, each of which is used for one micropayment. A more flexible mechanism is proposed in this paper, whereby coupons of variable value can be generated by a *spending program* without increasing the transaction cost. Moreover, the spending program allows one of several alternative ways of splitting the amount withdrawn into re-usable coupons to be selected in real-time.
Keywords: Micropayments, Electronic commerce, Hash functions, Hash chain, Spending program.

1 Introduction

Micropayments are electronic payments of low value and they are called to playing a major role in the expansion of electronic commerce: example applications are phone call payments, access to non-free web pages, pay-per-view TV, etc. The reason for designing specific micropayment schemes is that standard electronic payment systems (like CyberCash [3], e-cash [6] , *i*KP [2], SET [16]) for low-value payments suffer from too high transaction costs as compared to the amount of payments. The cost of transactions is kept high due to complex cryptographic protocols like digital signatures used for achieving a certain security level. However, micropayments do not need as much security as speed and simplicity (in terms of computing). For that reason, several micropayment proposals try to replace the use of digital signatures with faster operations.

1.1 Our Result

Current micropayment schemes allow a regular amount of money withdrawn from a bank to be split into fixed-value coupons, each of which is used for one micropayment. A more flexible mechanism is proposed in this paper, whereby

* This work is partly supported by the Spanish CICYT under grant no. TEL98-0699-C02-02.

M. Mambo, Y. Zheng (Eds.): ISW'99, LNCS 1729, pp. 1–13, 1999.

coupons of variable value can be generated, several currencies can be used in successive micropayments, and larger payments can be made without computational overcost for the merchant or the buyer. Moreover, the buyer can provide input at transaction time to select, skip or re-use coupons.

1.2 Plan of This Paper

Section 2 contains some background on hash-based micropayment schemes. Section 3 introduces the concept of spending program. Section 4 discusses non-iterative spending programs (where coupons cannot be re-used). Section 5 presents iterative spending programs (where coupons are re-used). Section 6 is a conclusion. The Appendix recalls the structural program coding which is used to ensure integrity for spending programs.

2 Background on Hash-Based Micropayments

Quite a number of micropayment systems can be found in the literature that use hash functions instead of digital signatures to reduce the computational burden. On a typical workstation, it may take half a second to compute an RSA [15] signature; in that period, 100 RSA signatures can be verified (assuming a small public exponent) and, more important, 10000 hash functions can be computed. Thus, unlike digital signatures, hash functions allow high-rate verification of micropayments by the merchant without committing too many computing resources. This is a key issue since, for low-value payments to be profitable, they must be collected in an inexpensive way and possibly on a large scale (*i.e.* from a large community of buyers). On the buyer's side, replacing digital signatures with hash functions facilitates the use of smart cards, which are very convenient portable devices but have little computing power. So the advantages of dropping digital signatures in favour of hash functions should be clear.

Micropayment systems based on hash functions include NetCard [1], μ-*i*KP [8] and PayWord [14]. The principle behind those systems is similar. Let F be a computationally secure one-way hash function (*i.e.* easy to compute and hard to invert). Now the buyer takes a value X that will be the root of the chain and computes the sequence $T_n, T_{n-1}, \cdots, T_0$, where

$$\begin{aligned} T_0 &= F(T_1) \\ T_1 &= F(T_2) \\ &\vdots \\ T_{n-1} &= F(T_n) \\ T_n &= X \end{aligned} \tag{1}$$

The values $T_1, \cdots, T_n$ are called coupons and will be used by the buyer to perform n micropayments to the same merchant. Each coupon has the same fixed value v. Before the first micropayment, the buyer sends T_0 to the merchant together

with the value v in an authenticated manner. The micropayments are thereafter made by successively revealing $T_1, \cdots, T_n$ to the merchant, who can check the validity of T_i by just verifying that $F(T_i) = T_{i-1}$.

We next mention some differences between the main micropayment systems based on hash functions.

NetCard and μ-iKP are both micropayment schemes bootstrapped with normal e-payment systems, SET and iKP:

- With NetCard the bank supplies the root X of the hash chain to the buyer. The buyer then computes the chain, signs its last element T_0, the total number of elements n and the value of each chain element v. These signed values are sent by the buyer to the merchant, who uses the SET protocol to obtain on-line authorization for the whole chain.
- With μ-iKP, the root of the chain is a random value chosen by the buyer and the payment structure is the same as in the iKP payment system. In other words, the on-line authorization of the chain is performed by authorizing a single iKP payment of regular amount.

PayWord [14] is a credit-based scheme that needs a broker. The buyer establishes an account with the broker who gives her a certificate that contains the buyer identity, the broker identity, the public key of the buyer, an expiration date and some other information. The hash chain is produced by the buyer using a random root. When the buyer wants to make a purchase, she sends to the merchant a commitment to a chain. The commitment includes the merchant's identity, the broker certificate, the last element of the chain, the current date, the length of the chain and some other information. In this scheme, the broker certificate certifies that the broker will redeem any payment that the buyer makes before the expiration date, and the buyer commitment authorizes the broker to pay the merchant. Notice that in this scheme the chain is related to a pair buyer/merchant through the commitment. After that, micropayments are made by the buyer by revealing successive elements of the chain to the merchant. PayTree [9] is an extension to PayWord which uses hash trees rather than hash chains; a hash tree is a tree whose leaf nodes are labeled by secret random values, whose internal nodes are labeled by the hash value of the nodes' successors, and whose root is signed. PayTree allows the buyer to use parts of the hash tree to pay multiple merchants, with possibly several different denominations or currencies.

Pedersen [12] also iterates a hash function with a random root to obtain a chain of coins but he does not provide much detail on what kind of system (credit or debit based) he implements nor does he give information about some other security issues.

The authors of μ-iKP emphasize that the use of hash chains implicitly assumes that micropayments take place repeatedly from the same buyer to the same merchant. Such stability assumption on buyer-merchant relationship can be relaxed at the cost of trusting an intermediate broker who maintains stable relationships with several buyers and several merchants: a buyer can send

coupons to the broker and the broker is trusted to relay (his own) coupons to the merchant for the same value.

3 Basic Construction

With the exception of PayTree, the micropayment systems described in Section 2 share a lack of flexibility, which results in at least two shortcomings:

- Since all coupons have the same value v, the only way to be able to pay any amount is to let v be the minimal value, for instance one cent. But this means that the merchant must verify fifty hash functions to get paid a sum as small as fifty cents (being undesirable, note that this is still faster than verifying one RSA signature!, see Section 2). It is true that the buyer just needs to send one hash value (the 50th), but in any case she must store or compute all intermediate hashes.
- Fixed-value coupons do not allow to deal with different currencies.

PayTree mitigates the above lack of flexibility by replacing hash chains with hash trees, but still does not allow coupons to be re-used or dynamically selected. The scheme presented in this paper goes one step further and uses a structure more general than a hash tree, namely a *spending program*:

Definition 1 (Spending program). *A spending program $i_1, \cdots, i_n$ is a program whose instructions i_k are either value instructions, flow-control instructions, input-output instructions or assignment instructions.*

Definition 2 (Value instruction). *A value instruction is one that carries a specific sum of money in a currency specified in the same instruction. When a value instruction of a spending program is retrieved by the merchant, the corresponding sum of money is spent by the buyer.*

Definition 3 (Flow-control instruction). *A flow-control instruction allows to modify the flow of a spending program. Four types of flow-control instructions are used:*

1. *Forward unconditional branch*
2. *Forward conditional branch*
3. *Backward unconditional branch*
4. *Backward conditional branch*

If i_k is a branch to instruction i_j, "forward" means that $k < j$ and "backward" that $k \geq j$. Backward branches allow instruction blocks to be executed more than once.