

# **Norwegian Symposium on Information Security 2009**

**(NISK 2009)**

**Trondheim, Norway  
24-25 November 2009**

ISBN: 978-1-61738-874-3

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571



**Some format issues inherent in the e-media version may also appear in this print version.**

Copyright© (2009) by Tapir Academic Press  
All rights reserved.

Printed by Curran Associates, Inc. (2010)

For permission requests, please contact Tapir Academic Press  
at the address below.

Tapir Academic Press  
Nardoveien 12  
NO-7005 Trondheim  
Norway

Phone: + 47 73 59 32 10  
Fax: + 47 73 59 32 04

[forlag@tapir.no](mailto:forlag@tapir.no)

**Additional copies of this publication are available from:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: 845-758-0400  
Fax: 845-758-2634  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# NISK 2009

## Table of Contents

### BIOMETRICS

Continuous Authentication using Biometric Keystroke Dynamics . . . . .	1
<i>Patrick Bours, Hafez Barghouthi</i>	
Gait Mimicking - Attack Resistance Testing of Gait Authentication Systems . . . . .	13
<i>Bendik Mjaaland, Patrick Bours, Danilo Gligoroski</i>	
Biocryptics: Towards Robust Biometric Public/Private Key Generation . . . . .	27
<i>Bendik Mjaaland, Danilo Gligoroski, Svein Knapskog</i>	

### ATTACKS & ANALYSES

Modified Template Attack: Detecting Address Bus Signals of Equal Hamming Weight . . . . .	43
<i>Geir Olav Dyrkolbotn, Einar Snekkenes</i>	
Eavesdropping Near Field Communication . . . . .	57
<i>Henning Siitonen Kortvedt, Stig Frode Mjølunes</i>	
All in a Day's Work: Password Cracking for the Rest of Us . .	69
<i>Jørgen Blakstad, Rune Walsø Nergård, Martin Gilje Jaatun, Danilo Gligoroski</i>	
Security Analysis of the SIP Handover Extension . . . . .	84
<i>Elin Sundby Boysen, Lars Strand</i>	

### CRYPTOGRAPHY

Reductionist Security Arguments for Public-Key Cryptographic Schemes Based on Group Action . . . . .	97
<i>Anton Stolbunov</i>	

A Multi-Receiver Public Key Crypto System . . . . .	110
<i>Sigurd Eskeland</i>	
Realizing Distributed RSA Key Generation Using VIFF . . . . .	122
<i>Atle Mauland, Tord Reistad, Stig Frode Mjølunes</i>	
<b>VOTING</b>	
Internet Voting using Multiparty Computations . . . . .	136
<i>Md. Abdul Based, Tord Ingolf Reistad, Stig Frode Mjølunes</i>	
A Non-interactive Zero Knowledge Proof Protocol in an Internet Voting Scheme . . . . .	148
<i>Md. Abdul Based, Stig Frode Mjølunes</i>	
<b>INCIDENT MANAGEMENT</b>	
Incident Response and User Awareness . . . . .	161
<i>Finn Olav Sveen, Jose Maria Sarriegi, Jose J. Gonzalez</i>	
Cascading Effect Affecting Situational Awareness in Power Cut Failures . . . . .	173
<i>Finn Olav Sveen, Jose J. Gonzalez</i>	
SOA Security - An Experience Report . . . . .	185
<i>Jostein Jensen, Åsmund Ahlmann Nyre</i>	
<b>Author Index . . . . .</b>	<b>197</b>
<b>Keyword Index . . . . .</b>	<b>198</b>