CONFERENCE TECHNICAL PROGRAM
First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)
Co-Sponsored by IEEE Communications Society and CreateNet; With Support from ICST
Corporate/Government Sponsors: NSF, Telcordia, Toshiba
Athens, Greece / Hotel Amarilia / 5 - 9 September, 2005
www.securecomm.org

TUESDAY, SEP 6, 2005
8.30AM - 9.00 AM: Welcome, Introduction
9.00AM - 10.30AM: Plenary Session:
Bill Cheswick, Lumeta, Title: Pondering and Patrolling Network Perimeters
Andrea Servida, EU, Title: Security, privacy and dependability in Information Society
10.30AM - 11.00AM: Break
11.00AM - 12.40PM: Session 1: Insecurity
Implications of Unlicensed Mobile Access (UMA) for GSM security
Sandro Grech, Pasi Eronen
Computationally, Memory and Bandwidth Efficient Distillation Codes to Mitigate DoS in Multicast
Roberto Di Pietro, Stefano Chessa, Piero Maestrini
Spread Identity mechanisms for Security
Dhananjay Phatak
On the Security of Distributed Position Services
Xiaoxin Wu, Cristina Nita-Rotaru
12.40PM - 2:00PM: Lunch
2:00PM - 2.45PM: Invited talk: David Wagner, Title: Privacy in pervasive computing
2.45 – 3.00PM: Break
3.00 PM – 4.40 PM: Session 2: RFID
Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems
Ziv Kfir, Avishal Wool
A Lightweight RFID Protocol to protect against Traceability and Cloning attacks
Tassos Dimitriou
An RFID distance bounding protocol
Gerhard Hancke, Markus Kuhn
Security and Privacy Issues in e-Passports
Ari Juels, David Molnar, David Wagner
4.40PM - 5.00PM: Break
5:00 PM - 6.30PM: Panel 1: RFID Security and Privacy, Lead Panelist: Gene Tsudik
WEDNESDAY, SEP 7, 2005
7.00PM – 9.00PM: Conference Dinner
8.30AM - 9.15 AM: Keynote: Jean Pierre-Hubaux, EPFL, Title: The Security of Vehicular Networks
9.30AM - 10.45AM: Session 3: Sensor Networks
DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks
Issa Khalil, Saurabh Bagchi, Cristina Nita-Rotaru
Securing Topology Maintenance Protocols for sensor networks: attacks and counter-measures
Andrea Gabrielli, Luigi Mancini, Sanjeev Setia, Sushil Jajodia
10.45AM - 11:00AM: Break
11.00AM - 12.40PM: Session 4: Authentication
Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks
Jing Deng, Richard Han, Shivakant Mishra
Improving Cross-domain Authentication over Wireless Local Area Networks
Hahnsang Kim, Kang Shin, Walid Dabbous
Reducing Reauthentication Delay in Wireless Networks
Tuomas Aura, Michael Roe
Providing Distributed Certificate Authority Service in Mobile Ad Hoc Networks
Yang Dong, Wing Go, Aifen Sui, Victor Li, Lucas C.K. Hui, Siu Ming Yiu
On Improving the Performance of Role-Based Cascaded Delegation in Ubiquitous Computing
Danfeng Yao, Roberto Tamassia, Seth Proctor
12.40PM - 2:00PM: Lunch
2:00PM - 2:45PM: Invited Talk: William Arbaugh, Title: Ad-hoc network security
2.45 – 3.00PM: Break
3:00PM - 4:40PM: Session 5: Privacy
A Privacy Preserving Reputation System for Mobile Information Dissemination Networks
Marco Voss, Andreas Heinemann, Max Mühläuser
A Privacy Service for Context-Aware Mobile Computing
Vagner Sacramento, Markus Endler, Fernando Nascimento
Protecting Location Privacy Through Path Confusion
Baik Hoh, Marco Gruteser
A Solution for Wireless Privacy and Payments based on E-cash
Yiannis Tsiounis, Tom Karygiannis, Anggelos Kiayias

4.40PM - 5.00PM: Break

5:00PM - 6:40PM: Short paper Session 1
A Signal Fingerprinting Paradigm for Physical Layer Security in Conventional and Sensor Networks, Thomas Daniels, Mani Mina, Steve Russell
Location Privacy with IP Mobility
R. Koodli, V. Devarapalli, H. Filinck, C. Perkins
Fellowship in Mobile Ad hoc Networks
Venkatesan Balakrishnan, Vijay Varadharajan
A Secure Interworking Scheme for UMTS-WLAN
Y-C Ouyang, Chung-Hua Chu, Cheng-Bu Jang
bufSTAT: A Tool for Early Detection and Classification of Buffer Overflow Attacks
Svetlana Radosavac, Karl Seamon, John S. Baras
LRBAC: A Location-Aware Role-Based Access Control Model
Indrakshi Ray, Lijun Yu
Tri-party TLS Adaptation for Trust Delegation in Home Networks
K. Masmoudi, M. Hussain, H. Afifi, D. Seret
PATRIOT: a Policy-Based, Multi-level Security Protocol for Safekeeping Audit Logs on Wireless Devices
Wassim Itani, Ayman Kayssi, Ali Chehab
Harnessing Emergent Ubiquitous Computing Properties to Prevent Malicious Code Propagation
D. Llewellyn-Jones, M. Merabti, Qi Shi, B. Askwith

THURSDAY, SEP 8, 2005

8.30AM - 10.35 AM: Session 6: Key management
A Level Key Infrastructure for Secure and Efficient Group Communication in Wireless Sensor Networks
Jyh-How Huang, Jason Buckingham, Richard Han
A Modified Secure Remote Password (SRP) Protocol for Key Initialization and Exchange in Bluetooth Systems
Amir Sayegh, Mahmoud El-hadidi
Hi-KD: An Efficient Key Management Algorithm for Hierarchical Group
H. Ragab Hassan, A. Bouabdallah, H. Bettahar, Y. Challal
A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks
David Sanchez, Heribert Baldus
A Practical Study of Transitory Master Key Establishment For Wireless Sensor Networks
J. Deng, C. Hartung, R. Han, Shivakant Mishra

10.35AM - 11.00AM: Break

11:00 - 12:40: Session 7: Routing
Applying emergence to the design of routing protocols for the security of wireless ad hoc networks
Ioannis Pavlosoglou, Mark Leeson, Roger Green
SPINAT: Integrating IPSec into Overlay Routing
Jukka Ylitalo, Patrik Salmela, Hannes Tschofenig
On the Survivability of Routing Protocols in Ad Hoc Wireless Networks
Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens
An Extensible Environment for Evaluating Secure MANET
Yongguang Zhang, Yi-an Huang, Wenke Lee

12.40PM - 2:00PM: Lunch

2:00PM - 3:40 PM: Session 8: Cryptographic algorithms and protocols
Soft-Timeout Distributed Key Generation for Digital Signature based on Elliptic Curve D-log for Low-power Devices
C. Tang, A, Chronopoulos, C. S. Raghavendra

A Uniform Framework for Cryptanalysis of the Bluetooth E_0 Cipher
Ophir Levy, Avishai Wool
MOTET: Mobile Transactions using Electronic Tickets
Daniele Quercia, Stephen Hailes
Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information
Urs Hengartner, Peter Steenkiste

3.40PM - 4.00PM: Break

4:00PM - 5:40 PM: Short paper Session 2
GKE: Efficient Group-based Key Establishment for Large Sensor Networks
Li Zhou, Jinfeng Ni, Chinya Ravishankar
Practically Unbounded One-Way Chains for Authentication with Adaptive Security
Vishwas Patil, Luigi Mancini, Antonio Durante, Roberto Di Pietro
Limitations of Key Escrow in Identity-Based Schemes in Ad Hoc Networks
Katrin Hoepner, Guang Gong
Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption
Daniel Socek, Shujun Li, Spyros Magliveras, Borko Furht
Schemes for Enhancing the Denial-of-Service Tolerance of SRTP
Sachin Garg, Navjot Singh, Timothy Tsai
Thor: The Hybrid Online Repository
Timothy van der Horst, Kent Seamons
Random IDs for preserving location privacy
Stefan Schlott, Frank Kargl, Michael Weber
A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks
Yu Liu, Yang Li, Hong Man
A Control Formulation of the Network Security Problem via a Risk Management Approach
Nicholas Bambos