TSP 2008 Advance Program

The 2008 IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-08)
http://trust.csu.edu.cn/conference/tsp2008/

In conjunction with
The 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC-08)
http://epcc.sjtu.edu.cn/euc2008/

17-20 December 2008
Shanghai, China

Organized by
Trusted Computing Institute at Central South University, China

Sponsored by
Shanghai Jiao Tong University
Shanghai Computer Society
IEEE Computer Society
IFIP

Supported by
National Natural Science Foundation of China
Shanghai Pudong New Area Association for Computer
Foundation of Science & Tech. Development of Shanghai Pudong New Area

TSP 2008 Program at a Glance

Thursday, 18 December 2008 - EUC 2008 main conference and TSP-08

<table>
<thead>
<tr>
<th>Room Time</th>
<th>Grand Ballroom</th>
<th>Function Room 4&amp;5</th>
<th>Function Room 7</th>
<th>Function Room 1&amp;2</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30-9:00</td>
<td>EUC-08 Opening Ceremony</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:00-10:00</td>
<td>Keynote Speech I (Yaoxue Zhang)</td>
<td></td>
<td></td>
<td>TSP-08 Opening Ceremony</td>
</tr>
<tr>
<td>10:00-10:30</td>
<td>Coffee Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30-11:30</td>
<td>EUC-08 Session 1A</td>
<td>EUC-08 Session 1B</td>
<td></td>
<td>TSP-08 Keynote Speech</td>
</tr>
<tr>
<td>11:30-12:10</td>
<td></td>
<td></td>
<td></td>
<td>TSP-08 Session 1</td>
</tr>
</tbody>
</table>
### Friday, 19 December 2008 - EUC 2008 main conference and TSP-08

<table>
<thead>
<tr>
<th>Time</th>
<th>Grand Ballroom</th>
<th>Function Room 4&amp;5</th>
<th>Function Room 7</th>
<th>Function Room 1&amp;2</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-10:00</td>
<td>Keynote Speech III</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Xiaodong Zhang)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00-10:30</td>
<td>Coffee Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30-12:10</td>
<td>EUC-08 Session 3A</td>
<td>EUC-08 Session 3B</td>
<td></td>
<td>TSP-08 Session 4</td>
</tr>
<tr>
<td>12:10-13:30</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30-15:10</td>
<td>EUC-08 Session 4A</td>
<td>EUC-08 Session 4B</td>
<td></td>
<td>TSP-08 Session 5</td>
</tr>
<tr>
<td>15:10-15:30</td>
<td>Coffee Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30-17:10</td>
<td>EUC-08 Session 5A</td>
<td>EUC-08 Session 5B</td>
<td></td>
<td>TSP-08 Session 6</td>
</tr>
<tr>
<td>17:10-18:30</td>
<td>Rest in the hotel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18:30-21:30</td>
<td>Banquet in the hotel</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Saturday, 20 December 2008 - EUC 2008 main conference and TSP-08

<table>
<thead>
<tr>
<th>Time</th>
<th>Function room 4&amp;5</th>
<th>Function Room 7</th>
<th>Function room 1&amp;2</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30-10:10</td>
<td>EUC-08 Session 6A</td>
<td>EUC-08 Session 6B</td>
<td>TSP-08 Session 7</td>
</tr>
<tr>
<td>10:10-10:30</td>
<td>Coffee Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30-12:10</td>
<td>EUC-08 Session 7A</td>
<td>EUC-08 Session 7B</td>
<td>TSP-08 Session 8</td>
</tr>
<tr>
<td>12:10-13:30</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30-15:10</td>
<td>EUC-08 Session 8A</td>
<td>EUC-08 Session 8B</td>
<td>TSP-08 Session 9</td>
</tr>
</tbody>
</table>
TSP 2008 Advance Program

The 2008 IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-08)

Thursday, 18 December, 2008

Opening Ceremony
Chair: Guojun Wang, Central South University, China
10:00 – 10:30am, Function Room 1&2

Keynote Speech:  Building Trustworthy Semantic Webs
Prof. Bhavani Thuraisingham, The University of Texas at Dallas (bhavani.thuraisingham AT utdallas.edu)
Chair: Wenbin Luo, St. Mary's University, San Antonio, Texas, USA (wluo AT stmarytx.edu)
10:30 – 11:30am, Function Room 1&2

Session 1: Secure Schemes and Metrics
Chair: Sancheng Peng, City University of Hong Kong, Hong Kong (psc346 AT gmail.com)
11:30 – 12:30pm, Function Room 1&2

- Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad Hoc Networks
  Sancheng Peng, Weijia Jia, Guojun Wang

- Secure Message Distribution Scheme with Configurable Privacy for Heterogeneous Wireless Sensor Networks
  YaHui Li, DingYong, JianFeng Ma

- A Sanitizing Signature Scheme with Indexing
  Atsushi Koide, Raylin Tso, Eiji Okamoto

- Error Detection Schemes for CED in Block Ciphers
  Ewa Idzikowska, Krzysztof Bucholc

Session 2: Trust Management and Privacy Protection I
Chair: Wenbin Luo, St. Mary's University, San Antonio, Texas, USA (wluo AT stmarytx.edu)
14:50 – 16:10pm, Function Room 1&2

- An Impact-Oriented Metric for Interference to Network Routing
  Song Huang, Lie-Gen Liu

- User-Directed Privacy Protection in the Ubiquitous Environment
  JaeHun Lee, JinKyu Park, SangWook Kim

- Provably Secure Trusted Access Protocol for WLAN Mesh Networks
  Zhuo Ma, Jianfeng Ma, Yulong Shen

- Towards Trustworthy and Secure Kiosk Computing for Mobile Users
### Session 3: Trust Management and Privacy Protection II

Chair: Jarrod Trevathan, James Cook University, Australia (jarrod.trevathan AT jcu.edu.au)
16:20 – 17:50pm, Function Room 1&2

- **Defending against the Propagation of Active Worms**  
  *Xiang Fan, Yang Xiang*

- **Convertible Undeniable Partially Blind Signature from Bilinear Pairings**  
  *Atsushi Koide, Raylin Tso, Eiji Okamoto*

- **Analyzing Privacy Designs of Mobile Social Networking Applications**  
  *Guanling Chen, Faruq Rahman*

- **Research on Endpoint Isolation and Remediation Mechanism Based on Trusted Access Technology**  
  *Zhenyu Wang, Xiangdong Li, Lining Yao, Qi Feng, Ruimin Wang*

- **Privacy Engine for Context-Aware Enterprise Application Services**  
  *Marion Blount, John Davis, Maria Ebling, William Jerome, Barry Leiba, Xuan Liu, Archan Misra*

- **The Trustworthiness Based on Hash Chain in Wireless Sensor Network**  
  *Xiong Peng, Zhang Wei*

- **Trust Similarity Measure in Trust Model for P2P Networks**  
  *Yizhi Ren, Mingchu Li, Cheng Guo, Yongrui Cui, Kouichi Sakurai*

---

### The 2008 IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-08)

Friday, 19 December, 2008

### Session 4: Encryption and Decryption I

Chair: Chien-Pen Chuang, National Taiwan Normal University, Taiwan (chuang AT ntnu.edu.tw)
10:30 – 12:10pm, Function Room 1&2

- **Distance Bounding Protocol for Multiple RFID Tag Authentication**  
  *Gaurav Kapoor, Wei Zhou, Selwyn Piramuthu*

- **Encryption and Decryption with Space Transformation for Bi-directional Association**  
  *Chien-Pen Chuang, Tin-Ying Huang, Li-Chi Yeh*

- **Cryptanalysis of Li et al.’s Identity-Based Threshold Signcryption Scheme**  
  *Ying Jin, Zepeng Li, Da Wei, Lei Liu*
## Session 5: Encryption and Decryption II
Chair: Feilong Tang, Shanghai Jiao Tong University, China (tang-fl AT cs.sjtu.edu.cn)
13:30 – 15:10pm, Function Room 1&2

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong Authentication Protocol for Secure RFID Tag Search without Help of Central Database</td>
<td>Tae Youn Won, Ji Young Chun, Dong Hoon Lee</td>
</tr>
<tr>
<td>Providing Stronger Authentication at a Low Cost to RFID Tags Operating under the EPCglobal Framework</td>
<td>Pedro Peris-Lopez, Tong-Lee Lim, Tieyan Li</td>
</tr>
<tr>
<td>Towards Successive Privacy Protection in Sensor Networks</td>
<td>Baokang Zhao, Dan Wang, Zili Shao, Jiannong Cao, Keith C.C. Chan, Jinshu Su, Yanqin Yang</td>
</tr>
<tr>
<td>Markov Model-Based Handwritten Signature Verification</td>
<td>Alan McCabe, Jarrod Trevathan</td>
</tr>
<tr>
<td>An Efficient RFID Authentication Protocol for Low-Cost Tags</td>
<td>Yanfei Liu</td>
</tr>
<tr>
<td>Trustworthy Semantic Web Technologies for Secure Knowledge Management</td>
<td>Bhavani Thuraisingham, Pranav Parikh</td>
</tr>
</tbody>
</table>

## Session 6: Key Management
Chair: Huawei Zhao, Shandong University of Finance, China (zhuav AT 163.com)
15:30 – 17:10pm, Function Room 1&2

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Improved Password-Based Authenticated Key Agreement Scheme for Pervasive Applications</td>
<td>Maw-Jinn Tsaur, Wei-Chi Ku, Hao-Rung Chung</td>
</tr>
<tr>
<td>Efficient Client-to-Client Password Authenticated Key Exchange</td>
<td>Yanjiang Yang, Feng Bao, Robert H. Deng</td>
</tr>
<tr>
<td>A Self-Healing and Mutual-Healing Key Distribution Scheme Using Bilinear Pairings for Wireless Networks</td>
<td>Biming Tian, Song Han, Tharam S. Dillon</td>
</tr>
<tr>
<td>Research on Pairwise Key Establishment for Cluster Heads in Sensor Networks</td>
<td>Li Ping, Wu Jia-ying, Xue Jing-ming</td>
</tr>
</tbody>
</table>
A Key Management Scheme for Cluster Based Wireless Sensor Networks

Key Management for Wireless Sensor Networks Using Trusted Neighbors
Xue Yuan, Helmut Jürgensen, Reza Azarderakhsh, Arash Reyhani-Masoleh

An Improved Key Management Scheme for WEP
Zhang Longjun, Zou Tao

The 2008 IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-08)
Saturday, 20 December, 2008

Session 7: Access Control and Anonymity
Chair: Xuan Liu, IBM T.J. Watson Research Center, USA (xuanliu AT us.ibm.com)
8:30 – 10:10am, Function Room 1&2

Property Verification for Generic Access Control Models
Vincent C. Hu, D. Richard Kuhn, Tao Xie

ALHACF: An Anonymity-Level Selected Hierarchical Anonymous Communication Framework
Xin Chen, Huaping Hu, Bo Liu, Fengtao Xiao, Zunguo Huang

Pool-Based APROB Channel to Provide Resistance against Global Active Adversary under Probabilistic Real-Time Condition
Minh-Triet Tran, Thanh-Trung Nguyen, Isao Echizen

Temporal UAS: Supporting Efficient RBAC Authorization in Presence of the Temporal Role Hierarchy
Yue Zhang, James B.D. Joshi

Identity Privacy Protection by Delayed Transmission in Pocket Switched Networks
Xiaofeng Lu, Pan Hui, Pietro Lio, Zhang Xiong

A Domain-Oriented Approach for Access Control in Pervasive Environments
Jun Li, Bruce Christianson

Using Context Quality Indicators for Improving Context-Based Access Control in Pervasive Environments
José Bringel Filho, Hervé Martin

Session 8: Security and Privacy in Wireless Networks
Chair: Guanling Chen, University of Massachusetts Lowell, USA (glchen AT cs.uml.edu)
10:30 – 12:10pm, Function Room 1&2

Trusted Spanning Tree for Delay Tolerant MANETs
A. Piyatumrong, P. Bouvry, F. Guinand, K. Lavangnananda

Scalable and Secure Routing for Large-Scale Sensor Networks
<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feilong Tang, Minyi Guo, Minglu Li, Zhijun Wang, Zixue Cheng</td>
<td>Securing Wireless Sensor Networks Using Cluster Reformations</td>
</tr>
<tr>
<td>Gicheol Wang, Deokjai Choi, Daewook Kang</td>
<td>Ubiquitous and Secure Certificate Service for Mobile Ad Hoc Network</td>
</tr>
<tr>
<td>Meng Ge, Kwok-Yan Lam, Jianbin Li, Siu-Leung Chung</td>
<td>HybridS: A Scheme for Secure Distributed Data Storage in WSNs</td>
</tr>
<tr>
<td>Wei Ren, Yi Ren, Hui Zhang</td>
<td>SARC: A Street-Based Anonymous Vehicular Ad Hoc Routing Protocol for City Environment</td>
</tr>
</tbody>
</table>

**Session 9: Secure Services and Security Analysis**

Chair: Zhenyu Wang, National Digital Switching System Engineering & Technology Research Center, China (wzyzw2008 AT yahoo.com.cn)

13:30 – 15:10pm, Function Room 1&2

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chaowang Shang, Zongkai Yang, Qingtang Liu, Chengling Zhao</td>
<td>A Context Based Dynamic Access Control Model for Web Service</td>
</tr>
<tr>
<td>Chun-Chao Yeh</td>
<td>Secure and Verifiable P2P Card Games</td>
</tr>
<tr>
<td>JoongMan Kim, SeokUng Yoon, HyunCheol Jeong, YooJae Won</td>
<td>Implementation and Evaluation of SIP-Based Secure VoIP Communication System</td>
</tr>
<tr>
<td>Nicolai Kuntze, Julian Schütte</td>
<td>Securing Decentralized Workflows in Ambient Environments</td>
</tr>
<tr>
<td>Yawen Wang, Yunzhan Gong, Junliang Chen, Qing Xiao, Zhaohong Yang</td>
<td>An Application of Interval Analysis in Software Static Analysis</td>
</tr>
<tr>
<td>Christos Xenakis, Danae Apostolopoulou, Angeliki Panou, Ioannis Stavrakakis</td>
<td>A Qualitative Risk Analysis for the GPRS Technology</td>
</tr>
</tbody>
</table>
Access Guide to EUC-08/TSP-08 Conference Venue

There are two airports in Shanghai, Pudong International Airport (PVG) and Hongqiao International Airport (SHA), and there are two railway stations in Shanghai, Shanghai Railway Station and Shanghai South Railway Station. Our hotel is at the crossing of Dong Fang Road and Wei Fang Road. The usual traffic direction is followed.

1. From Shanghai Pudong International Airport (PVG)
   - Taxi only
     A20 (Outside Circle) --- turn right onto Luo Shan Road --- turn left onto Hua Mu Road --- turn right onto Dong Fang Road --- turn left onto Wei Fang Road. It takes about 40 minutes to the hotel. Estimated taxi fare: 120 RMB (one way, if traffic condition is fine)
   - Maglev Train and Subway Line No.2
     Take Maglev Train from Pudong International Airport to Longyang Road Subway Station, and then take Subway Line No.2 to the Shiji (Century) Avenue Station. From here, go to the conference hotel on foot, which takes around 5 minutes. Totally about 60 RMB for Subway line No.2 and economy Maglev Train, 110 RMB for Subway line No.2 and VIP Maglev Train.
   - Airport bus Line No.3 and Subway Line No.2
Take Airport bus Line No.3 from Pudong International Airport to Longyang Road Subway Station, then take Subway Line No.2 to the Shiji (Century) Avenue Station. From here, go to the conference venue on foot, which takes around 5 minutes. Totally about 25 RMB is needed.

- **Airport bus Line No.5 and Taxi**
  Take Airport bus Line No.5 from Pudong International Airport to Oriental hospital, then take a taxi to the hotel. Totally about 35 RMB is needed.

2. **From Hongqiao International Airport (SHA)**
   - **Taxi only**
     Yan An Road Elevated High Way --- to Yan An East Road Tunnel --- to Shi Ji Da Dao (Century Blvd) --- turn right onto Dong Fang Road --- turn left onto Wei Fang Road. It takes about 30 minutes to the hotel. Estimated taxi fare: 70 RMB (one way, if traffic condition is fine)
   - **Bus No. 925A and Subway Line 2**
     Take Bus No. 925A from Hongqiao International Airport to People's Square, and then take Subway Line No.2 to the Shiji (Century) Avenue Station. From here, go to the conference hotel on foot, which takes around 5 minutes. Totally about 8 RMB is needed.

3. **From Shanghai Railway Station or Shanghai South Railway Station**
   - **Subway Line No.1 and No.2**
     Take Subway Line No.1 from either Railway Station to People's Square Station, and then interchanges to Subway Line No.2 to the Shiji (Century) Avenue Station. From here, go to the conference hotel on foot, which takes around 5 minutes. Totally about 5~7 RMB is needed.