SEC2000 Program

Tuesday, August 22, 2000 Beijing International Convention Center

8:30-9:15

Room SEC-0

Chairperson: Sihan Qing, China

Invited Talk: Public Key Infrastructure: managing the e-Business security

Xuejia Lai, Switzerland

9:20-10:05

Session1: New Information Security Technology : Room SEC-1

(9:20-9:45):�?/FONT>DNA-proofing�?/FONT> for computer systems - a new approach to computer security?

C.P.Louwrens, S.H. Von Solms, South Africa

(9:45-9:55): Biometric single sign-on: an Authenticating server approach

SH von Solms, Bobby Tai, South Africa

(9:55-10:05): A Approach to Secure Session Based on Smart Card

Chen Weifeng, Jiang Jianchun, Ma Hengtai, Qing Sihan, China

Session3: Network Security and Protocols : Room SEC-2

(9:20-9:45): A multi-party non-repudiation protocol

Steve Kremer , Olivier Markowitch, Belgium

(9:45-9:55): A Conceptual Intrusion Monitoring Architecture and Thoughts on Practical Implementation

P.S.Downland, S.M.Furnell, UK

(9:55-10:05): A Wavelet Neural Network-based Intrusion Detection Model

Song Rushun, Qian Gang, Chen Bo, China

Session5: Distributed Computing & Access Control : Room SEC-3

(9:20-9:45): A Context-Sensitive Access Control Model and Prototype Implementation

D.G. Cholewka, R.A. Botha, J.H.P. Elof, South Africa

(9:45-9:55): Mosaic: Model for Secure Anonymous Internet Communication

J.H.S. Geldenhuys[1] and S.H. von Solms, South Africa

(9:55-10:05): Improving Network Access Control Integrity Through Redundant Mechanisms

Olivier Paul, France

10:05-10:30 **break**

10:30-12:00

Room SEC-1

(10:30-10:55): Using Smart Cards in an Educational Environment: Services and Security Features

Costas Lambrinoudakis, Greece

(10:55-11:20): MASS: Model for an Auditing Security System

A.Liebenberg, J.H.P. Eloff, South Africa

(11:20-11:30): A Framework for Comparing Cryptographic libraries

Konstantinos Moulinos, Nikolaos Kyrloglou,, Theodore Tryfonas, Greece

(11:30-11:40): An Algorithm of Auto-adaptation Visible Watermark Based on Image

Du Jiang, Huang Jingxiong, Xie Weixin, China

(11:40-11:50): Java Card Security

Liu Songyan, Ye Yizheng, Mao Zhigang, China

(11:50-12:00): Visual Hiding of Digital Image

Wang Daoshun, Qi Dongxu, China

Room SEC-2

(10:30-10:55): Analysis and Design of E-voting Protocol

Jiang Shaoquan, Feng Dengguo, Qing Sihan, China

(10:55-11:20): Integrated Multi-Agent Approach to Network Security Assurance: Models of Agents' Community

V. Gorodetski, I. Kotenko, and V. Skormin, Russia

(11:20-11:30): An Adaptive Integrated Intranet Security System

Yang Lei; Sihan Qing; Xizhen Ni; Hangjing Zhang; Yan Weng, China

(11:30-11:40): Research of Security Mechanism for Virtual Enterprise Information System

Lina Wang, Ge Yu, Guoren Wang, Zhe Mei, Dan Wang, Xiaochun Yang, China

(11:40-11:50): A Suitable Protocol for Mobile Agent Authentication within an Intrusion Detection System

Damian Gregory, Q Shi; M. Merabti, UK

(11:50-12:00): The Research and Implementation on HTTP Tunneling

Shu Kun, Xu Yong, Wu Guoxin, China

Room SEC-3

(10:30-10:55): Regulating access to semistructured information on the Web

E.Damiani, S. De Capitanidi Vimercati, S. Paraboschi and Pierangela Samarati, Italy

(10:55-11:20): On the Practical Feasibility of Secure Distributed Computing: a case study

Gregory Neven, Frank Piessens, Bart De Decker, Belgium

(11:20-11:30): A Romote Password Authentication Scheme with Smart Card

Zhao Fuxiang, Wang Yumin, Zhao Hongyun, China

(11:30-11:40): Access Control: Its Representation and Evaluation

Yun Bai, Vijay Varadharajan, Australia

(11:40-11:50): Research on Network Security System with Access Control and Intrusion Detection

Li Xinman, Zhao Hong, China

(11:50-12:00): Separation of Duty in Role-based Access Control Model

Liu Qiongbo, Shi Jun and You Jinyuan, China

12:00-13:30 Lunch

13:30-15:15

Room SEC-1

(13:30-13:55): Classifying information for external release

S.Dawson, S.D.C.D. Vimercati, P. Lincoln; Pierangela Samarati, USA

(13:55-14:20): Using Mobile agent Results to Create Hard-to-Detect Computer Viruses

Yongge Wang, Canada

(14:20-14:45): CARDS: A Distributed System for Detecting Coordinated Attacks

Jiahai Yang, Peng Ning, X. Sean Wang, Sushil Jajodia, USA

(14:45-14:55): The Optimal Encoding Schemes

Dongyang Long and Weijia Jia, Hong Kong, China

(14:55-15:05): Secure Multicasting Survey

Ghassan Chaddoud, Isabelle Chrisment, Andre Schaff, France

(15:05-15:15): The Defects of Newton Channel and the Improvement

Zhang Tong, Li Zhenfu; Yang Bo; Wang Yumin, China

Room SEC-2

(13:30-13:55): Towards Network Denial of Service Resistant Protocols

Jussipekka Leiwo, Tuomas Aura; Pekka Nikander, Netherlands

(13:55-14:20): A Generic Graphical Specification Environment for Security Protocol Modeling

Elton Saul, Andrew Hutchison, South Africa

(14:20-14:45): Anonymous Electronic Voting System with Non-Transferable Voting Passes

Rosanna Y. Chan, Jonathan C. Wong, Alex C. Chan, Hong Kong, China

(14:45-14:55): The Model and Efficiency Analysis Of Distributed Certification System In Private Network

Lu Yu, Wang Yu, Lin Qi, Li Yongqi, China

(14:55-15:05): Developing a Filtering Proxy Server for Network Security

Savita Gupta, Harmesh Kansal and Dr. R.C. Chauhan, India

(15:05-15:15): Two New Attacks Against Otway-Rees Protocol

Wang Guilin, Qing Sihan, China

Room SEC-3

(13:30-13:55): Elements of A Language for Role Based Access Control

M. Hitchens & V. Varadharajan, Australia

(13:55-14:20): Disallowing unauthorized state changes of distributed shared objects

J. Leiwo, C.hanle, P. Homburg and A.S. Tanenbaum, Netherlands

(14:20-14:45): Framework for Security Analysis and Access Control on a Distributed Service Medical Imaging Network

Ian R Greenshields, Zhihong Yang, USA

(14:45-14:55): An Integrated Schemes of User Authentication And Access Control In A Distributed Computer Network

Dongyao Ji & Yuming Wang, China

(14:55-15:05): Dynamic Role Assignment in Role-Based Access Control Systems

SangYeob Na, SuhHyum Cheon, South Korea

15:15-15:45 **Coffee break**

15:45-17:40

Room SEC-1

(15:45-16:10): Robust Audio Watermarking based on Secure Spread Spectrum and Auditory Perception Model

Petar Horvatic, Jian Zhao, Niels J. Thorwirth, USA

(16:10-16:20): Bit-Operation Based Image Scrambling and Hiding

Yan Weiqi, Ding Wei, Qi Dongxu, China

(16:20-16:30): Hardware Implementation of Seed

Minglu Jin, Youngho Lee , Chuldong Lee, China

(16:30-16:40): Precautionary Measures against SYN Flooding Attacks

Li-Der Chou, Taiwan, China

(16:40-16:50): An Audio Watermarking Scheme with Hidden Signatures

Won-gyum Kim, Jong Chan Lee and Won Don Lee, South Korea

(16:50-17:00): Authentication using a Fingerprint in a Smart Card

Jeung-Seop Kim, Byung-Ho Cho, In-Gu Bae, Jae-Hyung Bae, and Kee-Young Yoo, South Korea

(17:00-17:10): Reference architecture-based smart card standardization: a possible way of future

Istvan, Mezgar; Zoltán Kincses; Tibor Rónai and Károly Kondorosi, Hungary

Room SEC-2

(15:45-16:10): Improving Packet Filters Management through Automatic and Dynamic Schemes

Olivier Paul, Maryline Laurent, France

(16:10-16:20): Field Programmable Firewall Model

Duan Yunsuo, Chen Zhong, China

(16:20-16:30): Making Kerberos Scalable

Brian May, H.R.Wu, Australia

(16:30-16:40): An Authentication Protocol for Loosely Coupled Distributed Information System

Song Jiaxing, Liu Weidong, Wang Cheng; Xu Ke; Liu Yaxiao, China

(16:40-16:50): A Fuzzy Pattern Matching Method In Instrusion Detection for Network Security

Luo Mingyu, Lu Xicheng,;Han Yaxin, Su Jinshu, China

(16:50-17:00): A Novel Sensor-Based Intrusion Detection System: SenIDS

Zhu Hui, Tan T H, Daniel, Singapore

(17:00-17:10): A Security Analysis Space for the Practitioner

Uttara Nerurkar, India

(17:10-17:20): A Hybrid Model for Intrusion Detection Based on Temporal-Probabilistic Networks

Alexandr Seleznyov, Finland

(17:20-17:30): T Temporal-Probabilistic Networks in Intrusion Detection: Detecting Abnormal Learning

Alexandr Seleznyov, Finland

(17:30-17:40): An approach to use knowledge about users' security requirements in a risk analysis

Ann Frisinger and Louise Yngstrom, Sweden

Wednesday, August 23, 2000 Beijing International Convention Center

8:30-9:15

Room SEC-0

Chairperson: Jan Eloff, South Africa

Invited Talk: On the Development of the Advanced Encryption Standard

Yiqun Lisa Yin, USA

9:20-10:05

Session2: Information Security Management: Room SEC-1

(9:20-9:45): IT Certification and criteria: Progress, problems and perspective

Kai Rannenberg, UK

(9:45-9:55): Data-compression aiding data-security

Tibor Nemetz, Pal Papp, Hungary

(9:55-10:05): An Analysis for Security Model of Apache SuEXEC

Luo Tiejian, Xu Haizhi, Dong Zhanqiu, Chian

Session4: Cryptography: Room SEC-2

(9:20-9:45): A Simple and Efficient Approach to Verifying Cryptographic Protocols

Sun Yongxing, Wang Xinmei, China

(9:45-9:55): A Multiplication-Addition Structure against the Linear Cryptanalysis

Zhu Feng, Baoan Guo, Yiqi Dai, China

(9:55-10:05): Two New Public Key Cryptosystems with Their Applications in Copyright Protection of Digital Products

Jianfeng Ma, Tee Chye Chiam, Alex C Kot, Singapore

Session6: E-Commerce: Room SEC-3

(9:20-9:45): A framework for electronic commerce security

Les Labuschagne, South Africa

(9:45-9:55): Electronic Commerce Security And its Application to Banking Transactions

Eugene Kozik, Qing Sihan, Yang Lei, USA

(9:55-10:05): The Design of Cardholder Registration Software for E-Commerce based on SET

Shaohua Tang, China

10:05-10:30 **Break**

10:30-12:00

Room SEC-1

(10:30-10:55): I Information Security: Process evaluation and Product evaluation

M.M. Eloff, S.H. Von Solms, South Africa

(10:55-11:20): Managing Information Security in Healthcare - an Action Research Experience

Helen Armstrong, Australia

(11:20-11:30): Independent Security Management for the Global Mobility Networks

Dong Yuguo, Zheng Lianqing and Zhang Zhonghui, China

(11:30-11:40): Computer System Security Evaluation Model

Lu Yu, Lin Qi, Wang Yu, China

(11:40-11:50): Quantum Key Distribution Scheme with Identity Verification

Guihua Zeng, Jinye Peng, Xinmei Wang and Hongwen Zhu, China

(11:50-12:00): Data Security Techniques in CIMS/MIS

Wang Jianqiang, Wu Xinru, China

Room SEC-2

(10:30-10:55): Power Analysis of RC6 and Serpent

Wu Wenling, Feng Dengguo, Qing Sihan, China

(10:55-11:20): A Simple Algorithm for Computing Several Sequences Synthesis

Wang Mingsheng, Qing Sihan, Feng Dengguo, China

(11:20-11:30): Voter-Entrusted Ballot-Opening Agents in a Practical Electronic Voting Scheme

Zhou Zhouyi, Xie Dongqing, China

(11:30-11:40): High Order Differential Attack and Trace Attack to Block Ciphers

Yupu Hu, Kai Chen, Guozhen Xiao, China

(11:40-11:50): Method for Breaking up a New Diffier-Hellman Public-key Scheme

Guoqiang Bai, Shimin Wei; Guozhen Xiao, China

(11:50-12:00): An Internet Certification Scheme

Changjie Wang, Fangguo Zhang, Yumin Wang, China

Room SEC-3

(10:30-10:55): Securing Mobile Agents in Electronic Commerce: an Experiment

Anthony H. W. Chan, Caris K. M. Wong, T. Y. Wong, Michae R. Lyu, Hong Kong, China

(10:55-11:20): Fair Electronic Cash System with Multiple Banks

Fangguo Zhang,Futai Zhang, Yumin Wang, China

(11:20-11:30): Scalable, Tax Evasion-Free Anonymous Investing

Shouhuai Xu, moti yung and Gendu Zhang, China

(11:30-11:40): A Study on Efficient Micropayment System with Anonymity

Hae-Man Kim, Seok-Cheol Jang, Im-Yeong Lee, South Korea

(11:40-11:50): A New Approach to the Divisible E-Cash System

Chen Kai,Wei Shimin and Xiao Guozhen, China

(11:50-12:00): Secure Trading of Domain Names

Harald Hauschen, Jarle G. Hulaas and Henrik Stormer, Switzerland

12:00-13:30 Lunch

13:30-15:15

Room SEC-1

(13:30-13:55): From Trusted Information Security Controls to a Trusted Information Security Environment

Rossouw Von Solms and Helen Van de Haar, South Africa

(13:55-14:20): A qualitative approach to information availability

Theodore Tryfonas, Dimitris Gritzalis, Spyros Kokolakis, Greece

(14:20-14:45): A Postgraduate Programme on Information and Communication Systems Security

Socrates K.Katsikas, Greece

(14:45-14:55): A D&C Mechanism to Solve the PNNI Topology Information Conflicting Problem

Xu Haizhi, Luo Tiejian, Dong Zhanqiu, China

(14:55-15:05): Research on Safety Measures of MIS Database

Zhang Qiuyu Yuan Zhanting *Zhao Ziwen;* Feng Tao; Wang Cunlai, China

(15:05-15:15): Research and Implementation of Extranet Key Technologies

Zhai Mingyu; Yuan Yuan; Ji Yi; Gu Guanqun, China

Room SEC-2

(13:30-13:55): GSFS -- a New Group-Aware Cryptographic File System

Claudia Eckert, Florian Erhard and Johannes Geiger, Germany

(13:55-14:20): Robustness-Agile Encryptor for ATM Networks

Herbert Leitold, Wolfgang Mayerwieser, Udo Payer, Karl Christian Posch, Reinhard Posch, Johannes Wolkerstorfer, Austria

(14:20-14:45): Fast construction of secure discrete logarithm problems over Jacobian varieties

*Jin*ihui Chao, Kazuto Matsuo and Shigeo Tsujii, Japan

(14:45-14:55): A Scheme for Public-key Based Key Recovery System with Limited Time Span

Chen-Hwa Song, Kwo-Jean Farn and Yi-Shiung Yeh, Taiwan, China

(14:55-15:05): Block Cipher Modes for non-standard Applications

P.Horster; Peter Schartner, Austria

(15:05-15:15): Design of a Systolic Multiplier/Squarer for the Fast Modular Exponentiation

Keon-Jik Lee, Won-Ho Lee, Kee-Won Kim; Kee-Young Yoo, South Korea

Room SEC-3

(13:30-13:55): Electronic Payment Systems with Fair On-line Verification

Feng Bao, Robert Deng, Jianying Zhou, Singapore

(13:55-14:20): A Flexible Management Framework for Certificate Status Validation

Antonio Corradi, Rebecca Montanari, Cesare Stefanelli, Diana Berbecaru, Antonio Lioy and Fabio

Maino, Italy

(14:20-14:45): A security architecture for electronic commerce applications

B. De Win, J. Van den Bergh, F. Matthijs, B. De Decker, W. Joosen, Belgium

15:15-15:45 **Coffee break**

15:45-17:20

Room SEC-1

(15:45-16:10): Information security management through measurement

E. Von Solms, S.H. Von Solms, South Africa

(16:10-16:35): The Defense Framework for Large -Scale Computer Network System

Jianchun Jiang, Weifeng Cheng, Sihan Qing, Dengguo Feng, China

(16:35-17:00): Identity Mapping: An Approach to Unravel Enterprise Security Management Policies

Wolfgang Essmayr; Edgar Weippl, Austria

(17:00-17:10): An Object-Oriented Framework for Risk Data Repository

Lam-for Kwok, Ching-hang Cheung, Dennis Longely, Hong Kong, China

(17:10-17:20): Auditing Information Security Management Systems - Towards a Practical Method

Fredrik Bjorck, Sweden

Room SEC-2

(15:45-16:10): A new serial/parallel architecture for a low power modular multiplier

Johann Groβschadl, Austria

(16:10-16:35): Defending Against Null Calls Stream Attacks by Using a Double-Threshold Dynamic Filter

Haizhi Xu Changwei Cui Ying Lin Tiejian Luo Zhanqiu Dong, China

(16:35-16:45): Analysis of cryptographic protocols: the environment and the application

Antonio Durante, Italy

Thursday, August 24, 2000 Beijing International Conference Center

8:30-9:15

Room SEC-0

Chairperson: Basie von Solms, South Africa

Invited Talk: Requirements for Safety and Security Policies in Networked Organisations

Prof. Dr Klaus Brunstein, Germany

9:20-10:05

Session2: Information Security Management : Room SEC-1

(9:20-9:45): Independent policy oriented layering of security services

Herbert Leitold; Peter Lipp; Andreas Sterbenz, Austria

(9:45-10:10): Reducing Computer Fraud through Situational Crime Prevention

Robert Willison, UK

Session7: Ethics/Privacy/Copyright : Room SEC-2

(9:20-9:45): On the role of human morality in Information System Security: the problems of descriptivism and non-descriptive foundations

Mikko T. Siponen, Finland

(9:45-9:55): Are future IT practitioners ethically responsible?

Lynette Drevin, J Mclean, JJR van der Walt, South Africa

(9:55-10:05): Expectations, Limitations and Problems in Information Security Research with Industry

Helen Armstrong, Lynette Drevin and Louise Yngstrom, Australia

10:05-10:30 **break**

10:30-12:00

Room SEC-1

(10:40-11:05): Policies for Construction of Information Systems' Security Guidelines: Five approaches

Mikko T. Siponen, Finland

Room SEC-2

(10:30-10:55): Information Warfare: Fact or Fiction?

M.J.Warren and W.Hutchinson, Australia

(10:55-11:20): Enforcing privacy by withholding private information

Frans Lategan, Martin S Olivier, South Africa

(11:20-11:30): Network Security Health Ckecking

H.S. Venter, J.H.P Eloff, South Africa

(11:30-11:40): Computer Security: Hacking Tendencies, Criteria and Solutions

Martin Botha & Rossouw von Solms, South Africa

(11:40-11:50): Human Rights Versus Security Technologies

Drakulic Ratimir, Drakulic Mirjana, Yugoslavia

(11:50-12:00): A formal language for the specification and manipulation of security policies

Hongxue Wang, Vijay Varadharajan and Yan Zhang, Australia

12:00-13:30 Lunch

13:30-15:45

Room SEC-2

(13:30-13:55): The Changing roles of Patent and Copyright Protection for Software and Communication Technology In the Internet Age

Gregory J. Kirsch, Tim Tingkang Xia, USA

(13:55-14:05): Will Self-Regulation Improve the Internet Security?

Jacques Berleur & Jean-Marc Dinant, Belgium

15:45- **Closure**