

[Home](#) > [Conference proceedings](#)

## Information Security and Cryptology

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

Conference proceedings | © 2008

[Save conference proceedings](#)

[Accessibility Information](#)

### Overview

Editors: [Dingyi Pei](#), [Moti Yung](#), [Dongdai Lin](#), [Chuankun Wu](#)

**Part of the book series:** [Lecture Notes in Computer Science \(LNCS, volume 4990\)](#)

↳ **Part of the book sub series:** [Security and Cryptology](#) (LNCS)

**Included in the following conference series:**

[Inscrypt: International Conference on Information Security and Cryptology](#)

Conference proceedings info: [Inscrypt 2007](#).

27k Accesses 4 Citations 12 [Altmetric](#)

This is a preview of subscription content, [log in via an institution](#) to check access.

### About this book

This book constitutes the thoroughly refereed post-conference proceedings of the Third SKLOIS (State Key Laboratory of Information Security) Conference on Information Security and Cryptology, Inscrypt 2007 (formerly CISC), held in Xining, China, in August/September 2007.

The 33 revised full papers and 10 revised short papers presented together with 2 invited papers were carefully reviewed and selected from 167 submissions. The papers are organized in topical sections on digital signature schemes, block cipher, key management, zero knowledge and secure computation protocols, secret sharing, stream cipher and

#### Access this book

[Log in via an institution](#) →

**Softcover Book**

USD 54.99

Price excludes VAT (USA)

- Compact, lightweight edition
- Free shipping worldwide – [view details](#)

[Buy Softcover Book](#) →

Tax calculation will be finalised at checkout

#### Other ways to access

[Licence this eBook for your library](#) →

[Institutional subscriptions](#) →

#### Sections

[Overview](#)

[About this book](#)

[Table of contents \(41 papers\)](#)

[Other volumes](#)

[Accessibility Information](#)

[Bibliographic Information](#)

[Publish with us](#)

pseudorandomness, boolean functions, privacy and deniability, hash functions, public key cryptosystems, public key analysis, application security, system security and trusted computing, and network security.



**Key-Establishment Protocols for Constrained Cyber-Physical Systems**

Chapter | © 2021



**A novel trusted third party based signcryption scheme**

Article | 29 May 2020



**Efficient Fully Secure Leakage-Deterring Encryption**

Chapter | © 2019

### Explore related subjects

Discover the latest articles, books and news in related subjects.

Algorithms

Computer Communication Networks

Computers and Society

Cryptology

Data and Information Security

IT Operations

Security Protocols for Networked Systems

Search within this book

Search

## Table of contents (41 papers)

Front Matter

[Download chapter PDF](#) 

### Invited Talks

#### Cryptanalysis of the SFLASH Signature Scheme

Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, Jacques Stern  
Pages 1–4

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

Moti Yung  
Pages 5–10

### Digital Signature Schemes

#### ECDSA-Verifiable Signcryption Scheme with Signature Verification on the Signcrypted Message

Raylin Tso, Takeshi Okamoto, Eiji Okamoto  
Pages 11–24

### **Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility**

Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang  
Pages 25–39

---

### **An Efficient ID-Based Proxy Signature Scheme from Pairings**

Chunxiang Gu, Yuefei Zhu  
Pages 40–50

---

## **Block Cipher**

---

### **Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent**

B. Collard, F. -X. Standaert, J. -J. Quisquater  
Pages 51–65

---

### **Linear Slide Attacks on the KeeLoq Block Cipher**

Andrey Bogdanov  
Pages 66–80

---

## **Key Management**

---

### **A Key Predistribution Scheme Based on 3-Designs**

Junwu Dong, Dingyi Pei, Xueli Wang  
Pages 81–92

---

### **Provably Secure N-Party Authenticated Key Exchange in the Multicast DPWA Setting**

Weijia Wang, Lei Hu, Yong Li  
Pages 93–107

---

### **A Provably Secure One-Pass Two-Party Key Establishment Protocol**

K. Chalkias, S. T. Halkidis, D. Hristu-Varsakelis, G. Stephanides, A. Alexiadis  
Pages 108–122

---

## **Zero Knowledge and Secure Computation Protocols**

---

### **Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model under Standard Assumption**

Yi Deng, Dongdai Lin  
Pages 123–137

---

### **Secure Two-Party Computation of Squared Euclidean Distances in the Presence of Malicious Adversaries**

Marc Mouffron, Frederic Rousseau, Huafei Zhu  
Pages 138–152

---

### **A Discrete-Logarithm Based Non-interactive Non-malleable Commitment Scheme with an Online Knowledge Extractor**

Ning Ding, Dawu Gu  
Pages 153–166

---

## **Secret Sharing**

---

### **Verifiable Multi-secret Sharing Schemes for Multiple Threshold Access Structures**

Christophe Tartary, Josef Pieprzyk, Huaxiong Wang  
Pages 167–181

**Key Management Based on Hierarchical Secret Sharing in Ad-Hoc Networks**

Chuangui Ma, Rui Cheng  
Pages 182–191

**Probabilistic  $(n, n)$  Visual Secret Sharing Scheme for Grayscale Images**

Daoshun Wang, Xiaobo Li, Feng Yi  
Pages 192–200

**Stream Cipher and Pseudorandomness**

**Mutually Clock-Controlled Feedback Shift Registers Provide Resistance to Algebraic Attacks**

Sultan Al Hinai, Lynn Margaret Batten, Bernard Colbert  
Pages 201–215

**Four Families of Binary Sequences with Low Correlation and Large Linear Complexity**

Jin-Song Wang, Wen-Feng Qi  
Pages 216–230

**Pseudo-Randomness of Discrete-Log Sequences from Elliptic Curves**

Zhixiong Chen, Ning Zhang, Guozhen Xiao  
Pages 231–245

**Other volumes**

- 1. Information Security and Cryptology

**Accessibility Information**

Accessibility information for this book is coming soon. We're working to make it available as quickly as possible. Thank you for your patience.

**Bibliographic Information**

| Book Title                          | Book Subtitle                                                                                                 | Editors                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Information Security and Cryptology | Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 – September 5, 2007, Revised Selected Papers | Dingyi Pei, Moti Yung, Dongdai Lin, Chuankun Wu |

|                                                                                                                                |                                                                                                                 |                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Series Title</b><br><a href="#">Lecture Notes in Computer Science</a>                                                       | <b>DOI</b><br><a href="https://doi.org/10.1007/978-3-540-79499-8">https://doi.org/10.1007/978-3-540-79499-8</a> | <b>Publisher</b><br>Springer Berlin, Heidelberg                                                                                                                                                                            |
| <b>eBook Packages</b><br><a href="#">Computer Science, Computer Science (RO), Springer Nature Proceedings Computer Science</a> | <b>Copyright Information</b><br>Springer-Verlag Berlin Heidelberg 2008                                          | <b>Softcover ISBN</b><br>978-3-540-79498-1<br>Published: 18 July 2008                                                                                                                                                      |
| <b>eBook ISBN</b><br>978-3-540-79499-8<br>Published: 17 August 2008                                                            | <b>Series ISSN</b><br>0302-9743                                                                                 | <b>Series E-ISSN</b><br>1611-3349                                                                                                                                                                                          |
| <b>Edition Number</b><br>1                                                                                                     | <b>Number of Pages</b><br>XII, 534                                                                              | <b>Topics</b><br><a href="#">Systems and Data Security, Cryptology, Management of Computing and Information Systems, Computers and Society, Computer Communication Networks, Algorithm Analysis and Problem Complexity</a> |

## Keywords

[Boolean function](#)
[Public Key](#)
[Trusted Computing](#)
[data security](#)
[information](#)
[privacy](#)
[security](#)
[trust](#)
[algorithm analysis and problem complexity](#)

## Publish with us

[Policies and ethics](#) 

[Back to top](#) 

### Discover content

[Journals A-Z](#)  
[Books A-Z](#)  
[Subjects A-Z](#)

### Publish with us

[Journal finder](#)  
[Publish your research](#)  
[Language editing](#)  
[Open access publishing](#)

### Products and services

[Our products](#)  
[Librarians](#)  
[Societies](#)  
[Partners and advertisers](#)

### Our brands

[Springer](#)  
[Nature Portfolio](#)  
[BMC](#)  
[Palgrave Macmillan](#)  
[Apress](#)  
[Discover](#)

[Your privacy choices/Manage cookies](#)
[Your US state privacy rights](#)
[Accessibility statement](#)
[Terms and conditions](#)
[Privacy policy](#)
[Help and support](#)  
[Legal notice](#)
[Cancel contracts here](#)

74.98.214.120

Not affiliated

**SPRINGER NATURE**

© 2026 Springer Nature

# 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 “*Someone 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)