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

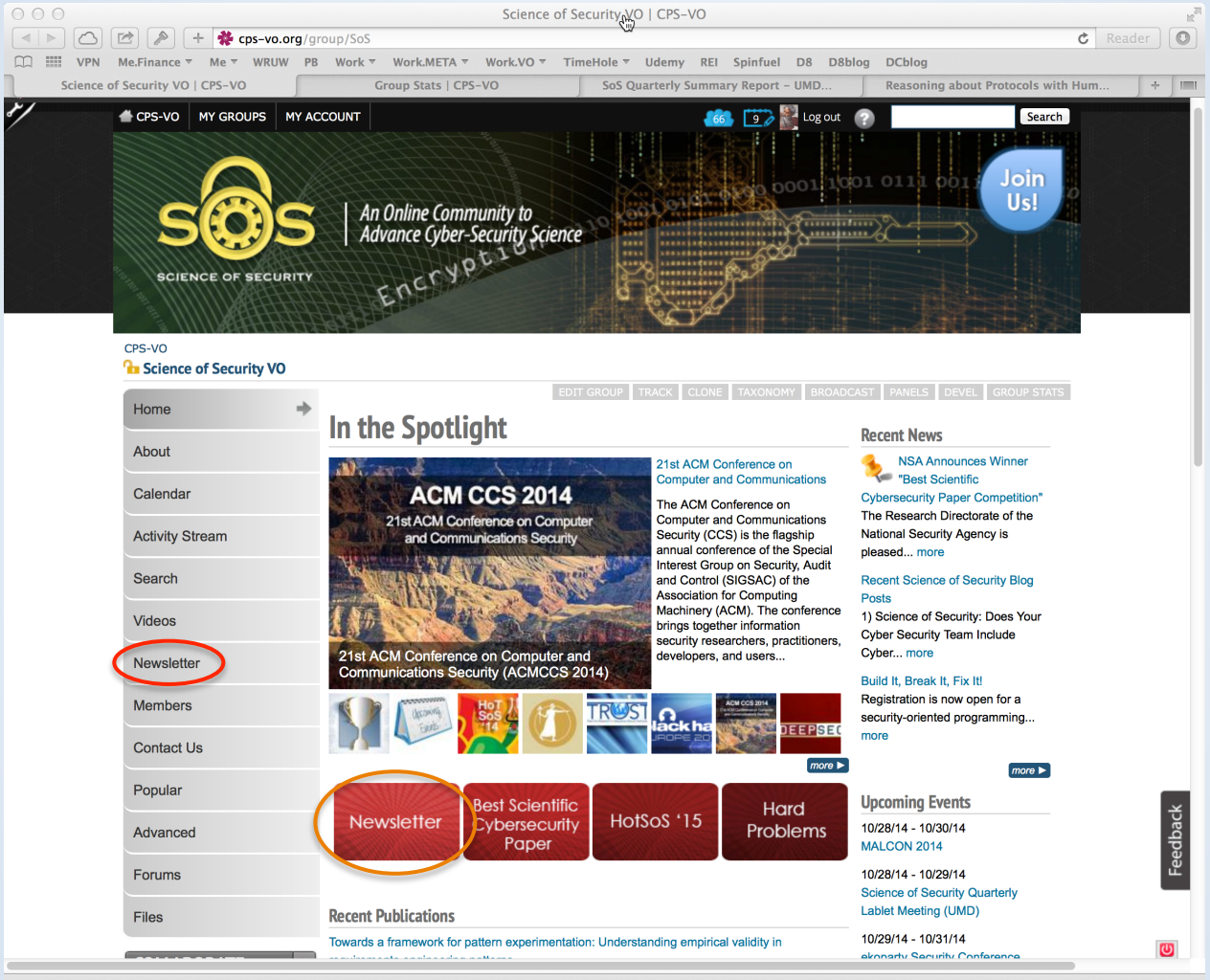
VANDERBILT UNIVERSITY

Agenda

- Support for Bibliographic References

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

Motivation


Science of Security VO | CPS-VO
cps-vo.org/group/SoS
CPS-VO
MY GROUPS
MY ACCOUNT
Log out
Search
An Online Community to Advance Cyber-Security Science
SCIENCE OF SECURITY
Join Us!
CPS-VO
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
ACM CCS 2014
21st ACM Conference on Computer and Communications Security
21st ACM Conference on Computer and Communications Security (ACMCCS 2014)
21st ACM Conference on Computer and Communications
The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users...
more
Newsletter
Best Scientific Cybersecurity Paper
HotSoS '15
Hard Problems
Recent News
NSA Announces Winner "Best Scientific Cybersecurity Paper Competition"
The Research Directorate of the National Security Agency is pleased... more
Recent Science of Security Blog Posts
1) Science of Security: Does Your Cyber Security Team Include Cyber... more
Build It, Break It, Fix It!
Registration is now open for a security-oriented programming... more
more
Upcoming Events
10/28/14 - 10/30/14
MALCON 2014
10/28/14 - 10/29/14
Science of Security Quarterly Lablet Meeting (UMD)
10/29/14 - 10/31/14
Recent Publications
Towards a framework for pattern experimentation: Understanding empirical validity in
Feedback

<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

SOS NEWSLETTER

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", Esmaeilzadeh, 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 Kubiatowicz, 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. Kubiatowicz, 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:

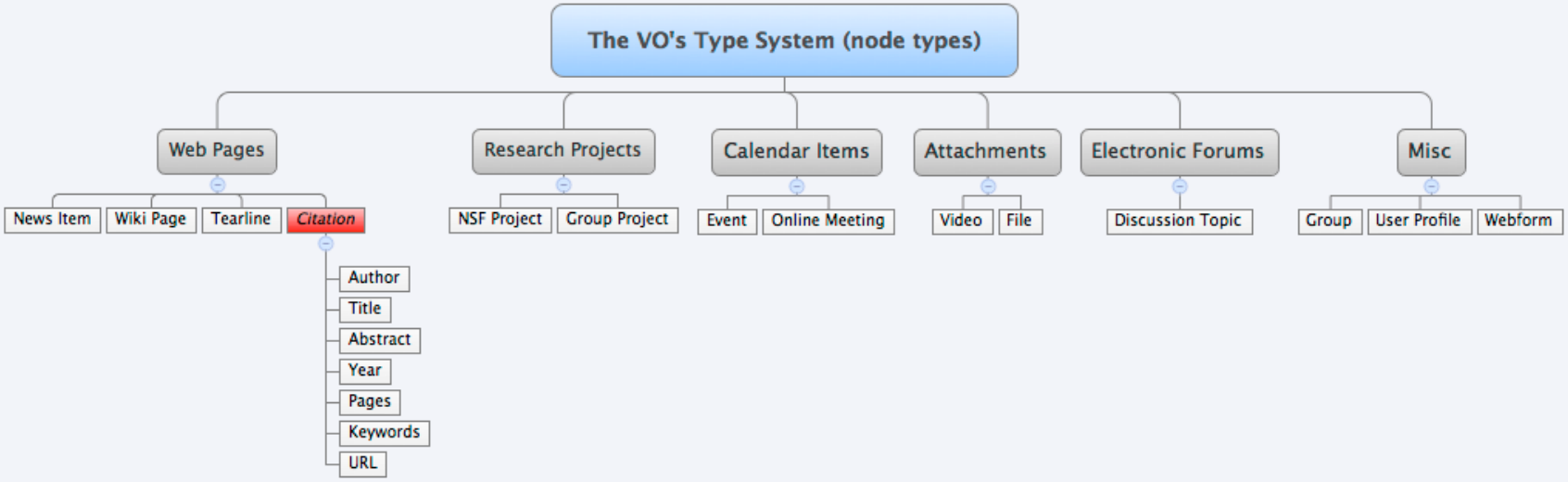
Articles listed on these pages have been found on publicly available internet pages and are cited with links to those pages. Some of the information included herein has been reprinted with permission from the authors or data repositories. Direct any requests via Email to SoS.Project (at) SecureDataBank.net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

‹ Automated Response Actions up Cryptography and Security ›

Problem #2:

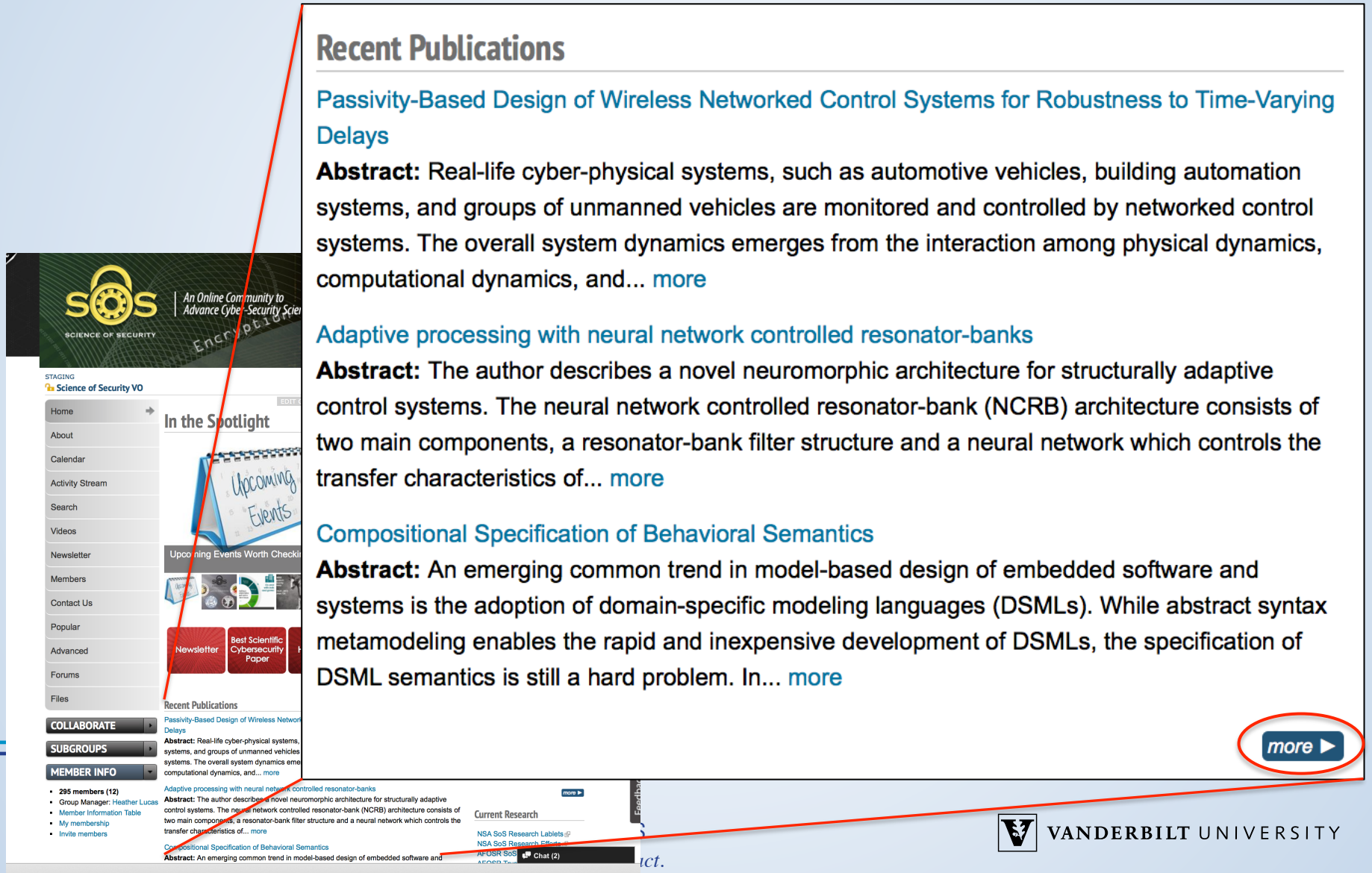
HOW TO EASILY FIND THINGS WHEN THERE ARE 1000'S OF CITATIONS ???

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



New Dashboard Widget

Searching for References



Biblio

GROUP STATS

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

COLLABORATE
SUBGROUPS
MEMBER INFO

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

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, IH.. 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**. Computing, Management and Telecommunications (ComManTel), 2014 International Conference on. :291-297. A

List | Filter | Import

control systems | 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, IH.. 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**.

List | Filter | Import

Biblio search

Found 11 results

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

List | Filter | Import

Biblio search

Found 9 results

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 &\#38; Communications Security. :173–186. Abstract

SITY

List | Filter | Import

Biblio search

Found 9 results

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 &\#38; 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

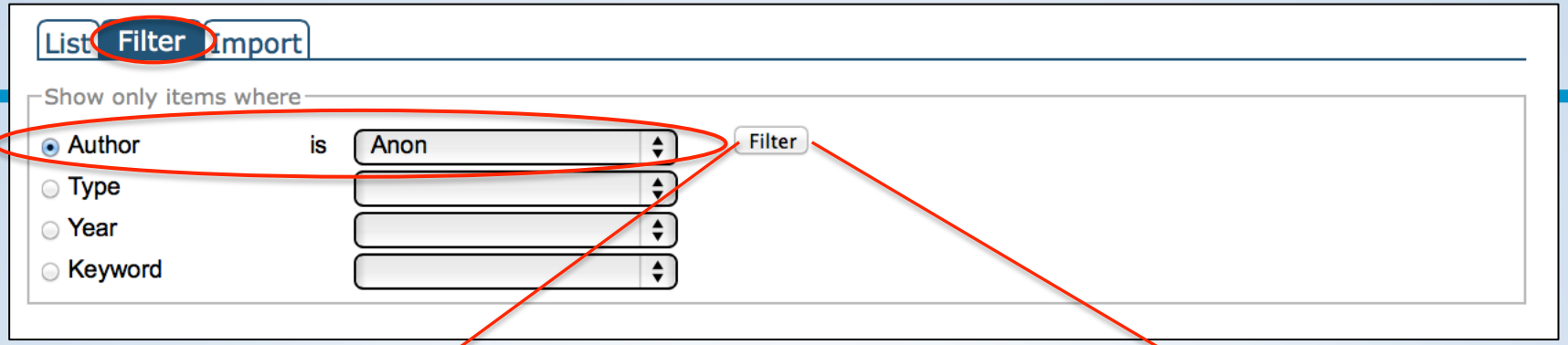
[ID#:14-1771] Chen, Shuai-Min, Wu, Mu-En, Sun, Hung-Min, Wang, King-Hang. 2014. **CRFID: An RFID System with a Cloud Database As a Back-end Server**. Future Gener. Comput. Syst.. 30:155–161. Abstract

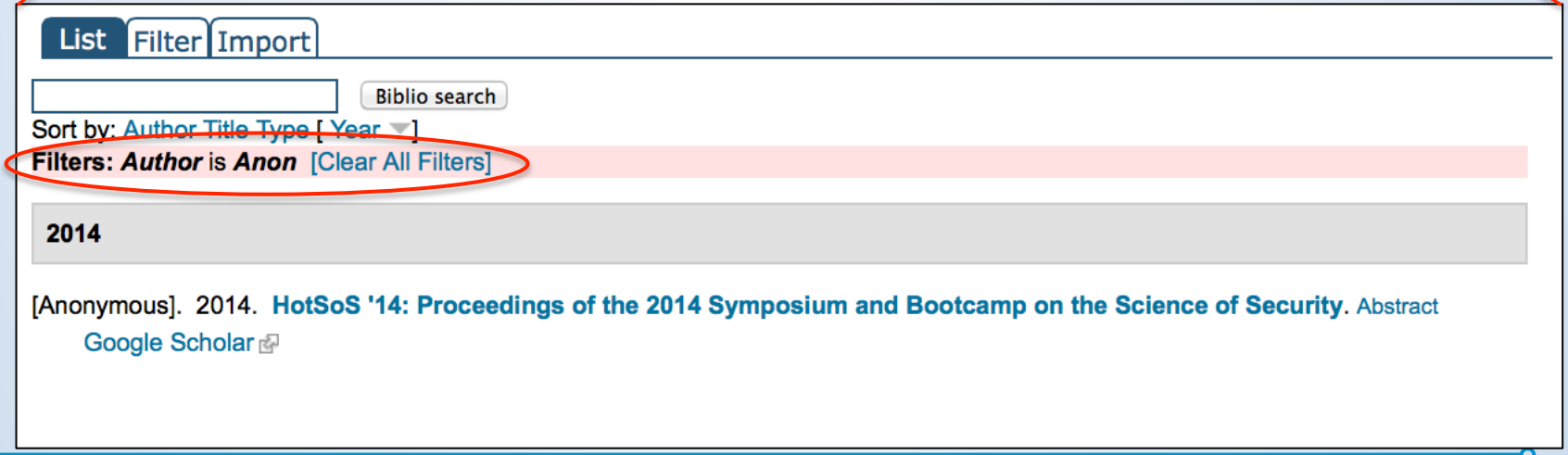
[ID#:14-1770] Rahman, Farzana, Ahamed, Sheikh Iqbal. 2014. **Efficient Detection of Counterfeit Products in Large-scale RFID Systems Using Batch Authentication Protocols**. Personal Ubiquitous Comput.. 18:177–188. Abstract

[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
Filter
Type
Year
Keyword


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

COLLABORATE

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	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.
URL	http://dl.acm.org/citation.cfm?id=2600176&picked=prox&cfid=561740640&cftoken=72764684
Citation Key	Williams:2014:2600176

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 addres 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 ho 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.
URL	http://dl.acm.org/citation.cfm?id=2600176&picked=prox&cfid=561740640&cftoken=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 DIGITAL LIBRARY

Vanderbilt University

SIGN IN SIGN UP

SEARCH

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

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

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:

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

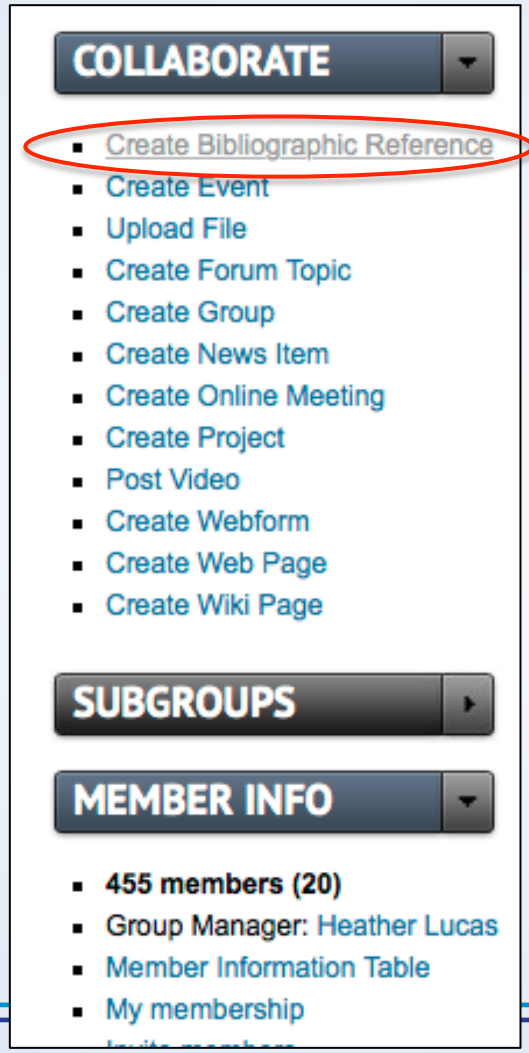
The Maude-NRL Protocol Analyzer (Maude-NPA) is a tool for reasoning about the security of cryptographic protocols in which the cryptosystems satisfy different equational properties. It tries to find secrecy or authentication attacks by searching backwards ... expand

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



Cyber-Physical Systems Virtual Organization

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

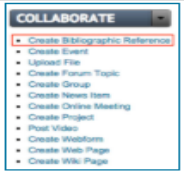
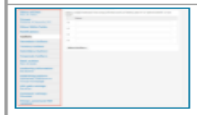
Tutorial ToC

Create a Bibliographic Reference

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.

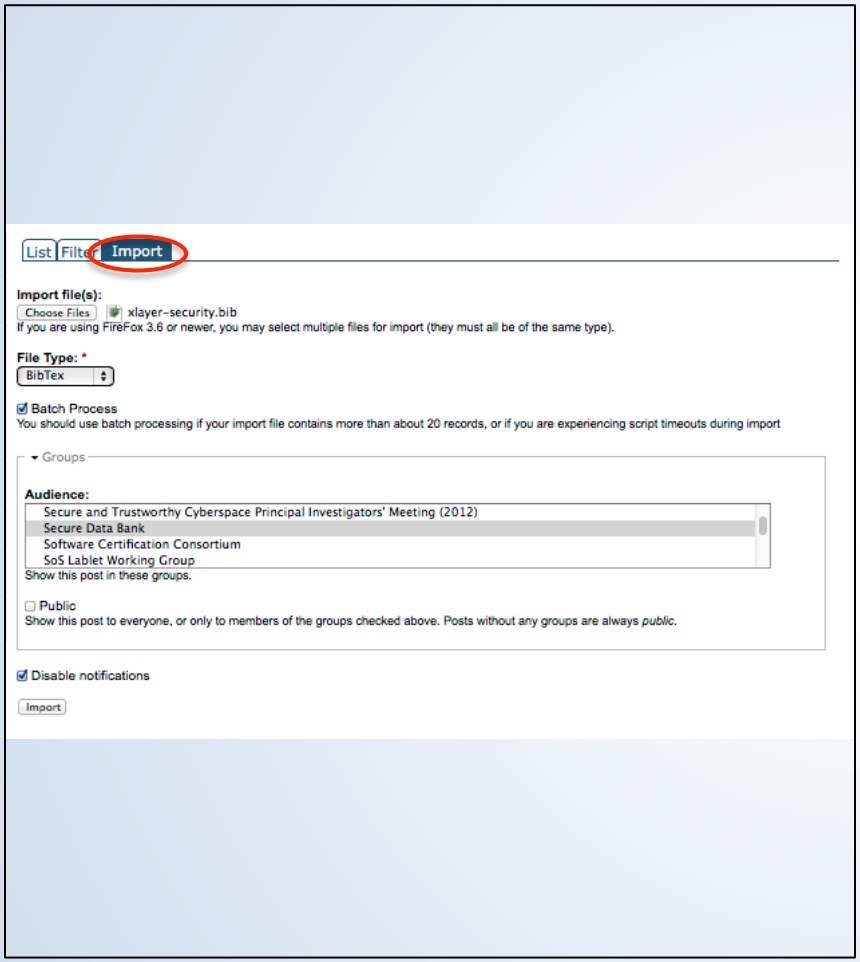
You can create single bibliographic references by following the instructions in the table below.

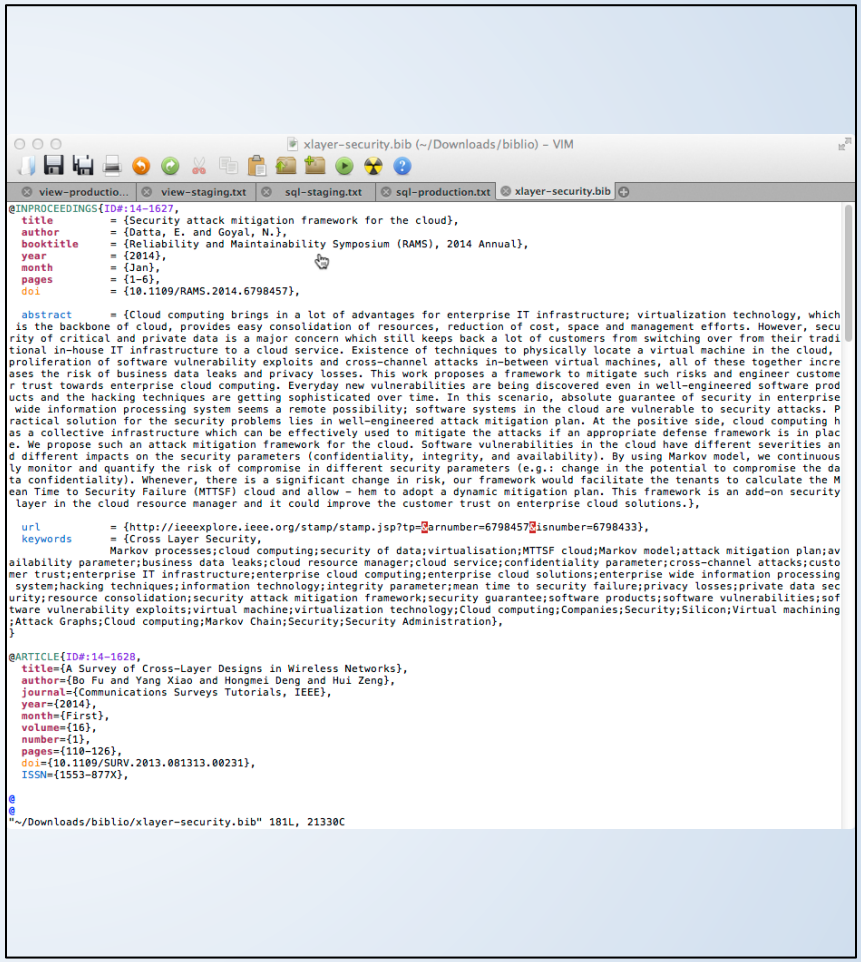
	Select the ***"Create Bibliographic Reference"*** link in the ***"Collaborate"*** toggle menu which is located in the lower left sidebar on your group page.
	1. Paste the BibTeX code copied from a digital library a. Paste BibTeX code into expanded ***"Paste BibTeX"*** text area. b. Select ***"Populate 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. *(The group which you created the bibliography reference from is selected by default).*
	2. Enter the publication details manually a. Select ***"Publication Type"*** from the dropdown menu b. Continue to fill in details as form fields emerge
	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. *(The group which you created the bibliography reference from is selected by default).*

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





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

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 [edit]

Main article: Comparison of reference management software

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

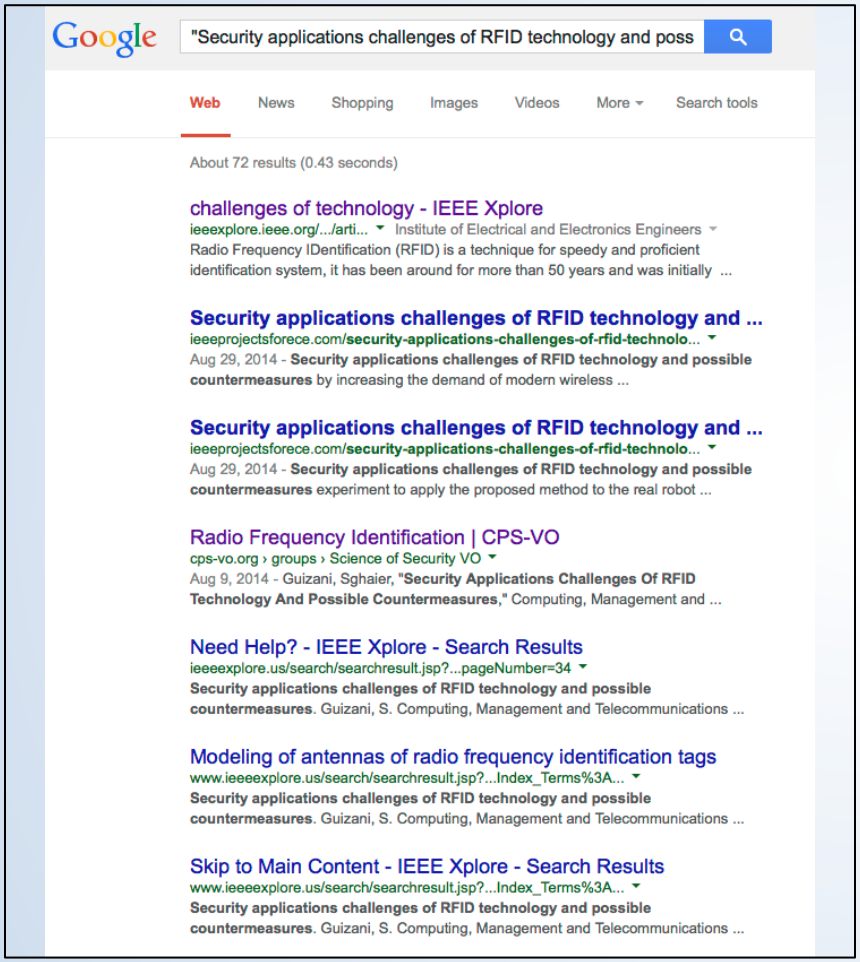
Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

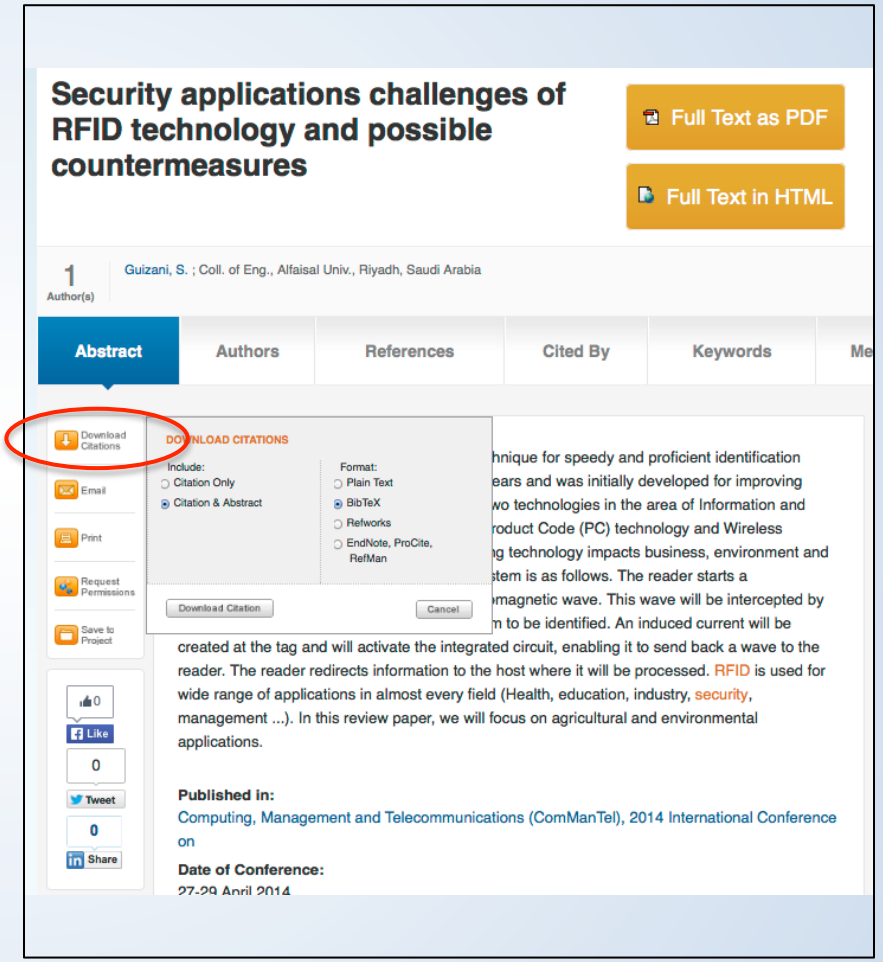
Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

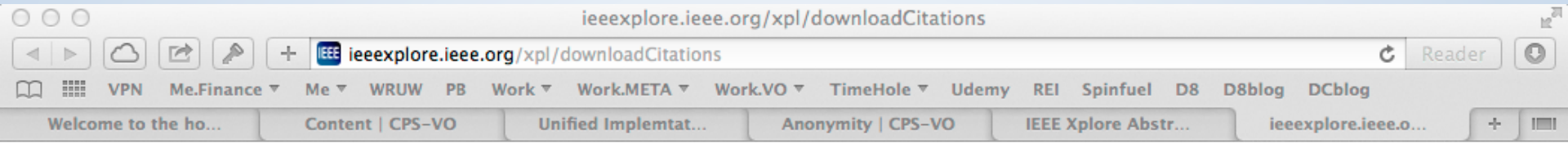
Languages
العربية
Català
Deutsch
فارسی
Français
日本語
Português
Русский
中文
Edit links

Discovering Citations



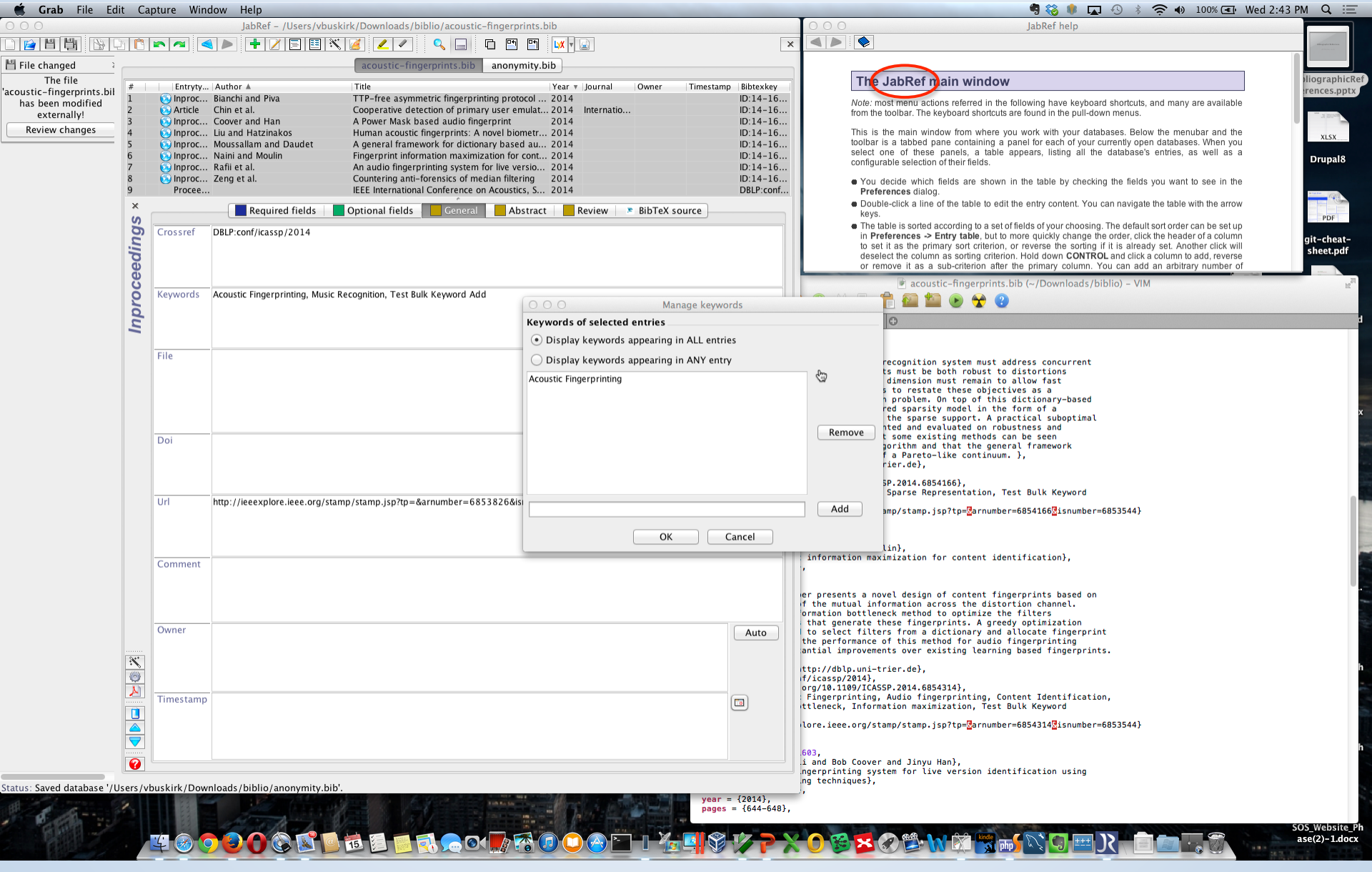


Cut

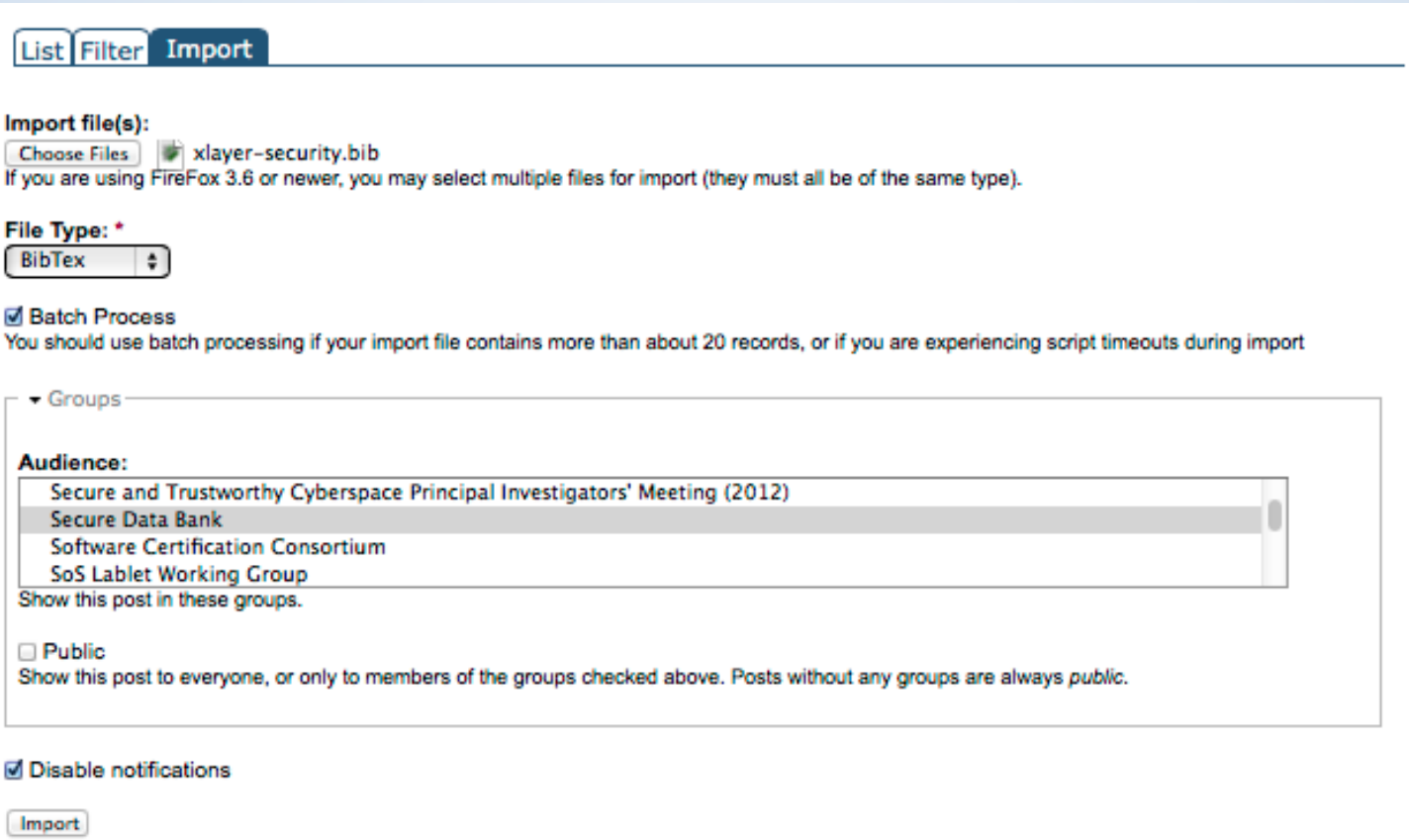



```
@INPROCEEDINGS{6785340,
author={Ren-Hung Hwang and Fu-Hui Huang},
booktitle={Computing, Networking and Communications (ICNC), 2014 International Conference on},
title={SocialCloaking: A distributed architecture for K-anonymity location privacy protection},
year={2014},
month={Feb},
pages={247-251},
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},}
```

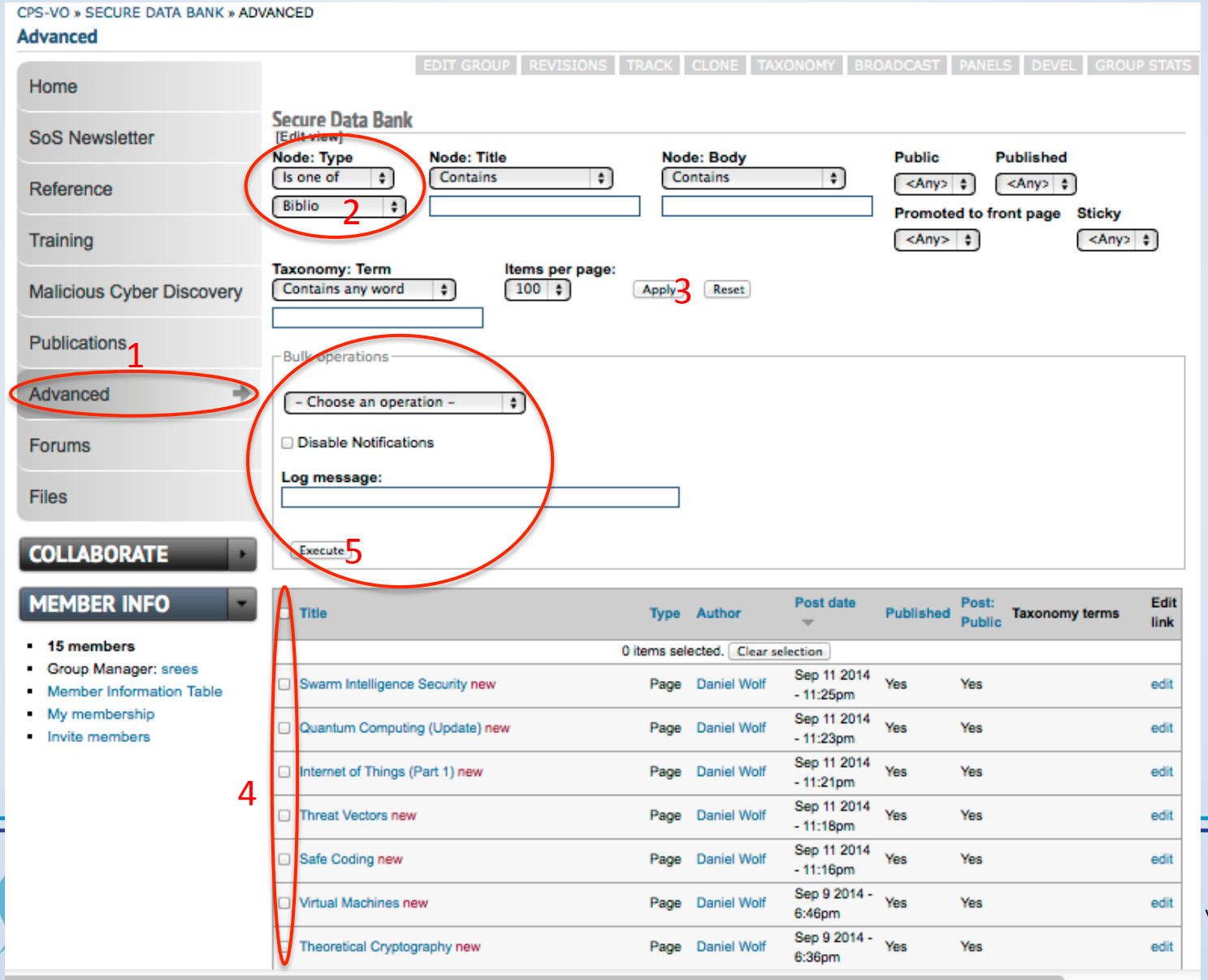
Paste & Customize Keywords



Import


List
Filter
Import
Import file(s):
Choose Files
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
Import

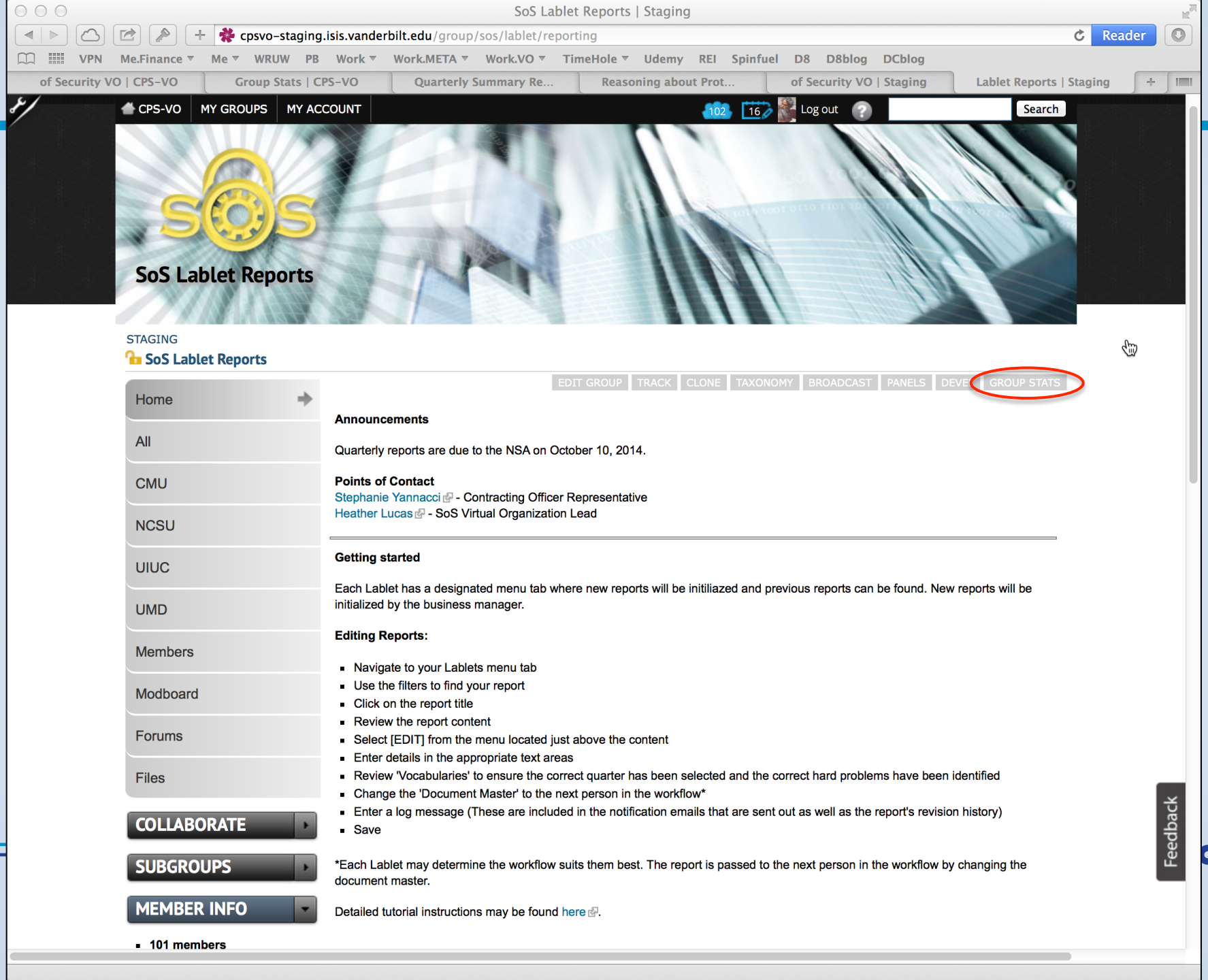
Batch Editing Biblio Nodes



Questions / Comments ?

Agenda

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


SoS Lablet Reports | Staging
cpsvo-staging.isis.vanderbilt.edu/group/sos/lablet/reporting
Reader
VPN Me.Finance Me WRUW PB Work Work.META Work.VO TimeHole Udemy REI Spinfuel D8 D8blog DCblog
of Security VO | CPS-VO
Group Stats | CPS-VO
Quarterly Summary Re...
Reasoning about Prot...
of Security VO | Staging
Lablet Reports | Staging
CPS-VO
MY GROUPS
MY ACCOUNT
102
16
Log out
Search
SoS Lablet Reports
STAGING
SoS Lablet Reports
EDIT GROUP
TRACK
CLONE
TAXONOMY
BROADCAST
PANELS
DEVE
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 initiliazed 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.
Feedback

SoS Lablet Reports

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

Group Stats

GROUP STATS

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

COLLABORATE

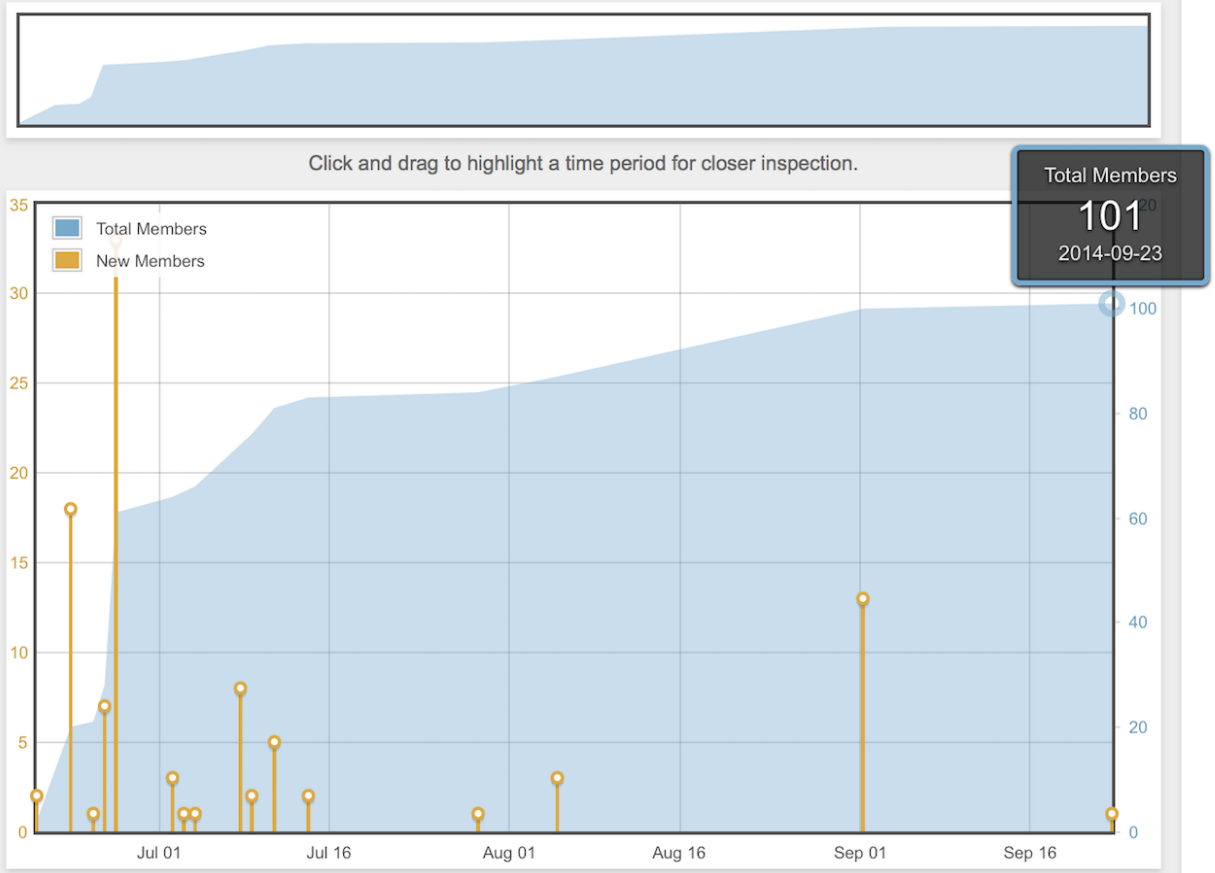
SUBGROUPS

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.



SoS Lablet Reports

Group Stats

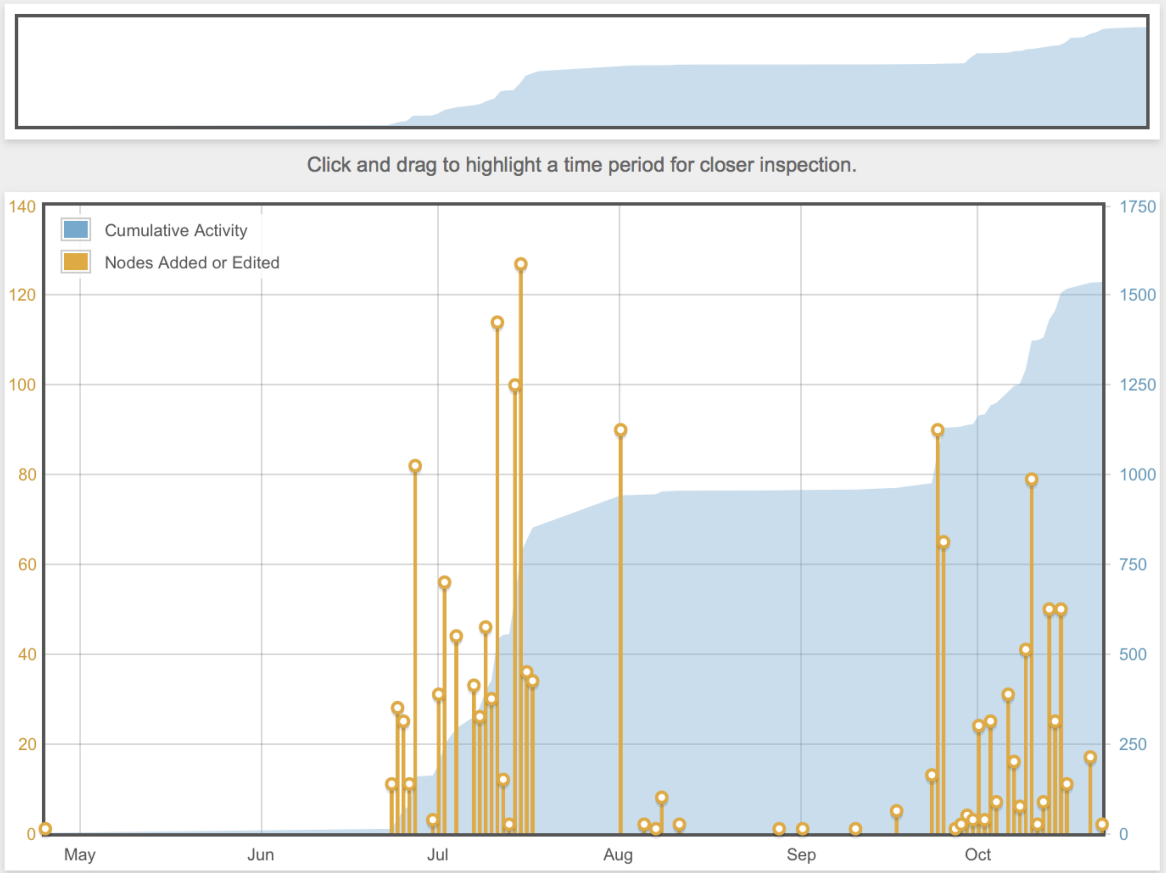
Home
All
CMU
NCSU
UIUC
UMD
Members
Modboard
Forums
Files

COLLAPSE
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.



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*

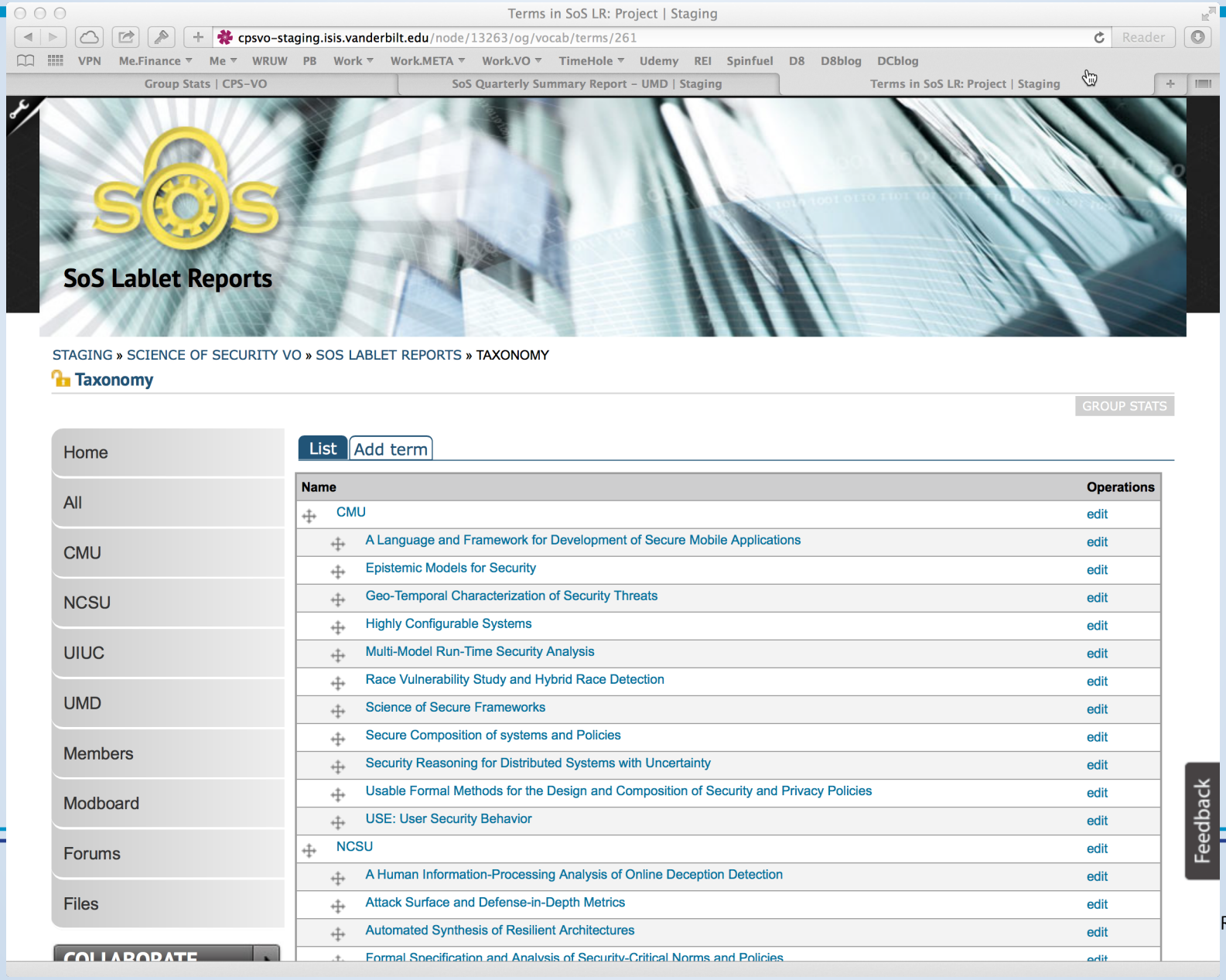
- Tearlines are Deployed

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

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

Proposal for Linking Group Project Descriptions to Quarterly Reports

1. Define a ‘Projects’ Taxonomy



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

Reasoning about Protocols with Human Participants

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

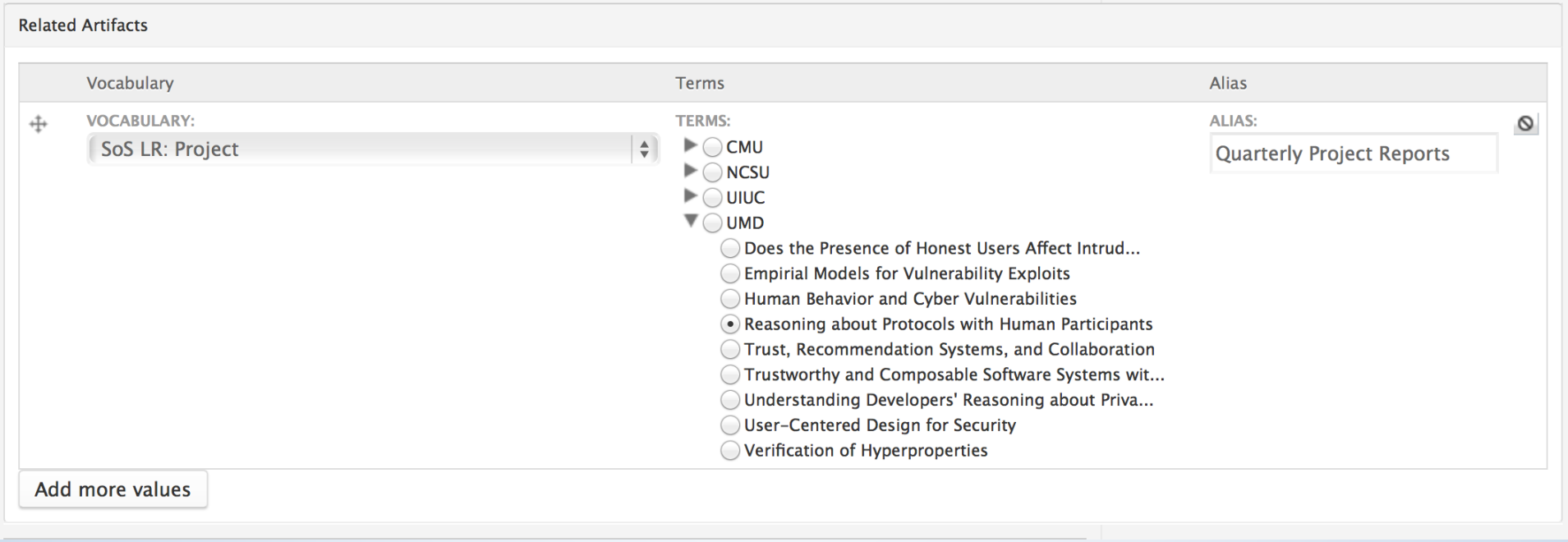
Related Artifacts

Quarterly Project Reports

Reasoning about Protocols with Human Participants

Reasoning about Protocols with Human Participants

Utilize 'Related Artifacts' Feature



Reasoning about Protocols with Human Participants

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

Related Artifacts

Quarterly Project Reports

Reasoning about Protocols with Human Participants

Reasoning about Protocols with Human Participants