SECURITY AND PROTECTION IN INFORMATION SYSTEMS

Proceedings of the Fourth IFIP TC 11 International Conference on Computer Security, IFIP/Sec '86
Monte Carlo, Monaco, 2–4 December, 1986

IFIP TC 11 International Conference on Computer Security (4th : 1986 : Monte Carlo, Monaco).

edited by

André GRISSONNANCHE
XP Conseil
Paris, France

1989

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD • TOKYO

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

© IFIP, 1989

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher, Elsevier Science Publishers B.V. (Physical Sciences and Engineering Division), P.O. Box 103, 1000 AC Amsterdam, The Netherlands.

Special regulations for readers in the U.S.A. – This publication has been registered with the Copyright Clearance Center Inc. (CCC), Salem, Massachusetts. Information can be obtained from the CCC about conditions under which photocopies of parts of this publication may be made in the U.S.A. All other copyright questions, including photocopying outside of the U.S.A., should be referred to the publisher, Elsevier Science Publishers B.V., unless otherwise specified.

No responsibility is assumed by the publisher or by IFIP for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

ISBN: 0 444 87345 7

Published by:

ELSEVIER SCIENCE PUBLISHERS B.V.
P.O. Box 103
1000 AC Amsterdam
The Netherlands

Sole distributors for the U.S.A. and Canada:

ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
655 Avenue of the Americas
New York, N.Y. 10010
U.S.A.

Library of Congress Cataloging-in-Publication Data

IFIP International Conference on Computer Security (4th : 1986 : Monte
-Carlo, Monaco)
Security and protection in information systems : proceedings of
the fourth IFIP International Conference on Computer Security,
IFIP/Sec '86, Monte Carlo, Monaco, 2-4 December, 1986 / edited by
Andre Grissonnanche.
p. cm.
Bibliography: p.
ISBN 0-444-87345-7
1. Computers--Access control--Congresses. 2. Electronic data
processing departments--Security measures--Congresses.
I. Grissonnanche, Andre. II. Title. III. Title: International
Federation for Information Processing.
QA76.9.A25I45 1986
658.4'78--dc19 89-2945
CIP

PRINTED IN THE NETHERLANDS

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

SECURITY AND PROTECTION IN INFORMATION SYSTEMS
A. Grissonnanche (Editor)
Elsevier Science Publishers B.V. (North-Holland)
IFIP, 1989

This material may be protected by Copyright law (Title 17 U.S. Code)

AN INTELLIGENT TOKEN FOR SECURE TRANSACTIONS

B J CHORLEY and W L PRICE

National Physical Laboratory, Teddington, Middx, UK

After reviewing the requirements for user identity verification in any transaction processing system, the paper describes the design of an intelligent token that offers much greater security than that of conventional tokens. Applications for intelligent tokens are explored and an attempt is made to identify further possible lines of progress.

1. INTRODUCTION

Teleprocessing systems for handling transactions are assuming ever increasing importance in many areas of finance and commerce. These systems range from those handling billions of pounds per day in transfers between major banking institutions to those where supermarket customers make their payments for purchases using plastic cards. A common need of all such systems, whatever their scale, is to achieve integrity so that their users can trust the outcome of the operations carried out on their behalf. Because of the enormous amounts of money involved there is an inevitable attraction for the criminal world to attempt to profit from unauthorised or altered transactions. There is therefore need for designers of these systems to take into account the attacks to which the systems may be subjected and to take appropriate security countermeasures. Attacks may involve attempts by intruders to masquerade as authorised users, they may involve attempts to alter transaction records, they may try to force the system to give authorisation to a transaction that should really be denied, and so forth. There are indeed many ways in which transaction processing systems may be open to attack.

Our purpose in presenting this paper is to examine some aspects of the process of verifying the identity of authorised users and also the integrity of the transactions carried out on their behalf. We shall then develop a specification for an intelligent token that can participate effectively in achieving identity verification and transaction integrity. Finally we examine some of the potential applications of such a token.

Identity verification is based classically on something known to the user, something possessed by the user or some physical characteristic of the user. 'Something known' usually implies a password or, in the case of systems operated by banks, the ubiquitous 'PIN' or personal identification number. 'Something possessed' may be a token, for example a plastic card or a key. Physical characteristics used for identity verification are often called 'biometrics'; examples include voice and signature verification. It is generally considered that they provide security superior to that offered by PINs, but there are other disadvantages which discourage their widespread introduction, not least the degree of imprecision that is inherent in many of the techniques proposed.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

There is no doubt that the commonest technique for user verification is that which uses the plastic card; there are very many millions of such cards in use throughout the world today, most of which carry a magnetic stripe. Strictly speaking the card only allows an identity to be claimed and does nothing in itself to help the verification of that identity. To prevent a lost card being used by someone other than the authorised user it is customary in many types of transaction to require that the user offer a memorised PIN in conjunction with the card; usually a derived function of the PIN is stored on the card. Human memory being what it is, the 'memorised' PIN is often written down, even on the card itself; the problem is compounded by many users possessing several cards, each with its own different PIN. There is an undoubted need to educate the public better in the use of PINs, but their eventual replacement by biometric methods of identity verification within the next few years may safely be predicted.

The magnetic stripe card is itself a source of insecurity for systems in which it is used. The problem is that the card is too easily counterfeited. The magnetic stripe can easily be copied unless special measures are taken to make this difficult, the embossing can easily be altered or simulated and the general appearance of the cards can be imitated in a way sufficiently sophisticated to deceive human counter clerks. Various security measures have been added to the cards in recent times to make these falsification methods less effective; the hologram on the face of the card and the use of 'watermark' magnetic tape are examples of such measures.

Because of the shortcomings of the magnetic stripe as a secure means of recording user parameters a great deal of attention has been paid in recent years to alternative card technologies. In particular we have the intelligent or 'smart' card, where integrated circuits (one or more) are embedded within the plastic; surface contacts are usually provided as part of a communication interface, though other means of communication are also being considered. It is well known that experiments have been carried out, particularly in France, to assess the performance of smart cards. The outcome of these experiments has not been widely publicised, but the French are showing their confidence in these devices by launching new applications with millions of cards in use.

It seems that counterfeiting of the smart card presents the criminal with much greater problems than are met with the magnetic stripe card. However, the problem of the PIN as a means of confirming claimed identity remains. Presentation of a PIN associated with the smart card requires that it be entered on a keyboard associated with the terminal. Because the field of application of the smart card is bound to include transactions such as point of sale, the insecurity of the average point of sale terminal is significant. Physical protection of such terminals is bound to be much less than that normally found in automatic teller machines. Therefore we may expect that some point of sale terminals will be bugged with the object of collecting personal account information and PINs. Exploitation of this knowledge may not necessarily involve fabrication of false cards; stealing of a smart card whose PIN has been discovered is a much simpler means.

For this reason (and others which will emerge later) there is considerable merit in an intelligent identity token which goes further than the smart card and provides its own keyboard for PIN entry and transaction confirmation.

Bugging of a transaction terminal in order to collect PINs is not the only risk to which system customers may be exposed. The transaction details are usually displayed to the customer on the terminal display and it is not beyond the bounds of criminal ingenuity to arrange that the terminal display shows a small amount whilst the transaction message, unseen by the customer, is constructed to contain a much larger amount. One precaution against this type of fraud is to insist on a transaction voucher being printed and retained by the customer.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

However, customer habits with vouchers are also notoriously bad; they too easily get lost or are deliberately thrown away, leaving no record in the hands of the customer.

There is therefore considerable merit in presenting the transaction details to the customer on a display that is under the customer's direct control - on the token itself. The customer will more readily trust such a display than that on the terminal. Inclusion of a display on a small token is facilitated by the development of very compact forms of liquid crystal display as found in many pocket calculators. If, later, the token is to be used to check on a series of transactions carried out by its owner, then it is a simple matter to arrange that a record of transactions be held in the token.

Ensuring the integrity of transaction messages is a different problem, since these are vulnerable to alteration unless appropriate protective measures are taken. Message encipherment is commonly used in transaction systems for message protection, but an even more powerful technique is offered by message signature. Using public key cryptography it is possible for the sender of a message to produce a transformation in the message such that the recipient of the transformed message can use a parameter associated with the alleged sender (the public key of the sender) and actually prove beyond doubt that the transformed message came from that sender; this ability is commonly referred to as 'digital signature'. Since the intelligent token whose specification we have been developing in this discussion is assumed to be trusted by its owner, the ability of the token to sign messages on behalf of the owner would be very attractive. Transaction messages could be read from terminal into token, checked on the token display and then, if approved by the owner of the token, signed by the token before being sent back to the terminal for processing within the transaction system. The correctness of the signature can be checked by any system entity possessing a copy of the public key belonging to the particular user.

We are therefore suggesting that desirable features of an intelligent token should include a keyboard and a display on the token, with internal hardware and software designed to provide digital signature; it goes without saying that a suitable interface must be provided. The remainder of this paper discusses the design, development and potential applications of such a token.

2. THE NPL INTELLIGENT TOKEN

Research and development at the National Physical Laboratory, beginning in 1982, sponsored by the British Technology Group, the UK Department of Trade and Industry and members of British commerce and industry, has produced a token [1] which possesses the desirable properties developed in the introduction to this paper, namely internal processing power and memory, integral keyboard and display, and appropriate interface. At present the token exists in the form of a fully working prototype which is the size of a small book, but it is intended that further development shall lead to miniaturisation of the token down to the size of a small pocket calculator. It is unlikely that attempts will be made to bring the token size down to the credit card dimensions which have governed the design of the smart card. The critical dimension is, of course, the thickness of the device; smart card manufacturers are seeking to create a viable device within the compass of 0.76 mm which is the thickness allowed for credit cards in the international standard for these.

A token can be designed to perform many different functions and may thereby replace a number of separate cards and calculators currently carried by users.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.