

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Dingyi Pei Moti Yung Dongdai Lin  
Chuankun Wu (Eds.)

# Information Security and Cryptology

Third SKLOIS Conference, Inscrypt 2007  
Xining, China, August 31–September 5, 2007  
Revised Selected Papers

 Springer

## Volume Editors

Dingyi Pei  
Guangzhou University  
Institute of Information Security  
Guangzhou, China  
E-mail: gztcdpei@scut.edu.cn

Moti Yung  
Google Inc., and Columbia University  
Department of Computer Science  
New York, NY, USA  
E-mail: moti@cs.columbia.edu

Dongdai Lin  
SKLOIS, Institute of Software  
Chinese Academy of Sciences  
Beijing, China  
E-mail: ddlin@is.iscas.ac.cn

Chuankun Wu  
SKLOIS, Institute of Software  
Chinese Academy of Sciences  
Beijing, China  
E-mail: ckwu@is.iscas.ac.cn

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

|         |                                                       |
|---------|-------------------------------------------------------|
| ISSN    | 0302-9743                                             |
| ISBN-10 | 3-540-79498-0 Springer Berlin Heidelberg New York     |
| ISBN-13 | 978-3-540-79498-1 Springer Berlin Heidelberg New York |

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2008  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 12263486      06/3180      5 4 3 2 1 0

## Preface

The Third SKLOIS Conference on Information Security and Cryptology (Inscrypt 2007) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences in cooperation with Qinhai University for Nationalities. This international conference was held in Xining, Qinhai Province of China, and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate University of the Chinese Academy of Sciences and the National Natural Science Foundations of China.

By now, Inscrypt (the International SKLOIS Conference on Information Security and Cryptology) has become a tradition, and it is, in fact, a leading event in this area, which takes place annually in China. We are pleased with the continuous support by authors, committee members, reviewers, sponsors and organizers. Indeed, the research areas covered by Inscrypt are important, since modern computing (including communication infrastructures and applications) requires increased security, trust, safety and reliability. This need has motivated the research community worldwide to produce important fundamental, experimental and applied work in the wide areas of cryptography and information security research in recent years. Accordingly, the program of Inscrypt 2007 covered numerous fields of research within these general areas.

The international Program Committee of the conference received a total of 167 submissions from 21 countries and regions, from which only 43 submissions were selected for presentation, 33 of which in the regular papers track and 10 submissions in the short papers track. All anonymous submissions were reviewed by experts in the relevant areas, and based on their ranking, technical remarks and strict selection criteria the papers were chosen for the various tracks. We note also that reviews of submissions by committee members were hidden from their authors throughout the entire review process. We also note that due to the conference format, many good papers were regrettably not accepted.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference program. We thank the conference Organizing Committee, the various sponsors and the conference attendees. Last but not least, we also express our thanks to all the authors who submitted papers to the conference, the invited speakers and the session Chairs.

August/September 2007

Dingyi Pei  
Moti Yung

# Inscrypt 2007

Third SKLOIS Conference  
on Information Security and Cryptology

Xining, Qinghai, China  
August 31 - September 2, 2007

*Sponsored and organized by*

State Key Laboratory of Information Security  
(Chinese Academy of Sciences)  
and  
Qinhai University for Nationalities

## General Co-chairs

Dengguo Feng  
Youyi Zhang

SKLOIS, Chinese Academy of Sciences, China  
Qinhai University for Nationalities, China

## Program Co-chairs

Dingyi Pei  
Moti Yung

Guangzhou University, China  
Google inc and Columbia University, USA

## Program Committee

Feng Bao  
Rana Barua  
Lejla Betina  
Emmanuel Bresson  
Bogdan Carbunar  
Robert H. Deng  
Cunsheng Ding  
Marc Girault  
Bok Min Goi  
Dieter Gollmann  
Goichiro Hanaoka  
Tor Helleseeth  
Lei Hu  
Stamatiou Iwannis  
Hongxia Jin  
Vladimir Kolesnikov  
Xuejie Lai

I2R, Singapore  
Indian Statistical Institute, India  
U.K. Leuven, Belgium  
DCSSI Crypto Lab, France  
Motorola Labs, USA  
SMU, Singapore  
HKUST, Hong Kong, China  
France Telecom, France  
Multimedia University, Malaysia  
TU Harburg, Germany  
AIST, Japan  
Bergen University, Norway  
SKLOIS, Chinese Academy of Sciences, China  
University of Patras, Greece  
IBM Almaden Research Center, USA  
Bell-Labs, USA  
Shanghai Jiaotong University, China

## VIII Organization

|                     |                                            |
|---------------------|--------------------------------------------|
| DongHoon Lee        | Korea University, Korea                    |
| Benoit Libert       | U.C. Louvain, Belgium                      |
| Dongdai Lin         | SKLOIS, Chinese Academy of Sciences, China |
| Michael Locasto     | Columbia University, USA                   |
| Masahiro MAMBO      | Tsukuba University, Japan                  |
| Wenbo Mao           | HP, Beijing, China                         |
| David Naccache      | ENS, France                                |
| Rei Safavi-Naini    | Calgary, Canada                            |
| Mridul Nandi        | Indian Statistical Institute, India        |
| Juan Gonzalez Nieto | QUT, Australia                             |
| Giuseppe Persiano   | University of Salerno, Italy               |
| Junji Shikata       | University of Yokohama, Japan              |
| Vitaly Shmatikov    | University of Texas at Austin, USA         |
| Francesco Sica      | Mount Allison University, Canada           |
| Rainer Steinwandt   | Florida Atlantic University, USA           |
| Willy Susilo        | UWO, Australia                             |
| Bogdan Warinschi    | University of Bristol, UK                  |
| DongHo Won          | Sungkyunkwan University, Korea             |
| Chuankun Wu         | SKLOIS, Chinese Academy of Sciences, China |
| Shouhuai Xu         | University of Texas at San Antonio, USA    |
| Yongjin Yeom        | NSRI, Korea                                |
| Yuefei Zhu          | Information Engineering University, China  |

## Organizing Committee Co-chairs

|             |                                            |
|-------------|--------------------------------------------|
| Dongdai LIN | SKLOIS, Chinese Academy of Sciences, China |
| Yanhui Niu  | Qinhai University for Nationalities, China |
| Chuankun Wu | SKLOIS, Chinese Academy of Sciences, China |

## Organizing Committee

|                |                                            |
|----------------|--------------------------------------------|
| Jiwu Jing      | SKLOIS, Chinese Academy of Sciences, China |
| Fuming Qi      | Qinhai University for Nationalities, China |
| Shengfu Zhang  | Qinhai University for Nationalities, China |
| Yuqing Zhang   | SKLOIS, Chinese Academy of Sciences, China |
| Zhenfeng Zhang | SKLOIS, Chinese Academy of Sciences, China |

## Secretary and Treasurer

|        |                                            |
|--------|--------------------------------------------|
| Yi Qin | SKLOIS, Chinese Academy of Sciences, China |
|--------|--------------------------------------------|

## WEB/Registration

|                 |                                            |
|-----------------|--------------------------------------------|
| Guangsheng Miao | SKLOIS, Chinese Academy of Sciences, China |
|-----------------|--------------------------------------------|

# Table of Contents

## Invited Talks

|                                                                           |   |
|---------------------------------------------------------------------------|---|
| Cryptanalysis of the SFLASH Signature Scheme<br>(Extended Abstract) ..... | 1 |
| <i>Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern</i>  |   |
| On the Evolution of User Authentication: Non-bilateral Factors .....      | 5 |
| <i>Moti Yung</i>                                                          |   |

## Digital Signature Schemes

|                                                                                                           |    |
|-----------------------------------------------------------------------------------------------------------|----|
| ECDSA-Verifiable Signcryption Scheme with Signature Verification on<br>the Signcrypted Message .....      | 11 |
| <i>Raylin Tso, Takeshi Okamoto, and Eiji Okamoto</i>                                                      |    |
| Provably Secure Identity-Based Undeniable Signatures with Selective<br>and Universal Convertibility ..... | 25 |
| <i>Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang</i>                                                       |    |
| An Efficient ID-Based Proxy Signature Scheme from Pairings .....                                          | 40 |
| <i>Chunxiang Gu and Yuefei Zhu</i>                                                                        |    |

## Block Cipher

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Improved and Multiple Linear Cryptanalysis of Reduced Round<br>Serpent ..... | 51 |
| <i>B. Collard, F.-X. Standaert, and J.-J. Quisquater</i>                     |    |
| Linear Slide Attacks on the KeeLoq Block Cipher .....                        | 66 |
| <i>Andrey Bogdanov</i>                                                       |    |

## Key Management

|                                                                                               |     |
|-----------------------------------------------------------------------------------------------|-----|
| A Key Predistribution Scheme Based on 3-Designs .....                                         | 81  |
| <i>Junwu Dong, Dingyi Pei, and Xueli Wang</i>                                                 |     |
| Provably Secure $N$ -Party Authenticated Key Exchange in the Multicast<br>DPWA Setting .....  | 93  |
| <i>Weijia Wang, Lei Hu, and Yong Li</i>                                                       |     |
| A Provably Secure One-Pass Two-Party Key Establishment Protocol ...                           | 108 |
| <i>K. Chalkias, S.T. Halkidis, D. Hristu-Varsakelis,<br/>G. Stephanides, and A. Alexiadis</i> |     |

**Zero Knowledge and Secure Computation Protocols**

Resettable Zero Knowledge with Concurrent Soundness in the Bare  
Public-Key Model under Standard Assumption ..... 123  
*Yi Deng and Dongdai Lin*

Secure Two-Party Computation of Squared Euclidean Distances in the  
Presence of Malicious Adversaries ..... 138  
*Marc Mouffron, Frederic Rousseau, and Huafei Zhu*

A Discrete-Logarithm Based Non-interactive Non-malleable  
Commitment Scheme with an Online Knowledge Extractor ..... 153  
*Ning Ding and Dawu Gu*

**Secret Sharing**

Verifiable Multi-secret Sharing Schemes for Multiple Threshold Access  
Structures ..... 167  
*Christophe Tartary, Josef Pieprzyk, and Huaxiong Wang*

Key Management Based on Hierarchical Secret Sharing in Ad-Hoc  
Networks ..... 182  
*Chuangui Ma and Rui Cheng*

Probabilistic  $(n, n)$  Visual Secret Sharing Scheme for Grayscale  
Images ..... 192  
*Daoshun Wang, Xiaobo Li, and Feng Yi*

**Stream Cipher and Pseudorandomness**

Mutually Clock-Controlled Feedback Shift Registers Provide Resistance  
to Algebraic Attacks ..... 201  
*Sultan Al Hinai, Lynn Margaret Batten, and Bernard Colbert*

Four Families of Binary Sequences with Low Correlation and Large  
Linear Complexity ..... 216  
*Jin-Song Wang and Wen-Feng Qi*

Pseudo-Randomness of Discrete-Log Sequences from Elliptic Curves .... 231  
*Zhixiong Chen, Ning Zhang, and Guozhen Xiao*

Improved Bounds on the Linear Complexity of Keystreams Obtained  
by Filter Generators..... 246  
*Nicholas Kolokotronis, Konstantinos Limniotis, and  
Nicholas Kalouptsidis*

## Boolean Functions

|                                                                                                                                   |     |
|-----------------------------------------------------------------------------------------------------------------------------------|-----|
| Linear Equation on Polynomial Single Cycle T-Functions .....                                                                      | 256 |
| <i>Jin-Song Wang and Wen-Feng Qi</i>                                                                                              |     |
| Weight Support Technique and the Symmetric Boolean Functions with<br>Maximum Algebraic Immunity on Even Number of Variables ..... | 271 |
| <i>Longjiang Qu and Chao Li</i>                                                                                                   |     |

## Privacy and Deniability

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Anonymity and $k$ -Choice Identities .....                                        | 283 |
| <i>Jacek Cichoń and Mirosław Kutylowski</i>                                       |     |
| Deniable Authentication on the Internet (Extended Abstract) .....                 | 298 |
| <i>Shaoquan Jiang</i>                                                             |     |
| Orthogonality between Key Privacy and Data Privacy, Revisited .....               | 313 |
| <i>Rui Zhang, Goichiro Hanaoka, and Hideki Imai</i>                               |     |
| Unlinkable Randomizable Signature and Its Application in Group<br>Signature ..... | 328 |
| <i>Sujing Zhou and Dongdai Lin</i>                                                |     |

## Hash Functions

|                                                     |     |
|-----------------------------------------------------|-----|
| An Improved Collision Attack on MD5 Algorithm ..... | 343 |
| <i>Shiwei Chen and Chenhui Jin</i>                  |     |
| Multivariate Polynomials for Hashing .....          | 358 |
| <i>Jintai Ding and Bo-Yin Yang</i>                  |     |

## Public Key Cryptosystems

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Efficient Public Key Encryption with Keyword Search Schemes from<br>Pairings ..... | 372 |
| <i>Chunxiang Gu, Yuefei Zhu, and Heng Pan</i>                                      |     |
| Multi-Identity Single-Key Decryption without Random Oracles .....                  | 384 |
| <i>Fuchun Guo, Yi Mu, Zhide Chen, and Li Xu</i>                                    |     |

## Public Key Analysis

|                                                           |     |
|-----------------------------------------------------------|-----|
| Kipnis-Shamir Attack on HFE Revisited .....               | 399 |
| <i>Xin Jiang, Jintai Ding, and Lei Hu</i>                 |     |
| Cryptanalysis of General Lu-Lee Type Systems .....        | 412 |
| <i>Haijian Zhou, Ping Luo, Daoshun Wang, and Yiqi Dai</i> |     |

A Timing-Resistant Elliptic Curve Backdoor in RSA ..... 427  
*Adam L. Young and Moti Yung*

**Application Security**

A Watermarking Scheme in the Encrypted Domain for Watermarking  
Protocol ..... 442  
*Bin Zhao, Lanjun Dang, Weidong Kou, Jun Zhang, Zan Li, and  
Kai Fan*

Security Enhancement of a Flexible Payment Scheme and Its  
Role-Based Access Control ..... 457  
*Chin-Chen Chang, Yi-Fang Cheng, and Iuon-Chang Lin*

**Systems Security and Trusted Computing**

Building Trusted Sub-domain for the Grid with Trusted Computing .... 463  
*Jing Zhan, Huanguo Zhang, and Fei Yan*

Enhanced Security by OS-Oriented Encapsulation in TPM-Enabled  
DRM ..... 472  
*Yongdong Wu, Feng Bao, Robert H. Deng, Marc Mouffron, and  
Frederic Rousseau*

Online Tracing Scanning Worm with Sliding Window ..... 482  
*Yang Xiang and Qiang Li*

**Network Security**

A New Proactive Defense Model Based on Intrusion Deception and  
Traceback ..... 497  
*Junfeng Tian and Ning Li*

On Modeling Post Decryption Error Processes in UMTS Air  
Interface ..... 507  
*Fouz Sattar and Muid Mufti*

A Simple, Smart and Extensible Framework for Network Security  
Measurement ..... 517  
*Feng Cheng, Christian Wolter, and Christoph Meinel*

**Author Index** ..... 533

# On the Evolution of User Authentication: Non-bilateral Factors

Moti Yung<sup>1,2</sup>

<sup>1</sup> Google Inc.

<sup>2</sup> Columbia University

**Abstract.** In this position note we review the notion of “User Authentication,” i.e., the idea of a person facing the computer and in need of authenticating herself to the system in order to get access to her account. We analyze the state of the art of user authentication and that of “Authentication Factors,” i.e., the techniques and instruments the user can present to the computer. We compare the state of the art of these factors with the acceptable textbook view.

## 1 Introduction

Authentication factors are the basic instruments available to a human user to authenticate herself in order, e.g., to convince a computing system of her true “identity” as is known or registered in the system. These factors, presented by a human claiming to be a specific user (and get access to that specific user’s account), are passed to elements of the system (e.g., a software program in a server) which, in turn, make a decision whether the human is the claimed specific user. Determination is based on registered information that the elements hold about the actual specific user. The accepted classification of authentication factors, as expressed in numerous textbooks, distinguishes three basic types of factors:

1. “Something You Know” (e.g., a password);
2. “Something You Have” (e.g., a device generating one-time passwords); and
3. “Something You Are” (e.g., biometrics information).

Given the current state of the art and the fact that nowadays, Internet Computing is based on human interaction with the computing infrastructure, this works re-examines the notion of authentication factors. Based on the evolution of computing systems and modern computing in general, the work reviews the parallel evolution of authentication factors and explains it and its impact on user security.

## 2 The Traditional Characteristics Vs. Non-bilateral Factors

The above three characteristics of the nature of authentication factors is very natural, since a user facing a system indeed can present to it evidence of the three

basic characteristics. However, these characteristics were made in the setting of a basic model of a user facing a machine or an operating system, which was a good view of a traditional time-sharing stand-alone system. What we note is that modern computing environment is much different, and we claim that in modern environments it is rarely the case that a user faces “alone” a single system. In fact, nowadays there are various system elements that are present in modern infrastructure. Elements can be part of the computing components, networking infrastructure components, or other aspects of the entire system. Today, when a user presents the factors, they may be directly given to the system or there may be a sequence of transfers. Even if virtually, the user believes he has interacted with “the system,” the infrastructure behind this interaction is complex.

A first demonstrative example consider the case where the user first presents a password to a smart card which activates the smartcard to produce an authenticator string; the card then authenticates on behalf of the user to a local system by presenting the string, that, in turn, validates the authenticator, and presents a credential that authenticates itself with an assertion about the authenticity of this user in this connection. The assertion may be a digitally signed statement accompanied by a certificate. The credential and assertion, in turn, are presented to a remote server or a member of a federation of server that mediates the authentication; this results in the connection to the user being validated as coming from the actual user and may allow this connecting user access the resources associated with this actual user. In fact, in this example we see how the user’s initial authentication is “carried through” the system via a chain of trust among system elements. The involvement of human players and system elements in the process led to calling this protocol that involves users, factors and machines, “a ceremony” [2].

The fact that modern environments include more than merely the user and a single system element gives the opportunity to extend the possible characteristics of user authentication factors. The participants do not even have to be a chain of system elements along a linear flow of a message. This basic issue can be summarized as following:

- The traditional characteristics assume a *Bilateral Relation* between the user and the system; modern environments include additional elements and components.

The above observation implies that we can now consider factors that involve additional parties, channels, computing elements and pieces of information available to the system. Thus, side parties and components can take part in the authentication ceremony, and we can use factors such as:

1. The mobile phone line of the user or of an e-mail account belonging to the user which generate an independent channel to the user; this is an independent validation channel (“Something Registered About the User”);
2. The IP address or the laptop computer mac address of the user’s computer, (“Something Embedded in the User’s Computing Environment”);

3. A remote server associated with the user that the user already logged into and expressed the intention to further authenticate with another system element (“Some Support Tools the Computing Environment Has”);.

The above are examples of factors based on the user’s computing environment: knowledge about it, its physical characteristics and available elements and channels in it. They can be used and are, indeed, used in identifying the likelihood of the claimed user being the specific authentic one. In some abstract general sense the user environment may be thought to be part of the user and these factors can all be thought of as “something the user has.” But, in reality these are not something the user possesses, but rather something in the environment associated with the user. They may be associated with the user at some time (when the user is at home) but not at other times (when the user is at a cyber cafe, say), and may change as the user re-configures parts of her environment (e.g., buys a new computer).

The independence of the factors that belong to the infrastructure is important in order for the system to use them as factors supporting the user’s identity. For example, the mobile phone platform and the computer platform may be the same, and a phone call over the wire and over wireless LAN may get mixed as the infrastructure gets more complicated. The relation and independence of infrastructure components has to be analyzed and the system has to be aware of the source of the various factors.

We note that the more the factor known by the infrastructure is actually a factor that is essential part of the infrastructure the stronger it is. If a factor gives some physical meaning to the computing, e.g., an IP address is hard to spoof as a factor if used for routing the communication of the interaction itself. The more the factor is part of the correctly completion of the overall interaction in this physical sense, the better it seems to be.

**Beyond Technical Components:** Factors do not have to be part of the computing and communication elements. It was pointed out [1] that human components have to be considered and can, in fact, help in the authentication process. Indeed, social relationships to which the user belongs and organizational structure in which the user takes place can serve as additional factors. Relying on already authenticated users in some formal and careful way amounts to “*Some-one You Know*” factor.

**Keep New Technologies in Mind:** It is important to remember that as technologies change one may attempt to employ them in the area of authentication factors. One such technology is “Internet Search Technology”. It can be used to find facts that the claimed user needs to know and use for extension of “something you know” (or perhaps “something you (virtually) are”) to “*something the infrastructure as a whole knows about you.*” The idea here is that the specialized search engine knows where to look for details about a user fast, while generic search is still slow when personal information of specific nature is involved. This example is an interesting twist on privacy on the web, where relative loss of privacy is exploited to secure the authentication process! With lack of privacy the

available details on the web may replace some of the registration process where users give personal details to be used as “something you know” factor.

### 3 How Are Factors Employed Nowadays?

**Enterprise User vs. Consumer User:** There are a number of different settings where authentication factors are used, which determines the possibility of usage and effectiveness of the factors. The enterprise setting where a user is an employee is much different from the e-commerce user which typifies the consumer case. It may be easier to provide devices to employees than to end consumers (who may be casual), which has been the case in reality. The participation of non-bilateral factors and mechanisms may depend on the setting as well, for example, vouching by a third party requires a well established social structure, typical inside enterprises.

**Absolute Reliance vs. statistical Reliance:** The level of reliance on factors is another issue. Authentication factors traditionally have been used to ensure the system with close to absolute certainty of the identity of the user. In modern systems the factors may be treated as providing some probability of assurance and by gathering enough factors (possibly incrementally), the probability of an identity can be calculated. In fact, at the end of a possibly lengthy session with many checks, the system can conclude that the user “has passed” the authentication protocol, based on statistics (i.e., some confidence level). The involvement of factors can be done adaptively based on assessment of the success so far in the process. It seems that absolute reliance (a factor that gives a yes/no answer) was the traditional method, where as the Internet evolves and the level of threat increases it makes sense to rely on factors statistically, and to collect multi-factor input. In this mode, not any single source of authentication needs to be perfect. (We note that engineering wise, it is often easier to build a system that is made out of imperfect components, and use multiplicity of such components to create a more reliable system. The “statistical confidence based factors” are mechanisms that possess this nature of relatively and possibly imperfect components).

**Changing the Task of Authentication:** As can be seen over the years, indeed, the use and purpose of authentication factors can be changed as systems evolve. One important issue in the context of Internet access and services is the fact that the server (e.g., of a bank or a merchant) has to prove its authenticity to the user as well (i.e., authentication in the reverse direction). Since the factors presented to the user have to be interpreted by a user looking at her browser, the security of user interfaces, human factors in user interfaces and defining end-to-end two way authentication to a browser user are important. The notions of how to prevent the user from getting into a wrong web page is especially important. User friendliness of interfaces and usability issues in general play now an important part in achieving the tasks of authentication. (Note that the extended nature and requirement of user authentication in various

web-based scenarios is beyond the scope of the current note; here it serves only to demonstrate the current issues with authentication factors).

## 4 Ask: Who Activates the Factors?

As noted above, lack of robust two-way authentication factors has opened the door for attacks that attempt social engineering *en masse*, namely trying to direct users to a fake web site where the user inserts her authentication credentials. This type of attacks called phishing attacks are common place nowadays. Besides social engineering via faked sites and tempting email, the attack of directing users to wrong sites that are faked can be done by contaminating the resolve infrastructure or by malware on the user computer.

In phishing attacks users give their factors such as answers to questions and passwords to the site, which may use them elsewhere. Thus an important issue is how limited in time the credentials are and whether they are limited and bound to the current site and cannot be used by attackers who may attempt to contact the real site and, say, extract money from the user account employing the stolen credentials. Credentials that are bound and are non-reusable are preferable, as they limit the opportunity of the attackers.

The user may give away credentials like passwords, account number, account name, answers to questions in the knowledge base, etc. These credentials can be used by the attackers. However, new factors like mac address of a computer, a cookie inserted in the user's browser, or a call to a mobile phone line owned by the user, do not change ownership by the user even if she becomes a victim of a social engineering attack and the attacker cannot "demand" to get them. Thus, the last type of credentials have been known as passive factors, whereas the first type of factors are activated by the user.

In the view of the multi-lateral nature of modern factors, to our belief, we can analyze the difference between the various credential types. We believe that the basic difference is the underlying fact of *who activates the factor*. If the user herself activates them and they are reusable within some time and space limitations, they can be re-used by attackers (in off-line or on-line attacks, depending on the "validity window" for the credential). If, on the other hand, the credentials are factors that are activated by third parties: the communication infrastructure, independent elements of the computing base and other parties, then the user is in no position to give it away. In fact, the advantage of some of the modern factors is due to the non-bilateral nature of these factor and the fact that the user does not possess them, even though the factors are employed to authenticate the user. Thus, one has to pay attention to analyze separately and carefully "User-Activated" vs. "Third-Party Activated" factors.

In order to attack the third party activation of factors (as opposed to the user self-activation), different methods are needed then merely attacking the user. One needs to pay attention to potential attacks on these new factors and to classify the parties that are involved: i.e., a cookie may be stolen more easily than a mobile phone owned by a user that is used to call the user back during

authentication. Factors related to the functioning of the interaction (IP address, say) are harder to change as was already mentioned. In any event, the involvement of multi-party in the new authentication game changes its nature as it is not bi-lateral anymore. Involving these new multi-lateral factors enhances the notion of user authentication and allows prevention of attacks that isolate the user. Granted, to be used successfully the new game may require further analysis of all parties involved, since an extended game with extra parties also means extra security analysis is required.

**Future Factors:** The computing infrastructure is evolving rapidly and information technology and physical aspects of the world are merging and computers are embedded in many new places. Given this trend, the above issues should be kept in mind. We expect to view ubiquitous computing as a new wave of opportunities for future user authentication by enabling new factors and new parties to take place in the process (e.g., physical location based factors, gadgets oriented factors, involvement of consumer electronic devices, ability to probe user familiarities with certain knowledge bases based on issues such as current location, background and recent interactions, and so on). We expect that the mixing of physical security, procedural security and information security is likely to increase the variability of authentication factors.

## 5 Conclusions

One important lesson of the above analysis and the position this note takes, is the fact that the notion of computer user authentication is deeply connected to the infrastructure of computing. As the latter evolves so does the former. Furthermore, technological changes should be considered and off the book traditional assumptions regarding security measures be updated appropriately (in the security area “following the book” and “ignoring the book” are equally important!).

**Acknowledgments.** Discussions over the years with many individuals have contributed to the position expressed here (which does not discuss any specific technology and does not express any preference among various methods). Given the dynamically changing nature of user authentication, these discussions have been and still are very helpful. Among others, many thanks are due to Ross Anderson, Louie Gasparini, Seth Gettic, Brian Gladstein, Lior Golan, Ari Juels, Burt Kaliski, Aaron Kechley Amit Klein, John Lin, Nasir Memon, Magnus Nyström, Ron Rivest, and Mike Szydło.

## References

1. Brainard, J., Juels, A., Rivest, R.L., Szydło, M., Yung, M.: Fourth factor authentication: somebody you know. In: ACM Conference on Computer and Communication Security (CCS), pp. 168–178 (2006)
2. Ellison, C.: UPnP security ceremonies design document (October 2003)

# Author Index

- Al Hinaï, Sultan 201  
Alexiadis, A. 108  
  
Bao, Feng 472  
Batten, Lynn Margaret 201  
Bogdanov, Andrey 66  
  
Chalkias, K. 108  
Chang, Chin-Chen 457  
Chen, Shiwei 343  
Chen, Zhide 384  
Chen, Zhixiong 231  
Cheng, Feng 517  
Cheng, Rui 182  
Cheng, Yi-Fang 457  
Cichoń, Jacek 283  
Colbert, Bernard 201  
Collard, B. 51  
  
Dai, Yiqi 412  
Dang, Lanjun 442  
Deng, Robert H. 472  
Deng, Yi 123  
Ding, Jintai 358, 399  
Ding, Ning 153  
Dong, Junwu 81  
Dubois, Vivien 1  
  
Fan, Kai 442  
Fouque, Pierre-Alain 1  
  
Gu, Chunxiang 40, 372  
Gu, Dawu 153  
Guo, Fuchun 384  
  
Halkidis, S.T. 108  
Hanaoka, Goichiro 313  
Hristu-Varsakelis, D. 108  
Hu, Lei 93, 399  
Huang, Xinyi 25  
  
Imai, Hideki 313  
  
Jiang, Shaoquan 298  
Jiang, Xin 399  
Jin, Chenhui 343  
  
Kalouptsidis, Nicholas 246  
Kolokotronis, Nicholas 246  
Kou, Weidong 442  
Kutylowski, Mirosław 283  
  
Li, Chao 271  
Li, Ning 497  
Li, Qiang 482  
Li, Xiaobo 192  
Li, Yong 93  
Li, Zan 442  
Limniotis, Konstantinos 246  
Lin, Dongdai 123, 328  
Lin, Iuon-Chang 457  
Luo, Ping 412  
  
Ma, Chuangui 182  
Meinel, Christoph 517  
Mouffron, Marc 138, 472  
Mu, Yi 25, 384  
Mufti, Muid 507  
  
Okamoto, Eiji 11  
Okamoto, Takeshi 11  
  
Pan, Heng 372  
Pei, Dingyi 81  
Pieprzyk, Josef 167  
  
Qi, Wen-Feng 216, 256  
Qu, Longjiang 271  
Quisquater, J.-J. 51  
  
Rousseau, Frederic 138, 472  
  
Sattar, Fouz 507  
Shamir, Adi 1  
Standaert, F.-X. 51  
Stephanides, G. 108  
Stern, Jacques 1  
Susilo, Willy 25  
  
Tartary, Christophe 167  
Tian, Junfeng 497  
Tso, Raylin 11

534 Author Index

- |                   |          |                |         |
|-------------------|----------|----------------|---------|
| Wang, Daoshun     | 192, 412 | Yi, Feng       | 192     |
| Wang, Huaxiong    | 167      | Young, Adam L. | 427     |
| Wang, Jin-Song    | 216, 256 | Yung, Moti     | 5, 427  |
| Wang, Weijia      | 93       |                |         |
| Wang, Xueli       | 81       | Zhan, Jing     | 463     |
| Wolter, Christian | 517      | Zhang, Huanguo | 463     |
| Wu, Wei           | 25       | Zhang, Jun     | 442     |
| Wu, Yongdong      | 472      | Zhang, Ning    | 231     |
|                   |          | Zhang, Rui     | 313     |
| Xiang, Yang       | 482      | Zhao, Bin      | 442     |
| Xiao, Guozhen     | 231      | Zhou, Haijian  | 412     |
| Xu, Li            | 384      | Zhou, Sujing   | 328     |
| Yan, Fei          | 463      | Zhu, Huafei    | 138     |
| Yang, Bo-Yin      | 358      | Zhu, Yuefei    | 40, 372 |