DECLARATION OF CRISTINA L. ABAD, Ph.D.

I, Cristina L. Abad, Ph.D., do hereby state that:

1. I am currently a Professor at Escuela Superior Politécnica Del Litoral (ESPOL) University in Guayaquil, Ecuador, where I lead the Distributed Systems @ ESPOL Research Lab (DiSEL) and co-direct the Big Data Research Group. My office address is Oficina 15A-044, Facultad de Ingeniería en Electricidad y Computación, Campus Gustavo Galindo, Km 30.5 vía Perimetral, Guayaquil, EC.

2. In connection with this declaration, I am being compensated for my time at my standard rate of $250 per hour. I do not have a financial interest in this action or its outcome, and my compensation in this matter is not based in any way on the substance of my declaration rendered here or the outcome of this case.

3. I received a degree from the Universidad Católica de Santiago de Guayaquil in Guayaquil, Ecuador in Ingeniero en Sistemas Computacionales in October 1999.

4. In August 2003, I received a Masters of Science in Computer Science from the University of Illinois at Urbana-Champaign.

5. Following the receipt of my Masters, I received a Ph.D. in Computer Science from University of Illinois at Urbana-Champaign (UIUC). My Ph.D. dissertation is titled *Big Data storage workload characterization, modeling and synthetic generation*. I worked on my Ph.D. from August 2003 through July 2004. I then took an approved leave of absence from UIUC, returned to Ecuador and started working at ESPOL, my current employer, as an Assistant Professor. From May 2010 to May 2014, I took an approved leave of absence from ESPOL to complete my degree and work on my Ph.D. thesis. After that, I returned to ESPOL.

6. I have been a co-author of many publications over the years pertaining to various avenues in the computer science field, including with respect to cyber and network security. Some of these publications include the following:

- C. Abad, J. Taylor, C. Sengul, W. Yurcik, Y. Zhou, and K. Rowe, "Log correlation for intrusion detection: A proof of concept," in *19th Annual Computer Security Applications Conference (ACSAC)*, 2003;

- C. Abad, N. Roberts, Y. Lu, and R. Campbell, "A storage-centric analysis of mapreduce workloads: File popularity, temporal locality and arrival patterns," in *IEEE International Symposium on Workload Characterization (IISWC)*, 2012;

- S. Talluri, A. Luszczak, C. Abad, and A. Iosup, "Characterization of a big data storage workload in the cloud," in *ACM/SPEC International Conference on Performance Engineering (ICPE)*, 2019;

Sophos Ex. 1015
Sophos Ltd. and Sophos Inc., v. Webroot Inc.
IPR2024-00252
Page 1 of 61

- E. Boza, C. San-Lucas, C. Abad, and J. Viteri, "Benchmarking key-value stores via trace replay," in *IEEE Intl. Conference on Cloud Eng. (IC2E)*, 2017; and

- C. Abad, A. Abad, and L. Lucio, "Dynamic memory partition for cloud caches with heterogeneous backends," in *ACM/SPEC International Conference on Performance Engineering (ICPE)*, 2017.

7. I have received various awards, grants, and achievements since receiving my Ph.D. in Computer Science, including the following:

- Grant Award, Google Faculty Research Award, Oct 2015 call (2016);

- Research Grant, Unrestricted Gift from Microsoft, by invitation (2017);

- Grant Award, Google Faculty Research Award, Oct 2017 call (2018); and

- Grant Award, AT&T Virtual University Research Initiative (VURI) Award (2019).

8. During my academic studies, and even now in academia, I (along with co-authors) regularly write papers describing our research. We write papers and find places to present or publish them, such as at conferences and/or journals. The purpose of presenting or publishing these papers is so that others in the field can learn from our research. Likewise, I regularly review papers presented at conferences or in journals related to my research.

9. I am one of the co-authors of the reference Li, Z. et al., *UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection* (the "Li Reference"), which was originally published in the Proceedings of the Twelfth International Conference on Telecommunication Systems Modeling and Analysis ("ICTSM Conference").

10. The ICTSM Conference covered subjects relating to the modeling and analysis of telecommunication and systems and computer networks, including a focus on non-functional properties like performance, availability, security, and privacy. Individuals from industry and academia attend the ICTSM.

11. The ICTSM Conference took place in Monterey, California at the Naval Postgraduate School from July 22-25, 2004. This date is consistent with my recollection as I was not able to attend this conference because I was relocating to Ecuador.

12. I have attached a copy of the ICTSM Conference schedule as Exhibit A to my declaration, indicating that this conference took place from July 22-25, 2004. *See* Ex. A, pg. 6;[1] *see also* EX-1009 (indicating that the ICTSM Conference took place from July 22-25, 2004).

---

[1] I obtained Exhibit A from the ICTSM Conference webpage hosted on the Southern Methodist University, Cox School of Business's website, through the Wayback Machine at the following link: https://web.archive.org/web/20041204234240/http:/tecom.cox.smu.edu/icts/ictsm12/. *See* Ex. B (Wayback Machine indicates that this snapshot was taken on December 4, 2004).

13. The ICTSM Conference schedule also shows that individuals from industry and academia attended ICTSM conferences. There are papers authored by both industry and academia. For example, the ICTSM Conference schedule indicates that Session 1 was on "Wireless Networking," and Session 13 was on "Network Security." Ex. A, pgs. 1, 6.

14. The Li Reference was presented at the ICTSM Conference. Specifically, Exhibit A indicates that the Li Reference was presented on Sunday, July 25, 2004 during Session 13, held from 8:30-10:00 AM. *See* Ex. A, pg. 6. Exhibit A further indicates that one of the co-authors of the Li Reference; William Yurcik, whom I personally knew at the time, attended the ICTSM Conference at which the Li Reference was presented. Moreover, Exhibit A indicates that Mr. Yurcik was the presenter of the Li Reference at the ICTSM Conference. *See* Ex. A, pg. 6. I remember that Mr. Yurcik is the one who initially suggested that we submit the Li Reference to ICTSM, as he had previously attended the ICTSM conferences.

15. The ICTSM Conference webpage indicates that "[c]onference participants will be provided with the conference proceeding (a collection of papers presented at the conference)[.]" *See* Ex. C.[2]

16. Attached hereto is a copy of a PowerPoint presentation presenting the Li Reference. *See* Ex. D.[3]

17. As indicated on the NCASSR website, "NCSA and partner sites address the nation's critical need for a dynamic, adaptive cybersecurity infrastructure by completing projects." Ex. E.[4] Year 2 Project 1.7 related to Security Incident Fusion Tools (SIFT). Ex. F.[5] The SIFT Project is described as follows:

> "The SIFT project is defining the new specialty field of 'Internet security visualization' as evidenced by our paper/software productivity and leadership in IEEE/ACM forums. [A] high-level overview of our research follows:
>
> Government and business organizations use computer network infrastructures that hold a vast amount of information for system administrators and security engineers. There are typical logs common to most computer networks, but the systems are often large and dynamic, making it difficult to extract knowledge from the sea of information.

---

[2] Exhibit C is a copy of the ICTSM Conference webpage hosted on the Southern Methodist University, Cox School of Business's website, through the Wayback Machine at the following link: https://web.archive.org/web/20041204234240/http://tecom.cox.smu.edu/icts/ictsm12/ (Wayback Machine indicates that this snapshot was taken on December 4, 2004).

[3] I obtained this presentation from the ncassr.org website through the Wayback Machine at the following link: https://web.archive.org/web/20051214205926/http://www.ncassr.org/projects/sift/papers/ictsm04-uclog.ppt (Wayback Machine indicates that this snapshot was taken on December 14, 2005).

[4] I obtained a copy of this webpage from the ncassr.org website through the Wayback Machine at the following link: https://web.archive.org/web/20051215131057/http://www.ncassr.org/about/index.html (Wayback Machine indicates that this snapshot was taken on December 15, 2005).

[5] I obtained a copy of this webpage from the ncassr.org website through the Wayback Machine at the following link: https://web.archive.org/web/20051215120659/http://www.ncassr.org/projects/index.html (Wayback Machine indicates that this snapshot was taken on December 15, 2005).

> Individually, each system log can be massive, causing operator overload. When overload occurs, security events can slide by unnoticed. Overload can also cause operators to disregard alarms due to high false positive rates. Even in homogeneous infrastructures, solutions from a single vendor fail to scale to medium or large networks. However, the problem is compounded because many organizations have network infrastructures from multiple vendors.
>
> We are developing the Security Incident Fusion Tool (SIFT), an integrated framework for evaluating the security of an entire computer network on a single screen. The project will address the need to discover security incidents that currently go undetected by security operations systems. Two new SIFT tools, NVisionIP and VisFlowConnect, leverage human visual cognitive abilities to process log data into knowledge for situational awareness of network security. It is estimated that human beings can visually process a screen of information at 150 Mbits per second, with the ability to discriminate relatively minor shifts in color, shape, and motion. By presenting network data visually, it can be scanned quickly, patterns in complex data rise to the surface, and inferences become intuitive. Once a security professional becomes familiar with the normal appearance of the network being monitored, it is much easier to spot attacks, including new so-called 'zero-day attacks.' The tools are designed to give security engineers situational awareness of an entire network in order to help them determine when a network is under attack, what is being attacked, and what form the attack is taking."

See Ex. G.[6]

18. The SIFT Project was widely publicized. For example, several events are listed at NCASSR's website. *See* Ex. G. Our work was also been published on the SIFT website so others in the field could obtain and review. This included the Li Reference.

19. I have also attached a copy of a snapshot of the ncassr.org website taken on February 5, 2005 showing that the Li Reference was available for review through ncassr.org. *See* Ex. H.[7]

20. As mentioned in the footnotes, Exhibits D through H were obtained from Wayback Machine snapshots of the website ncassr.org, a website dedicated to cyber and network security and that was led by the National Center for Supercomputing Applications (NCSA). I am familiar with the NCASSR website. I was a member of NCSA and my research was funded by NCSA.

21. I have also attached here as Exhibit I a copy of an email I received from Mr. Yurcik on November 5, 2004, providing a link to the Li Reference on the ncassr.org website, and asking me to review it.

---

[6] I obtained a copy of this webpage from the ncassr.org website through the Wayback Machine at the following link: https://web.archive.org/web/20041216182045/http://www.ncassr.org/projects/sift/ (Wayback Machine indicates that this snapshot was taken on December 16, 2004).

[7] I obtained a copy of this webpage from the ncassr.org website through the Wayback Machine at the following link: https://web.archive.org/web/20050205214439/http://www.ncassr.org/projects/sift/papers/ (Wayback Machine indicates that this snapshot was taken on February 5, 2005).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: September 26, 2023

Cristina L. Abad, Ph.D.

EXHIBIT A

ICTSM12 schedule - *Naval Postgraduate School*

Registration — Room

Thursday 04:00-6:00PM Registration — **Front of Ingersol 122**

Registration

,

Thursday Reception — Room

Thursday 6:30-8:00PM Reception **Chairman: Gavish** — **Tower Room top of Hermann Hall**

Reception Thursday

Bezalel Gavish, Southern Methodist University Dallas USA

Session: 1 Wireless Networking — Room

Friday 8:30-10:00AM Parallel Session **Chairman: Bartolacci** — **Ingersol 271**

Agents for Wireless Environments

Badr Benmammar, Univeristy of Paris XIII France
Francine Krief, University of Paris XIII Paris France

An Optimization Approach for Connectivity in Wireless Networks

Michael R. Bartolacci, Penn State Berks/LeHigh Valley College Fogelsville USA
Abdullah Konak, Penn State University Reading USA
Roger M. Whitaker, Cardiff University (Center for Mobile Communications) Cardiff, CF24 3XF United Kingdom

An Architecture for m-Learning with Wireless Networks

Michael R. Bartolacci, Penn State Berks/LeHigh Valley College Fogelsville USA
John C. Wiginton, University of South Florida Tampa USA

Session: 2 New Applications — Room

Friday 8:30-10:00AM Parallel Session **Chairman: Radovilsky** — **Ingersol 280**

On-Time Performance and the Value of RFID in Cross-Docking

H. Steve Peng, California State University Hayward USA

CDN Economics and Exogenous Congestion

Eugenio de la Rosa, University of Arizona Tucson USA
John H. Hartman, University of Arizona USA
Terril Hurst, Hewlett-Packard Palo Alto USA

Four Dimensions of Enterprise Resource Planning (ERP) Systems: A New Classification Approach

Zinovy Radovilsky, California State University Hayward USA

Coffee Morning Break (Friday) — Room

Friday 10:00-10:30AM Coffee Break — **Front of Ingersol 122**

Coffee Morning Break

,

Session: 3 Opening Session — Room

Friday 10:30-11:45AM Opening Session **Chairman: Bordetsky** — **Ingersol 122**

Overview and Welcome

Bezalel Gavish, Southern Methodist University Dallas USA

Welcome Message

Leonard Ferrari, Naval Postgraduate School Monterey

Model-based Communication Networks: Filtering Information by Value to Improve Collaborative Decision-Making

Rick Hayes-Roth, NPS Monterey

Sophos Ex. 1015
Page 7 of 61

Lunch Friday — Room

Friday 12:00-1:30PM Lunch — **El Prado Room in Hermann Hall**

Lunch Friday

,

Session: 4 Network Testbeds — Room

Friday 1:30-3:15PM Parallel Session **Chairman: McNeill** **ME 385**

The Network Testbed Sizing Problem - A Proposed Research Framework

Kevin McNeill, University of Arizona USA
Roman Statnikov, Monterey USA
Ed Koharek, Northrup Grumman Information Technology Sierra Vista USA
Les Claudio, Joint Interoperability Test Command Fort Huachuca USA

Management and Control Plane Techniques in Self-Aware Networks

Natalia Gaviria, University of Arizona Tucson USA
Kevin McNeill, University of Arizona USA
Jerzy Rozenblit, University of Arizona Tucson USA

Coupling Network Simulators to Real-World Networks

Kevin McNeill, University of Arizona USA
Wenji Wu, University of Arizona Tucson USA

Army Entrprise Infostructure - Transport (AEI-T) Modeling and System (M&S) Engineering Effort

Carl Agren, Technology Integration Center Fort Huachuca USA

Session: 5 Battle Space Communication Architectures - 1 — Room

Friday 1:30-3:15PM Parallel Session **Chairman: Boger** **ME 378**

Network Aware Self-Organizing Sensor-Decision Maker Grid

Alex Bordetsky, Naval Postgraduate School USA
Eugene Bourakov, Policy Management Systems Corporation Columbia USA

FORCENet: We've been here before

Rex Buddenberg, Navy Postgraduate School USA

Towards Device-Aware Networks

Su Wen, Naval Postgraduate School Monterey USA
Gurminder Singh, Naval Postgraduate School USA
John Gibson, Naval Postgraduate School Monterey USA
Arijit Das, Naval Postgraduate School Monterey USA

Solving the "Last Mile" Problem for the Global Information Grid Bandwidth Expansion to Tactical Units

James E. Just, Global InfoTek.Inc. Arlington USA
Dhananjay Phatak, University of Maryland Baltimore County Baltimore USA
Thomas Goff, University of Maryland Baltimore County Baltimore USA

Coffee Afternoon Break (Friday) — Room

Friday 3:15-3:45PM Coffee Break — **Front of Ingersol 122**

Coffee Afternoon Break

,

Sophos Ex. 1015
Page 8 of 61

Session: 7 P2P Networks — Room

Friday 3:45-5:15PM Parallel Session **Chairman: Matuszewski** **ME 385**

Developing IP Network Structures with Regard to Traffic Engineering and Failure Resilience

Gerhard Hasslinger, Deutsche Telecom D-64259 Darmstadt Germany
Stefan Schnitter, Duetsche Telekom Darmstadt Germany
Martin Franzke, Duetsche Telekom Darmstadt Germany

Peer-to-Peer Music Distribution

Marcin Matuszewski, Helsinki University of Technology Helsinki Finland

Autonomous Multicriteria Fan-Out Mechanism or Peer-to-Peer Collaborative Networking

Alex Bordetsky, Naval Postgraduate School USA
Roman Statnikov, Monterey USA

Session: 6 Battle Space Communication Architectures - 2 — Room

Friday 3:45-5:15PM Parallel Session **Chairman: Boger** **ME 378**

A Policy Based Collaboration Infrastructure for P2P Networking

Mark R. Cornwell, Global Info Tek, Inc. Arlington USA
Lalana Kagal, University of Maryland Baltimore County Baltimore USA
James E. Just, Global InfoTek.Inc. Arlington USA
Tim Finin, University of Maryland Baltimore County Baltimore USA

Dynamic Adaptive Epidemic Models for Peer-to-Peer Network Access

Donald P. Gaver, Naval Postgraduate School Monterey USA
Patricia A Jacobs, Naval Postgraduate School Monterey USA
Cheng-Chung Kao, Naval Postgraduate School Monterey USA

Towards a First Responder Contingency Information Capability

Geoffrey Xie, Naval Postgraduate School USA
Su Wen, Naval Postgraduate School Monterey USA
John Gibson, Naval Postgraduate School Monterey USA
Gurminder Singh, Naval Postgraduate School USA

Session: 8 Dinner Friday — Room

Friday 6:00-8:30PM Dinner **Gavish** **LaNovia terrace Hermann Hall**

Dinner Friday

,

Sophos Ex. 1015
Page 9 of 61

Session: 8 Stochastic Models — Room

Saturday 8:30-10:00AM Parallel Session **Chairman: Morita** **ME 385**

Packet Loss and Delay Jitter Characteristics of the Internet -- VoD Trial Service with Packet Recovery

Tetsuo Morita, Transmission System Department Osaka 554-0024 Japan
Yukata Majima, Sumitomo Electric Industries Ltd Konohana-ku Japan
Toshihiro Takashima, Sumitomo Electric Industries, Ltd. Konoshana-ku Japan
Takahiro Kusumoto, Sumitomo Electric Industries, Ltd. Konoshana-ku Japan
Takashi Sasaki, Kyoto University Kyoto 606-8501 Japan
Yutaka Takahashi, Kyoto University Kyoto 606-8501 Japan

Analysis of The Packet Loss Process for Multimedia Traffic

Gyorgy Dan, KTH, Royal Institute of Technology Stockholm Sweden
Viktoria Fodor, KTH, Royal Institute of Technology Stockholm Sweden
Gunnar Karlsson, KTH, Royal Institute of Technology Stockholm Sweden

The Channel Characterization for Mobile Communication Employing Stratospheric Platform

Iskandar Febryn, Waseda University Japan
Shigeru Shimamoto, Waseda University Japan

Dependence on Angle-of-Arrival Fluctuations on Source Coherence for Free Space Optics Links in a Turbulent Atmosphere

Yahya Baykal, Cankaya University Balgat Ankara Turkey
Halil Tanyer Eyyuboglu, Cankaya University Balgat Ankara Turkey

Session: 9 Network Management — Room

Saturday 8:30-10:00AM Parallel Session **Chairman: Hoag** **ME 378**

A Role Model for Classification and Analysis of Internet Service Providers

Oliver Heckmann, Darmstadt University of Technology Darmstadt Germany
Ralf Steinmetz, Darmstadt University of Technology D-64283 Darmstadt Germany

Network Management Using Active Probing

Marat Zhanikeev, Waseda University Tokyo Japan
Yoshiaki Tanaka, Waseda University Japan

Telecommunications in Complex Systems Failure: The Electricity Blackout of August 14, 2003

John Hoag, Ohio University USA

Coffee Morning Break (Saturday) — Room

Saturday 10:00-10:30AM Break **Front of Ingersol 122**

Coffee Morning Break

,

Session: 10 Personal Mobile Networks — Room

Saturday 10:30-11:30AM Plenary Session **Chairman: Gavish** **Ingersol 122**

The warrior as a networking and computing node

Ralph Osterholtz, CEO INTER-4 USA

Lunch Saturday (Boxed) — Room

Saturday 11:30-12:15PM Lunch **El Prado Room in Hermann Hall**

Lunch Saturday

,

Sophos Ex. 1015
Page 10 of 61

Session: 11 Challenges of Integrating and operating Tactical Sensor - UAV Networks — Room

Saturday 12:15-2:30PM Panel Session **Chairman: Bordetsky** **Ingersol 122**

UAV Research Introduction
Alex Bordetsky, Naval Postgraduate School USA

Center for Interdisciplinary Remotely piloted Aircraft Studies - Challenges of UAV experimentation
Dave Netzer, Naval Postgraduate School Monterey USA

Military reuirements from UAV-based tactical networks
Chris Manuel, USA

Network integration and operational constraints for OFDM 802.16a links
Ryan Blazevich, Naval Postgraduate School Monterey USA

Operational constraints of mesh peer-to-peer networking over 802.11 and OFDM links
Eric Bach, Naval Postgraduate School Monterey USA

Tracking antennas and 802.11 infrastructure solutions
Axel Schumann, German Navy

Sensor cluster architectures
Ken Paxton, Naval Postgraduate School Monterey USA

Collaboration tools
Jack Fay, Naval Postgraduate School Portsmouth USA

Challenges of enabling network facilitator role within the network operations crew
Kristina Jeoun, Naval Postgraduate School Monterey USA

Failures and Intrusion detection
Sean Cooney, US Navy

Challenges of integrating tactical network operation procedures in higher level command and control environments
Sue Higgins, NPS

Walking Tour of Monterey — Room

Saturday 4:30-6:30PM Walking Tour **Fisherman Warf**

Walking Tour of Monterey
,

Dinner Saturday (Stokes) — Room

Saturday 6:30-9:00PM Dinner **Stokes Restaurant**

Dinner Saturday
,

Session: 12 Mobile Systems — Room

Sunday 8:30-10:00AM Parallel Session **Chairman: Frikha** **ME 385**

Integration application with Public WLAN married to GPRS/3G
Wei Ye, University of Southern California USA

Mobility in the IP Networks
Mounir Frikha, Ecole Supe3rieure des Communications de Tunis Rawed Tunisie
Lilia Maalej, Ecole Superieure des Commuications De Tunis, Tunisia Rawed Tunisie

Intracell and intercell interference reduction in FBWA networks through enhanced resource allocation techniques
A Vavoulas, University of Athens Athens Greece
T. Rokkas, University of Athens Athens Greece
Dimitris Varoutas, University of Athens Athens Greece
Thomas Sphicopoulos, University of Athens Athens Greece

Sophos Ex. 1015
Page 11 of 61

Session: 13 Network Security — Room

Sunday 8:30-10:00AM Parallel Session **Chairman: Yurcik** **ME 378**

Georgraphical NetFlows Visualization for Network Situational Awareness: NaukaNet Administrative Data Analysis System (NADAS)

Greg Cole, National Center for Supercomputing Applications Arlington USA
Natasha Bulashova, National Center for Supercomputing Applications Arlington USA
William Yurcik, NCSA/University of Illinois Urbana-Champaign USA

Design of an Economics-Based Software Infrastructure for Secure Utility Computing on Supercomputing Clusters

Gregory A. Koenig, University of Illinois at Urbana-Champaign Urbana USA
William Yurcik, NCSA/University of Illinois Urbana-Champaign USA

UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection

Zhenmin Li, University of Illinois at Urbana/Champaign Champaign USA
Jed Taylor, University of Illinois at Urbana/Champaign Champaign USA
Elizabeth Partridge, University of Illinois at Urbana/Champaign Champaign USA
Yuanyuan Zhou, University of Illinois at Urbana/Champaign Champaign USA
William Yurcik, NCSA/University of Illinois Urbana-Champaign USA
Cristina Abad, University of Illinois at Urbana-Champaign Champaign USA

Coffee Morning Break (Sunday) — Room

Sunday 10:00-10:30AM Coffee Break **Front of Ingersol 122**

Coffee Morning Break

,

Session: 14 Routing — Room

Sunday 10:30-12:00AM Parallel Session **Chairman: Duffany** **ME 385**

A GRASP Heuristic for the Delay-Constained Multicast Routing Problem

Nina Skorin-Kapov, University of Zagreb Zagreb Croatia
Mladen Kos, University of Zagreb Zagreb Croatia

Virtual Path Optimization in ATM Networks

Jeffrey L. Duffany, Universidad del Turabo Gurabo Puerto Rico

IPv6 Interoperability Network - Lessons Learned

Scott J. Baier, Technology Integration Center Fort Huachuca USA

Session: 15 Security and Trust — Room

Sunday 10:30-12:00AM Parallel Session **Chairman: Rozenbroek** **ME 378**

An Architecture for Managing Access to and Permission for Multiple Versions of Objects in a Distributed Environment

Tom Rozenbroek, George Mason University Fairfax USA

An Distributed Architecture for the Publication and Management of Objects, which provides End-to-End Security

Randall Breeden, Omega Information Solutions, Inc. Rockville USA
Tom Rozenbroek, George Mason University Fairfax USA

I3MP Defense in Depth Security Levels

Steven K. Bates, Signal Solutions, Inc. Sierra Vista USA

Session: 16 Closing Session — Room

Sunday 12:00-12:15 Closing Session **Chairman: Gavish** **ME 378**

Closing Session

Bezalel Gavish, Southern Methodist University Dallas USA
Alex Bordetsky, Naval Postgraduate School USA

Sophos Ex. 1015
Page 12 of 61

EXHIBIT B

The Wayback Machine - https://web.archive.org/web/20041204234240/http://tecom.cox.smu.edu:80/icts/ictsm12/

12th

International Conference on

Conference Scope
Registration Form
Conf. Hosting Possibility
List of Topics
Important Dates
Submission of Abstract/Paper
Manuscript Prep. Instructions
Purchasing Past Conf. Proceedings
Committee Members
Program schedule (pdf)
Accepted Papers (pdf)
Conference Sponsors
Travel
Monterey Info.
Hotel Reservation
Related Conferences
Related Journals
E-mail to Conf. Chairman

ICTSM Sessions a... 1 / 6 68%

ICTSM12 schedule - *Naval Postgraduate School*

Registration — **Room**

Thursday 04:00-6:00PM Registration — **Front of Ingersol 122**

Registration

Thursday Reception — **Room**

Thursday 6:30-8:00PM Reception **Chairman: Gavish** — **Tower Room top of Hermann Hall**

Reception Thursday

Bezalel Gavish, Southern Methodist University Dallas USA

Session: 1 Wireless Networking — **Room**

Friday 8:30-10:00AM Parallel Session **Chairman: Bartolacci** — **Ingersol 271**

Agents for Wireless Environments

Badr Benmammar, Univeristy of Paris XIII France
Francine Krief, University of Paris XIII Paris France

An Optimization Approach for Connectivity in Wireless Networks

Michael R. Bartolacci, Penn State Berks/LeHigh Valley College Fogelsville USA
Abdullah Konak, Penn State University Reading USA
Roger M. Whitaker, Cardiff University (Center for Mobile Communications) Cardiff, CF24 3XF United Kingdom

An Architecture for m-Learning with Wireless Networks

Michael R. Bartolacci, Penn State Berks/LeHigh Valley College Fogelsville USA
John C. Wiginton, University of South Florida Tampa USA

Session: 2 New Applications — **Room**

Friday 8:30-10:00AM Parallel Session **Chairman: Radovilsky** — **Ingersol 280**

On-Time Performance and the Value of RFID in Cross-Docking

H. Steve Peng, California State University Hayward USA

CDN Economics and Exogenous Congestion

Eugenio de la Rosa, University of Arizona Tucson USA
John H. Hartman, University of Arizona USA
Terril Hurst, Hewlett-Packard Palo Alto USA

Four Dimensions of Enterprise Resource Planning (ERP) Systems: A New Classification Approach

Zinovy Radovilsky, California State University Hayward USA

Coffee Morning Break (Friday) — **Room**

Friday 10:00-10:30AM Coffee Break — **Front of Ingersol 122**

Coffee Morning Break

Session: 3 Opening Session — **Room**

Friday 10:30-11:45AM Opening Session **Chairman: Bordetsky** — **Ingersol 122**

Overview and Welcome

Bezalel Gavish, Southern Methodist University Dallas USA

Welcome Message

Leonard Ferrari, Naval Postgraduate School Monterey

Model-based Communication Networks: Filtering Information by Value to Improve Collaborative Decision-Making

Rick Hayes-Roth, NPS Monterey

Wednesday, July 14, 2004 Page 1 of 6

Lunch Friday — **Room**

Friday 12:00-1:30PM Lunch — **El Prado Room in Hermann Hall**

Lunch Friday

Session: 4 Network Testbeds — **Room**

Friday 1:30-3:15PM Parallel Session **Chairman: McNeill** — **ME 385**

The Network Testbed Sizing Problem - A Proposed Research Framework

EXHIBIT C

The Wayback Machine - https://web.archive.org/web/20041204234240/http://tecom.cox.smu.edu:80/icts/ictsm12/

12th International Conference on Telecommunication Systems, Modeling

- Conference Scope
- Registration Form
- Conf. Hosting Possibility
- List of Topics
- Important Dates
- Submission of Abstract/Paper
- Manuscript Prep. Instructions
- Purchasing Past Conf. Proceedings
- Committee Members
- Program schedule (pdf)
- Accepted Papers (pdf)
- Conference Sponsors
- Travel
- Monterey Info.
- Hotel Reservation
- Related Conferences
- Related Journals
- E-mail to Conf. Chairman

Conference Scope

The 12th International Conference on Telecommunication Systems - Modeling and Analysis will be held at the Naval Postgraduate School, Monterey, CA on July 22-25, 2004. The conference will build on the tradition of the earlier conferences. The general idea is to encourage informal interaction and exchanges of ideas by limiting the number of participants, concentrating on a few topics, and by presenting new problems and problem areas. The objective is to advance the state of the modeling and analysis in telecommunications by stimulating research activity on new and important problems.

The conference will be divided into segments with each segment devoted to a specific topic. This will allow for little conflict between segments. Papers will be screened by the Program Committee to ensure the quality of presentations. Abstracts and papers should be submitted directly to the Conference Chairman who will handle its review. Social and cultural activities will be included in the 2004 agenda. The organizing committee is planning special events for this conference. The conference site is the Naval Postgraduate School at Monterey, CA.

The Program Committee is open to any ideas you might have regarding additional topics or format of the conference. The intention is, to limit the number of parallel sessions to three. The conference is scheduled over a weekend to reduce teaching conflicts for academic participants and to enable participants to take advantage of weekend hotel and airfare rates and of events that take place in the Monterey area.

Potential participants should send by May 15, 2004 a paper to the conference general chair. The technical program committee will evaluate the papers, and a decision will be sent to the authors by May 20, 2004 with instructions for the final version of the paper, which is due by June 10, 2004. Full paper contributions will be considered for publication in the Telecommunication Systems Journal. Conference participants will be provided with the conference proceedings (a collection of papers presented at the conference)

Conference General Chair: Bezalel Gavish, Cox school of business, Dallas TX 75205, email Conference Chairman

EXHIBIT D

UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection

Zhenmin Li, Jed Taylor, Elizabeth Partridge, Yuanyuan Zhou, William Yurcik*

Cristina Abad, Jim Barlow, Jeff Rosendale

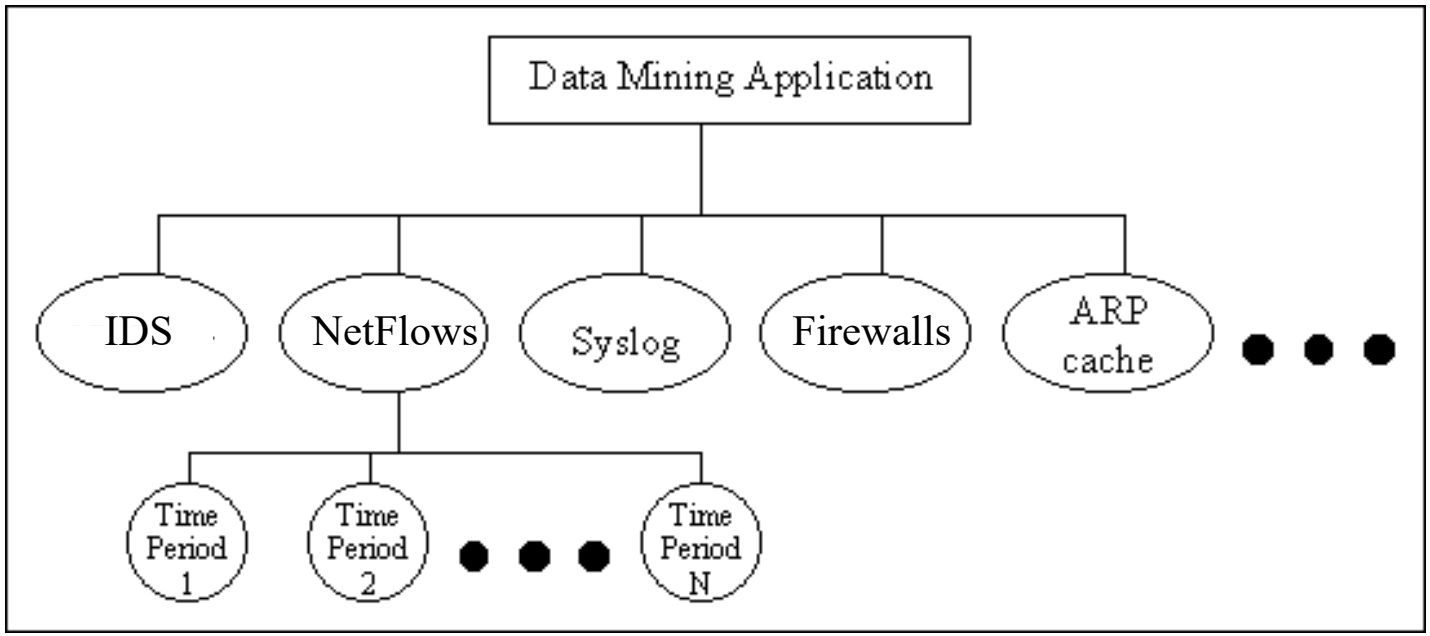
National Center for Supercomputing Applications (NCSA)

University of Illinois at Urbana-Champaign

On Intrusion Detection

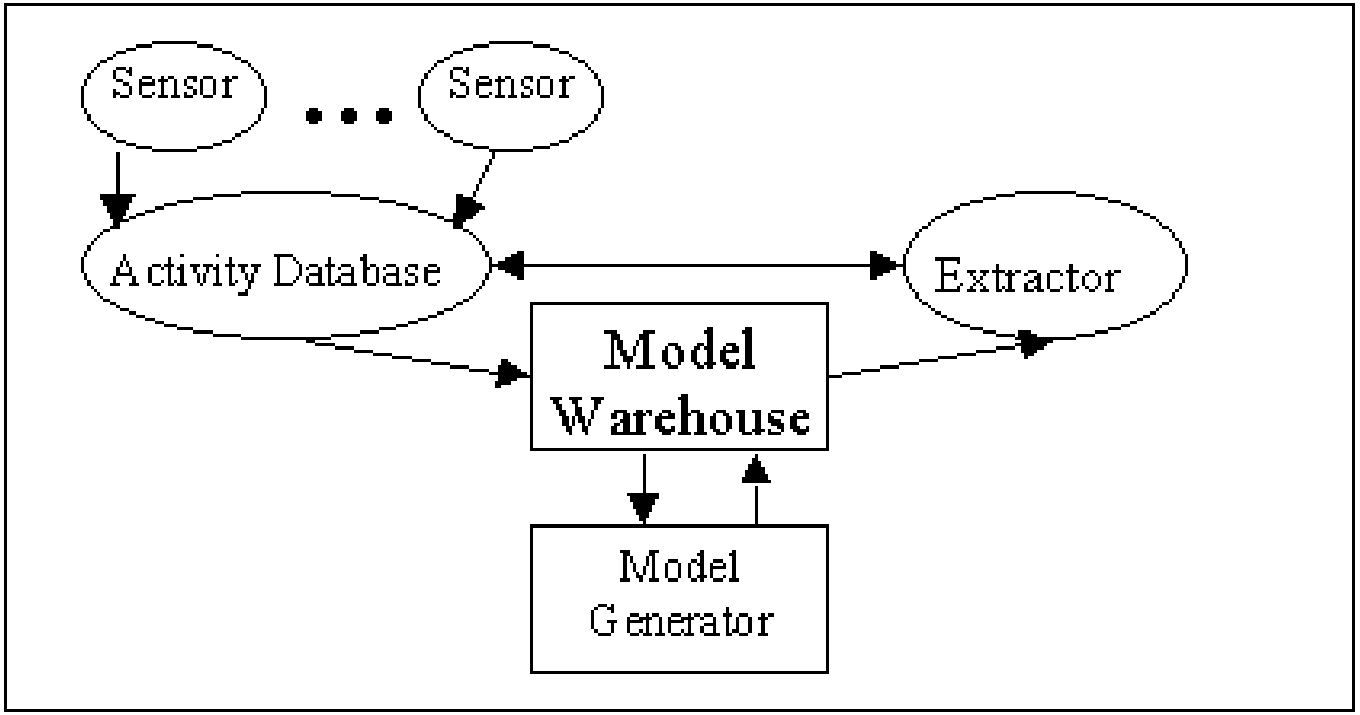
- *IDSs are important to protect networked systems*
- *However, intrusion detection is difficult:*
  - *poor performance (accuracy)*
  - *limitations under current techniques (false positives)*
  - *many attacks, new attacks, changing all the time*
  - *information overload to human users*
  - *scalability (huge data volume, data management)*
  - *many logs, each with different purposes and formatting*

The Data Management Problem

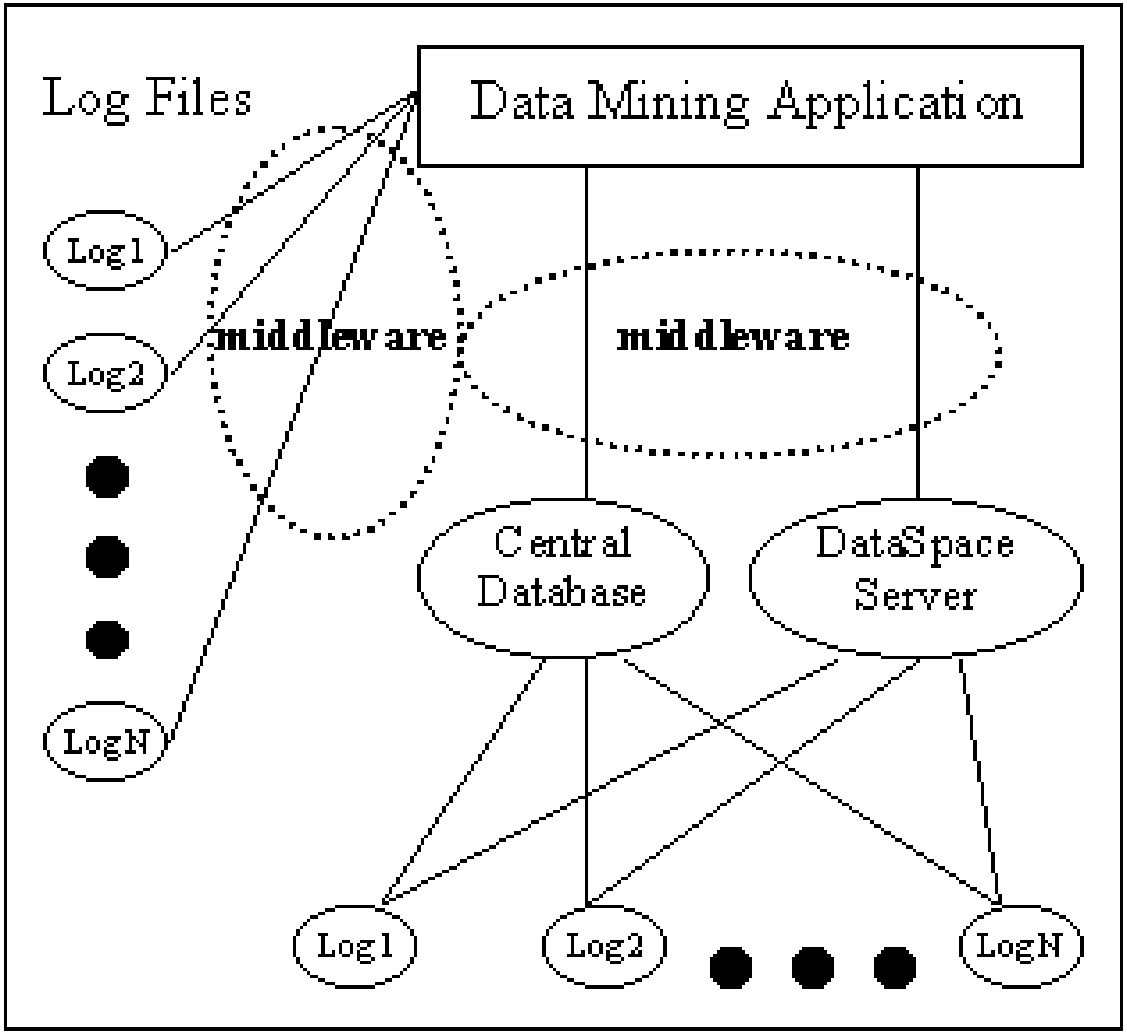


time dimension

(1) Central Database Architecture



(2) Middleware Architecture



Log Correlation

- **Correlate data across heterogeneous logs to increase IDS accuracy and/or reduce false positives**
- **Logic:**
  - ***attacks leave traces in multiple different logs***
  - ***different attacks more easily identified in different logs***
  - ***different logging sensors makes gaming sensors (evasion or squealing) by attackers more difficult***
  - ***some attacks are not evident if a single log is analyzed***

Methodology

- *Goal: show how log correlation can help improve intrusion detection*
- *Approach:*
  - *Top-down approach (attacks → logs)*
    - *Take known attacks and analyze their behavior to infer which logs may contain attack traces*
  - *Bottom-up approach (logs → attacks)*
    - *Gather relevant information from multiple logs to identify specific attack instances*

Sophos Ex. 1015

An example mapping: Attack to log traces

1) DNS v. query probe to learn if BIND is vulnerable (syslog)
2) System is attacked with 'noop' attack (tcpdump)
3) Users are created to gain root access (telnet log)
4) Gains superuser access (syslog)
5) Tries to use the system for malicious purposes (Snort)
   - ***Downloads (ftp) attack toolkit from another system.***
   - ***Installs backdoor***
   - ***Covers moves by deleting affected logs***
   - ***Days later comes back and logs in using the backdoor***
   - ***Downloads and installs Trinoo client***
   - ***Attempts to launch Trinoo DDoS***

Source: Honeynet Project. "Know your enemy"

Attack	Log								
	Syslog	Firewall	Netflow	TCP	DNS	Auth	Web	Mail	FTP
Dictionary	×	×	×	×		×	×	×	×
FTP-Write	×			×		×			×
Imap	×	×	×	×				×	
Named	×		×		×				
Phf	×			×			×		
Sendmail	×	×	×	×	×	×		×	
Xsnoop	×		×						
Apache2	×	×	×	×			×		
Back	×			×			×		
Mailbomb	×	×	×	×				×	
SYN Flood	×	×	×	×	×				
Ping of Death		×	×	×					
Process Table		×	×	×				×	
Smurf			×	×					
Udpstorm			×	×	×				

Bottom-up: A case of anomaly detection

- Detect virus Yaha (an e-mail virus)
- Correlate:
  - host information (system call sequence)
    - APISpy32 with small modifications
  - network traffic information
    - WinDump
- "Predict the next system call" method
- RIPPER, a data mining tool for rule learning
  - Fed RIPPER with ***normal*** sequences only

Training Data

- 20 hours of users normal and abnormal activity was logged
- Normal: sending and receiving e-mail messages
- Abnormal: sending and receiving e-mail messages including a message infected with the Yaha virus
- 1.9 million data points were generated
- 20% of the captured data was saved for testing (and not used for training)

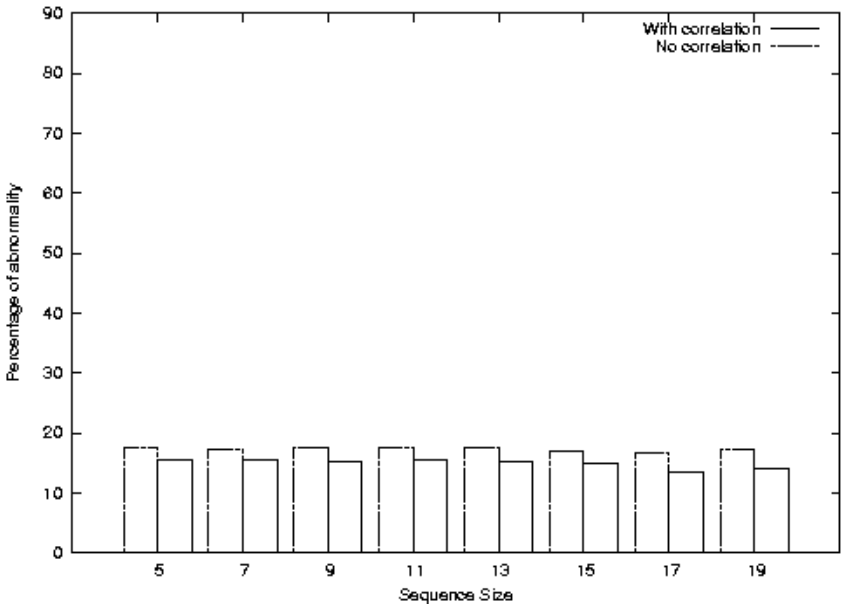
Generating Rules

- RIPPER expects a list of system calls followed by the value to predict
  - A sliding window was used to scan the normal traces and create a list of unique sequences of system calls
- Heuristic: Number of connections per past 10 seconds was included as a data point
- RIPPER generated the rules based on the training data, to predict
  - Next system call
  - Number of connections on the next 10 seconds

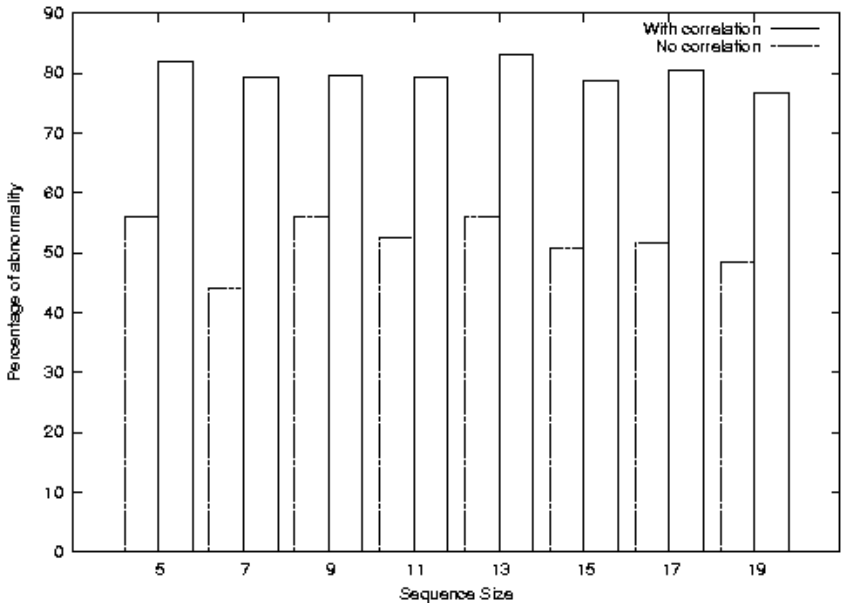
Applying Rules

- A sliding window was passed over the list of predicted values and actual values
  - If predicted value differs from actual value, penalty value is set to confidence level of broken rule
  - Penalty values from sliding window are added. If greater than threshold, region is “abnormal”
- Number of abnormal regions is added up and divided by total number of regions. This value represents how abnormal a trace is
- Same process (learning and applying rules was used for the number of connections)

Results



A normal behavior trace



An abnormal behavior trace

CONCLUSIONS

- UCLOG explores correlation for Intrusion Detection
  - Correlation between logs vs simple logs
- Experiment Results: (YaHa virus)

  comparing a single IDS to correlating system call logs and network traffic logs
  - increased accuracy by 2.5
  - reduces false positives
- Enhance and Relieve Human Operators

Questions?

http://www.ncsa.uiuc.edu/~cabad
http://www.ncassr.org

RIPPER

- **RIPPER: R**epeated **I**ncremental **P**runing to **P**roduce **E**rror **R**eduction
- William Cohen, 1995
- Obtains error rates lower than C4.5 rules, scales nearly linearly with number of training examples, and can efficiently process noisy datasets containing hundreds of thousands of examples
- Improvement of IREP (Incremental reduced error pruning)

Example output of RIPPER

- 38:- p3 = 40, p4 = 4
  - If p3 is lstat and p4 is write, then p5 is stat
- ...
- 5:- true
  - If none of the above, then p5 is open
- Each of these rules has a “confidence” level: obtained from the number of matched examples and the number of unmatched examples in the training data
- But, the training data should be nearly “complete” with regard to all possible “normal” behavior

Table 2. Normal behavior traces table

Sequence Size		No Corr.	With Corr.	Diff.
5				
	t3	8.19%	7.39%	-0.80%
	t7	16.31%	14.54%	-1.77%
	t10	31.16%	31.73%	0.57%
	t14	30.81%	29.86%	-0.95%
	t45	10.66%	10.21%	-0.45%
	t23	6.36%	6.04%	-0.32%
	t24	8.14%	7.59%	-0.55%
	t51	26.16%	25.32%	-0.84%
	t53	14.52%	13.87%	-0.65%
	t33	7.02%	6.73%	-0.29%
	t35	13.28%	13.52%	0.24%
	t40	17.89%	15.55%	-2.34%
				-0.68%
7				
	t3	7.87%	7.08%	-0.79%
	t7	15.97%	14.39%	-1.58%
	t10	30.85%	31.79%	0.94%
	t14	30.62%	29.73%	-0.89%
	t45	10.38%	9.94%	-0.44%
	t23	6.29%	5.96%	-0.33%
	t24	7.97%	7.42%	-0.55%
	t51	25.96%	25.19%	-0.77%
	t53	14.30%	13.74%	-0.56%
	t33	6.75%	6.59%	-0.16%
	t35	13.29%	13.29%	0.00%
	t40	17.41%	15.42%	-1.99%
				-0.59%
9				
	t3	8.26%	7.15%	-1.11%
	t7	16.70%	14.45%	-2.25%
	t10	30.38%	31.28%	0.90%
	t14	30.58%	29.74%	-0.84%
	t45	10.42%	9.92%	-0.50%
	t23	6.29%	5.95%	-0.34%
	t24	7.94%	7.42%	-0.52%
	t51	25.98%	25.17%	-0.81%
	t53	14.33%	13.77%	-0.56%
	t33	6.86%	6.60%	-0.26%
	t35	13.20%	13.12%	-0.08%
	t40	17.46%	15.34%	-2.12%
				-0.71%

Sequence Size		No Corr.	With Corr.	Diff.
13				
	t3	7.85%	7.16%	-0.69%
	t7	16.00%	14.45%	-1.55%
	t10	30.54%	31.52%	0.98%
	t14	30.59%	29.66%	-0.93%
	t45	10.37%	9.91%	-0.46%
	t23	6.33%	5.95%	-0.38%
	t24	8.07%	7.53%	-0.54%
	t51	26.04%	25.17%	-0.87%
	t53	14.41%	13.72%	-0.69%
	t33	6.92%	6.64%	-0.28%
	t35	13.27%	13.02%	-0.25%
	t40	17.52%	15.34%	-2.18%
				-0.65%
15				
	t3	7.84%	7.17%	-0.67%
	t7	15.79%	14.48%	-1.31%
	t10	30.64%	31.51%	0.87%
	t14	30.48%	29.57%	-0.91%
	t45	10.34%	9.87%	-0.47%
	t23	6.32%	5.93%	-0.39%
	t24	7.96%	7.43%	-0.53%
	t51	25.96%	25.14%	-0.82%
	t53	14.35%	13.66%	-0.69%
	t33	6.99%	6.60%	-0.39%
	t35	13.29%	13.06%	-0.23%
	t40	17.01%	14.96%	-2.05%
				-0.63%
17				
	t3	7.83%	6.80%	-1.03%
	t7	15.92%	13.73%	-2.19%
	t10	30.85%	30.29%	-0.56%
	t14	30.38%	27.59%	-2.79%
	t45	10.32%	9.09%	-1.23%
	t23	6.66%	5.55%	-1.11%
	t24	7.97%	6.83%	-1.14%
	t51	25.91%	22.84%	-3.07%
	t53	14.27%	12.33%	-1.94%
	t33	6.86%	5.71%	-1.15%
	t35	13.23%	11.83%	-1.40%
	t40	16.64%	13.82%	-2.82%
				-1.70%

Table 3. Abnormal behavior traces table

Sequence Size		No Corr.	With Corr	Diff.
5				
	t100	39.28%	40.37%	1.09%
	t101	56.04%	82.04%	26.00%
	t102	27.21%	32.51%	5.30%
	t103	32.73%	43.23%	10.50%
	t104	26.33%	25.03%	-1.30%
				8.32%
7				
	t100	38.45%	39.66%	1.21%
	t101	44.06%	79.41%	35.35%
	t102	25.80%	31.52%	5.72%
	t103	30.39%	41.46%	11.07%
	t104	25.41%	24.52%	-0.89%
				10.49%
9				
	t100	38.96%	40.19%	1.23%
	t101	56.07%	79.53%	23.46%
	t102	27.26%	32.23%	4.97%
	t103	31.31%	40.35%	9.04%
	t104	26.37%	25.27%	-1.10%
				7.52%
11				
	t100	38.77%	40.22%	1.45%
	t101	52.56%	79.29%	26.73%
	t102	26.45%	32.01%	5.56%
	t103	32.09%	41.42%	9.33%
	t104	25.94%	24.89%	-1.05%
				8.40%

Sequence Size		No Corr.	With Corr.	Diff.
13				
	t100	39.03%	40.15%	1.12%
	t101	55.91%	83.18%	27.27%
	t102	26.74%	31.85%	5.11%
	t103	31.57%	41.03%	9.46%
	t104	26.15%	24.84%	-1.31%
				8.33%
15				
	t100	38.79%	40.02%	1.23%
	t101	50.83%	78.82%	27.99%
	t102	26.76%	31.89%	5.13%
	t103	31.38%	40.02%	8.64%
	t104	26.15%	24.84%	-1.31%
				8.34%
17				
	t100	38.64%	39.28%	0.64%
	t101	51.54%	80.56%	29.02%
	t102	26.61%	31.35%	4.74%
	t103	30.80%	39.27%	8.47%
	t104	26.10%	24..16%	-1.94%
				8.19%
19				
	t100	39.01%	39.13%	0.12%
	t101	48.44%	76.79%	28.35%
	t102	26.23%	30.08%	3.85%
	t103	29.48%	36.82%	7.34%
	t104	26.54%	24.25%	-2.29%
				7.47%

Yaha

- E-mail virus
- Sends itself to all email addresses in MS Address Book, Messenger, Yahoo Pager and ICQ list
- Appears to be a screen saver
- Uses its own SMTP implementation
- Selects “Subject” line randomly from a list
- Messages are sent signed with the infected computer's user name
- Attachment name is randomly selected from a list
- Kills anti-virus and firewall processes running on infected computer
- Configures itself to execute each time an “.exe” files is executed

EXHIBIT E

The Wayback Machine - https://web.archive.org/web/20051215131057/http://www.ncassr.org:80/about/index.html

About NCASSR

The National Center for Advanced Secure Systems Research (NCASSR) was launched in May 2003 with an initial $5.7 million grant from the Office of Naval Research (ONR) to address the nation's critical need for a dynamic, adaptive cybersecurity infrastructure.

The center enhances and safeguards the computing and networking tools available to the nation's military forces through a variety of projects in three main categories:

- authentication and authorization
- networking and communications
- data analysis

These include the development of better ways of monitoring network security to prevent hostile cyberattacks, such as computer worms and viruses, and the creation of adaptable software radios that will allow military and emergency personnel from crisis response agencies to communicate more effectively. The research effort at NCASSR is intended to define, prototype, and test components for a next generation cybersecurity system.

The bulk of the NCASSR research is conducted at the National Center for Supercomputing Applications (NCSA) and the University of Illinois at Urbana-Champaign (UIUC), with collaborating partners at Battelle Pacific Northwest National Laboratory (PNNL), The Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPR), InfoAssure, Inc., and the University of Tennessee.

NCASSR and its projects are overseen by an Executive Committee.

The National Center for Advanced Secure Systems Research (NCASSR) is funded by the Office of Naval Research (ONR) and is led by the National Center for Supercomputing Applications (NCSA). Contact the NCASSR webmaster with questions regarding this page.

EXHIBIT F

The Wayback Machine - https://web.archive.org/web/20051215120659/http://www.ncassr.org:80/projects/index.html

NCASSR Year 2 Projects

NCSA and partner sites address the nation's critical need for a dynamic, adaptive cybersecurity infrastructure by completing projects in five main research thrusts:

Year 2 Projects:

Research Thrust: **Cyberinformatics**

1.1 Capturing and Accessing Complex Time-Sequenced Instrument Data With HDF5
1.2 Model-Based Data Aggregation for Large-Scale Sensor Networks
1.3 Application-Based Sequential Pattern Matching
1.4 Mining Hidden Networks
1.5 Cross-Document Entity Identification and Training
1.6 Interactive Visualization for Varying Spatiotemporal Data
1.7 Security Incident Fusion Tools (SIFT)
1.8 Distributed Innovation/Scalable Collaboration in Uncertain Settings (DISCUS)

Research Thrust: **Security Tools**

2.1 Policy and Key Management for Secure Group Communication in Dynamic Coalitions
2.2 Credential Management Services
2.3 Continuous Hardware Component Validation (CHCV)
2.4 Trusted Computing Exemplar (TCX)
2.5 Multicast Survivability and Security
2.6 Cluster Security as an Emergent Property
2.7 Malicious Code Reverse Engineering and Analysis (MCREA)
2.8 Secure Middleware Services for Wireless Sensor Networks
2.9 Key Management Scalability Study

Research Thrust: **Sensors and Software Defined Radio (SDR)**

3.1 Software-Defined Radio and Extensible Sensor Platform
3.2 GNU SDR Policy Enforcement System
3.3 Hazard Aware Spaces
3.4 Antennas for Wireless Sensors
3.5 Mobile Sensor Network Authentication
3.6 Secure Virtual Machine / SDR
3.7 Hardware Acceleration for Information Security (HAIS)

Research Thrust: **Secure Access Grid Laboratory Testbed**

4.1 SABRE (Simulated Anomalous Behavior & Recognition)
4.2 PAWNS: Programming and testing Applications on a Wireless Network of Sensors
4.3 Multilevel Testbed Encryption Experiments/Trusted Channel Implementation
4.4 PKI Testbed
4.5 CyberCIEGE (Extended Scenarios)

Research Thrust: **SCADA Protocol Authenticator Project**

5.1 SCADA Functional Reqs/Establish Development Framework
5.2 Authentication SCADA Protocols Conceptual Design
5.3 Demonstrate SCADA Authenticator Prototype in Real Time

Year 1 Project List

The National Center for Advanced Secure Systems Research (NCASSR) is funded by the Office of Naval Research (ONR) and is led by the National Center for Supercomputing Applications (NCSA). Contact the NCASSR webmaster with questions regarding this page.

EXHIBIT G

The Wayback Machine - https://web.archive.org/web/20041216182045/http://www.ncassr.org:80/projects/sift/

Security Incident Fusion Tools (SIFT)

Publications Software Sponsored-Forums Invited Participation
SIFT-in-the-News SIFT Team Collaborators Funding

The SIFT project is defining the new specialty field of "Internet security visualization" as evidenced by our paper/software productivity and leadership in IEEE/ACM forums. An high-level overview of our research follows:

Government and business organizations use computer network infrastructures that hold a vast amount of information for system administrators and security engineers. There are typical logs common to most computer networks, but the systems are often large and dynamic, making it difficult to extract knowledge from the sea of information. Individually, each system log can be massive, causing operator overload. When overload occurs, security events can slide by unnoticed. Overload can also cause operators to disregard alarms due to high false positive rates. Even in homogeneous infrastructures, solutions from a single vendor fail to scale to medium or large networks. However, the problem is compounded because many organizations have network infrastructures from multiple vendors.

We are developing the Security Incident Fusion Tool (SIFT), an integrated framework for evaluating the security of an entire computer network on a single screen. The project will address the need to discover security incidents that currently go undetected by security operations systems. Two new SIFT tools, NVisionIP and VisFlowConnect, leverage human visual cognitive abilities to process log data into knowledge for situational awareness of network security. It is estimated that human beings can visually process a screen of information at 150 Mbits per second, with the ability to discriminate relatively minor shifts in color, shape, and motion. By presenting network data visually, it can be scanned quickly, patterns in complex data rise to the surface, and inferences become intuitive. Once a security professional becomes familiar with the normal appearance of the network being monitored, it is much easier to spot attacks including new so-called "zero-day attacks". The tools are designed to give security engineers situational awareness of an entire network in order to help them determine when a network is under attack, what is being attacked, and what form the attack is taking.

Our plans for Year 2 NCASSR funding build on our successes in Year 1 with the following tasks:

- release of NVisionIP and VisFlowConnect for Internet distribution
- use human factors feedback to improve NVisionIP and VisFlowConnect
- develop advanced algorithms for processing security data and incorporate these into our visualization tools

back to the top

Sophos Ex. 1015
Page 44 of 61

SIFT Publications

- link to full-text papers and corresponding publication forums (current count is 24 papers)

back to the top

SIFT Software

- **NVisionIP software** (visualizing system state for Internet security situational awareness)
- **VisFlowConnect software** (visualizing link analysis for Internet security situational awareness)

back to the top

SIFT-Sponsored-Forums

- **FloCon - Network Flow Analysis Workshop 2005**
  (Network Flow Analysis for Security Situational Awareness)
  Hotel Monteleone, New Orleans LA, September 20-22, 2005.
- **VizSEC/DMSEC-2004**
  SIFT is Co-Chairing this Workshop on Visualization and Data Mining for Computer Security to be held in conjunction with the 11th ACM Conference on Computer and Communications Security (CCS), Washington DC, 29 October 2004.
- Organizer and presenter: Panel session on ***"Building Usable Security Systems"*** presented at the **8th International Financial Cryptography Conference (FC04)** Key West, Florida, 10 February 2004. Panelists: Andrew Patrick, L. Jean Camp, Bill Yurcik, Ka-Ping Yee.
  > brief description: This panel reviewed some of the human-factors issues encountered when building usable security systems. It explored the roles and demands placed on users of security systems, and provide examples of design solutions that can assist in making security systems usable and effective. The goal of the panel was to bring awareness of human-factors issues to the conference community, build a network of interested people, discuss high priority areas for research and development, and explore opportunities for collaboration.
- Organizer and presenter: Panel session on ***"Advances in Visualization of Cyber Security Attacks and Alerts"*** at the **Forum on Information Warfare** Georgetown University, 4 December 2003.
  > brief description: a panel discussion from the leaders in security visualization research and commercial products, sexy demonstrations and lively discussion about what goes on under-the-hood of various security visualization systems.

back to the top

Sophos Ex. 1015
Page 45 of 61

Invited Participation

{Note: This list is for invited talks of various types to show people want to hear about our achievements in person including sponsoring us to present. This list does not include published papers at conferences - see publications link above for these talks. Also NCSA/UIUC talks/demonstrations are not included here since they are too numerous, in the spring of 2005 the SIFT team gave an estimated 30 talks of various forms, most with extensive demonstrations.}

- **DETER Laboratory Experimenters Workshop**
  Washington DC, 25 October 2004. Specialists familiarize themselves with the DETER testbed and EMIST tools aimed at bolstering Internet defenses against malicious attacks.

- **DARPA Network Metrics Workshop**
  Kaiwat Island, South Carolina, 18-20 October 2004.
  Network Metrics Project Phase brings together two groups: (1) computer scientists who are intrusion detection specialists, and (2) physicists, mathematicians and computer scientists who are familiar with the mathematical representations of networks, entropy research, group theory and complexity theory.

- **Talk: "NVisionIP and VisFlowConnect: Two Interactive Tools for Visualizing Network Flows for Security,"** abstract.
  - 20 July 2004, Hewlett-Packard Research Laboratories (San Jose CA)
  - 21 July 2004, IBM Almaden Research Laboratory (San Jose CA)
  - 22 July 2004, Cisco Systems Inc. Headquarters (San Jose CA)
  - 23 July 2004, Lawrence Livermore National Laboratory - LLNL (US Dept of Energy, Livermore CA)
  - 27 July 2004, University of California at Davis (Davis CA)
  - 28 July 2004, Lawrence Berkeley National Laboratory - LBL (US Dept of Energy, Berkeley CA)

- **FloCon: Network Flow Analysis Workshop**. 20-22 July 2004, sponsored by the CERT Coordination Center, Carnegie Mellon University/Software Engineering Institute.
  brief description: a small invitation-only meeting bringing together members of the security operations and analysis community to discuss their experiences with systems for large-scale network flow-based traffic monitoring and analysis.
  - "**Security at Line Speed with NetFlows**" (Flow Collection Architecture Panel)
  - "**Shared Intelligence is our Best Defense: Incentives That Work versus Disincentives That Can Be Solved** " (Data Sharing Panel)

- **PORTIA Workshop on Sensitive Data in Medical, Financial, and Content-Distribution Systems** . 8-9 July 2004, Stanford University.
  brief description: This workshop is intended to foster collaborations between computer scientists who seek to enhance the security and privacy of sensitive data about people and organizations and domain experts in fields that need technological solutions to address customer concerns and to fulfill legal obligations. The goal is to formulate specific technical problems that are important to user communities that deal with large amounts of sensitive data but are not satisfactorily solved by current technology.

- Talk: ***"Better Tools for Security Administration: Enhancing the Human-Computer Interface with Visualization"*** at the **DIMACS Workshop on Usable Privacy and Security Software**. 7-9 July 2004 - DIMACS Center, Rutgers University, Piscataway, NJ
  brief description: This workshop and working group is intended to bring together security and privacy experts with human-computer interaction experts

Sophos Ex. 1015
Page 46 of 61

to discuss approaches to developing more usable privacy and security software. The workshop sessions on July 7 and July 8 will include invited talks and discussion. July 9 will feature a "working group" of invited participants who will spend the day identifying important problems, discussing some of the research issues raised during the workshop in more depth, and brainstorming about approaches to future research, collaboration, and more user-centered design of security and privacy software.

- Talk: ***"What You Don't Know Can Hurt You: An Overview of Scalable Security Data Management for Internal/External Data Sharing"*** at the **ISMA Data Catalog 2004 Workshop** sponsored by CAIDA and held at the San Diego Supercomputing Center (SDSC), University of California at San Diego, 3 June 2004.
  brief description: CAIDA is designing an Internet Measurement Data Catalog (IMDC) which is a repository to archive meta-data for many heterogeneous data sets. The objective of the IMDC project is to facilitate access, archiving, and reproducibility of Internet data and research results as well as sharing data among Internet researchers.

- **Security Operators and Researchers Workshop for Higher Education** 17-18 November, 2003, Cisco Systems, Inc. Corporate Headquarters, San Jose, CA.
  brief description: Cisco Systems gathered input from leaders in security research and operations to help in developing a Cisco specific security blueprint for the academic computing environment while also identifying new technologies and directions that will drive new product development.

- **Security at Line Speed (S@LS) Internet2 Workshop** held 11-13 August 2003 in Chicago, IL.
  brief description: Invitation-only workshop to disseminate information on security problems and best-known solutions. As a result, workshop attendees jointly drafted a document that identifies best security practices specifically for the academic community.

- Talk: ***"Enabling Proactive Prediction, Avoidance, and Diagnosis by Providing Visual Situational Awareness to Human Operators,"*** at the **IBM Academy Conference on Proactive Problem Prediction, Avoidance, and Diagnosis** IBM T. J. Watson Research Center, Yorktown Heights, NY. 28 April 2003.
  brief description: abstract

- **New Directions in Scalable Cyber-Security in Large-Scale Networks: Deployment Obstacles**, sponsored by Large-Scale Network Group of Interagency Working Group on Information Technology R&D; (DOE, NSF, NSA, NIST, NASA, and DARPA), Reston VA USA, 13-14 March 2003.
  brief description: This invitation-only workshop was intended to identify and describe challenging issues for large-scale cyber security and obstacles to security deployments. The workshop itself and subsequent report served to help define funding priorities for the DoE, NSF, NSA, NIST, and DARPA.

- Keynote Speech: ***"Insights on the Future of Data Mining Highlighting Storage and Visualization"***
  at the **FBI Information Technology Study Group (ITSG) Workshop on Data Mining for Intelligence**, 17 October 2002, San Antonio, Texas.
  brief description: Closed forum to the US Government law enforcement and intelligence communities for learning state-of-the-art techniques in specific areas, this workshop was focused on data mining.

- **Conference Program Committees:**
  - **2nd Annual FloCon Workshop**
    (Network Flow Analysis for Security Situational Awareness)
    (2005)

- **International Workshop on Assurance in Distributed Systems and Networks (ADSN)**
  (2005)
- **Financial Cryptography and Data Security**
  (2005)
- **1st International Workshop on Broadband Wireless Services and Applications (BroadWISE)**
  (2004)
- **Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)** held in conjunction with the 11th ACM Conference on Computer and Communications Security (CCS), Washington D.C.
  (2004)
- **IEEE International Conference on Computer Communications and Networks**
  (2000-2004)
- **International Conference on Telecommunications Systems Modeling and Analysis (ICTSM)**
  (2001-2004)
- **IEEE Conference on Local Computer Networks**
  (2001-2003)

back to the top

SIFT-in-the-News

- **"UI Chosen to Safeguard Military Computers from Attacks"**
  The Daily Illini 7-13-03

- **"Visualizing the Enemy"**
  NCSA 2-17-04 News Release
  - reprinted in SuperComputing Online, 2-27-2004.

- **"Two NCSA-Developed Tools Set Sights On Network Attacks"**
  Grid Today: Daily News and Information for the Global Grid Community, Vol 3 No 8, 2-23-2004.

- **"Tools Let Network Operators See Their Way to Security"**
  Champaign-Urbana News Gazette, 3-4-2004.
  - reprinted here by ACM TechNews Volume 6, Issue 614 3-5-2004

- **"Researchers Develop Network-Security Visualization Tools"**
  IEEE Computer Magazine, April 2004.

- **"Visualization Software Allows Close Examination of Networks"**
  HPCwire, 4-4-04.

- **"The Latest Research From Major Institutions With Advances In Security, Interoperability & Software, The Future Looks Bright"**
  Processor, 5-21-2004 • Vol. 26 Issue 21.

back to the top

SIFT Team

SIFT Staff Mailing List {sift-sec AT ncsa.uiuc.edu}

William (Bill) Yurcik
SIFT Principal Investigator (PI)
Manager, NCSA Security Research
{specialty: security situational awareness, security visualization, NetFlows processing for security}
byurcik AT ncsa.uiuc.edu
{contact for external inquiries especially from the mass media}

Adam Slagell
NCASSR SIFT Project Lead
NCSA Security Engineer
{specialty: cryptography, log anonymization, intrusion detection sytems}
slagell AT ncsa.uiuc.edu

Cristina Abad
UIUC Computer Science Ph.D. student
{speciality: UCLog+, security event correlation, security situational awareness systems}

Ratna Bearavolu
NCSA Senior Software Engineer
{specialty: NVisionIP & VisFlowConnect software development}

Kiran Lakkaraju
UIUC Computer Science Ph.D. student
{specialty: AI/Machine learning, NVisionIP lead developer}

Adam Lee
UIUC Computer Science Ph.D. student
{specialty: computer network security}

Greg Pluta
NCSA Technical Program Manager
{specialty: windows/linux process/event monitoring, windows/linux administration}

Ramona Su
UIUC Human Factors M.S. student
{specialty: human-computer interaction, usability studies}

Mike Treaster
UIUC Computer Science Ph.D. student
{specialty: autonomic security}

Xiaoxin Yin
UIUC Computer Science Ph.D. student
{specialty: link analysis, relational data mining, VisFlowConnect lead developer}

Yifan Li
UIUC Computer Science Ph.D. student {specialty: geospatial data mining, time series data, NetFlows processing}

back to the top

SIFT Collaborators

NCSA Collaborators

Jim Barlow
NCSA Manager of Security Operations

Tim Brooks
Security Engineer, NCSA Security Operations

Donna Cox
NCSA Division Leader Experimental Technologies

Jeff Rosendale
NCSA TeraGrid Security

Dave Semeraro
NCSA Division Leader Visualization and Virtual Environments

Aashish Sharma
Security Engineer, NCSA Security Operations

University of Illinois at Urbana-Champaign (UIUC) Collaborators

Jiawei Han , Prof. of Computer Science

Yuanyuan Zhou , Asst. Prof. of Computer Science

External Collaborators

Andrey Bobyshev
Network Analyst/Data Communications Group
Fermi National Accelerator Laboratory

Paul Dokas
Office of Information Technology Security

Matthew Luallen
President
Sph3r3.com

Scott Pinkerton
Argonne National Laboratory

Sophos Ex. 1015
Page 50 of 61

and Assurance, University of Minnesota Eser Kandogan IBM Almaden Research Eben Haber IBM Almaden Research Donna LaMore Asst. Group Leader/Data Communications Group Fermi National Accelerator Laboratory	Chris Poetzel Argonne National Laboratory Jim Rothfuss Lawrence Berkeley National Laboratory Ken Rowe Independent Security Consultant Rowe Systems

back to the top

SIFT Funding

- 2004-2005 Cisco Systems Grant (pending)
- 2004-2005 ONR NCASSR Year Two Grant
- 2003-2004 ONR NCASSR Year One Grant
- 2002-2003 ONR TRECC Seed Funding Grant

back to the top

EXHIBIT H

The Wayback Machine - https://web.archive.org/web/20050205214439/http://www.ncassr.org:80/projects/sift/papers/

{link to SIFT Project homepage}.

SIFT Publications

All SIFT Publications in Reverse Chronological Order
Previous Work on Human-in-the-Loop Security
Previous Work on Visualization for Network Management
Previous Work on Intrusion Detection
or
SIFT Publications Grouped into Five Topic Areas:
(1) Scalable NetFlows Processing for Security

(2) Security Visualization Tools (for Security Situational Awareness)
▪ **NADAS** (IP Network Management)
▪ **NVision(s)** (System State)
  ▪ **NVisionIP** (IP)
  ▪ **NVisionCC** (Cluster Security)
  ▪ **NVisionPorts** (Network Port Traffic - in development)
  ▪ **NVisionSS** (Storage Security - in development)
▪ **VisFlowConnect(s)** (Link Analysis)
  ▪ **VisFlowConnect-IP** (IP)
  ▪ **VisFlowConnect-CC** (Cluster Security - in development)
  ▪ **VisFlowConnect-Ports** (Network Port Traffic - in development)
  ▪ **VisFlowConnect-SS** (Storage Security - in development)
▪ **KiteTail(s)** (integrated views)
  ▪ **KiteTailIP** (IP - in development)
  ▪ **KiteTailCC** (Cluster Security - in development)
  ▪ **KiteTailPorts** (Network Port Traffic - in development)
  ▪ **KiteTailSS** (Storage Security - in development)

(3) Security Event Correlation (UCLog+)
(4) Data Mining
(5) Log Anonymization for Security Data Sharing

Reverse Chronological Order

26. Xiaoxin Yin, William Yurcik, and Adam Slagell, " **The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness** ," *Third IEEE International Information Assurance Workshop* University of

Sophos Ex. 1015
Page 53 of 61

Maryland, March 23-24, 2005.

25. Michael Treaster, " **A Survey of Distributed Intrusion Detection Approaches** ," *ACM Computing Research Repository (CoRR)* Technical Report cs.CR/0501001, January 2005.

24. William Yurcik " **Visualization Tools for Security Administrators** ," *8th International Financial Cryptography (FC) Conference,* , Key West FL, 2004; also republished in *Lecture Notes in Computer Science (LNCS): Financial Cryptography (FC 2004 revised papers)*, Vol. 3110, Springer Verlag, 2004, pp. 112-113;

23. Adam Slagell, Jun Wang, and William Yurcik " **Network Log Anonymization: Application of Crypto-PAn to Cisco Netflows** ," *NSF/AFRL Workshop on Secure Knowledge Management (SKM)* , 2004.

22. Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, and Kiran Lakkaraju " **VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004.

21. Kiran Lakkaraju, William Yurcik, Adam J. Lee, Ratna Bearavolu, Yifan Li, and Xiaoxin Yin, " **NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004.

20. Adam Slagell and William Yurcik " **Sharing Computer Network Logs for Security and Privacy: A Motivation for New Methodologies of Anonymization** ," *ACM Computing Research Repository (CoRR) Technical Report 0409005*, September 2004.

19. William Yurcik, " **The Design of an Imaging Application for Computer Network Security Based on Visual Information Processing** ," *{to appear in} SPIE Defense and Security Symposium / Visual Information Processing XIII* , 2004.

18. Kiran Lakkaraju, William Yurcik, Ratna Bearvolu, and Adam J. Lee, "**NVisionIP: An Interactive Network Flow Visualization Tool for Security**," *IEEE International Conference on Systems, Man and Cybernetics (SMC)* , 2004.

17. Greg Cole, Natasha Bulashova, and William Yurcik "**Geographical NetFlows Visualization for Network Situational Awareness: NaukaNet Administrative Data Analysis System (NADAS)**," *12th International Conference on Telecommunication Systems - Modeling and Analysis (ICTSM)* , 2004.

16. Zhenmin Li, Jed Taylor, Elizabeth Partridge, Yuanyuan Zhou, William Yurcik, Cristina Abad, James J. Barlow, and Jeff Rosendale, "***UCLog*: A Unified, Correlated Logging Architecture for Intrusion Detection** ," *12th International Conference on Telecommunication Systems - Modeling and Analysis (ICTSM)* , 2004.

15. Yifan Li, Jiawei Han, and Jiong Yang, " **Clustering Moving Objects** ," *International Conference on Knowledge Discovery and Data Mining (KDD)* , 2004.

14. Yifan Li, Jiong Yang, and Jiawei Han, " **Continuous K-Nearest Neighbor Search for Moving Objects** ," *International Conference on Scientific and Statistical Database Management (SSDBM)* , 2004.

13. Xiaoxin Yin, Jiawei Han, Jiong Yang, and Philip S. Yu, " **CrossMine: Efficient Classification Across Multiple Database Relations** ," *International Conference on Data Engineering (ICDE)* , 2004.

12. Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, " **Correlation Between NetFlow System and Network Views for Intrusion Detection** ," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)* , 2004.

11. Xiaoxin Yin, William Yurcik, Yifan Li, Kiran Lakkaraju, Cristina Abad, " **VisFlowConnect: Providing Security Situational Awareness by Visualizing Network Traffic Flows** ", *Workshop on Information Assurance (WIA04)* held in conjunction with the *23rd IEEE International Performance Computing and Communications Conference (IPCCC 2004)* , 2004.

10. Cristina Abad, Jed Taylor, Cigdem Sengul, William Yurcik, Yuanyuan Zhou, and Ken Rowe, " **Log Correlation for Intrusion Detection: A Proof of Concept** ," *19th Annual Computer Security Applications Conference (ACSAC)* , 2003.

9. William Yurcik, Kiran Lakkaraju, James Barlow, and Jeff Rosendale, " **A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection** ," *3rd IEEE International Conference on Data Mining (ICDM) Workshop on Data Mining for Computer Security (DMSEC)* , 2003.

8. Ratna Bearavolu, Kiran Lakkaraju, William Yurcik, and Hrishikesh Raje, " **A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks** ," *IEEE Military Communications Conference (Milcom)* , 2003.

7. Xiaoxin Yin, Kiran Lakkaraju, Yifan Li, and William Yurcik, " **Selecting Log Data Sources to Correlate Attack Traces for Computer Network Security: Preliminary Results** ," *11th International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM11)* , U.S. Naval Postgraduate School, 2003.

6. Kiran Lakkaraju, Ratna Bearavolu, and William Yurcik, " **NVisionIP - A Traffic Visualization Tool for Security Analysis of Large and Complex Networks** ," *International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS)* , 2003.

5. Xiaoxin Yin, Jiawei Han, and Jiong Yang, " **Efficient Multi-relational Classification by Tuple ID Propagation** ," *2nd Workshop on Multi-Relational Data Mining in conjunction with The 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (MRDM)* , 2003.

4. Xiaoxin Yin and Jiawei Han, " **CPAR: Classification Based on Predictive Association Rules** ," *SIAM International Conference on Data Mining* , 2003.

3. William Yurcik, James Barlow, Yuanyuan Zhou, Hrishikesh Raje, Yifan Li, Xiaoxin Yin, Mike Haberman, Dora Cai, and Duane Searsmith, " **Scalable Data Management Alternatives to Support Data Mining Heterogeneous Logs for Computer Network Security** ," *SIAM Workshop on Data Mining for Counter Terrorism and Security* , 2003.

2. William Yurcik, James Barlow, and Jeff Rosendale, " **Maintaining Perspective on Who Is The Enemy in the Security Systems Administration of Computer Networks**," *ACM CHI Workshop on System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems* , 2003.

1. William Yurcik, James Barlow, Kiran Lakkaraju, and Mike Haberman, "**Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements**," *ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC)*, 2003.

Previous Work on Human-in-the-Loop Security

3. Alex Korzyk and William Yurcik,, " **On Integrating Human-In-The-Loop Supervision Into Critical Infrastructure Process Control Systems** ," *Advanced Simulation Technologies Conference(ASTC), Infrastructure Protection/Emergency Management Symposium (IPEM)*, Society for Computer Simulation Intl., San Diego, CA USA, April 2002.

2. William Yurcik, Aashish Sharma, and David Doss, " **False Impressions: Contrasting Perceptions of Security as a Major Impediment to Achieving Survivable Systems** ," *IEEE/CERT/SEI Fourth Information Survivability Workshop (ISW)*, IEEE Computer Society Press, Vancouver, BC Canada, March 2002.

1. Carl Turner, Merrill Zavod, and William Yurcik, " **Factors That Affect The Perception of Security and Privacy of E-Commerce Web Sites** ," *Proceedings of the 4th International Conference on Electronic Commerce Research (ICER-4)*, Dallas TX USA, Nov. 2001, Vol 2, pp. 628-636.

Previous Work on Visualization for Network Management

Sophos Ex. 1015
Page 55 of 61

2. Alexander Gubin, William Yurcik, and Larry Brumbaugh, " **Network Management Visualization with PingTV** ," *26th IEEE Conference on Local Computer Networks (LCN)* , 2001.

1. Alexander Gubin, William Yurcik, and Larry Brumbaugh, " **PingTV: A Case Study in Visual Network Monitoring** ," *IEEE Visualization (Vis)* , 2001, pp. 421-424, 580.

Previous Work on Intrusion Detection

2. William Yurcik, " **Controlling Intrusion Detection Systems by Generating False Positives: Squealing Proof-of-Concept** ," *27th IEEE Conference on Local Computer Networks (LCN)* , 2002.

1. Samuel Patton, William Yurcik, and David Doss " **An Achilles' Heel in Signature-Based IDS: Squealing False Positives in SNORT** ," *Fourth International Symposium on Recent Advances in Intrusion Detection (RAID)* , University of California-Davis USA, Oct. 2001.

Scalable NetFlows Processing for Security

- under peer review at present, to be listed soon

NADAS (Visualizing IP Network Management)

1. Greg Cole, Natasha Bulashova, and William Yurcik "**Geographical NetFlows Visualization for Network Situational Awareness: NaukaNet Administrative Data Analysis System (NADAS)**," *12th International Conference on Telecommunication Systems - Modeling and Analysis (ICTSM)* , 2004.

NVisionCC (Visualizing Cluster Security System State)

for more information on Cluster Security here is a link to our Cluster Security Project

3. William Yurcik, Xin Meng, Nadir Kiyanclar " **NVisionCC: A Visualization Framework for High Performance Cluster Security** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the 11th ACM Conference on Computer and Communications Security, 2004.

2. William Yurcik, Xin Meng, Gregory A. Koenig " **A Cluster Process Monitoring Tool for Intrusion Detection: Proof-of-Concept** ," *29th IEEE Conference on Local Computer Networks (LCN)* , 2004.

1. William Yurcik, Xin Meng, Gregory A. Koenig " **Cluster Security as a Unique Problem with Emergent Properties: Issues and Techniques** ," *5th LCI International Conference on Linux Clusters* , 2004.

NVisionIP (Visualizing IP System State)

9. Kiran Lakkaraju, William Yurcik, Adam J. Lee, Ratna Bearavolu, Yifan Li, and Xiaoxin Yin, " **NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the *11th ACM Conference on Computer and Communications Security*, 2004.

8. William Yurcik, " **The Design of an Imaging Application for Computer Network Security Based on Visual Information Processing** ," *{to appear in}* *SPIE Defense and Security Symposium / Visual Information Processing XIII*,

Sophos Ex. 1015
Page 56 of 61

2004.

7. Kiran Lakkaraju, William Yurcik, Ratna Bearvolu, and Adam J. Lee, "**NVisionIP: An Interactive Network Flow Visualization Tool for Security**," *IEEE International Conference on Systems, Man and Cybernetics (SMC)* , 2004.

6. Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, " **Correlation Between NetFlow System and Network Views for Intrusion Detection** ," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)* , 2004.

5. William Yurcik, Kiran Lakkaraju, James Barlow, and Jeff Rosendale, " **A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection** ," *3rd IEEE International Conference on Data Mining (ICDM) Workshop on Data Mining for Computer Security (DMSEC)* , 2003.

4. Ratna Bearavolu, Kiran Lakkaraju, William Yurcik, and Hrishikesh Raje, " **A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks** ," *IEEE Military Communications Conference (Milcom)* , 2003.

3. Kiran Lakkaraju, Ratna Bearavolu, and William Yurcik, " **NVisionIP - A Traffic Visualization Tool for Security Analysis of Large and Complex Networks** ," *International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS)* , 2003.

2. William Yurcik, James Barlow, and Jeff Rosendale, " **Maintaining Perspective on Who Is The Enemy in the Security Systems Administration of Computer Networks**," *ACM CHI Workshop on System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems* , 2003.

1. William Yurcik, James Barlow, Kiran Lakkaraju, and Mike Haberman, "**Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements**," *ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC)*, 2003.

VisFlowConnect-IP (Visualizing IP Link Analysis)

5. Xiaoxin Yin, William Yurcik, and Adam Slagell, " **The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness** ," *Third IEEE International Information Assurance Workshop* University of Maryland, March 23-24, 2005.

4. Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, and Kiran Lakkaraju " **VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness** ," *CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC)* held in conjunction with the *11th ACM Conference on Computer and Communications Security*, 2004.

3. William Yurcik, " **The Design of an Imaging Application for Computer Network Security Based on Visual Information Processing** ," *{to appear in}* *SPIE Defense and Security Symposium / Visual Information Processing XIII* , 2004.

2. Xiaoxin Yin, William Yurcik, Yifan Li, Kiran Lakkaraju, Cristina Abad, " **VisFlowConnect: Providing Security Situational Awareness by Visualizing Network Traffic Flows** ", *Workshop on Information Assurance (WIA04)* held in conjunction with the *23rd IEEE International Performance Computing and Communications Conference(IPCCC 2004)* , 2004.

1. Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, " **Correlation Between NetFlow System and Network Views for Intrusion Detection** ," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)* , 2004.

Security Event Correlation (UCLog+)

Sophos Ex. 1015
Page 57 of 61

6. Michael Treaster, "**A Survey of Distributed Intrusion Detection Approaches**," *ACM Computing Research Repository (CoRR)* Technical Report cs.CR/0501001, January 2005.

5. Zhenmin Li, Jed Taylor, Elizabeth Partridge, Yuanyuan Zhou, William Yurcik, Cristina Abad, James J. Barlow, and Jeff Rosendale, "***UCLog*: A Unified, Correlated Logging Architecture for Intrusion Detection**," *12th International Conference on Telecommunication Systems - Modeling and Analysis (ICTSM)*, 2004.

4. Cristina Abad, Yifan Li, Kiran Lakkaraju, Xiaoxin Yin, and William Yurcik, "**Correlation Between NetFlow System and Network Views for Intrusion Detection**," *Workshop on Link Analysis, Counter-terrorism, and Privacy* held in conjunction with the *SIAM International Conference on Data Mining (ICDM)*, 2004.

3. Cristina Abad, Jed Taylor, Cigdem Sengul, William Yurcik, Yuanyuan Zhou, and Ken Rowe, "**Log Correlation for Intrusion Detection: A Proof of Concept**," *19th Annual Computer Security Applications Conference (ACSAC)*, 2003.

2. Xiaoxin Yin, Kiran Lakkaraju, Yifan Li, and William Yurcik, "**Selecting Log Data Sources to Correlate Attack Traces for Computer Network Security: Preliminary Results**," *11th International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM11)*, U.S. Naval Postgraduate School, 2003.

1. William Yurcik, James Barlow, Yuanyuan Zhou, Hrishikesh Raje, Yifan Li, Xiaoxin Yin, Mike Haberman, Dora Cai, and Duane Searsmith, "**Scalable Data Management Alternatives to Support Data Mining Heterogeneous Logs for Computer Network Security**," *SIAM Workshop on Data Mining for Counter Terrorism and Security*, 2003.

Data Mining

5. Yifan Li, Jiawei Han, and Jiong Yang, "**Clustering Moving Objects**," *International Conference on Knowledge Discovery and Data Mining (KDD)*, 2004.

4. Yifan Li, Jiong Yang, and Jiawei Han, "**Continuous K-Nearest Neighbor Search for Moving Objects**," *International Conference on Scientific and Statistical Database Management (SSDBM)*, 2004.

3. Xiaoxin Yin, Jiawei Han, Jiong Yang, and Philip S. Yu, "**CrossMine: Efficient Classification Across Multiple Database Relations**," *International Conference on Data Engineering (ICDE)*, 2004.

2. Xiaoxin Yin, Jiawei Han, and Jiong Yang, "**Efficient Multi-relational Classification by Tuple ID Propagation**," *2nd Workshop on Multi-Relational Data Mining* held in conjunction with *The 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (MRDM)*, 2003.

1. Xiaoxin Yin and Jiawei Han, "**CPAR: Classification Based on Predictive Association Rules**," *SIAM International Conference on Data Mining*, 2003.

Log Anonymization for Security Data Sharing

2. Adam Slagell, Jun Wang, and William Yurcik "**Network Log Anonymization: Application of Crypto-PAn to Cisco Netflows**," *NSF/AFRL Workshop on Secure Knowledge Management (SKM)*, 2004.

3. Adam Slagell and William Yurcik "**Sharing Computer Network Logs for Security and Privacy: A Motivation for New Methodologies of Anonymization**," *ACM Computing Research Repository (CoRR)* *Technical Report 0409005*, September 2004.

EXHIBIT I

Original message

Message ID	<Pine.SOL.3.95.1041105111807.14109a-100000@pecos.ncsa.uiuc.edu>
Created on:	5 November 2004 at 12:29 (Delivered after 3 seconds)
From:	Bill Yurcik <byurcik@ncsa.uiuc.edu>
To:	Christina Abad <cabad@ncsa.uiuc.edu>
Subject:	ISDS paper for IEEE database engineering conference
SPF:	NONE with IP 0.0.0.0 Learn more

Download original

Copy to clipboard

```
X-Gmail-Received: a1eb8ed5c1f33326ef765286edd985960b233522
Delivered-To: cristina.abad@gmail.com
Received: by 10.38.83.28 with SMTP id g28cs37058rnb;
        Fri, 5 Nov 2004 09:29:10 -0800 (PST)
Received: by 10.38.99.5 with SMTP id w5mr427406rnb;
        Fri, 05 Nov 2004 09:29:09 -0800 (PST)
Return-Path: <byurcik@ncsa.uiuc.edu>
Received: from mail.ncsa.uiuc.edu (mail.ncsa.uiuc.edu [141.142.2.28])
        by mx.gmail.com with ESMTP id 70si200745rnc;
        Fri, 05 Nov 2004 09:29:09 -0800 (PST)
Received-SPF: pass (gmail.com: domain of byurcik@ncsa.uiuc.edu designates
141.142.2.28 as permitted sender)
X-Envelope-From: byurcik@ncsa.uiuc.edu
Received: from pecos.ncsa.uiuc.edu (pecos.ncsa.uiuc.edu [141.142.4.6]) by
mail.ncsa.uiuc.edu (8.11.7/8.11.7) with SMTP id iA5HT7H12598; Fri, 5 Nov 2004
11:29:07 -0600
Date: Fri, 5 Nov 2004 11:29:06 -0600 (CST)
From: Bill Yurcik <byurcik@ncsa.uiuc.edu>
To: Christina Abad <cabad@ncsa.uiuc.edu>
cc: cabad@fiec.espol.edu.ec, Rafael Bonilla <bonilla@ncsa.uiuc.edu>
Subject: ISDS paper for IEEE database engineering conference
Message-ID: <Pine.SOL.3.95.1041105111807.14109a-100000@pecos.ncsa.uiuc.edu>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII
X-NCSA-MailScanner-Information: Please contact the help@ncsa.uiuc.edu for more
information
X-NCSA-MailScanner: Found to be clean


Cristina:

now for the next paper!

here is the conference for the rejected ISDS

1st IEEE International Workshop on Networking Meets Databases (NetDB)
in cooperation with 21st IEEE Conference on Data Engineering (ICDE 2005)
April 8th and 9th, 2005
National Center of Science
Tokyo, Japan
http://infolab.usc.edu/netdb05/index.html
we will figure out who goes to Japan later, lets just submit and get
accepted firts

here are my ideas to start:

(1) I think you should start a new paper in the IEEE double-column format
since we opnly have 5 pages to work with.
pull from the ISDS paper what you think is most important,
 author instructions from the cfp:
```


Sophos Ex. 1015
Page 60 of 61

"Submissions should be in the form of extended abstracts following the IEEE double-column format and no longer than 5 pages."

(2) re-read the UCLog paper found here:
www.ncassr.org/projects/sift/papers/uclog.pdf

(2) change all references of ISDS to UCLog+
and the + is the added correlation between
alarms and *raw data* not found in UClog or most other systems

(3) Email me what you have in pdf and .tex
next week and I will help add/modify things as well
as set up some new pictures/figures depending on
how much space we have.

let me know if you have different ideas about how to start the paper,
I'm flexible but we don't have much time, the deadline is
Monday Nov 15th

Cheers! - Bill