Theo Dimitrakos
Fabio Martinelli
Peter Y.A. Ryan
Steve Schneider (Eds.)

Formal Aspects in Security and Trust

Third International Workshop, FAST 2005
Newcastle upon Tyne, UK, July 2005
Revised Selected Papers

LNCS 3866

Springer

Theo Dimitrakos Fabio Martinelli
Peter Y.A. Ryan Steve Schneider (Eds.)

Formal Aspects in Security and Trust

Third International Workshop, FAST 2005
Newcastle upon Tyne, UK, July 18-19, 2005
Revised Selected Papers

Springer

Volume Editors

Theo Dimitrakos
Security Research Centre
BT Group Chief Technology Office
2A Rigel House, Adastral Park, Martlesham, Ipswich IP5 3RE, UK
E-mail: Theo.Dimitrakos@bt.com

Fabio Martinelli
Istituto di Informatica e Telematica - IIT
National Research Council - C.N.R.
Pisa Research Area, Via G. Moruzzi, Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

Peter Y.A. Ryan
University of Newcastle upon Tyne
School of Computing Science
Newcastle upon Tyne, NE1 7RU, UK
E-mail: Peter.Ryan@newcastle.ac.uk

Steve Schneider
University of Surrey
Department of Computing
Guildford, Surrey, GU2 7XH, UK
E-mail: S.Schneider@surrey.ac.uk

Library of Congress Control Number: 2006921788

CR Subject Classification (1998): C.2.0, D.4.6, E.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-32628-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-32628-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11679219 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3866

Preface

This volume contains the post-proceedings of the Third International Workshop on Formal Aspects in Security and Trust (FAST 2005), held in Newcastle upon Tyne, July 18-19, 2005. FAST is an event affiliated with the Formal Methods 2005 Congress (FM05).

FAST 2005 aimed at continuing the successful effort of the previous two FAST workshop editions for fostering the cooperation among researchers in the areas of security and trust. The new challenges offered by the so-called ambient intelligence space, as a future paradigm in the information society, demand for a coherent and rigorous framework of concepts, tools and methodologies to increase users' trust&confidence in the underlying communication/interaction infrastructure. It is necessary to address issues relating to both guaranteeing security of the infrastructure and the perception of the infrastructure being secure. In addition, user confidence in what is happening must be enhanced by developing trust models which are not only effective but also easily comprehensible and manageable by users.

FAST sought original papers focusing on formal aspects in: security and trust policy models; security protocol design and analysis; formal models of trust and reputation; logics for security and trust; distributed trust management systems; trust-based reasoning; digital assets protection; data protection; privacy and ID issues; information flow analysis; language-based security; security and trust aspects in ubiquitous computing; validation/analysis tools; Web service security/trust/privacy; GRID security; security risk assessment; case studies etc.

This volume contains revised versions of 17 papers selected out of 37 submissions and the extended abstract of one invited contribution. Each paper was reviewed by at least three members of the international Program Committee (PC).

We wish to thank the PC members for their valuable efforts in properly evaluating the submissions, and the FM05 organizers for accepting FAST as an affiliated event and for providing a perfect environment for running the workshop.

Thanks are also due to BCS-FACS and IIT-CNR for the financial support for FAST 2005.

October 2005

Theo Dimitrakos
Fabio Martinelli
Peter Y.A. Ryan
Steve Schneider
FAST 2005 Co-chairs

Workshop Organization

Workshop Organizers

Theo Dimitrakos, BT, UK
Fabio Martinelli, IIT-CNR, Italy
Peter Y.A. Ryan, University of Newcastle, UK
Steve Schneider, University of Surrey, UK

Invited Speakers

Cédric Fournet, Microsoft Research (Cambridge), UK
Brian Randell, University of Newcastle, UK

Program Committee

Elisa Bertino, Purdue University, USA
John A. Clark, University of York, UK
Frédéric Cuppens, ENST Bretagne, France
Rino Falcone, ISTC-CNR, Italy
Simon Foley, University College Cork, Ireland
Roberto Gorrieri, University of Bologna, Italy
Masami Hagiya, University of Tokyo, Japan
Chris Hankin, Imperial College (London), UK
Valerie Issarny, INRIA, France
Christian Jensen, DTU, Denmark
Audun Jøsang, DSTC, Australia
Jan Jürjens, TU München, Germany
Yuecel Karabulut, SAP, Germany
Igor Kotenko, SPIIRAS, Russia
Heiko Krumm, University of Dortmund, Germany
Fabio Massacci, University of Trento, Italy
Stefan Poslad, Queen Mary College, UK
Catherine Meadows, Naval Research Lab, USA
Ron van der Meyden, University of New South Wales, Australia
Andrew Myers, Cornell University, USA
Mogens Nielsen, University of Aarhus, Denmark
Indrajit Ray, Colorado State University, USA
Babak Sadighi Firozabadi, SICS, Sweden
Pierangela Samarati, University of Milan, Italy
Ketil Stølen, SINTEF, Norway
Kymie Tan, Carnegie Mellon University, USA
William H. Winsborough, George Mason University, USA

Local Organization

Alessandro Falleni, IIT-CNR, Italy
Ilaria Matteucci, IIT-CNR, Italy

Lecture Notes in Computer Science

For information about Vols. 1–3798

please contact your bookseller or Springer

Vol. 3901: P.M. Hill (Ed.), Logic Based Program Synthesis and Transformation. X, 179 pages. 2006.

Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).

Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), Architecture of Computing Systems - ARCS 2006. XII, 496 pages. 2006.

Vol. 3890: S.G. Thompson, R. Ghanea-Hercock (Eds.), Defence Applications of Multi-Agent Systems. XII, 141 pages. 2006. (Sublibrary LNAI).

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3887: J. Correa, A. Hevia, M. Kiwi (Eds.), LATIN 2006: Theoretical Informatics. XVI, 814 pages. 2006.

Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), Knowledge Discovery in Life Science Literature. XIV, 147 pages. 2006. (Sublibrary LNBI).

Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), Modeling Decisions for Artificial Intelligence. XII, 374 pages. 2006. (Sublibrary LNAI).

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3875: S. Ur, E. Bin, Y. Wolfsthal (Eds.), Haifa Verification Conference. X, 265 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmidt (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part II. XXXI, 977 pages. 2006.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3830: D. Weyns, H. V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems II. VIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D.-Z. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing – EUC 2005 Workshops. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3820: L.T. Yang, X.-s. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

Vol. 3819: P. Van Hentenryck (Ed.), Practical Aspects of Declarative Languages. X, 231 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3817: M. Faundez-Zanuy, L. Janer, A. Esposito, A. Satue-Villar, J. Roure, V. Espinosa-Duro (Eds.), Nonlinear Analyses and Algorithms for Speech Processing. XII, 380 pages. 2006. (Sublibrary LNAI).

Vol. 3816: G. Chakraborty (Ed.), Distributed Computing and Internet Technology. XXI, 606 pages. 2005.

Vol. 3815: E.A. Fox, E.J. Neuhold, P. Premsmit, V. Wuwongse (Eds.), Digital Libraries: Implementing Strategies and Sharing Experiences. XVII, 529 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Sublibrary LNAI).

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3812: C. Bussler, A. Haller (Eds.), Business Process Management Workshops. XIII, 520 pages. 2006.

Vol. 3811: C. Bussler, M.-C. Shan (Eds.), Technologies for E-Services. VIII, 127 pages. 2006.

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Sublibrary LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Sublibrary LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3802: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part II. XLII, 1166 pages. 2005. (Sublibrary LNAI).

Vol. 3801: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part I. XLI, 1122 pages. 2005. (Sublibrary LNAI).

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

¥385.00元

Table of Contents

Voting Technologies and Trust
Brian Randell, Peter Y.A. Ryan 1

On the Formal Analyses of the Zhou-Gollmann Non-repudiation Protocol
Susan Pancho-Festin, Dieter Gollmann 5

Formal Reasoning About a Specification-Based Intrusion Detection for Dynamic Auto-configuration Protocols in Ad Hoc Networks
Tao Song, Calvin Ko, Chinyang Henry Tseng, Poornima Balasubramanyam, Anant Chaudhary, Karl N. Levitt 16

A Formal Approach for Reasoning About a Class of Diffie-Hellman Protocols
Rob Delicata, Steve Schneider 34

Eliminating Implicit Information Leaks by Transformational Typing and Unification
Boris Köpf, Heiko Mantel 47

Abstract Interpretation to Check Secure Information Flow in Programs with Input-Output Security Annotations
N. De Francesco, L. Martini 63

Opacity Generalised to Transition Systems
Jeremy W. Bryans, Maciej Koutny, Laurent Mazaré, Peter Y.A. Ryan 81

Unifying Decidability Results on Protection Systems Using Simulations
Constantin Enea 96

Proof Obligations Preserving Compilation
Gilles Barthe, Tamara Rezk, Ando Saabas 112

A Logic for Analysing Subterfuge in Delegation Chains
Hongbin Zhou, Simon N. Foley 127

Probable Innocence Revisited
Konstantinos Chatzikokolakis, Catuscia Palamidessi 142

Relative Trustworthiness
Johan W. Klüwer, Arild Waaler 158

Secure Untrusted Binaries — Provably!
Simon Winwood, Manuel M.T. Chakravarty 171

Normative Specification: A Tool for Trust and Security
Olga Pacheco 187

Type-Based Distributed Access Control vs. Untyped Attackers
Tom Chothia, Dominic Duggan 203

A Security Management Information Model Derivation Framework: From Goals to Configurations
R. Laborde, F. Barrère, A. Benzekri 217

On Anonymity with Identity Escrow
Aybek Mukhamedov, Mark D. Ryan 235

Towards Verification of Timed Non-repudiation Protocols
Kun Wei, James Heather 244

Author Index 259

Voting Technologies and Trust

(Extended Abstract)

Brian Randell and Peter Y. A. Ryan

School of Computing Science, University of Newcastle upon Tyne
{brian.randell, peter.ryan}@ncl.ac.uk

In this extended abstract we describe initial steps towards a secure voting scheme that could gain as high a level of public trust as is achieved by the existing UK voting scheme. Such a scheme would, we suggest, need to be regarded by the general public as being as understandable as well as at least as trustworthy (*i.e.* dependable and secure) as the system they are already used to. Note that trustworthiness is a necessary, but by no means always sufficient condition for achieving trusted status. The challenge we are addressing is thus as much a socio-technical as a technical one.

The present-day voting process used in the UK national elections is a manual one which involves the use of pre-printed paper ballots. These have a column of candidates' names printed down the left-hand column, and a right-hand column which provides a corresponding set of boxes in which a vote or votes can be marked. The entire voting process takes place under the close supervision of a set of independent officials and, in the case of the vote-counting process, also representatives of the rival candidates, under the protection of a strict legal regime.

Voters must previously have ensured that their names are on the electoral register. They have to cast their votes at a particular voting station, and each such station has a list of the voters who are registered to vote there. This list is marked as each voter is given a ballot paper. Thus the same individual attempting to vote more than once, or different individuals trying to vote using the same identity, especially at the same voting station, is fairly readily detected, though using means which cause some to have concerns regarding vote secrecy.

The current level of trust in the manual system used in UK national elections appears to be due to its many years of largely unchallenged use, and the fact that the general public can readily understand the system. The fact that it involves a large number of independent, and probably rather hostile, observers, suggests that a large number of votes cannot be subverted (changed, replicated or lost) other than by the malicious activities of a large number of individuals, who would have to act for the most part in collusion. This has led us to propose a rather simplistic but useful and generally understandable measure of the merit of a voting system that we term its *insubvertibility*, a robustness-related characteristic that is assessed by dividing the number of votes that could be altered, faked or lost into the number of people who are needed to achieve such alteration, faking or loss.

We take ballot secrecy, insubvertibility and understandability as the key characteristics that need to be maximised. These are all too easily undermined by ill-thought-out schemes of electronic voting, in which a very small number of people in the right position might well be able to subvert the entire election! The approach we

T. Dimitrakos et al. (Eds.): FAST 2005, LNCS 3866, pp. 1 – 4, 2006.

take is to explore some possible improvements to the existing manual UK voting system, in particular with regard to vote secrecy, accuracy and overall system efficiency (via the introduction of automation), without compromising the system's existing merits. In this extended abstract we describe just the initial step in this exploration.

In order to improve the voter secrecy provided by the existing manual system we suggest use of a ballot paper based on that used in the Prêt à Voter scheme[1]. In this scheme:

- the ballot papers are perforated vertically so that the column with the list of candidates can readily be separated from that on which the voter has recorded her vote,
- the order in which the candidates are listed varies randomly from ballot paper to ballot paper, and
- the voter is allowed to choose a ballot paper for herself at random from a large well-shuffled bundle of such papers.

However, as shown in the Figure, and in contrast to the Prêt à Voter scheme, at the foot of *each* column is printed a unique vote identification number (VIN). The left-hand column of the ballot paper (LHC) constitutes a vote receipt that can be retained by the voter, while the right-hand portion (RHC) is carried forward into the vote counting process. Although the LHC does not, once separated from the RHC, provide any indication of how the voter cast her vote, it does provide an identifiable record of the fact that a vote has been cast.

The crucial aspect of our scheme, inspired by the cryptographic technique involved in the Prêt à Voter scheme, is that the RHC is, in effect, a so-called "scratch card", in that it contains a small rectangle of opaque coating which is initially obscuring a pre-printed code. This code (OCN) identifies the order in which the candidates' names were printed in the left-hand column. The copy of the VIN at the foot of this RHC is printed *on* this opaque coating. This coating can be scratched off, simultaneously destroying the VIN and revealing the OCN.

As well as permitting the voter to choose her own ballot paper at random, she would also be permitted – indeed encouraged – to take other ballot papers and (i) assure herself that they varied with regard to the ordering of the candidates, (ii) scratch off the VINs (thereby invalidating their use as ballots) and verify that the revealed OCNs match the order of the candidates. (Such testing and discarding of RHCs should be done under the supervision of the polling station officials to prevent multiple voting.).

Actual vote casting requires the voter to proceed to a booth with a single ballot paper with its VIN strip still intact. In the booth, she indicates her vote by placing a cross in the appropriate cell on the RHC against the candidate of her choice in the usual fashion. She then splits the ballot paper along the perforation down the middle

[1] David Chaum, Peter Y.A. Ryan and Steve A. Schneider. *A Practical, Voter-verifiable Election Scheme.* Proc. 10th European Symposium on Research in Computer Security - ESORICS. Springer Verlag (2005).

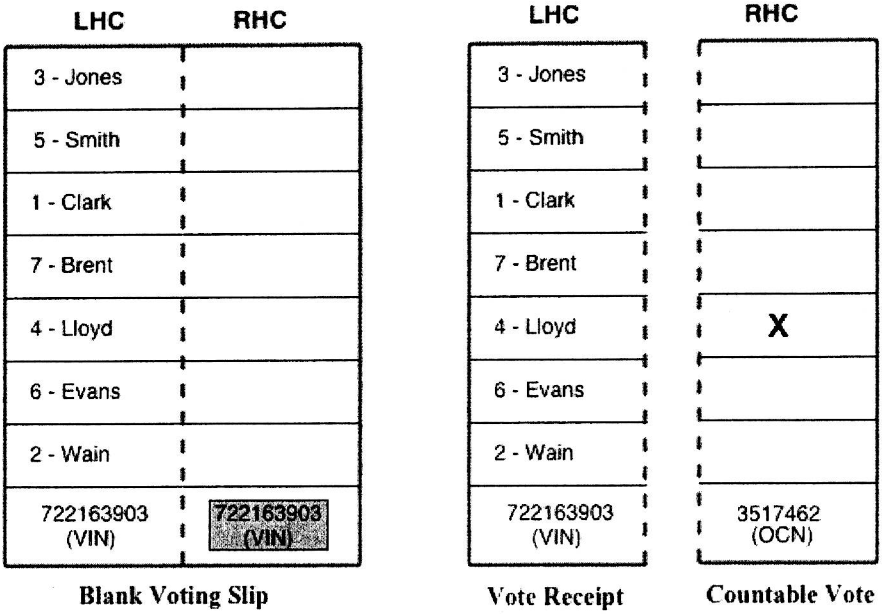

Fig. 1. A ballot paper – before voting and after it has been split and its OCN made visible

and, leaving the scratch strip intact so as to preserve the secrecy of her vote, posts the RHC into a locked ballot box. When the vote casting period has ended, the secure boxes of votes (RHCs) are taken from each voting station to a vote counting centre. In order to interpret the vote value encoded on each RHC, the VIN strip must be scratched off under supervision. (This is so as to minimise the possibility that ballots are lost, altered or injected whilst at the same time ensuring that no-one can link the VIN numbers to the resulting ballot papers reveal the OCN hidden underneath.) Before the RHCs have their VINs scratched off, however, the VINs would be recorded and published (e.g. via a secure web bulletin board) so that each voter can use her vote receipt to check that her vote was indeed entered into the counting process.

Once their OCNs have been revealed the RHCs can be used in a near-conventional process of (well-scrutinised) manual vote counting. Given the general public's experience of and trust in scratch cards (which are likely to be even more familiar to them than ballot papers) and in the act of shuffling playing cards, we believe that this vote counting process and indeed the whole voting scheme could gain a level of acceptance from the public regarding its overall trustworthiness comparable to that enjoyed by the manual scheme that is currently in use in the UK. The additional vote secrecy it provides should also be manifest to the general public.

However, major trust concerns arise when one moves away from the use of paper ballots either partly (in that paper voting receipts might still be retained) or completely, so that the vote casting as well as counting is all done essentially invisibly, *e.g.* electronically. Even if the public have good reason to believe that electronic versions of their votes are reaching the vote counting process safely, the problem is to provide the public with continued reason to trust a vote counting process that is not directly visible to ordinary officials and scrutineers.

For example, vote counting machines, or indeed voting machines, i.e. DRE (direct recording electronic) devices, that have a conventional general-purpose computer and operating system incorporated into them are problematic and likely to remain controversial. Their use normally requires a degree of trust that the more technically-aware voters in particular are, quite correctly, likely to be reluctant to provide. Indeed, with electronic votes various forms of "online" manual checking by multiple observers will normally have to be replaced or supplemented by (i) prior checking of the design of possibly very sophisticated algorithms and devices, and (ii) ensuring the continued relevance of the results of these checks up to and during the actual voting process.

The Voter Verifiable Paper Audit Trail (VVPAT) scheme has therefore been advocated as an adjunct to an electronic voting casting and counting system. Such an approach depends on somehow ensuring (i) that the audit trail mechanism, rather than the actual voting system *per se*, is adequately trustworthy, and (ii) that recourse will be had to this audit trail mechanism whenever necessary.

An alternative approach is to use cryptographic mechanisms to make the counting process highly transparent and auditable, within the constraints of ballot secrecy, and to make the auditing processes public and open to scrutiny– this is the approach taken in the Prêt à Voter scheme, for example. However, although with such voting schemes the computers and the software involved need not be trusted, the arguments for the trustworthiness of the overall voting system are subtle and require specialist knowledge in order to be properly appreciated.

In our full paper, to appear in the IEEE Journal of Security & Privacy, we go on to explore various developments of the basic scratch-card system, in a series of steps towards actual e-voting. However, we have deliberately tried - in pursuit of user acceptance and trust - to retain the familiarity and simplicity of current well-accepted devices and systems. As a result, in most of our proposals we have deliberately sought to retain at least some use of paper, and to avoid, or at least minimize the use of, electronics and computers.

On the Formal Analyses of the Zhou-Gollmann Non-repudiation Protocol

Susan Pancho-Festin[1] and Dieter Gollmann[2]

[1] Dept. of Computer Science, University of the Philippines-Diliman
sbpancho@up.edu.ph
[2] TU Hamburg-Harburg, Germany
diego@tu-harburg.de

Abstract. Most of the previous comparisons of formal analyses of security protocols have concentrated on the tabulation of attacks found or missed. More recent investigations suggest that such cursory comparisons can be misleading. The original context of a protocol as well as the operating assumptions of the analyst have to be taken into account before conducting comparative evaluations of different analyses of a protocol. In this paper, we present four analyses of the Zhou-Gollmann non-repudiation protocol and trace the differences in the results of the four analyses to the differences in the assumed contexts. This shows that even contemporary analyses may unknowingly deviate from a protocol's original context.

1 Introduction

The observations derived from the comparative evaluation of formalisations and analyses of the Needham-Schroeder public key and shared key protocols [1] suggest that different protocol models affect the resulting analysis results, to the extent that it explains why some analyses fail to find attacks detected by other methods [2]. Although it is now generally accepted that this explains the previously undocumented attack discovered by Lowe [3] on the Needham-Schroeder public key protocol, the wider effects of protocol models have not been always considered in previous comparisons of protocol results. This results in the continued misinterpretation of a protocol's security particularly when it is implicitly assumed that different analyses are directly comparable without recourse to the details of their protocol models.

Contemporary protocols encompass a larger scope. Some attempt to offer security guarantees that do not fit traditional definitions of authentication, confidentiality or integrity. The scope of newer protocols is broader, their properties often more complex and the implementation details more convoluted. This provides a richer ground for misinterpretation of requirements and conflicts in both formalisation and implementation. Intuition suggests that if differences in formalisation are already observed in relatively simple protocols such as those in the Needham-Schroeder family, then the more recent and more complex protocols are even more susceptible to the production of different protocol models, and possibly, to different analysis results. In this paper we present the Zhou-Gollmann

T. Dimitrakos et al. (Eds.): FAST 2005, LNCS 3866, pp. 5–15, 2006.

Non-repudiation protocol as an example of a contemporary, non-conventional security protocol where differences in the results from several analyses are attributed to changes in the assumed protocol context.

2 The Zhou-Gollmann Non-repudiation Protocol

The Zhou-Gollmann non-repudiation protocol [4] was analysed by its authors using the SVO logic [5], by Schneider using CSP/FDR [6] and by Bella and Paulson using the Isabelle theorem prover [7]. These analyses did not report the more recent attacks reported by Gürgens and Rudolph [8] using asynchronous product automata (APA) and the simple homomorphism verification tool (SHVT). The primary cause for the conflicting results is in the differences in assumptions among the four analyses with respect to the storage of evidence and the behaviour of participants, particularly the trusted third party (TTP).

Non-repudiation is a fairly new security requirement compared to authentication and confidentiality. As such, there are fewer protocols that provide this property; there are even fewer formal analyses of these protocols. The Zhou-Gollmann (ZG) protocol [4] is unique in the sense that there are several existing analyses of it; this allows us to compare how different methods formalise the new concept of non-repudiation.

Non-repudiation is the property wherein both the message sender and recipient obtain evidence of having sent or received a message, respectively. This evidence must be independently verifiable by a third party. Evidence of receipt is given to the message sender to prove that the recipient has received a message. Evidence of origin is given to the message recipient to prove that the sender has indeed sent a message.

In the ZG protocol, there is an additional requirement of fairness. It should not be possible for either sender or recipient to be in a more advantageous position over the other. Fairness ensures that both evidence of receipt and origin can only be held after the protocol completes. If one party abandons a protocol session, no acceptable evidence must be generated for that session.

The ZG protocol is shown in Figure 1. Note that, even if the commitment C is produced via the encryption of the message M with key K, this is not undertaken to ensure message secrecy. Rather, the commitment is first sent to the recipient who signs it and returns it to the sender. Both the sender and recipient's signature on this commitment and its corresponding label L comprises the first part of the evidence of receipt and evidence of origin respectively. To complete both evidence, the sender and recipient must individually obtain *con_K* from the trusted third party via an *ftp-get* operation.

If A denies having sent the message M, B presents to the judge M, C, L, K, EOO and *con_K*. The judge will check if [4]:

- *con_K* was signed by the TTP.
- EOO was signed by A.
- $M = \{C\}_{K^{-1}}$