Hsinchun Chen
Fei Yue Wang
Christopher C. Yang
Daniel Zeng
Michael Chau
Kuiyu Chang (Eds.)

LNCS 3917

Intelligence and Security Informatics

International Workshop, WISI 2006
Singapore, April 2006
Proceedings

Springer

Hsinchun Chen Fei Yue Wang
Christopher C. Yang Daniel Zeng
Michael Chau Kuiyu Chang (Eds.)

Intelligence and Security Informatics

International Workshop, WISI 2006
Singapore, April 9, 2006
Proceedings

Springer

Volume Editors

Hsinchun Chen
Daniel Zeng
University of Arizona, College of BPA
Department of MIS, Tucson, AZ 85721, USA
E-mail: {hchen, zeng}@eller.arizona.edu

Fei Yue Wang
Chinese Academy of Sciences
P.O.Box 2728, Beijing 100080, China
E-mail: feiyue.wang@ia.ac.cn

Christopher C. Yang
The Chinese University of Hong Kong
Department of Systems Engineering and Engineering Management
Shatin, New Territories, Hong Kong, China
E-mail: yang@se.cuhk.edu.hk

Michael Chau
The University of Hong Kong, School of Business
Faculty of Business and Economics, Pokfulam Road, Hong Kong, China
E-mail: mchau@business.hku.hk

Kuiyu Chang
Nanyang Technological University, School of Computer Engineering
Singapore 639798, Singapore
E-mail: kuiyu.chang@pmail.ntu.edu.sg

Library of Congress Control Number: 2006922999

CR Subject Classification (1998): H.4, H.3, C.2, H.2, D.4.6, K.4.1, K.5, K.6

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-540-33361-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33361-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11734628 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3917

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

Intelligence and security informatics (ISI) can be broadly defined as the study of the development and use of advanced information technologies and systems for national and international security-related applications. The First and Second Symposiums on ISI were held in Tucson, Arizona, in 2003 and 2004, respectively. In 2005, the IEEE International Conference on ISI was held in Atlanta, Georgia. These ISI conferences brought together academic researchers, law enforcement and intelligence experts, information technology consultants and practitioners to discuss their research and practice related to various ISI topics including ISI data management, data and text mining for ISI applications, terrorism informatics, deception detection, terrorist and criminal social network analysis, crime analysis, monitoring and surveillance, policy studies and evaluation, and information assurance, among others. We continued these stream of ISI conferences by organizing the Workshop on Intelligence and Security Informatics (WISI 2006) in conjunction with the Pacific Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2006). WISI 2006 provided a stimulating forum for ISI researchers in Pacific Asia and other regions of the world to exchange ideas and report research progress.

WISI 2006 was hosted by the Chinese University of Hong Kong, the University of Arizona, the Nanyang Technological University, and the Chinese Academy of Sciences. The one-day program included one keynote speech, four refereed paper sessions, two invited sessions and a poster reception. The keynote speech was delivered by Professor Bhavani Thuraisingham, who is the director of Cyber Security Research Center at the University of Texas at Dallas. There were seven long papers and eight short papers presented in the refereed paper sessions and 17th poster presentations in the poster reception. We had four invited speakers presenting on the topic of terrorism research tools in the two invited sessions. The workshop was co-sponsored by the Chinese University of Hong Kong, the University of Arizona, and other funding agencies.

We wish to express our gratitude to all workshop Program Committee members and additional reviewers, who provided high-quality, valuable and constructive review comments. Special thanks go to Ee Peng Lim and Ah Hwee Tan, who supported the local arrangement.

April 2006

Hsinchun Chen
Feiyue Wang
Christopher C. Yang
Daniel Zeng
Michael Chau
Kuiyu Chang

Organization

WISI 2006 was hosted by the Chinese University of Hong Kong, the University of Arizona, the Nanyang Technological University, and the Chinese Academy of Sciences. The one-day program included one keynote speech, four refereed paper sessions, two invited sessions and a poster reception. The workshop was co-sponsored by the Chinese University of Hong Kong, the University of Arizona, and other funding agencies.

Organizing Committee

Honorary Co-chairs	Hsinchun Chen, The University of Arizona Feiyue Wang, Chinese Academy of Sciences
Honorary Co-chairs	Christopher C. Yang, The University of Hong Kong Daniel Zeng, The University of Arizona
Program Co-chairs	Michael Chau, The University of Hong Kong Kuiyu Chang, Nanyang Technological University

Program Committee

Andy Chen, National Taiwan University, Taiwan
David Cheung, University of Hong Kong, Hong Kong, China
Lee-Feng Chien, Academia Sinica, Taiwan
Ruwei Dai, Chinese Academy of Sciences, China
Jason Geng, Chinese Academy of Sciences, China
Rohan Gunaratna, Institute for Defense & Strategic Studies, Singapore
Eul Guy Im, Hanyang University, Korea
Moshe Koppel, Bar-Ilan University, Israel
Kai Pui Lam, Chinese University of Hong Kong, Hong Kong, China
Wai Lam, Chinese University of Hong Kong, Hong Kong, China
Ee-peng Lim, Nanyang Technological University, Singapore
Ruqian Lu, Chinese Academy of Sciences and Fudan University, China
Anirban Majumdar, University of Auckland, New Zealand
Edna Reid, University of Arizona, USA
Dmitri Roussinov, Arizona State University, USA
Gheorghe Muresan, Rutgers University, USA
Marc Sageman, University of Pennsylvania, USA
Raj Sharman, State University of New York, Buffalo, USA

Andrew Silke, University of East London, UK
David Skillicorn, Queen's University, Canada
Aixin Sun, University of New South Wales, Australia
Fu Lee Wang, City University of Hong Kong, Hong Kong, China
Jau-Hwang Wang, National Central Police University, Taiwan
Jue Wang, Chinese Academy of Sciences, China
Jun Wang, Peking University, China
Ke Wang, Simon Fraser University, Canada
Chih-Ping Wei, National Tsinghua University, Taiwan
Zhaohui Wu, Zhejiang University, China
Yiyu Yao, University of Regina, Canada
Jerome Yen, Chinese University of Hong Kong, Hong Kong, China
Jeffrey Yu, Chinese University of Hong Kong, Hong Kong, China
William Zhu, University of Auckland, New Zealand

Additional Reviewers

Ahmed Abbasi, The University of Arizona
Wei Chang, The University of Arizona
Reynold Cheng, Hong Kong Polytechnic University
Yiuming Cheung, Hong Kong Baptist University
Siddharth Kaza, The University of Arizona
James Kwok, California State University, Long Beach
Jiexun Li, The University of Arizona
Kar Wing Jaffe Li, City University of Hong Kong
Xin Li, The University of Arizona
Byron Marshall, Oregon State University
Jialun Qin, The University of Arizona
Robert Schumaker, The University of Arizona
Chik How Tan, Gjøvik University College
Gang Wang, The University of Arizona
Haotian Wu, Hong Kong Baptist University
Jennifer Xu, Bentley College
Yilu Zhou, The University of Arizona

Lecture Notes in Computer Science

For information about Vols. 1–3828

please contact your bookseller or Springer

Vol. 3933: F. Bonchi, J.-F. Boulicaut (Eds.), Knowledge Discovery in Inductive Databases. VIII, 251 pages. 2006.

Vol. 3931: B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri (Eds.), Neural Nets. XIII, 370 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3927: J. Hespanha, A. Tiwari (Eds.), Hybrid Systems: Computation and Control. XII, 584 pages. 2006.

Vol. 3925: A. Valmari (Ed.), Model Checking Software. X, 307 pages. 2006.

Vol. 3924: P. Sestoft (Ed.), Programming Languages and Systems. XII, 343 pages. 2006.

Vol. 3923: A. Mycroft, A. Zeller (Eds.), Compiler Construction. XIII, 277 pages. 2006.

Vol. 3922: L. Baresi, R. Heckel (Eds.), Fundamental Approaches to Software Engineering. XIII, 427 pages. 2006.

Vol. 3921: L. Aceto, A. Ingólfsdóttir (Eds.), Foundations of Software Science and Computation Structures. XV, 447 pages. 2006.

Vol. 3920: H. Hermanns, J. Palsberg (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XIV, 506 pages. 2006.

Vol. 3917: H. Chen, F.Y. Wang, C.C. Yang, D. Zeng, M. Chau, K. Chang (Eds.), Intelligence and Security Informatics. XII, 186 pages. 2006.

Vol. 3916: J. Li, Q. Yang, A.-H. Tan (Eds.), Data Mining for Biomedical Applications. VIII, 155 pages. 2006. (Sublibrary LNBI).

Vol. 3915: R. Nayak, M.J. Zaki (Eds.), Knowledge Discovery from XML Documents. VIII, 105 pages. 2006.

Vol. 3909: A. Apostolico, C. Guerra, S. Istrail, P.A. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 612 pages. 2006. (Sublibrary LNBI).

Vol. 3907: F. Rothlauf, J. Branke, S. Cagnoni, E. Costa, C. Cotta, R. Drechsler, E. Lutton, P. Machado, J.H. Moore, J. Romero, G.D. Smith, G. Squillero, H. Takagi (Eds.), Applications of Evolutionary Computing. XXIV, 813 pages. 2006.

Vol. 3906: J. Gottlieb, G.R. Raidl (Eds.), Evolutionary Computation in Combinatorial Optimization. XI, 293 pages. 2006.

Vol. 3905: P. Collet, M. Tomassini, M. Ebner, S. Gustafson, A. Ekárt (Eds.), Genetic Programming. XI, 361 pages. 2006.

Vol. 3904: M. Baldoni, U. Endriss, A. Omicini, P. Torroni (Eds.), Declarative Agent Languages and Technologies III. XII, 245 pages. 2006. (Sublibrary LNAI).

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3901: P.M. Hill (Ed.), Logic Based Program Synthesis and Transformation. X, 179 pages. 2006.

Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3896: Y. Ioannidis, M.H. Scholl, J.W. Schmidt, F. Matthes, M. Hatzopoulos, K. Boehm, A. Kemper, T. Grust, C. Boehm (Eds.), Advances in Database Technology - EDBT 2006. XIV, 1208 pages. 2006.

Vol. 3895: O. Goldreich, A.L. Rosenberg, A.L. Selman (Eds.), Theoretical Computer Science. XII, 399 pages. 2006.

Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), Architecture of Computing Systems - ARCS 2006. XII, 496 pages. 2006.

Vol. 3890: S.G. Thompson, R. Ghanea-Hercock (Eds.), Defence Applications of Multi-Agent Systems. XII, 141 pages. 2006. (Sublibrary LNAI).

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3888: D. Draheim, G. Weber (Eds.), Trends in Enterprise Application Architecture. IX, 145 pages. 2006.

Vol. 3887: J.R. Correa, A. Hevia, M. Kiwi (Eds.), LATIN 2006: Theoretical Informatics. XVI, 814 pages. 2006.

Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), Knowledge Discovery in Life Science Literature. XIV, 147 pages. 2006. (Sublibrary LNBI).

Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), Modeling Decisions for Artificial Intelligence. XII, 374 pages. 2006. (Sublibrary LNAI).

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3882: M.L. Lee, K.L. Tan, V. Wuwongse (Eds.), Database Systems for Advanced Applications. XXI, 923 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3880: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development I. IX, 335 pages. 2006.

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3875: S. Ur, E. Bin, Y. Wolfsthal (Eds.), Hardware and Software, Verification and Testing. X, 265 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmidt (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3865: W. Shen, K.-M. Chao, Z. Lin, J.-P.A. Barthès, A. James (Eds.), Computer Supported Cooperative Work in Design II. XII, 659 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3862: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 267 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3854: I. Stavrakakis, M. Smirnov (Eds.), Autonomic Communication. XIII, 303 pages. 2006.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part II. XXXI, 977 pages. 2006.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3830: D. Weyns, H. V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems II. VIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Table of Contents

Crime Data Mining

Posters

Data Mining for Security Applications

Bhavani M. Thuraisingham[1,2]

[1] Eric Jonsson School of Engineering and Computer Science,
University of Texas at Dallas,
Richardson, Texas 75083-0688, USA
bhavani.thuraisingham@utdallas.edu
http://www.cs.utdallas.edu/people/thuraisingham.html
[2] Bhavani Security Consulting, LLC,
Dallas, Texas, USA
http://www.dr-bhavani.org

Abstract. Dr. Bhavani M. Thuraisingham is the invited keynote speaker for WISI 2006. She is a Professor at the Eric Jonsson School of Engineering and Computer Science, University of Texas at Dallas. She is also director of the Cyber Security Research Center and President of Bhavani Security Consulting.

1 Keynote Summary

Data mining is the process of posing queries and extracting patterns, often previously unknown from large quantities of data using pattern matching or other reasoning techniques. Data mining has many applications in security including for national security as well as for cyber security. The threats to national security include attacking buildings, destroying critical infrastructures such as power grids and telecommunication systems. Data mining techniques are being investigated to find out who the suspicious people are and who is capable of carrying out terrorist activities. Cyber security is involved with protecting the computer and network systems against corruption due to Trojan horses and viruses. Data mining is also being applied to provide solutions such as intrusion detection and auditing.

This presentation will first discuss the various types of threats to national security and describe data mining techniques for handling such threats. Threats include non real-time threats and real-time threats. We need to understand the types of threats and also gather good data to carry out mining and obtain useful results. We also need to reason with incomplete data. Once the data is collected, the data has to be formatted and organized. Essentially one may need to build a warehouse to analyze the data. Data may be structured or unstructured. Once the data is gathered and organized, the next step is to carry out mining. The question is what mining tools to use and what outcomes to find? Do we want to find associations, links or clusters? Finally, how do we know that the mining results are useful? There could be false positives and false negatives. We will also explore techniques such as association rule mining and link analysis for national security.

The second part of the presentation will discuss data mining for cyber security applications For example, anomaly detection techniques could be used to detect unusual

H. Chen et al. (Eds.): WISI 2006, LNCS 3917, pp. 1 – 3, 2006.

patterns and behaviors. Link analysis may be used to trace the viruses to the perpetrators. Classification may be used to group various cyber attacks and then use the profiles to detect an attack when it occurs. Prediction may be used to determine potential future attacks depending in a way on information learnt about terrorists through email and phone conversations. Data mining is also being applied for intrusion detection and auditing.

The third part of the presentation will discuss some of the research challenges. There is a critical need to analyze the data in real-time and give the results to the war fighter to carry out actions. There is also a need to analyze the data about a passenger from the time he or she checks in at the ticket counter until he or she boards the plane. That is, while we need some form of real-time data mining, that is, the results have to be generated in real-time, we also need to build models in real-time for real-time intrusion detection. Data mining is also being applied for credit card fraud detection and biometrics related applications. Other challenges include mining unstructured data types. While some progress has been made on topics such as stream data mining, there is still a lot of work to be done here. Another challenge is to mine multi-media data including surveillance video. Finally, we need to maintain the privacy of individuals. Much research has been carried out on privacy preserving data mining. The presentation will analyze the developments made in the areas and determine the research directions.

In summary, the presentation will provide an overview of data mining, the various types of threats and then discuss the applications of data mining for national security and cyber security. Then we will discuss the consequences to privacy. That is, data mining enables one to put pieces of public data and infer data that is highly sensitive or private. We will discuss threats to privacy and discuss the developments in privacy preserving data mining. Other challenges such as real-time data mining as well as mining surveillance data will also be discussed.

2 Biography

Dr. Bhavani Thuraisingham joined The University of Texas at Dallas in October 2004 as a Professor of Computer Science and Director of the Cyber Security Research Center in the Erik Jonsson School of Engineering and Computer Science. She is an elected Fellow of three professional organizations: the IEEE (Institute for Electrical and Electronics Engineers), the AAAS (American Association for the Advancement of Science) and the BCS (British Computer Society) for her work in data security. She received the IEEE Computer Society's prestigious 1997 Technical Achievement Award for "outstanding and innovative contributions to secure data management."

Dr Thuraisingham's work in information security and information management has resulted in over 70 journal articles, over 200 refereed conference papers and workshops, and three US patents. She is the author of seven books in data management, data mining and data security including one on data mining for counter-terrorism and another on Database and Applications Security and is completing her eighth book on Trustworthy Semantic Web. She has given over 30 keynote presentations at various technical conferences and has also given invited talks at the White House Office of Science and Technology Policy and at the United Nations on Data Mining for

counter-terrorism. She serves (or has served) on editorial boards of leading research and industry journals and currently serves as the Editor in Chief of Computer Standards and Interfaces Journal. She is also an Instructor at AFCEA's (Armed Forces Communications and Electronics Association) Professional Development Center and has served on panels for the Air Force Scientific Advisory Board and the National Academy of Sciences.

Dr Thuraisingham is the Founding President of "Bhavani Security Consulting" - a company providing services in consulting and training in Cyber Security and Information Technology.

Prior to joining UTD, Thuraisingham was an IPA (Intergovernmental Personnel Act) at the National Science Foundation from the MITRE Corporation. At NSF she established the Data and Applications Security Program and co-founded the Cyber Trust theme and was involved in inter-agency activities in data mining for counter-terrorism. She has been at MITRE since January 1989 and has worked in MITRE's Informa-tion Security Center and was later a department head in Data and Information Management as well as Chief Scientist in Data Management. She has served as an expert consultant in information security and data management to the Department of Defense, the Department of Treasury and the Intelligence Community for over 10 years. Thuraisingham's industry experience includes six years of research and development at Control Data Corporation and Honeywell Inc. Thuraisingham was educated in the United Kingdom both at the University of Bristol and at the University of Wales.

Unraveling International Terrorist Groups' Exploitation of the Web: Technical Sophistication, Media Richness, and Web Interactivity

Jialun Qin[1], Yilu Zhou[1], Edna Reid[1], Guanpi Lai[2], and Hsinchun Chen[1]

[1] Department of Management Information Systems, The University of Arizona, Tucson, AZ 85721, USA
{qin, ednareid, yiluz, hchen}@bpa.arizona.edu
[2] Department of Systems and Industry Engineering, The University of Arizona, Tucson, AZ 85721, USA
guanpi@email.arizona.edu

Abstract. Terrorists and extremists have become mainstream exploiters of the Internet beyond routine communication operations and dramatically increased their own ability to influence the outside world. Although this alternate side of the Internet, referred to as the "Dark Web," has recently received extensive government and media attention, the terrorists/extremists' Internet usage is still under-researched because of the lack of systematic Dark Web content collection and analysis methodologies. To address this research gap, we explore an integrated approach for identifying and collecting terrorist/extremist Web contents. We also propose a framework called the Dark Web Attribute System (DWAS) to enable quantitative Dark Web content analysis from three perspectives: technical sophistication, media richness, and Web interactivity. Using the proposed methodology, we collected and examined more than 200,000 multimedia Web documents created by 86 Middle Eastern multi-lingual terrorist/extremist organizations. In our comparison of terrorist/extremist Web sites to U.S. government Web sites, we found that terrorists/extremist groups exhibited similar levels of Web knowledge as U.S. government agencies. We also found that the terrorists/extremist groups are as effective as the U.S. government agencies in terms of supporting communications and interaction using Web technologies. Based on our case study results, we believe that the DWAS is an effective framework to analyze the technical sophistication of terrorist/extremist groups' Internet usage and our Dark Web analysis methodology could contribute to an evidence-based understanding of the applications of Web technologies in the global terrorism phenomena.

1 Introduction

International terrorist/extremist groups' use of the Internet has expanded beyond routine communication and propaganda operations to training, organizing logistics for their campaign, exploring collaborative networks, and developing their strategic intelligence and virtual communities. Their Web sites and online forums have increased in number, technical sophistication, content, and media richness. These dynamic Web

H. Chen et al. (Eds.): WISI 2006, LNCS 3917, pp. 4 – 15, 2006.