

SoS-VO Developments

<http://sos-vo.org>

Q3 2014



Tel (615) 343-7472 Fax (615) 343-7440
1025 16th Avenue South | Nashville, TN 37212
www.isis.vanderbilt.edu



VANDERBILT UNIVERSITY

Agenda

- Support for Bibliographic References
- *Initial Group Statistics Feature Released*
- *Graphical Sitemaps are in Development*

Motivation

The screenshot shows a web browser window displaying the Science of Security VO website. The browser's address bar shows the URL `cps-vo.org/group/SoS`. The website header features the Science of Security logo, which includes a stylized padlock and the text "An Online Community to Advance Cyber-Security Science". A "Join Us!" button is visible in the top right corner of the header. Below the header, there is a navigation menu with options like "Home", "About", "Calendar", "Activity Stream", "Search", "Videos", "Newsletter", "Members", "Contact Us", "Popular", "Advanced", "Forums", and "Files". The "Newsletter" link in the navigation menu is circled in red. The main content area is titled "In the Spotlight" and features a large banner for the "ACM CCS 2014" conference. Below the banner, there are several smaller images and a row of buttons: "Newsletter", "Best Scientific Cybersecurity Paper", "HotSoS '15", and "Hard Problems". The "Newsletter" button is circled in orange. To the right of the main content, there are sections for "Recent News" and "Upcoming Events". The "Recent News" section includes a headline about "NSA Announces Winner 'Best Scientific Cybersecurity Paper Competition'" and a list of recent blog posts. The "Upcoming Events" section lists dates and event names like "MALCON 2014" and "Science of Security Quarterly Label Meeting (UMD)".

<html> </html>

- ☐ Science of Security (SoS) Newsletter
 - ☒ Science of Security (SoS) Newsletter (2014 - Issue 4)
 - ☒ Science of Security (SoS) Newsletter (2014 - Issue 3)
 - ☒ Science of Security (SoS) Newsletter (2014 - Issue 2)
 - ☒ Science of Security (SoS) Newsletter (2014 - Issue 1)
 - ☒ General Topics of Interest
 - ☒ Publications of Interest
 - Authentication and Authorization
 - Automated Response Actions
 - Computer Science
 - Cryptography and Security
 - Cyber-Physical Systems
 - Dynamic Execution
 - End to End Computing
 - Game Theoretic Approaches
 - Intrusion Tolerance
 - IPv6 and Other Protocols
 - Mathematics
 - Mobile Computing
 - Mobile Computing and Security
 - Moving Target Defense
 - Operating Systems
 - Peer to Peer Systems
 - Quantum Computing
 - Resiliency
 - Signals Processing
 - Situational Awareness
 - Software Assurance
 - Virtual Machines
 - Recent NSF Research Grants 2012-2013



2014-01

Computer Science

This set of citations covers a broad range of articles about research conducted across a wide range of computer science security topics from 2013. These include human factors, software development, trust mechanisms, cloud computing, and more.

- ☐ "Conceptual Design of Software: A Research Agenda" D. Jackson, MIT, 2013 A research agenda in software design is outlined, focusing on the role of concepts. The notions of concepts as "abstract affordances" and of conceptual integrity are discussed, and a series of small examples of conceptual models is given. (ID#:14-1066) See <http://dspace.mit.edu/bitstream/handle/1721.1/79826/MIT-CSAIL-TR-2013-020.pdf?sequence=2>
- ☐ "Expectation-Oriented Framework for Automating Approximate Programming", Esmailzadeh, H., Ni, K., Naik, M., Georgia Institute of Technology, 2013 This paper discusses ExpAX, the concept of automated, approximate programming based on error expectations as detailed by the programmer. ExpAX falls under the domain of general-purpose approximate computing, which explores the necessary concession of absolute computational accuracy in order to advance energy efficiency and performance. (ID#:14-1067 See: <https://smartech.gatech.edu/handle/1853/49755>)
- ☐ "Approximating the AND-OR tree" A. A. Sherstov, Theory of Computing, 9(20):653-663, 2013. This article explores the role representations of Boolean functions by real polynomials have played in theoretical computer science. The main result of this paper, according to the author, translates into lower bounds on communication complexity. (ID#:14-1068) Available at: <http://www.cs.ucla.edu/~sherstov/pdf/and-or.pdf>
- ☐ "Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits". Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters. July 21, 2013. This study examines indistinguishability obfuscation and functional encryption for general circuits and give constructions that support all polynomial-size circuits. They further how to use indistinguishability obfuscation for circuits, public-key encryption, and non-interactive zero knowledge to achieve functional encryption for all circuits. The functional encryption scheme they construct includes succinct ciphertexts, which enable several

- "Juggle: addressing extrinsic load imbalances in SPMD applications on multicore computers". Steven A. Hofmeyr, Juan A. Colmenares, Costin Iancu, John Kubiawicz, Appears in Cluster Computing. Vol. 16, No. 2, pp 299-319, June 2013. This study investigates proactive dynamic load balancing on multicore systems, in which threads are continually migrated to reduce the impact of processor/thread mismatches. (ID#:14-1075) Available at: <http://www.cs.berkeley.edu/~kubitron/papers/parlab/juggle-cluster-computer-journal-2012.pdf>
- "A Multicore Operating System with QoS Guarantees for Network Audio Applications". Juan A. Colmenares, Nils Peters, Gage Eads, Ian Saxton, Israel Jacquez, John D. Kubiawicz, and David Wessel. Appears in Journal of Audio Engineering, Vol 61, No. 4, April 2013. The authors explore the role of the operating system (OS) within computer nodes of network audio systems. They highlight the importance of the OS for network audio applications and present Tessellation, an experimental OS tailored to multicore processors. The article may be of interest in signal processing. (ID#:14-1076) Available at: <http://www.cs.berkeley.edu/~kubitron/papers/parlab/JAES-1163-tess.pdf>
- "A Case Study on the Lightweight Verification of a Multi-Threaded Task Server" N'estor Cata~no, Ijaz Ahmed, Radu I. Siminiceanu, Jonathan Aldrich,. Preprint submitted to Science of Computer Programming December 1, 2013. This article should be of interest in massive parallelizing of computational tasks. The authors developed a methodology and tool for verifying the design of a commercial multi-threaded task server (MTTS). Their method uses a Data Flow Analysis in the first phase. In a second phase, they developed a Pulse tool that enhances the analysis they performed. They conclude exhaustive model-checking approach scales reasonably well and is efficient at finding errors in specifications that were not previously detected with the Data Flow Analysis (DFA) alone. (ID#:14-1077) See <http://www.cs.cmu.edu/~aldrich/papers/main-pulse-scp.pdf>

Note:

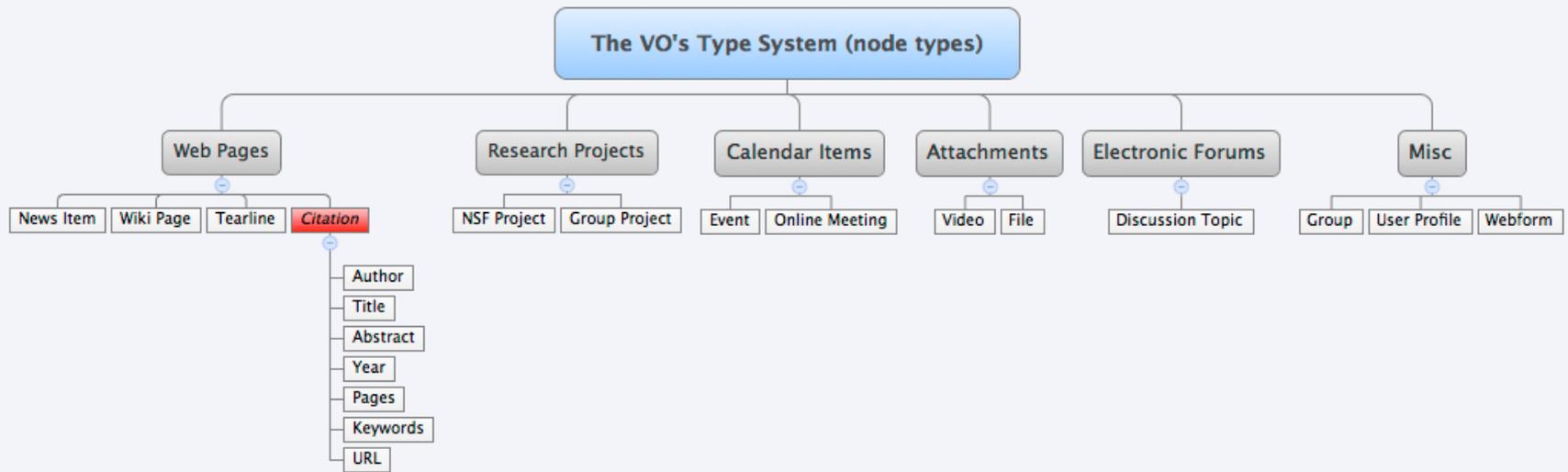
Articles listed on these pages have been found on publicly available internet pages and are cited with links to those pages. Some of the information included herein has been reprinted with permission from the authors or data repositories. Direct any requests via Email to SoS.Project (at) SecureDataBank.net for removal of the links or modifications to specific citations. Please include the ID# of the specific citation in your correspondence.



Problem #2:

HOW TO EASILY FIND THINGS WHEN THERE ARE 1000'S OF CITATIONS ???

THE VO IS NOT A WEBSITE; IT IS A 'CONTENT MANAGEMENT SYSTEM'



New Dashboard Widget



STAGING
Science of Security VO

EDIT GROUP TRACK CLONE TAXONOMY BROADCAST PANELS DEVEL GROUP STATS

- Home
- About
- Calendar
- Activity Stream
- Search
- Videos
- Newsletter
- Members
- Contact Us
- Popular
- Advanced
- Forums
- Files

In the Spotlight



Upcoming Events Worth Checking Out

Upcoming Events Worth Checking Out

The latest information on all upcoming science of security related events.

Recent News

NSA Announces New "Lablets" in Support of the Science of Security
For the past three years, the National Security Agency (NSA) and US... [more](#)

Build It, Break It, Fix It!
Registration is now open for a security-oriented programming... [more](#)

HotSoS 2014 - Meeting Artifacts Available Online
The 2014 Symposium and Bootcamp on the Science of Security (HotSoS)... [more](#)

Upcoming Events

09/24/14 - 09/26/14
Intelligence and Security Informatics, and European Intelligence and Security Informatics Conference

10/13/14 - 10/15/14
9th International Workshop on Critical Information Infrastructures Security (CRITIS 2014)

11/12/14 - 11/13/14
2014 TCIPG Industry Workshop

Recent Publications

Passivity-Based Design of Wireless Networked Control Systems for Robustness to Time-Varying Delays
Abstract: Real-life cyber-physical systems, such as automotive vehicles, building automation systems, and groups of unmanned vehicles are monitored and controlled by networked control systems. The overall system dynamics emerges from the interaction among physical dynamics, computational dynamics, and... [more](#)

Adaptive processing with neural network controlled resonator-banks
Abstract: The author describes a novel neuromorphic architecture for structurally adaptive control systems. The neural network controlled resonator-bank (NCRB) architecture consists of two main components, a resonator-bank filter structure and a neural network which controls the transfer characteristics of... [more](#)

Compositional Specification of Behavioral Semantics
Abstract: An emerging common trend in model-based design of embedded software and

Current Research

NSA SoS Research Lablets
NSA SoS Research Efforts
AFOSR SoS
AFOSR Twitter

Chat (2)

Feedback

295 members (12)
Group Manager: Heather Lucas
Member Information Table
My membership
Invite members

ISIS Institut World-cl

UNIVERSITY

Searching for References

Recent Publications

Passivity-Based Design of Wireless Networked Control Systems for Robustness to Time-Varying Delays

Abstract: Real-life cyber-physical systems, such as automotive vehicles, building automation systems, and groups of unmanned vehicles are monitored and controlled by networked control systems. The overall system dynamics emerges from the interaction among physical dynamics, computational dynamics, and... [more](#)

Adaptive processing with neural network controlled resonator-banks

Abstract: The author describes a novel neuromorphic architecture for structurally adaptive control systems. The neural network controlled resonator-bank (NCRB) architecture consists of two main components, a resonator-bank filter structure and a neural network which controls the transfer characteristics of... [more](#)

Compositional Specification of Behavioral Semantics

Abstract: An emerging common trend in model-based design of embedded software and systems is the adoption of domain-specific modeling languages (DSMLs). While abstract syntax metamodeling enables the rapid and inexpensive development of DSMLs, the specification of DSML semantics is still a hard problem. In... [more](#)

[more](#)

The screenshot shows the Science of Security VO website. At the top, there is a logo with the letters 'SOS' and a padlock icon, with the text 'An Online Community to Advance Cyber-Security Science' and 'SCIENCE OF SECURITY'. Below the logo is a navigation menu with items like Home, About, Calendar, Activity Stream, Search, Videos, Newsletter, Members, Contact Us, Popular, Advanced, Forums, and Files. There are also buttons for 'COLLABORATE', 'SUBGROUPS', and 'MEMBER INFO'. A sidebar on the right contains a 'In the Spotlight' section with a 'Upcoming Events' graphic and a 'Recent Publications' section listing the three articles shown in the main content area. At the bottom, there is a 'Current Research' section and a 'Chat (2)' button.





An Online Community to Advance Cyber-Security Science

Join Us!

STAGING » SCIENCE OF SECURITY VO » BIBLIO



GROUP STATS

- Home
- About
- Calendar
- Activity Stream
- Search
- Videos
- Newsletter
- Members
- Contact Us
- Popular
- Advanced
- Forums
- Files

List Filter Import

Biblio search

Found 76 results

Sort by: Author Title Type [Year ▼]

2014

[ID#:14-1758] Urien, Pascal, Piramuthu, Selwyn. 2014. **Elliptic Curve-based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks**. Decis. Support Syst.. 59:28–36. Abstract

[ID#:14-1766] Li Chen, Demirkol, I, Heinzelman, W.. 2014. **Token-MAC: A Fair MAC Protocol for Passive RFID Systems**. Mobile Computing, IEEE Transactions on. 13:1352-1365. Abstract

[ID#:14-1760] Weiping Zhu, Jiannong Cao, Chan, H.C.B., Xuefeng Liu, Raychoudhury, V.. 2014. **Mobile RFID with a High Identification Rate**. Computers, IEEE Transactions on. 63:1778-1792. Abstract

[ID#:14-1771] Chen, Shuai-Min, Wu, Mu-En, Sun, Hung-Min, Wang, King-Hang. 2014. **CRFID: An RFID System with a Cloud Database As a Back-end Server**. Future Gener. Comput. Syst.. 30:155–161. Abstract

[ID#:14-1770] Rahman, Farzana, Ahamed, Sheikh Iqbal. 2014. **Efficient Detection of Counterfeit Products in Large-scale RFID Systems Using Batch Authentication Protocols**. Personal Ubiquitous Comput.. 18:177–188. Abstract

[ID#:14-1763] Morgado, T.A, Alves, J.M., Marcos, J.S., Maslovski, S.I, Costa, J.R., Fernandes, C.A, Silveirinha, M.G.. 2014. **Spatially Confined UHF RFID Detection With a Metamaterial Grid**. Antennas and Propagation, IEEE Transactions on. 62:378-384. Abstract

[ID#:14-1759] Sangyup Lee, Choong-Yong Lee, Wonse Jo, Dong-Han Kim. 2014. **An efficient area coverage algorithm using passive RFID system**. Sensors Applications Symposium (SAS), 2014 IEEE. :366-371. Abstract

[ID#:14-1761] Sabesan, S., Crisp, M.J., Penty, R.V., White, I.H.. 2014. **Wide Area Passive UHF RFID System Using Antenna Diversity Combined With Phase and Frequency Hopping**. Antennas and Propagation, IEEE Transactions on. 62:878-888. Abstract

[ID#:14-1764] Cook, B.S., Vyas, R., Sangkil Kim, Trang Thai, Taoran Le, Traille, A, Aubert, H., Tentzeris, M.M.. 2014. **RFID-Based Sensors for Zero-Power Autonomous Wireless Sensor Networks**. Sensors Journal, IEEE. 14:2419-2431. Abstract

COLLABORATE

[ID#:14-1767] Measel, R., Lester, C.S., Yifei Xu, Primerano, R., Kam, M.. 2014. **Detection performance of spread spectrum signatures for passive, chipless RFID**. RFID (IEEE RFID), 2014 IEEE International Conference on. :55-59. Abstract

SUBGROUPS

[ID#:14-1762] Goller, M., Feichtenhofer, C., Pinz, A. 2014. **Fusing RFID and computer vision for probabilistic tag localization**. RFID (IEEE RFID), 2014 IEEE International Conference on. :89-96. Abstract

MEMBER INFO

[ID#:14-1768] Baloch, F., Pendse, R.. 2014. **A New anti-collision protocol for RFID networks**. Wireless Telecommunications Symposium (WTS), 2014. :1-5. Abstract

- 295 members (12)
- Group Manager: Heather Lucas
- Member Information Table

[ID#:14-1757] Guizani, S.. 2014. **Security applications challenges of RFID technology and possible countermeasures**. Computing, Management and Telecommunications (ComManTel), 2014 International Conference on. :291-297. Abstract

Chat (1)



UNIVERSITY

Sort by: Author Title Type [Year ▼]

2014

[ID#:14-1758] Urien, Pascal, Piramuthu, Selwyn. 2014. **Elliptic Curve-based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks**. Decis. Support Syst.. 59:28–36. [Abstract](#)

[ID#:14-1766] Li Chen, Demirkol, I, Heinzelman, W.. 2014. **Token-MAC: A Fair MAC Protocol for Passive RFID Systems**. Mobile Computing, IEEE Transactions on. 13:1352-1365. [Abstract](#)

[ID#:14-1760] Weiping Zhu, Jiannong Cao, Chan, H.C.B., Xuefeng Liu, Raychoudhury, V.. 2014. **Mobile RFID with a High Identification Rate**. Computers, IEEE Transactions on. 63:1778-1792. [Abstract](#)

[ID#:14-1771] Chen, Shuai-Min, Wu, Mu-En, Sun, Hung-Min, Wang, King-Hang. 2014. **CRFID: An RFID System with a Cloud Database As a Back-end Server**. Future Gener. Comput. Syst.. 30:155–161. [Abstract](#)

[ID#:14-1770] Rahman, Farzana, Ahamed, Sheikh Iqbal. 2014. **Efficient Detection of Counterfeit Products in Large-scale RFID Systems Using Batch Authentication Protocols**. Personal Ubiquitous Comput.. 18:177–188. [Abstract](#)

[ID#:14-1763] Morgado, T.A, Alves, J.M., Marcos, J.S., Maslovski, S.I, Costa, J.R., Fernandes, C.A, Silveirinha, M.G.. 2014. **Spatially Confined UHF RFID Detection With a Metamaterial Grid**. Antennas and Propagation, IEEE Transactions on. 62:378-384. [Abstract](#)

[ID#:14-1759] Sangyup Lee, Choong-Yong Lee, Wonse Jo, Dong-Han Kim. 2014. **An efficient area coverage algorithm using passive RFID system**. Sensors Applications Symposium (SAS), 2014 IEEE. :366-371. [Abstract](#)

[ID#:14-1761] Sabesan, S., Crisp, M.J., Penty, R.V., White, I.H.. 2014. **Wide Area Passive UHF RFID System Using Antenna Diversity Combined With Phase and Frequency Hopping**. Antennas and Propagation, IEEE Transactions on. 62:878-888. [Abstract](#)

[ID#:14-1764] Cook, B.S., Vyas, R., Sangkil Kim, Trang Thai, Taoran Le, Traille, A, Aubert, H., Tentzeris, M.M.. 2014. **RFID-Based Sensors for Zero-Power Autonomous Wireless Sensor Networks**. Sensors Journal, IEEE. 14:2419-2431. [Abstract](#)

[ID#:14-1767] Measel, R., Lester, C.S., Yifei Xu, Primerano, R., Kam, M.. 2014. **Detection performance of spread spectrum signatures for passive, chipless RFID**. RFID (IEEE RFID), 2014 IEEE International Conference on. :55-59. [Abstract](#)

[ID#:14-1762] Goller, M., Feichtenhofer, C., Pinz, A. 2014. **Fusing RFID and computer vision for probabilistic tag localization**. RFID (IEEE RFID), 2014 IEEE International Conference on. :89-96. [Abstract](#)

[ID#:14-1768] Baloch, F., Pendse, R.. 2014. **A New anti-collision protocol for RFID networks**. Wireless Telecommunications Symposium (WTS), 2014. :1-5. [Abstract](#)

[ID#:14-1757] Guizani, S. 2014. **Security applications challenges of RFID technology and possible countermeasures**

Sort by: Author Title Type [Year ▼]

Search results for control systems [Reset Search]

2014

[Hwang:2014:ACP:2600176.2600204] Hwang, JeeHyun, Williams, Laurie, Vouk, Mladen. 2014. **Access Control Policy Evolution: An Empirical Study**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :28:1–28:2. [Abstract](#)

[Biswas:2014:ERW:2600176.2600195] Biswas, Trisha, Lesser, Kendra, Dutta, Rudra, Oishi, Meeko. 2014. **Examining Reliability of Wireless Multihop Network Routing with Linear Systems**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :19:1–19:2. [Abstract](#)

2013

[6547101] Szekeres, L., Payer, M., Tao Wei, Song, D.. 2013. **SoK: Eternal War in Memory**. Security and Privacy (SP), 2013 IEEE Symposium on. :48-62. [Abstract](#)

[700] Benoit Dupont. 2013. **Cybersecurity Futures: How Can We Regulate Emergent Risks?** Technology Innovation Management Review. 3:6-11. [Abstract](#)

[702] Xinxin Fan, Guang Gong. 2013. **Security Challenges in Smart-Grid Metering and Control Systems**. Technology Innovation Management Review. 3:42-49. [Abstract](#)

2012

[6231636] Chasaki, D., Wolf, T.. 2012. **Attacks and Defenses in the Data Plane of Networks**. Dependable and Secure Computing, IEEE Transactions on. 9:798-810. [Abstract](#)

2008

[4700419] Kottenstette, N., Koutsoukos, X., Hall, J., Sztipanovits, J., Antsaklis, P.. 2008. **Passivity-Based Design of Wireless Networked Control Systems for Robustness to Time-Varying Delays**. Real-Time Systems Symposium, 2008. :15-24. [Abstract](#)

1992

[202388] Waknis, P., Karsai, G., Sztipanovits, J.. 1992. **A graphical programming environment for simulation of control and signal processing systems**. Southeastcon '92, Proceedings., IEEE. :447-450vol.1. [Abstract](#)

Sort by: Author Title Type [Year ▼]

Search results for Authentication [Reset Search]

2014

[ID#:14-1758] Urien, Pascal, Piramuthu, Selwyn. 2014. **Elliptic Curve-based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks**. Decis. Support Syst.. 59:28–36. [Abstract](#)

[ID#:14-1771] Chen, Shuai-Min, Wu, Mu-En, Sun, Hung-Min, Wang, King-Hang. 2014. **CRFID: An RFID System with a Cloud Database As a Back-end Server**. Future Gener. Comput. Syst.. 30:155–161. [Abstract](#)

[ID#:14-1770] Rahman, Farzana, Ahamed, Sheikh Iqbal. 2014. **Efficient Detection of Counterfeit Products in Large-scale RFID Systems Using Batch Authentication Protocols**. Personal Ubiquitous Comput.. 18:177–188. [Abstract](#)

[Chakraborty:2014:EKA:2600176.2600210] Chakraborty, Arpan, Harrison, Brent, Yang, Pu, Roberts, David, St. Amant, Robert. 2014. **Exploring Key-level Analytics for Computational Modeling of Typing Behavior**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :34:1–34:2. [Abstract](#)

[ID#:14-1769] Niu, Ben, Zhu, Xiaoyan, Chi, Haotian, Li, Hui. 2014. **Privacy and Authentication Protocol for Mobile RFID Systems**. Wirel. Pers. Commun.. 77:1713–1731. [Abstract](#)

[Escobar:2014:RFS:2600176.2600186] Escobar, Santiago, Meadows, Catherine, Meseguer, José, Santiago, Sonia. 2014. **A Rewriting-based Forwards Semantics for Maude-NPA**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :3:1–3:12. [Abstract](#)

[Yu:2014:SHC:2600176.2600202] Yu, Xianqing, Ning, Peng, Vouk, Mladen A.. 2014. **Securing Hadoop in Cloud**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :26:1–26:2. [Abstract](#)

2013

[702] Xinxin Fan, Guang Gong. 2013. **Security Challenges in Smart-Grid Metering and Control Systems**. Technology Innovation Management Review. 3:42-49. [Abstract](#)

[Mazurek:2013:MPG:2508859.2516726] Mazurek, Michelle L., Komanduri, Saranga, Vidas, Timothy, Bauer, Lujo, Christin, Nicolas, Cranor, Lorrie Faith, Kelley, Patrick Gage, Shay, Richard, Ur, Blase. 2013. **Measuring Password Guessability for an Entire University**. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. :173–186. [Abstract](#)

Sort by: Author Title [Type ▲] Year

Search results for *Authentication* [Reset Search]

Conference Paper

[Chakraborty:2014:EKA:2600176.2600210] Chakraborty, Arpan, Harrison, Brent, Yang, Pu, Roberts, David, St. Amant, Robert. 2014. **Exploring Key-level Analytics for Computational Modeling of Typing Behavior**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :34:1–34:2. [Abstract](#)

[Mazurek:2013:MPG:2508859.2516726] Mazurek, Michelle L., Komanduri, Saranga, Vidas, Timothy, Bauer, Lujo, Christin, Nicolas, Cranor, Lorrie Faith, Kelley, Patrick Gage, Shay, Richard, Ur, Blase. 2013. **Measuring Password Guessability for an Entire University**. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. :173–186. [Abstract](#)

[Escobar:2014:RFS:2600176.2600186] Escobar, Santiago, Meadows, Catherine, Meseguer, José, Santiago, Sonia. 2014. **A Rewriting-based Forwards Semantics for Maude-NPA**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :3:1–3:12. [Abstract](#)

[Yu:2014:SHC:2600176.2600202] Yu, Xianqing, Ning, Peng, Vouk, Mladen A.. 2014. **Securing Hadoop in Cloud**. Proceedings of the 2014 Symposium and Bootcamp on the Science of Security. :26:1–26:2. [Abstract](#)

Journal Article

[ID#:14-1771] Chen, Shuai-Min, Wu, Mu-En, Sun, Hung-Min, Wang, King-Hang. 2014. **CRFID: An RFID System with a Cloud Database As a Back-end Server**. Future Gener. Comput. Syst.. 30:155–161. [Abstract](#)

[ID#:14-1770] Rahman, Farzana, Ahamed, Sheikh Iqbal. 2014. **Efficient Detection of Counterfeit Products in Large-scale RFID Systems Using Batch Authentication Protocols**. Personal Ubiquitous Comput.. 18:177–188. [Abstract](#)

[ID#:14-1758] Urien, Pascal, Piramuthu, Selwyn. 2014. **Elliptic Curve-based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks**. Decis. Support Syst.. 59:28–36. [Abstract](#)

[ID#:14-1769] Niu, Ben, Zhu, Xiaoyan, Chi, Haotian, Li, Hui. 2014. **Privacy and Authentication Protocol for Mobile RFID Systems**. Wirel. Pers. Commun.. 77:1713–1731. [Abstract](#)

[702] Xinxin Fan, Guang Gong. 2013. **Security Challenges in Smart-Grid Metering and Control Systems**. Technology Innovation Management Review. 3:42-49. [Abstract](#)

List **Filter** Import

Show only items where

Author is Anon Type Year Keyword

Filter

List Filter Import

Biblio search

Sort by: Author Title Type [Year ▼]

Filters: Author is Anon [Clear All Filters]

2014

[Anonymous]. 2014. [HotSoS '14: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security](#). Abstract
[Google Scholar](#)

List Filter Import

Biblio search

Sort by: Author Title Type [Year ▼]

Filters: Author is Anon [Clear All Filters]

2014

[Anonymous]. 2014. **HotSoS '14: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security**. Abstract

Google Scholar



STAGING » SCIENCE OF SECURITY VO » BIBLIO LIST

HotSoS '14: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security

VIEW EDIT REVISIONS TRACK TAXONOMY BROADCAST PANELS DEVEL GROUP STATS

- Home
- About
- Calendar
- Activity Stream
- Search
- Videos
- Newsletter
- Members
- Contact Us
- Popular
- Advanced
- Forums
- Files

Submitted by Laurie Williams on Wed, 09/17/2014 - 5:30pm

Title	HotSoS '14: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security
Publication Type	Conference Proceedings
Year of Publication	2014
Conference Name	Symposium and Bootcamp on the Science of Security
Publisher	ACM
Conference Location	Raleigh, NC
ISBN Number	978-1-4503-2907-1
Keywords	Access Control, Architectures, Control, Distributed Systems Security, Foundations, Human and Societal Aspects of Security and Privacy, Modeling, Moving-Target Defense, Network security, phishing, science of security, Social Engineering Attacks
Abstract	<p>The Symposium and Bootcamp on the Science of Security (HotSoS), is a research event centered on the Science of Security (SoS). Following a successful invitational SoS Community Meeting in December 2012, HotSoS 2014 was the first open research event in what we expect will be a continuing series of such events. The key motivation behind developing a Science of Security is to address the fundamental problems of cybersecurity in a principled manner. Security has been intensively studied, but a lot of previous research emphasizes the engineering of specific solutions without first developing the scientific understanding of the problem domain. All too often, security research conveys the flavor of identifying specific threats and removing them in an apparently ad hoc manner. The motivation behind the nascent Science of Security is to understand how computing systems are architected, built, used, and maintained with a view to understanding and addressing security challenges systematically across their life cycle. In particular, two features distinguish the Science of Security from previous research programs on cybersecurity. Scope. The Science of Security considers not just computational artifacts but also incorporates the human, social, and organizational aspects of computing within its purview. Approach. The Science of Security takes a decidedly scientific approach, based on the understanding of empirical evaluation and theoretical foundations as developed in the natural and social sciences, but adapted as appropriate for the "artificial science" (paraphrasing Herb Simon's term) that is computing.</p>
URL	http://dl.acm.org/citation.cfm?id=2600176&picked=prox&cfid=561740640&cftoken=72764684
Citation Key	Williams:2014:2600176

COLLABORATE



Institute for Software Research

World-class, interdisciplinary research with global impact.

Title	HotSoS '14: Proceedings of the 2014 Symposium and Bootcamp on the Science of Security
Publication Type	Conference Proceedings
Year of Publication	2014
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-2907-1
Abstract	The Symposium and Bootcamp on the Science of Security (HotSoS), is a research event centered on the Science of Security (SoS). Following a successful invitational SoS Community Meeting in December 2012, HotSoS 2014 was the first open research event in what we expect will be a continuing series of such events. The key motivation behind developing a Science of Security is to address the fundamental problems of cybersecurity in a principled manner. Security has been intensively studied, but a lot of previous research emphasizes the engineering of specific solutions without first developing the scientific understanding of the problem domain. All too often, security research conveys the flavor of identifying specific threats and removing them in an apparently ad hoc manner. The motivation behind the nascent Science of Security is to understand how computing systems are architected, built, used, and maintained with a view to understanding and addressing security challenges systematically across their life cycle. In particular, two features distinguish the Science of Security from previous research programs on cybersecurity. Scope. The Science of Security considers not just computational artifacts but also incorporates the human, social, and organizational aspects of computing within its purview. Approach. The Science of Security takes a decidedly scientific approach, based on the understanding of empirical evaluation and theoretical foundations as developed in the natural and social sciences, but adapted as appropriate for the <i>artificial</i> sciences. (paraphrasing Herodotus's terminology on composing)
URL	http://dl.acm.org/citation.cfm?id=2600176&picked=prox&cfid=561740640&ctxoken=72764684
Citation Key	Williams-2014-2600176

Proceedings of the 2014 Symposium and Bootcamp on the Science of Security

dl.acm.org/citation.cfm?id=2600176&picked=prox

VPN Me.Finance Me WRUW PB Work Work.META Work.VO TimeHole Udemy REI Spinfuel D8 D8blog

VO-CyP... Issue N... Issue N... Issue N... Issue N... Issue N... Scott D... Procee... >> +

ACM DL DIGITAL LIBRARY Vanderbilt University

SIGN IN SIGN UP

SEARCH

Proceedings of the 2014 Symposium and Bootcamp on the Science of Security

2014 Proceeding

Bibliometrics

- Downloads (6 Weeks): 302
- Downloads (12 Months): 302
- Downloads (cumulative): 302
- Citation Count: 0

Tools and Resources

- TOC Service:
 - Email
 - RSS
- Save to Binder
- Export Formats:
 - BibTeX
 - EndNote
 - ACM Ref
- Share:
 - Facebook
 - Twitter
 - LinkedIn
 - Reddit
 - StumbleUpon
 - Print

General Chairs: **Laurie A. Williams** North Carolina State University
 Program Chairs: **David M. Nicol** University of Illinois, Urbana-Champaign
Munindar P. Singh North Carolina State University

Publication of:

- Conference
- HotSoS '14 Symposium and Bootcamp on the Science of Security (HotSoS)
- Raleigh, NC, USA — April 08 - 09, 2014
- ACM New York, NY, USA ©2014

Feedback | Switch to [single page view](#) (no tabs)

Abstract Source Materials Authors References Cited By Index Terms Publication Reviews Comments Table of Contents

Proceedings of the 2014 Symposium and Bootcamp on the Science of Security

Table of Contents

[In-nimbo sandboxing](#)

Michael Maass, William L. Scherlis, Jonathan Aldrich
 Article No.: 1
 doi>[10.1145/2600176.2600177](#)
 Full text: [PDF](#)

Sandboxes impose a security policy, isolating applications and their components from the rest of a system. While many sandboxing techniques exist, state of the art sandboxes generally perform their functions within the system that is being defended. ... [expand](#)

[Architecture-based self-protection: composing and reasoning about denial-of-service mitigations](#)

Bradley Schmerl, Javier Cámara, Jeffrey Gennari, David Garlan, Paulo Casanova, Gabriel A. Moreno, Thomas J. Glazier, Jeffrey M. Barnes
 Article No.: 2
 doi>[10.1145/2600176.2600181](#)
 Full text: [PDF](#)

Security features are often hardwired into software applications, making it difficult to adapt security responses to reflect changes in runtime context and new attacks. In prior work, we proposed the idea of architecture-based self-protection ... [expand](#)

[A rewriting-based forwards semantics for Maude-NPA](#)

Santiago Escobar, Catherine Meadows, José Meseguer, Sonia Santiago
 Article No.: 3
 doi>[10.1145/2600176.2600186](#)
 Full text: [PDF](#)

The Maude-NRL Protocol Analyzer (Maude-NPA) is a tool for reasoning about the security of cryptographic protocols in which the cryptosystems satisfy different equational properties. It tries to find secrecy or authentication attacks by searching backwards ... [expand](#)

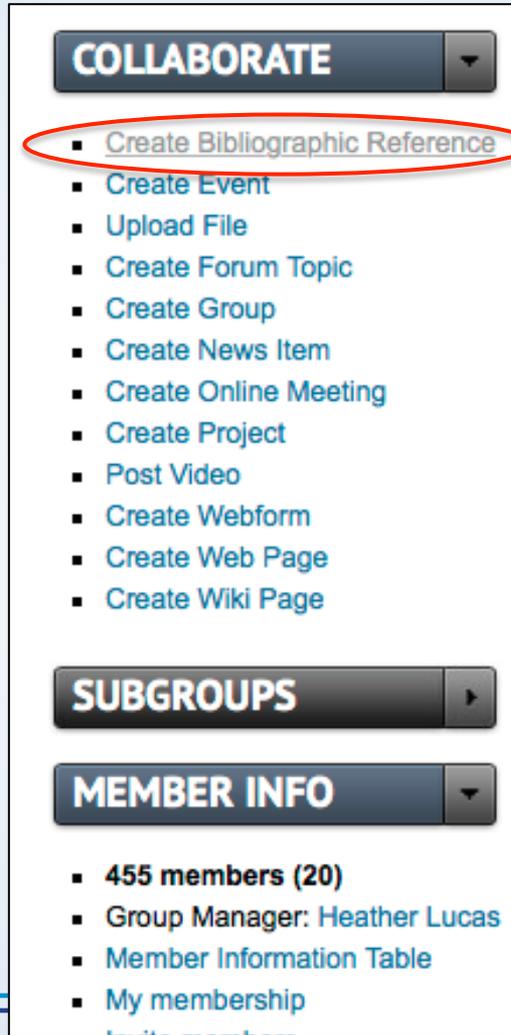
[Open vs. closed systems for accountability](#)

Joan Feigenbaum, Aaron D. Jaggard, Rebecca N. Wright
 Article No.: 4
 doi>[10.1145/2600176.2600179](#)
 Full text: [PDF](#)

The relationship between accountability and identity in online life presents many interesting questions. Here, we first systematically survey the various (directed) relationships among principals, system identities (nyms) used by principals, and actions ... [expand](#)

[Log your CRUD: design principles for software logging mechanisms](#)

New Menu Item



The image shows a vertical menu with three main sections: 'COLLABORATE', 'SUBGROUPS', and 'MEMBER INFO'. The 'COLLABORATE' section is expanded, showing a list of options. The first option, 'Create Bibliographic Reference', is circled in red. The 'SUBGROUPS' section is collapsed, and the 'MEMBER INFO' section is also collapsed.

- COLLABORATE**
 - [Create Bibliographic Reference](#)
 - [Create Event](#)
 - [Upload File](#)
 - [Create Forum Topic](#)
 - [Create Group](#)
 - [Create News Item](#)
 - [Create Online Meeting](#)
 - [Create Project](#)
 - [Post Video](#)
 - [Create Webform](#)
 - [Create Web Page](#)
 - [Create Wiki Page](#)
- SUBGROUPS**
- MEMBER INFO**
 - **455 members (20)**
 - [Group Manager: Heather Lucas](#)
 - [Member Information Table](#)
 - [My membership](#)



Cyber-Physical Systems Virtual Organization

Fostering collaboration among CPS professionals in academia, government, and industry



Tutorial ToC

- [-] Tutorial
 - Navigate this Tutorial
 - Create an Account
 - User Roles
 - [+] Participate in Groups
 - [+] Explore 'My Account'
 - [+] Find Posts and Publications
 - [-] Collaborate with Colleagues
 - Seek out Colleagues
 - Contribute to Forum Discussions
 - Create a Global Forum Announcement
 - Create a Calendar Event
 - Create Event Invitations
 - [+] Online Meetings
 - Upload a File
 - Activity Messaging
 - Comment on Files and Events
 - Use the Chat Feature
 - Create a News Item
 - Create a Group Project
 - Post a Video
 - Create Wiki Pages
 - Create a Bibliographic Reference
 - Create a Tearline
 - Search, Sort, and Filter Biblios
 - Logging and Viewing Revisions
 - [+] Form and Manage Groups
 - [+] Appendix: The VO Architecture
 - Appendix: FAQ
 - Appendix: Glossary
 - Contact Support

CPS-VO » TUTORIAL » COLLABORATE WITH COLLEAGUES

Create a Bibliographic Reference

VIEW EDIT REVISIONS TRACK CLONE TAXONOMY BROADCAST PANELS DEVEL

Submitted by [akarns](#) on Thu, 09/11/2014 - 12:36pm

As a member of the CPS-VO, you can create a bibliographic reference that can be added to the groups of which you are a member. If you are a "Trusted User", you have permissions to import a batch of bibliographic references using a BibTeX file.

You can create single bibliographic references by following the instructions in the table below.

	<p>Select the "Create Bibliographic Reference" link in the "Collaborate" toggle menu which is located in the lower left sidebar on your group page.</p>
	<ol style="list-style-type: none"> 1. Paste the BibTeX code copied from a digital library <ol style="list-style-type: none"> a. Paste BibTeX code into expanded "Paste BibTeX" text area. b. Select "Populate using BibTeX" c. You will be taken to an edit page where you may review the information in the fields that have been populated and make any necessary changes d. Select the "Save" button to the bottom left of the editing window. Your bibliography reference will populate on the biblio page of the group(s) you selected. <i>(The group which you created the bibliography reference from is selected by default).</i>
	<ol style="list-style-type: none"> 2. Enter the publication details manually <ol style="list-style-type: none"> a. Select "Publication Type" from the dropdown menu b. Continue to fill in details as form fields emerge
	<ol style="list-style-type: none"> c. Select "Authors", "Other Biblio Fields", and/or other pertinent information from the gray vertical menu at the bottom of the form. d. Select the "Save" button to the bottom left of the editing window. Your bibliography reference will populate on the biblio page of the group(s) you selected. <i>(The group which you created the bibliography reference from is selected by default).</i>

Trusted users can import a BibTeX file to create a batch of bibliographic references. You should use batch processing if your import file contains more than about 20 records, or if you are experiencing script timeouts during import. See instructions in the table below.

Importing New References

<http://en.wikipedia.org/wiki/BibTeX>

The screenshot shows a web interface with a navigation bar containing 'List', 'Filter', and 'Import' buttons. The 'Import' button is circled in red. Below the navigation bar, there is a section for 'Import file(s):' with a 'Choose Files' button and a file named 'xlayer-security.bib'. A note states: 'If you are using FireFox 3.6 or newer, you may select multiple files for import (they must all be of the same type)'. Below this is a 'File Type:' dropdown menu set to 'BibTeX'. There is a checked checkbox for 'Batch Process' with a note: 'You should use batch processing if your import file contains more than about 20 records, or if you are experiencing script timeouts during import'. A 'Groups' section is visible, showing a list of audience groups: 'Secure and Trustworthy Cyberspace Principal Investigators' Meeting (2012)', 'Secure Data Bank', 'Software Certification Consortium', and 'SoS Label Working Group'. The 'Public' checkbox is unchecked. At the bottom, there is a 'Disable notifications' checkbox (checked) and an 'Import' button.

The screenshot shows a Vim editor window titled 'xlayer-security.bib (~/.Downloads/biblio) - VIM'. The editor displays BibTeX code for two references. The first reference is an entry from the 'INPROCEEDINGS' database with fields for title, author, booktitle, year, month, pages, and doi. The second reference is an 'ARTICLE' with fields for title, author, journal, year, month, volume, number, pages, doi, and ISSN. The code is as follows:

```
@INPROCEEDINGS{ID#14-1627,
  title = {Security attack mitigation framework for the cloud},
  author = {Datta, E. and Goyal, N.},
  booktitle = {Reliability and Maintainability Symposium (RAMS), 2014 Annual},
  year = {2014},
  month = {Jan},
  pages = {1-6},
  doi = {10.1109/RAMS.2014.6798457},

  abstract = {Cloud computing brings in a lot of advantages for enterprise IT infrastructure; virtualization technology, which is the backbone of cloud, provides easy consolidation of resources, reduction of cost, space and management efforts. However, security of critical and private data is a major concern which still keeps back a lot of customers from switching over from their traditional in-house IT infrastructure to a cloud service. Existence of techniques to physically locate a virtual machine in the cloud, proliferation of software vulnerability exploits and cross-channel attacks in-between virtual machines, all of these together increase the risk of business data leaks and privacy losses. This work proposes a framework to mitigate such risks and engineer customer trust towards enterprise cloud computing. Everyday new vulnerabilities are being discovered even in well-engineered software products and the hacking techniques are getting sophisticated over time. In this scenario, absolute guarantee of security in enterprise wide information processing system seems a remote possibility; software systems in the cloud are vulnerable to security attacks. Practical solution for the security problems lies in well-engineered attack mitigation plan. At the positive side, cloud computing has emerged as a collective infrastructure which can be effectively used to mitigate the attacks if an appropriate defense framework is in place. We propose such an attack mitigation framework for the cloud. Software vulnerabilities in the cloud have different severities and different impacts on the security parameters (confidentiality, integrity, and availability). By using Markov model, we continuously monitor and quantify the risk of compromise in different security parameters (e.g., change in the potential to compromise the data confidentiality). Whenever, there is a significant change in risk, our framework would facilitate the tenants to calculate the Mean Time to Security Failure (MTTSF) cloud and allow them to adopt a dynamic mitigation plan. This framework is an add-on security layer in the cloud resource manager and it could improve the customer trust on enterprise cloud solutions.},

  url = {http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=6798457&number=6798433},
  keywords = {Cross Layer Security, Markov processes;cloud computing;security of data;virtualisation;MTTSF cloud;Markov model;attack mitigation plan;availability parameter;business data leaks;cloud resource manager;cloud service;confidentiality parameter;cross-channel attacks;customer trust;enterprise IT infrastructure;enterprise cloud computing;enterprise cloud solutions;enterprise wide information processing system;hacking techniques;information technology;integrity parameter;mean time to security failure;privacy losses;private data security;resource consolidation;security attack mitigation framework;security guarantee;software products;software vulnerabilities;software vulnerability exploits;virtual machine;virtualization technology;Cloud computing;Companies;Security;Silicon;Virtual machining;Attack Graphs;Cloud computing;Markov Chain;Security;Security Administration},
}

@ARTICLE{ID#14-1628,
  title={A Survey of Cross-Layer Designs in Wireless Networks},
  author={Bo Fu and Yang Xiao and Hongmei Deng and Hui Zeng},
  journal={Communications Surveys Tutorials, IEEE},
  year={2014},
  month={First},
  volume={16},
  number={1},
  pages={110-126},
  doi={10.1109/SURV.2013.001313.00231},
  ISSN={1553-877X},
}
```

* Only 'trusted users' are allowed to import batches of references!



Institute for Software Integrated Systems
World-class, interdisciplinary research with global impact.



VANDERBILT UNIVERSITY



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

Languages 

العربية
Català
Deutsch
فارسی
Français
日本語
Português
Русский
中文

 Edit links

Article Talk

Read Edit View history

Search

Reference management software

From Wikipedia, the free encyclopedia

Reference management software, **citation management software** or **personal bibliographic management software** is software for scholars and authors to use for recording and utilising bibliographic citations (references).^[1] Once a citation has been recorded, it can be used time and again in generating bibliographies, such as lists of references in scholarly books, articles and essays. The development of reference management packages has been driven by the rapid expansion of scientific literature.

These software packages normally consist of a database in which full bibliographic references can be entered, plus a system for generating selective lists of articles in the different formats required by publishers and scholarly journals. Modern reference management packages can usually be integrated with word processors so that a reference list in the appropriate format is produced automatically as an article is written, reducing the risk that a cited source is not included in the reference list. They will also have a facility for importing the details of publications from bibliographic databases.

Reference management software does not do the same job as a bibliographic database, which tries to list all articles published in a particular discipline or group of disciplines; examples are those provided by Ovid Technologies (e.g. Medline), the Institute for Scientific Information (e.g. Web of Knowledge) or monodisciplinary learned societies e.g. the American Psychological Association (PsycINFO). These databases are large and have to be housed on major server installations. Reference management software collects a much smaller database, of the publications that have been used or are likely to be used by a particular author or group, and such a database can easily be housed on an individual's personal computer.

Apart from managing references, most reference management software also enables users to search references from online libraries. These online libraries are usually based on Z39.50 public protocol. Users just need to specify the IP address, database name and keywords to start a Z39.50 search. It is quicker and more efficient than a web browser. However, Z39.50 is a little out of date. Some popular scientific websites, such as Google Scholar, IEEE Xplore and arXiv, do not support the Z39.50 protocol.

Contents [hide]

- Comparison of reference management software
- Reference management in Wikipedia
- Alternatives to reference management software
- Reference checkers
- Citation creators
- See also
- References
- External links

Comparison of reference management software [edit]

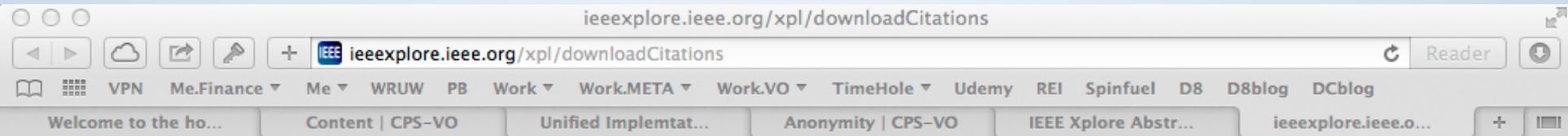
Main article: Comparison of reference management software

Discovering Citations

Google search results for "Security applications challenges of RFID technology and possible countermeasures". The search bar shows the query and a magnifying glass icon. Below the search bar are tabs for Web, News, Shopping, Images, Videos, More, and Search tools. The results show about 72 results in 0.43 seconds. The top result is from IEEE Xplore, titled "challenges of technology - IEEE Xplore". Other results include "Security applications challenges of RFID technology and possible countermeasures" from IEEE Projects for Engineers, "Radio Frequency Identification | CPS-VO" from cps-vo.org, and "Need Help? - IEEE Xplore - Search Results" from ieeeexplore.us. The bottom result is "Skip to Main Content - IEEE Xplore - Search Results" from ieeeexplore.us.

Abstract page for "Security applications challenges of RFID technology and possible countermeasures" by Guizani, S. The page includes a "Full Text as PDF" button and a "Full Text in HTML" button. The author is listed as Guizani, S. ; Coll. of Eng., Alfaisal Univ., Riyadh, Saudi Arabia. The abstract text discusses the challenges of RFID technology and possible countermeasures. A "Download Citations" dialog box is open, showing options to download citations in various formats (BibTeX, RefWorks, EndNote, ProCite, RefMan) and to include citation information (Citation Only or Citation & Abstract). The dialog box also includes a "Download Citation" button and a "Cancel" button. The abstract text is partially visible on the right side of the page.

Cut



```
@INPROCEEDINGS{6785340,  
author={Ren-Hung Hwang and Fu-Hui Huang},  
booktitle={Computing, Networking and Communications (ICNC), 2014 International Conference on},  
title={SocialCloaking: A distributed architecture for K-anonymity location privacy protection},  
year={2014},  
month={Feb},  
pages={247-251},  
abstract={As location information becomes commonly available in smart phones, applications of Location Based Service (LBS) has also become very popular and are widely used by smart phone users. Since the query of LBS contains user's location, it raises a privacy concern of exposure of user's location. K-anonymity is a commonly adopted technique for location privacy protection. In the literature, a centralized architecture which consists of a trusted anonymity server is widely adopted. However, this approach exhibits several apparent weaknesses, such as single point of failure, performance bottleneck, serious security threats, and not trustable to users, etc. In this paper, we re-examine the location privacy protection problem in LBS applications. We first provide an overview of the problem itself, to include types of query, privacy protection methods, adversary models, system architectures, and their related works in the literature. We then discuss the challenges of adopting a distributed architecture which does not need to set up a trusted anonymity server and propose a solution by combining unique features of structured peer-to-peer architecture and trust relationships among users of their on-line social networking relations.},  
keywords={data privacy;mobile computing;query processing;social networking (online);trusted computing;K-anonymity location privacy protection;LBS query;SocialCloaking;adversary model;centralized architecture;distributed architecture;failure point;location information;location-based service;on-line social networking relation;security threat;smart phones;structured peer-to-peer architecture;system architecture;trust relationship;trusted anonymity server;user location;Computer architecture;Mobile communication;Mobile handsets;Peer-to-peer computing;Privacy;Servers;Trajectory;Distributed Anonymity Server Architecture;Location Based Service;Location Privacy;Peer-to-Peer;Social Networking},  
doi={10.1109/ICCNC.2014.6785340},}
```



Paste & Customize Keywords

The screenshot displays the JabRef application interface. The main window shows a table of database entries with columns for #, Entry..., Author, Title, Year, Journal, Owner, Timestamp, and BibTeXkey. A 'Manage keywords' dialog box is open, showing a list of keywords for selected entries, with 'Acoustic Fingerprinting' highlighted. A help window titled 'The JabRef main window' is also visible, providing instructions on how to use the software.

The JabRef main window

Note: most menu actions referred in the following have keyboard shortcuts, and many are available from the toolbar. The keyboard shortcuts are found in the pull-down menus.

This is the main window from where you work with your databases. Below the menubar and the toolbar is a tabbed pane containing a panel for each of your currently open databases. When you select one of these panels, a table appears, listing all the database's entries, as well as a configurable selection of their fields.

- You decide which fields are shown in the table by checking the fields you want to see in the Preferences dialog.
- Double-click a line of the table to edit the entry content. You can navigate the table with the arrow keys.
- The table is sorted according to a set of fields of your choosing. The default sort order can be set up in Preferences -> Entry table, but to more quickly change the order, click the header of a column to set it as the primary sort criterion, or reverse the sorting if it is already set. Another click will deselect the column as sorting criterion. Hold down CONTROL and click a column to add, reverse or remove it as a sub-criterion after the primary column. You can add an arbitrary number of

Manage keywords

Keywords of selected entries

- Display keywords appearing in ALL entries
- Display keywords appearing in ANY entry

Acoustic Fingerprinting

Remove

Add

OK Cancel

year = {2014},
pages = {644-648},

recognition system must address concurrent dimension must remain to allow fast to restate these objectives as a problem. On top of this dictionary-based red sparsity model in the form of a the sparse support. A practical suboptimal ited and evaluated on robustness and t some existing methods can be seen orithm and that the general framework f a Pareto-like continuum. }, rier.de),
SP.2014.6854166),
Sparse Representation, Test Bulk Keyword
amp/stamp.jsp?tp=&arnumber=6854166&isnumber=6853544)
(lin),
information maximization for content identification),
,
er presents a novel design of content fingerprints based on f the mutual information across the distortion channel. oration bottleneck method to optimize the filters that generate these fingerprints. A greedy optimization to select filters from a dictionary and allocate fingerprint the performance of this method for audio fingerprinting antial improvements over existing learning based fingerprints.
(http://dblp.uni-trier.de),
f/icassp/2014),
org/10.1109/ICASSP.2014.6854314),
Fingerprinting, Audio fingerprinting, Content Identification, ttleneck, Information maximization, Test Bulk Keyword
lore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6854314&isnumber=6853544)
603,
i and Bob Coover and Jinyu Han),
ingerprinting system for live version identification using ng techniques),

Status: Saved database '/Users/vbuskirk/Downloads/biblio/anonymity.bib'.

Import

List Filter **Import**

Import file(s):

xlayer-security.bib

If you are using FireFox 3.6 or newer, you may select multiple files for import (they must all be of the same type).

File Type: *

BibTex

Batch Process

You should use batch processing if your import file contains more than about 20 records, or if you are experiencing script timeouts during import

▼ Groups

Audience:

Secure and Trustworthy Cyberspace Principal Investigators' Meeting (2012)

Secure Data Bank

Software Certification Consortium

SoS Lablet Working Group

Show this post in these groups.

Public

Show this post to everyone, or only to members of the groups checked above. Posts without any groups are always public.

Disable notifications



Batch Editing Biblio Nodes

CPS-VO » SECURE DATA BANK » ADVANCED

Advanced

EDIT GROUP REVISIONS TRACK CLONE TAXONOMY BROADCAST PANELS DEVEL GROUP STATS

Home
SoS Newsletter
Reference
Training
Malicious Cyber Discovery
Publications
Advanced
Forums
Files

Secure Data Bank
(Edit view)

Node: Type
Is one of
Biblio

Node: Title
Contains

Node: Body
Contains

Public <Any>
Published <Any>
Promoted to front page <Any>
Sticky <Any>

Taxonomy: Term
Contains any word

Items per page: 100 Apply Reset

Bulk operations
- Choose an operation -
 Disable Notifications
Log message:

Execute

MEMBER INFO

- 15 members
- Group Manager: srees
- Member Information Table
- My membership
- Invite members

Title	Type	Author	Post date	Published	Post: Public	Taxonomy terms	Edit link
0 items selected. Clear selection							
<input type="checkbox"/> Swarm Intelligence Security new	Page	Daniel Wolf	Sep 11 2014 - 11:25pm	Yes	Yes		edit
<input type="checkbox"/> Quantum Computing (Update) new	Page	Daniel Wolf	Sep 11 2014 - 11:23pm	Yes	Yes		edit
<input type="checkbox"/> Internet of Things (Part 1) new	Page	Daniel Wolf	Sep 11 2014 - 11:21pm	Yes	Yes		edit
<input type="checkbox"/> Threat Vectors new	Page	Daniel Wolf	Sep 11 2014 - 11:18pm	Yes	Yes		edit
<input type="checkbox"/> Safe Coding new	Page	Daniel Wolf	Sep 11 2014 - 11:16pm	Yes	Yes		edit
<input type="checkbox"/> Virtual Machines new	Page	Daniel Wolf	Sep 9 2014 - 6:46pm	Yes	Yes		edit
<input type="checkbox"/> Theoretical Cryptography new	Page	Daniel Wolf	Sep 9 2014 - 6:36pm	Yes	Yes		edit

Questions / Comments ?

Agenda

- *Support Bibliographic References*
- **Initial Group Statistics Feature Released**
- *Graphical Sitemaps are in Development*





SoS Lablet Reports

STAGING

SoS Lablet Reports

 EDIT GROUP TRACK CLONE TAXONOMY BROADCAST PANELS DEVELOP **GROUP STATS**

Home →

All

CMU

NCSU

UIUC

UMD

Members

Modboard

Forums

Files

COLLABORATE ▶

SUBGROUPS ▶

MEMBER INFO ▼

- 101 members

Announcements

Quarterly reports are due to the NSA on October 10, 2014.

Points of Contact

[Stephanie Yannacci](#) - Contracting Officer Representative

[Heather Lucas](#) - SoS Virtual Organization Lead

Getting started

Each Lablet has a designated menu tab where new reports will be initialized and previous reports can be found. New reports will be initialized by the business manager.

Editing Reports:

- Navigate to your Lablets menu tab
- Use the filters to find your report
- Click on the report title
- Review the report content
- Select [EDIT] from the menu located just above the content
- Enter details in the appropriate text areas
- Review 'Vocabularies' to ensure the correct quarter has been selected and the correct hard problems have been identified
- Change the 'Document Master' to the next person in the workflow*
- Enter a log message (These are included in the notification emails that are sent out as well as the report's revision history)
- Save

*Each Lablet may determine the workflow suits them best. The report is passed to the next person in the workflow by changing the document master.

Detailed tutorial instructions may be found [here](#).



SoS Lablet Reports

STAGING » SCIENCE OF SECURITY VO » SOS LABELT REPORTS » GROUP STATS

Group Stats

GROUP STATS

- Home
- All
- CMU
- NCSU
- UIUC
- UMD
- Members
- Modboard
- Forums
- Files

COLLABORATE

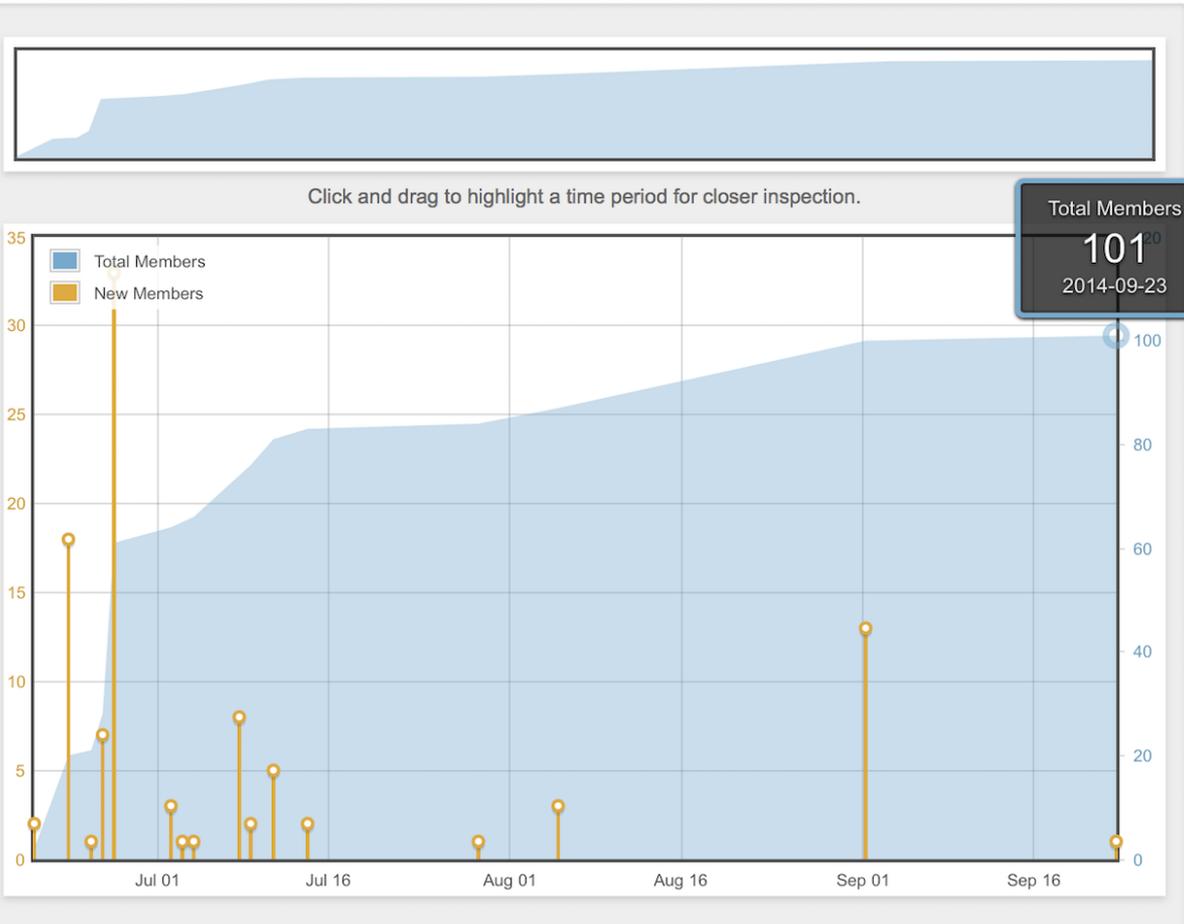
SUBGROUPS

MEMBER INFO

- **101 members**
- Group Manager: [stuart](#)
- [Member Information Table](#)
- [My membership](#)
- [Invite members](#)

Member Stats | [Invite Stats](#) | [Node Creation Stats](#) | [Node Activity Stats](#)

[Download this data as a Microsoft Excel compatible CSV file.](#)



Total Members
101
2014-09-23

Agenda

- *Support Bibliographic References*
- *Initial Group Statistics Feature Released*
- **Graphical Sitemaps are in Development**



LIVE DEMO

APPENDIX

Agenda

- *Support for Bibliographic References*
- *Initial Group Statistics Feature Released*
- *Graphical Sitemaps are in Development*

- **Tearlines are Deployed**



http://cps-vo.org/group/sos/lablet/reporting

The screenshot shows the 'SoS Lablet Reports' web application. The page title is 'SoS Lablet Reports' and the breadcrumb is 'CPS-VO > SCIENCE OF SECURITY VO > SOS LABLET REPORTS > ALL'. The interface includes a navigation sidebar on the left with options like Home, All, CMU, NCSU, UIUC, UMD, Members, Modboard, Forums, and Files. The main content area features a table with columns for Quarter, Status, Lablet, Hard Problem(s), Title, Status, Created, Updated, and Public. The table lists several reports, including 'SoS Quarterly Summary Report - CMU', 'Verification of Hyperproperties - UMD', 'Trustworthy and Composable Software Systems with Contracts - UMD', 'Empirical Models for Vulnerability Exploits - UMD', 'Human Behavior and Cyber Vulnerabilities - UMD', 'Does the Presence of Honest Users Affect Intruders' Behavior? - UMD', and 'User-Centered Design for Security - UMD'. The interface also includes a search bar, a 'Log out' button, and a 'Feedback' button.

Project Title	Lablet	Quarter	Hard Problem(s)	Status	Created	Updated	Public
<input type="checkbox"/> SoS Quarterly Summary Report - CMU updated	CMU	Oct'14	Scalability and Compossibility, Policy-Governed Secure Collaboration, Metrics, Resilient Architectures, Human Behavior	NSA Program Manager	Oct 14 2014 - 5:07pm	Oct 15 2014 - 9:01am	Yes
<input type="checkbox"/> Verification of Hyperproperties - UMD updated	UMD	Oct'14	Scalability and Compossibility	NSA Program Manager	Oct 10 2014 - 1:26pm	Oct 15 2014 - 12:49pm	No
<input type="checkbox"/> Trustworthy and Composable Software Systems with Contracts - UMD updated	UMD	Oct'14	Scalability and Compossibility	NSA Program Manager	Oct 10 2014 - 1:26pm	Oct 15 2014 - 1:10pm	No
<input type="checkbox"/> Empirical Models for Vulnerability Exploits - UMD updated	UMD	Oct'14	Metrics	NSA Program Manager	Oct 10 2014 - 1:25pm	Oct 15 2014 - 1:03pm	No
<input type="checkbox"/> Human Behavior and Cyber Vulnerabilities - UMD updated	UMD	Oct'14	Metrics, Human Behavior	NSA Program Manager	Oct 10 2014 - 1:24pm	Oct 15 2014 - 1:09pm	No
<input type="checkbox"/> Does the Presence of Honest Users Affect Intruders' Behavior? - UMD updated	UMD	Oct'14	Human Behavior	NSA Program Manager	Oct 10 2014 - 1:23pm	Oct 15 2014 - 1:16pm	No
<input type="checkbox"/> User-Centered Design for Security - UMD	UMD	Oct'14	Scalability and Compossibility, Policy-Governed Secure Collaboration, Metrics, Resilient Architectures, Human Behavior	Lead PI	Oct 10 2014 - 1:16pm	Oct 14 2014 - 1:16pm	No

* See <http://cps-vo.org/node/13494> for an intro/review of Tearlines

Proposal for Linking Group Project Descriptions to Quarterly Reports

The screenshot shows a web browser displaying the 'Projects | CPS-VO' page. The URL is 'cps-vo.org/group/sos/lablet/ncsu/projects'. The page header includes navigation links like 'Welcome...', 'Content', 'Unified Im...', 'Anonymity...', 'IEEE Xplor...', 'All | CPS-VO', 'Reporting...', and 'Projects...'. Below the header is a banner for the 'Science of Security Lablet Research Initiative' with a logo featuring a padlock and the letters 'SOS'. The main content area is titled 'CPS-VO » SCIENCE OF SECURITY VO » NSCU SCIENCE OF SECURITY LABLET RESEARCH INITIATIVE » PROJECTS' and 'Projects'. A sidebar on the left contains navigation options: Home, Projects (selected), Past Projects, Activity Stream, Members, Content Editor, Forums, and Files. Below these are buttons for 'COLLABORATE', 'SUBGROUPS', and 'MEMBER INFO'. The 'MEMBER INFO' section shows 53 members, with Group Manager Laurie Williams. The main content area contains a table of project titles and descriptions.

Project Title	Description
An Investigation of Scientific Principles Involved in Attack...	High-assurance systems, for which security is especially critical, should be designed to a) auto-detect attacks (even when correlated); b) isolate or interfere with the activities of a potential or actual attack; and (3) recover a secure state and...
Understanding the Fundamental Limits in Passive Inference of...	It is widely accepted that wireless channels decorrelate fast over space, and half a wavelength is the key distance metric used in existing wireless physical layer security mechanisms for security assurance. We believe that this channel correlation model...
Modeling the risk of user behavior on mobile devices	It is already true that the majority of users' computing experience is a mobile one. Unfortunately that mobile experience is also more risky; users are often multitasking, hurrying or uncomfortable, leading them to make poor decisions. Our goal is to use...
An Adoption Theory of Secure Software Development Tools	Programmers interact with a variety of tools that help them do their jobs, from "undo" to FindBugs' security warnings to entire development environments. However, programmers typically know about only a small subset of tools that are available, even when...
Low-level Analytics Models of Cognition for Novel Security P...	A key concern in security is identifying differences between human users and "bot" programs that emulate humans. Users with malicious intent will often utilize wide-spread computational attacks in order to exploit systems and gain control. Conventional...
Normative Trust Toward a Principled Basis for Enabling Trust...	This project seeks to develop a deeper understanding of trust than is supported by current methods, which largely disregard the underlying relationships based on which people trust or not trust each other. Accordingly, we begin from the notion of what we...
A Science of Timing Channels in Modern Cloud Environments	The eventual goal of our research is to develop a principled design for comprehensively mitigating access-driven timing channels in modern compute clouds, particularly of the "infrastructure as a service" (IaaS) variety. This type of cloud permits the...
Studying Latency and Stability of Closed-Loop Sensing-Based...	In this project, our focus is on understanding a class of security systems in analytical terms at a certain level of abstraction. Specifically, the systems we intend to look at are (I) multipath routing (for increasing reliability), (II) dynamic...
Spatiotemporal Security Analytics and Human Cognition	A key concern in security is identifying differences between human users and "bot" programs that emulate humans. Users with malicious intent will often utilize wide-spread computational attacks in order to exploit systems and gain control. Conventional...
Towards a Scientific Basis for User Center Security Design	Human interaction is an integral part of any system. Users have daily interactions with a system and make many decisions that affect the overall state of security. The fallibility of users has been shown but there is little research focused on the...
Quantifying Mobile Malware Threats	In this project, we aim to systematize the knowledge base about existing mobile malware (especially on Android) and quantify their threats so that we can develop principled solutions to provably determine their presence or absence in existing marketplaces...
An Investigation of Scientific Principles Involved in Softwa...	Fault elimination part of software security engineering hinges on pro-active detection of potential vulnerabilities during software development stages. This project is currently working on a) an attack operational profile definition based on know...
Argumentation as a Basis for Reasoning about Security	This project involves the application of argumentation techniques for reasoning about policies, and security decisions in particular. Specifically, we are producing a security-enhanced argumentation framework that (a) provides not only inferences to draw...
Shared Perceptual Visualizations For System Security	We are studying how to harness human visual perception in information display, with a specific focus on ways to combine layers of data in a common, well-understood display framework. Our visualization techniques are designed to present data in ways that...
Empirical Privacy and Empirical Utility of Anonymized Data	TEAM Pi Ting Yu Students: Xi Gong, Entong Shen
Improving the Usability of Security Requirements by Software...	This project aims to discover general theory to explain what cues security experts use to decide when to apply security requirements and how to present those cues in the form of security patterns to novice designers in a way that yields improved security...
Software Security Metrics	Software security metrics are commonly considered as one critical component of science of security. We propose to investigate existing metrics and new security metrics to predict which code locations are likely to contain vulnerabilities. In particular...
Developing a User Profile to Predict Phishing Susceptibility...	Phishing has become a serious threat in the past several years, and combating it is increasingly important. Why do certain people get phished and others do not? In this project, we aim to identify the factors that cause people to be susceptible and...



1. Define a 'Projects' Taxonomy

Terms in SoS LR: Project | Staging

cpsvo-staging.isis.vanderbilt.edu/node/13263/og/vocab/terms/261

Group Stats | CPS-VO | SoS Quarterly Summary Report - UMD | Staging | Terms in SoS LR: Project | Staging

SoS Lablet Reports

STAGING » SCIENCE OF SECURITY VO » SOS LABELT REPORTS » TAXONOMY

Taxonomy

GROUP STATS

Home | All | CMU | NCSU | UIUC | UMD | Members | Modboard | Forums | Files

List | **Add term**

Name	Operations
+ CMU	edit
+ A Language and Framework for Development of Secure Mobile Applications	edit
+ Epistemic Models for Security	edit
+ Geo-Temporal Characterization of Security Threats	edit
+ Highly Configurable Systems	edit
+ Multi-Model Run-Time Security Analysis	edit
+ Race Vulnerability Study and Hybrid Race Detection	edit
+ Science of Secure Frameworks	edit
+ Secure Composition of systems and Policies	edit
+ Security Reasoning for Distributed Systems with Uncertainty	edit
+ Usable Formal Methods for the Design and Composition of Security and Privacy Policies	edit
+ USE: User Security Behavior	edit
+ NCSU	edit
+ A Human Information-Processing Analysis of Online Deception Detection	edit
+ Attack Surface and Defense-in-Depth Metrics	edit
+ Automated Synthesis of Resilient Architectures	edit
+ Formal Specification and Analysis of Security-Critical Norms and Policies	edit

COLLABORATE

Feedback

RSITY

2. Tag every Quarterly Project Report correctly with it's 'Project X' term from this new Taxonomy





Science of Security Lablet Research Initiative



STAGING » GROUPS » UMD SCIENCE OF SECURITY LABLET RESEARCH INITIATIVE

Reasoning about Protocols with Human Participants

VIEW **EDIT** REVISIONS TRACK CLONE TAXONOMY BROADCAST PANELS DEVEL GROUP STATS

Home

Submitted by [jkatz](#) on Thu, 04/10/2014 - 2:20pm

Projects →

Existing protocol analysis are typically confined to the electronic messages exchanged among computer systems running at the endpoints. In this project we take a broader view in which a protocol additionally encompasses both physical technologies as well as human participants. Our goal is to develop techniques for analyzing and proving security of protocols involving all these entities, with open-audit, remote voting systems such as Remotegrity as our starting point.

Activity Stream

Members

PI



[jkatz](#)

Content Editor

Forums

Files

Co-PI(s)



[poorvi](#)

COLLABORATE

SUBGROUPS

- Science of Security VO
 - [NCSU Science of Security Lablet Research Initiative](#)
 - [CMU Science of Security Lablet Research Initiative](#)
 - [UIUC Science of Security Lablet Research Initiative](#)
 - [Moving Target Research](#)
 - [SoS Working Group](#)
 - [SoS-VO Training Group](#)
 - [Symposium and Bootcamp](#)

Related Artifacts

Quarterly Project Reports

[Reasoning about Protocols with Human Participants](#)

[Reasoning about Protocols with Human Participants](#)

83 reads | [PDF version](#) | [Printer-friendly version](#)



Utilize 'Related Artifacts' Feature

Related Artifacts

Vocabulary	Terms	Alias
<p>+ VOCABULARY:</p> <p>SoS LR: Project</p>	<p>TERMS:</p> <ul style="list-style-type: none"><input type="radio"/> CMU<input type="radio"/> NCSU<input type="radio"/> UIUC<input checked="" type="radio"/> UMD<input type="radio"/> Does the Presence of Honest Users Affect Intrud...<input type="radio"/> Empirical Models for Vulnerability Exploits<input type="radio"/> Human Behavior and Cyber Vulnerabilities<input checked="" type="radio"/> Reasoning about Protocols with Human Participants<input type="radio"/> Trust, Recommendation Systems, and Collaboration<input type="radio"/> Trustworthy and Composable Software Systems wit...<input type="radio"/> Understanding Developers' Reasoning about Priva...<input type="radio"/> User-Centered Design for Security<input type="radio"/> Verification of Hyperproperties	<p>ALIAS:</p> <p>Quarterly Project Reports</p>

Add more values





STAGING » GROUPS » UMD SCIENCE OF SECURITY LABLET RESEARCH INITIATIVE

Reasoning about Protocols with Human Participants

VIEW EDIT REVISIONS TRACK CLONE TAXONOMY BROADCAST PANELS DEVEL GROUP STATS

- Home
- Projects →
- Activity Stream
- Members
- Content Editor
- Forums
- Files

Submitted by [jkatz](#) on Thu, 04/10/2014 - 2:20pm

Existing protocol analysis are typically confined to the electronic messages exchanged among computer systems running at the endpoints. In this project we take a broader view in which a protocol additionally encompasses both physical technologies as well as human participants. Our goal is to develop techniques for analyzing and proving security of protocols involving all these entities, with open-audit, remote voting systems such as Remotegrity as our starting point.

PI



[jkatz](#)

Co-PI(s)



[poorvi](#)

COLLABORATE

SUBGROUPS

- Science of Security VO
 - NCSU Science of Security Lablet Research Initiative
 - CMU Science of Security Lablet Research Initiative
 - UIUC Science of Security Lablet Research Initiative
 - Moving Target Research
 - SoS Working Group
 - SoS-VO Training Group
 - Symposium and Bootcamp

Related Artifacts

- Quarterly Project Reports
 - Reasoning about Protocols with Human Participants
 - Reasoning about Protocols with Human Participants

83 reads | PDF version | Printer-friendly version