Resiliency Research Snapshot

June 2011

Rich Pietravalle
Dan Lanz

Contents

Executive Summary

This report offers a snapshot of unclassified government, academic, and commercial cyber resiliency efforts gathered as background for MITRE Cyber-Resiliency research.

Toward that end, the authors gathered information to note current cyber resiliency research, and assist in generating new ideas for MITRE research and sponsor action. The information was collected through MITRE library research resources in iterative passes, the last pass completed in mid-Spring, 2011.

The authors first related a characterization of the resiliency landscape to library research professionals, who then used that characterization to perform a search of available literature sources. Several iterations were run, with earlier searches influencing those that followed. The authors defined categories for binning the results under a few recognized resiliency themes such as dynamic reconfiguration, detection, and isolation. The search yielded about 300 items, most of them published after 2005. The items had contributors from academic institutions in about 75% of the total, government in about 50% of the articles, and about 25% had commercial participation. About 70% of the articles had one or more USA affiliated participants, 28% had European participants, and 15% had participants from other parts of the world. Detection was the most frequent item categorization with twice the volume of any other category, and isolation and deception articles were the least well represented.

1.0 Introduction

This report offers one snapshot of unclassified government, academic, and commercial cyber resiliency efforts with the intent to identify promising research areas, capability gaps to fill, and questions that would guide future research actions. The material is gathered here as a public release document for the benefit of other cyber security and cyber resilience[1] researchers.

The sections that follow contain references to research papers, ongoing projects, and other resiliency-related efforts. Research from 2006[2] to the report release date is included.

It should be noted that commercial organizations with the most resiliency experience are not well represented in this report. Google, Akamai, Amazon, and Verizon are examples of companies that achieve impressive resiliency against failures through the use of many of the techniques that appear in this report's categorized lists. Such organizations generally do not publish in the literature captured by the databases searched for this report, if at all. A better understanding of their focus areas and lessons learned would be useful information to guide future resiliency research. These organizations are also in a unique position to assist in increasing the resiliency of their customers' systems; e.g., detecting attacks and communicating this information to their customers for action.

This report is organized as five major sections followed by six appendices. Section 2 of this paper describes the categories under which the resiliency references in this report have been organized. Section 3 identifies those organizations with a commitment to resiliency research, and the major organizations funding resiliency research. Appendix I contains the identified resiliency literature references, organized by category. Appendix II lists commercial organizations known to perform resiliency research. Appendix III contains a matrix of institutions that are associated with the Appendix I resiliency references by category.

[1] The term “resiliency” or “resilience” has multiple connotations, depending on the context in which it is used. In RAMBO, “resiliency” is short for “cyber resiliency,” and means the ability of cyber systems and cyber-dependent missions to anticipate, withstand, and recover from attacks, including those by an advanced persistent threat (APT) actor, and to evolve to be more robust in the face of such attacks. Note that APT attacks differ from the type of scenarios assumed by researchers and practitioners for most forms of resilience (including many of the research efforts cited in this paper). In the high-performance computing, fault-tolerance, and dependability literature, as in the literature on organizational resilience and on resilience engineering, resilience involves the ability to withstand a (single, one-time, limited-duration) disruption, maintaining a minimum acceptable level of performance and recovering within an acceptable time. APT attacks occur over extended time periods. The APT may use capabilities developed in the course of long-term intrusions and insertions to create an intense, limited-duration disruption. The APT may also use such capabilities to create a less intense but near-permanent degree of disruption. Disruption may be an undesirable side effect from the standpoint of the APT (as when the organization identifies and seeks to remediate long-term exfiltration activities).

[2] In some cases, research prior to 2006 is included. However, our literature survey has focused on work published after 2005.

2.0 Overview

2.1 Methodology

The report authors and library services utilized traditional library research methods to search for reports, papers, and journal articles relating to cyber resilience. Sources included the open Internet, Inspec/Compendex literature database, government and commercial research lab web sites, and internal materials, entries for reports, conference papers and journal articles. The original topics searched related to cyber security and cyber-attack resilience, resilient networks/systems/architectures, cascading failure, fault tolerance, attack detection/containment, randomization, and redundancy.

2.2 Description of Categories

The resiliency references presented in this report have been organized by resiliency category. These categories were established by the report authors based upon a set of objectives for resilient systems defined by Harriet Goldman in her background paper entitled "Building Secure, Resilient Architectures for Cyber Mission Assurance"[3] and related survey materials. The eight categories used throughout the report are presented in Table 1. The categories were selected with a view to allow separation of concepts into bins of related articles yet to not fragment the collection so much that its utility to a resiliency researcher would be diminished. A traditional library search was performed after the authors described the attributes of cyber resiliency to the library research professionals applied this to retrieve a set of articles that would fit that overall characterization. The authors then reviewed the titles, abstracts, and some of the available full text of the articles to review the suitability of the article and its category assignment.

Categorizing the articles was often subjective, given broad themes and topics that bridge more than one category. Other researchers may have arrived at a different set of category assignments. For example, the "detection" category included many articles that covered traditional intrusion detection or networking topics, but were then judged (usually from the abstract) to contain some innovative or interesting element for resiliency purposes.

[3] Goldman, H. G. Building Secure, Resilient Architectures for Cyber Mission Assurance. Paper presented at the 2010 Secure & Resilient Cyber Architectures Conference, McLean, VA.

Table 1: Resiliency categories

Resiliency Category	Short Name	Description
Adaptive Response	**Adaptive**	Provide more resilient system by actively countering an attack after it has been detected
Integrity (for Resilience)	**Integrity**	Capability to preserve integrity of key part of system while under attack
Deception	**Deception**	Misinformation (providing attacker with incorrect information about attack in progress to complicate his/her ability to mount a successful attack), honeypots, hiding from attacker
Dynamic variations: Distributedness, Moving Targets, Non-Persistence, Unpredictability, Randomness, Diversity, Redundancy	**Dynamic**	Characteristics of architecture or general environment that are modifying in a way that provides resilience to attack; keep parameters of execution varying; prevent single technology point of failures and attacks from impacting critical operations
Isolation/Containment	**Isolation**	Segregate components of dubious pedigree from trusted ones to reduce the attack surface, simplify systems and interfaces, and limit the damage and spread of exploits, when they occur; includes virtualization and network level separation/segmentation
Detection/Monitoring	**Detection**	Monitor system condition or sense anomalies, and analyze/correlate resulting data
Metrics/Assessment	**Metrics**	Assessing, measuring and benchmarking cyber resilience of computer systems
Cross-Area, Modeling, Architectures, Background	**Cross-Area**	Background, framework or architectural articles on resiliency, and items that bridge more than one resiliency category.

2.3 Overall Observations

Figure 1 and Figure 2 summarize the results for the approximately 320 articles identified as part of this effort. Figure 1 depicts the total number of resiliency-related research articles by category.

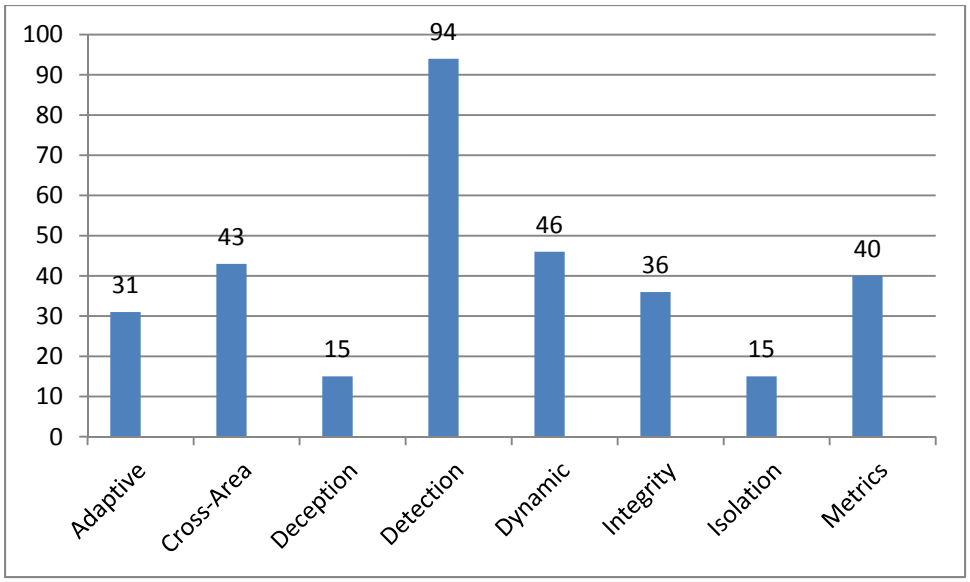

Figure 1: Item count by category

Figure 2 shows the distribution of categories for all identified research.

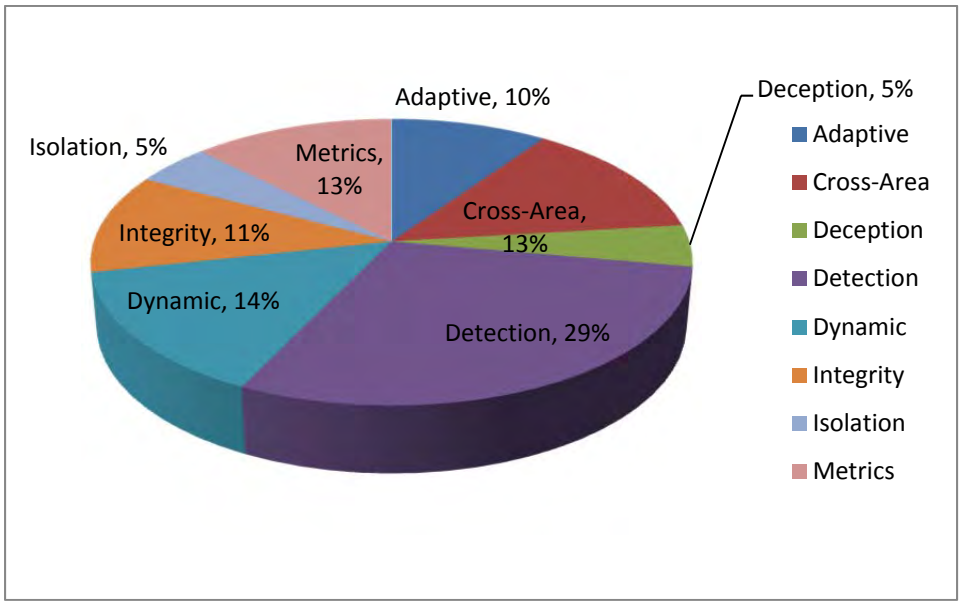

Figure 2: Category as percentage of items

Clearly, significant resources are being applied to detection research. This may be due to the maturity and relatively high activity level of network and intrusion detection-related research, as well as the fact that detection is the first step in security across many domains of security research. Research regarding the collection of metrics to assess, measure and benchmark computer system resiliency also has received considerable interest.

During the data collection phase of this project, the authors tagged each resiliency reference with the sectors (academic, government, and/or commercial) that the research authors are affiliated with or in

which the item originated or was funded. Figure 3 depicts the distribution of each sector within each category. In Figure 4, the number of resiliency references for each category by sector is depicted, noting that many papers have contributors from more than one sector. Overall, for the 320 items, 74% had at least one participant from the academic sector, 55% had participants from the government sector, and 25% had participation from the commercial sector.

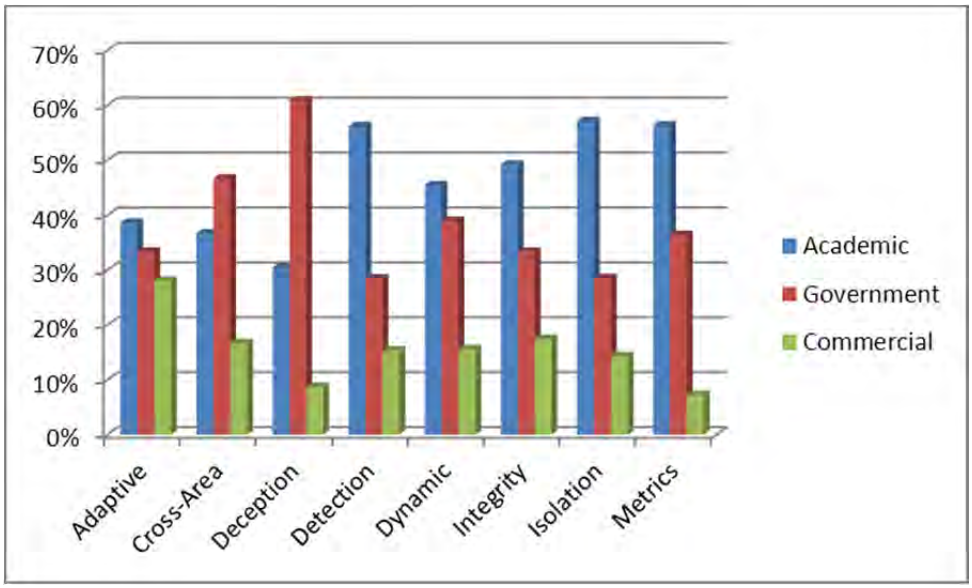

Figure 3: Percent Sector contribution within each category

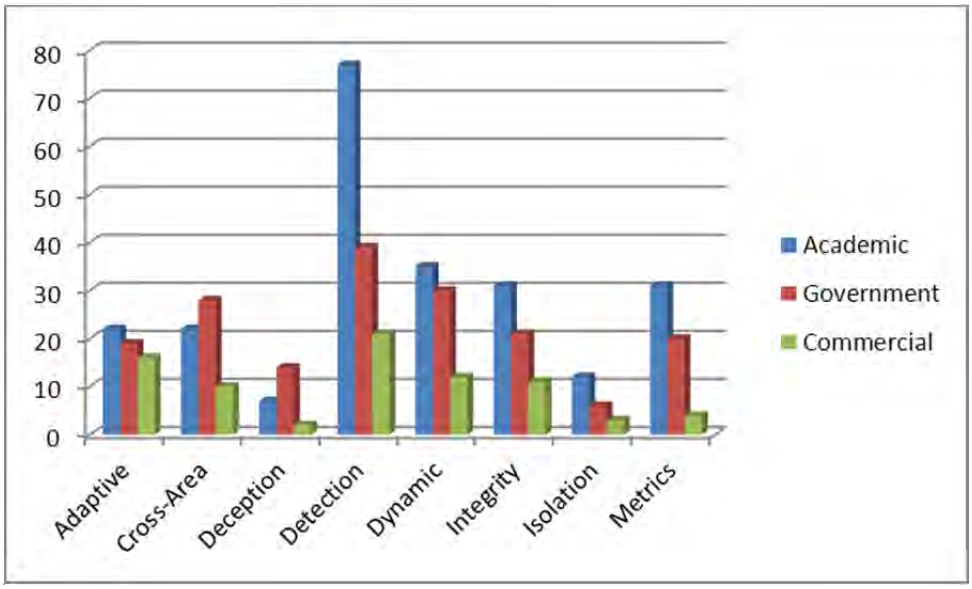

Figure 4: Count of sector contributors for items by category

See Appendix IV for a matrix of research institutions by resilience areas for the resiliency references represented in this report.

Figure 5 and Figure 6 depict the number and percentage of contributing institutions for research items by region (several institutions may contribute to one research item). The regional associations were recorded through an internet search for the location for each of the affiliation names captured by the library professionals in the database record. Not surprisingly, the U.S. and Europe dominate. However, it is likely that actual Asian resiliency research is under-represented given better coverage of American and European items by the ultimate sources for this study.

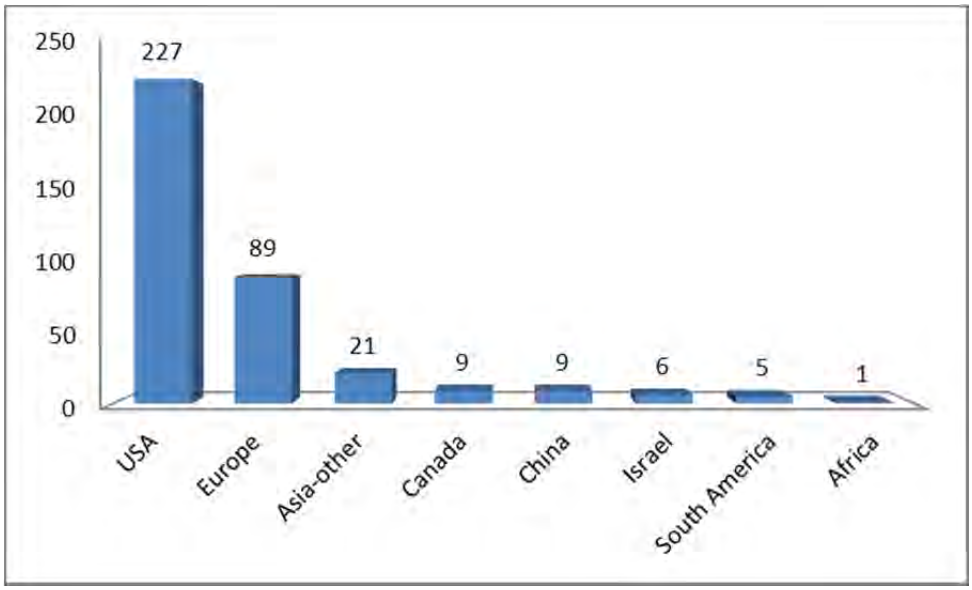

Figure 5: Total number of items by count of item regional participation

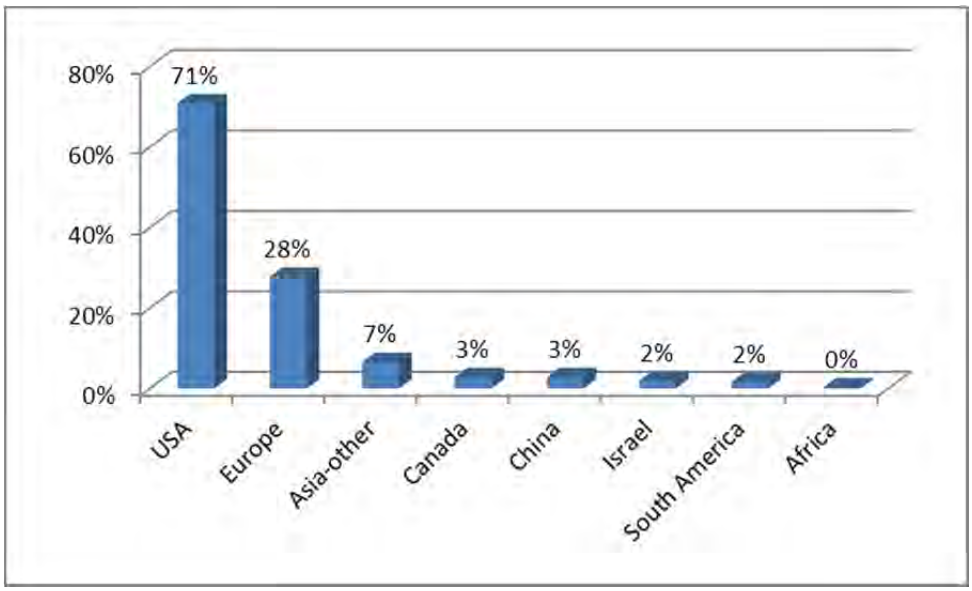

Figure 6: Item regional participation as percent of total item count

3.0 Research Organizations

Appendix IV presents a matrix of institutions associated with resiliency references listed in Appendix I. Several of the organizations listed in the matrix appear to have a significant commitment to resiliency research through the number or type of research items noted in publicly available information.

3.1 Research Organization Highlights

3.1.1 BBN Technologies

BBN—in collaboration with universities and other commercial organizations—has published research dating back to 2000 involved with intrusion tolerance and detecting and recovering from cyber-attacks. Much of the research is DARPA, AFRL and Navy funded.

3.1.2 Carnegie Mellon University

CMU has collaborated with American and European universities in attack defense, intrusion detection, and process improvement research. Some research is Army Research Laboratory, Army Research Office, NSF, CMU CyLab, and foreign funded.

3.1.3 Columbia University

Columbia has performed research under NSA and DARPA funding involved with intrusion and crimeware prevention.

3.1.4 Institute EURECOM (France)

EURECOM has collaborated with American, Canadian and European universities in research regarding malware/botnet modeling/detection.

3.1.5 George Mason University

GMU has collaborated with DoD contractors and other universities to perform research regarding intrusion tolerance, intrusion detection and code injection.

3.1.6 Georgia Institute of Technology

GIT has collaborated with other educational institutions to undertake research regarding reliability against cyber-attacks, intrusion detection, malware/botnets, and DoS attacks.

3.1.7 Idaho National Labs

INL has become a national leader in research regarding securing control systems.

3.1.8 Institute Eurecom – France

IE has collaborated with US and foreign universities on intrusion detection research. Some research is at least partially EU-funded.

3.1.9 International Business Machines (IBM) Research

IBM Research has collaborated with other commercial organizations and both US and foreign universities in intrusion tolerance and DOS prevention research.

3.1.10 Lancaster University (UK)

LU has participated with commercial organizations on research involving networks resilient to cyber-attack.

3.1.11 Lawrence Berkeley National Laboratory

LBNL has collaborated with other educational institutions on research involving intrusion detection and computer system diversity.

3.1.12 Los Alamos National Laboratory

LANL is involved in research regarding resilient computing environments, high-end computing resilience, and attack detection/defense.

3.1.13 Pacific Northwest National Laboratory

PNNL is involved in research regarding cyber-attack detection and adaptive defense.

3.1.14 Purdue University

Purdue has collaborated with commercial organizations and US and foreign universities in research regarding intrusion detection/response/containment and system reliability. Some of this research is Purdue CERIAS, Office of Naval Research, NSF, DARPA, and Microsoft Research funded.

3.1.15 Sandia National Laboratories

Sandia has worked with government, commercial and academic organizations in system and networking resiliency, as well as hardware/software tamper-resistance, high performance computer resilience, and many other unclassified and classified security research projects.

3.1.16 Stanford University

Stanford has collaborated with US and foreign universities in research regarding intrusion detection, isolation, and resilient system architectures. Some research is Focus Center Research Program (FCRP), Gigascale Systems Research Center (GSRC), and NSF funded.

3.1.17 Symantec Corp.

Symantec has partnered with educational institutions on research involving intrusion response, honeypots, intrusion detection, and data space randomization.

3.1.18 University of California, Davis

UC-Davis has collaborated with commercial organizations in research regarding intrusion detection and response. Some research is NSF and DoE funded, and with gifts received from VMware, Dell, and Symantec.

3.1.19 University of California, Santa Barbara

UC-Santa Barbara has collaborated with foreign universities for intrusion detection research.

3.1.20 University of Coimbra – Portugal

This Portuguese university has performed security measurement and honeypot research.

3.1.21 University of Illinois at Urbana-Champaign

UI has partnered with other universities on research involving intrusion detection, tolerance, response, and containment. Some research has been funded by DARPA and NSF.

3.1.22 University of Lisbon

UL has performed research regarding intrusion detection/tolerance under EU funding.

3.1.23 University of Maryland-College Park

UM-College Park has partnered with commercial organizations and US and foreign universities to perform research regarding intrusion tolerance and attack data analysis. Some research has been funded by DARPA and NSF.

3.1.24 University of Michigan-Ann Arbor

UM-Ann Arbor has performed research regarding intrusion detection and attack analysis, some of which was funded by NSF.

3.2 Organizations Funding Cyber Resiliency Efforts

The organizations below provided significant resiliency research funding to government, academic and commercial organizations.

Air Force Office of Scientific Research
Air Force Research Laboratory
Army Research Laboratory
Army Research Office
Defense Advanced Research Projects Agency
Defense Threat Reduction Agency
Department of Defense
Department of Energy
Department of Homeland Security
European Commission
European Network and Information Security Agency (ENISA)
Federal Networking and Information Technology Research and Development (NITRD)
National Science Foundation
Office of Naval Research

Appendix I: Resiliency Literature References

I.1 Adaptive

DoD SBIR Award: Malicious Binary Code Automated Response Forensics and Immunity - Tools and Methods (2004). from http://sba-sbir-qa.reisys.com/sbirsearch/detail/68493
(PI affiliated with 2LRESEARCH.)

Toward a Safer and More Secure Cyberspace (2007). Washington, DC: National Academies Press. http://www.cyber.st.dhs.gov/docs/Toward_a_Safer_and_More_Secure_Cyberspace-Full_report.pdf
Research note: NRC report on securing cyberspace, recommending certain resiliency research. See the Self Regenerative Systems (SRS) program, page 297, although the research may be marginally out-of-date at this point.

DoD SBIR Award: System Self-Protection and Autonomic Response for Hardware Based Software Protection (2008). from https://sba-sbir-qa.reisys.com/content/system-self-protection-and-autonomic-response-hardware-based-software-protection-2
(PI affiliated with AFCO Systems Development, Inc.)

National Science Foundation Award: Collaborative Research - CT-M: Hardware Containers for Software Components (2009). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0830910&WT.z_pims_id=6191
(PIs are affiliated with George Washington University.)
Research note: NSF research award focusing on hardware features to improve the security of software systems. The goal is to rapidly detect and also recover from attacks that improperly access memory or take over the CPU.

Abie, H., Savola, R., Bigham, J., Dattani, I., Rotondi, D., & Da Bormida, G. (2010). Self-healing and secure adaptive messaging middleware for business critical systems. *International Journal on Advances in Security, 3*(1&2), 34-51. http://www.iariajournals.org/security/sec_v3_n12_2010_paged.pdf
(Author affiliation: Norwegian Computing Center - Norway; VTT Technical Research Centre - Finland; Queen Mary University of London; Q-Sphere Ltd - UK; TXT e-solutions SpA - Italy; and CNIT - Italy)
This research is in the context of the EU project GEMOM (Genetic Message-Oriented Secure Middleware, www.gemom.eu), 2008-2010, Grant Agreement No. 215327, approved by the EU Commission.

Alphatech Inc. (2004). *Real-Time Evaluation of Cyber-Course of Action (COA) Impact on Performance & Effectiveness* (Final Technical Report). Rome, NY: Air Force Research Laboratory. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA422197&Location=U2&doc=GetTRDoc.pdf
(Author affiliation: Alphatech Inc)
Sponsored by DARPA, Order No. J353 and AFRL/IFTB

Alsubhi, K., Aib, I., Francois, J., & Boutaba, R. (2009). *Policy-based security configuration management, application to intrusion detection and prevention.* Paper presented at the IEEE International

Conference on Communications.
(Author affiliation: University of Waterloo - Canada and MADYNES - INRIA - France)
This research was partially supported by WCU (World Class University) program through the Korea Science and Engineering Foundation funded by the Ministry of Education, Science and Technology (Project No. R31-2008- 000-10100-0) and partially supported by the Natural Science and Engineering Council of Canada (NSERC).

Bachwani, R., Gryz, L., Bianchini, R., & Dubnicki, C. (2008, 6-8 Oct.). *Dynamically quantifying and improving the reliability of distributed storage systems.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Naples.
(Author affiliation: Rutgers University and NEC Labs America)

Badishi, G., Herzberg, A., Keidar, I., Romanov, O., & Yachin, A. (2008, 6-8 Oct.). *An empirical study of denial of service mitigation techniques.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Naples.
(Author affiliation: Israel Institute of Technology and Bar-Ilan University, Israel)
Supported by the Israeli Ministry of Science.

Brun, Y., & Medvidovic, N. (2007, September 4). *Fault and adversary tolerance as an emergent property of distributed systems' software architectures.* Paper presented at the Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia.
(Author affiliation: University of Southern California)
This work is sponsored in part by the National Science Foundation under Grant number ITR-0312780.

Bu, T., Norden, S., & Woo, T. (2006). A survivable DoS-resistant overlay network. *Computer Networks, 50*(9), 1281-1301.
(Author affiliation: Bell Labs/Lucent Technologies)

Cheetancheri, S., Agosta, J.-M., Levitt, K., Wu, F., & Rowe, J. (2008). Optimal cost, collaborative, and distributed response to zero-day worms - a control theoretic approach. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 231-250). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Davis and Intel Research)

Chong, J., Pal, P., Atigetchi, M., Rubel, P., & Webber, F. (2006). *Survivability architecture of a mission critical system: The DPASA example.* Paper presented at the Computer Security Applications Conference, Los Alamitos, CA.
(Author affiliation: BBN Technologies)
This work has been supported by DARPA under contract number F30602-02-C-0134.

Dasgupta, D., & Carvalho, M. (2010, October 29). *Designing Resilient Mission Critical Systems.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Frias-Martinez, V., Stolfo, S. J., & Keromytis, A. D. (2008). Behavior-based network access control: a proof-of-concept *Lecture Notes in Computer Science No. 5222: Information Security* (pp. 175-190): Springer-Verlag.
(Author affiliation: Columbia University)

This work was partially supported by NSF Grant CNS-06-27473 and by DARPA Grant HR0011-06-1-0034.

Jintao, X. (2007). *PID: A queue management scheme for improving network resilience under worm attacks.* Paper presented at the International Performance, Computing and Communications Conference
(Author affiliation: University of Turabo, Puerto Rico)
This work is supported in part by Puerto Rico Industrial Development Company (PRIDCO) grant R&D 2003-18.

Li, L., Cornwell, M. R., Hultman, E., Just, J. E., & Sekar, R. (2009, June 29). *Practical techniques for regeneration and immunization of COTS applications.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: Stony Brook University and Global InfoTek, Inc)
This work was funded in part by Defense Advanced Research Project Agency (DARPA) under contract N00178-07-C-2005. Sekar's work was also supported by ONR grant N000140710928 and NSF grants CNS- 0627687 and CNS-0831298.

Liao, Q., Cieslak, D. A., Striegel, A. D., & Chawla, N. V. (2008). Using selective, short-term memory to improve resilience against DDoS exhaustion attacks. *Security and Communication Networks, 1*(4), 287-299.
(Author affiliation: University of Notre Dame)

Linlin, X., Smith, P., Banfield, M., Leopold, H., Sterbenz, J. P. G., & Hutchison, D. (2009). Towards resilient networks using programmable networking technologies *Lecture Notes in Computer Science No. 4388: Active and Programmable Networks* (pp. 83-95): Springer-Verlag.
(Author affiliation: Lancaster University, UK)
Linlin Xie and Paul Smith are supported by Telekom Austria.

Locasto, M., Wang, K., Keromytis, A., & Stolfo, S. (2006). FLIPS: Hybrid adaptive intrusion prevention. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 82-101). Berlin / Heidelberg: Springer
(Author affiliation: Columbia University)

Nagarajan, A., & Sood, A. (2010, June 28). *SCIT and IDS architectures for reduced data ex-filtration.* Paper presented at the Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS), Chicago.
(Author affiliation: MIT and SCIT Labs)
This research was partially supported by NSF grant OISE - 0940922.

Nguyen, Q., & Sood, A. (2009, June 29). *Quantitative approach to tuning of a time-based intrusion-tolerant system architecture.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: George Mason)
Dr. Sood's research is partially supported by a research grant made to George Mason University by Lockheed Martin Corporation.

Pal, P., Rubel, P., Atighetchi, M., Webber, F., Sanders, W. H., Seri, M., et al. (2006). An architecture for

adaptive intrusion-tolerant applications. *Software - Practice and Experience, 36*(11-12), 1331-1354.
(Author affiliation: BBN Technologies; University of Illinois at Urbana-Champaign; University of Maryland, College Park; Boeing Company; IBM Research; and Technion – Israel Institute of Technology)
Contract/grant sponsor: DARPA; contract/grant number: F30602-00-C-0172

Pal, P., Webber, F., & Schantz, R. (2007, March 23). *The DPASA survivable JBI-A high-water mark in intrusion-tolerant systems.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: BBN Technologies)
This research was funded by DARPA under AFRL contract no. F30602-02-C-0134

Smart Information Flow Technologies (SIFT). GRASP, from http://www.sift.net/projects/computer-security/grasp

Wang, S.-H., Tseng, C., Levitt, K., & Bishop, M. (2007). Cost-sensitive intrusion responses for mobile ad hoc networks. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 127-145). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Davis)
This work is in part supported by the NSF (awards ANI-0093221, ANI-0301108, and EIA-0224449), the DOE via ORNL, and by gifts from VMware, Dell, and Symantec.

Wong, C., Bielski, S., Studer, A., & Wang, C. (2006). Empirical analysis of rate limiting mechanisms. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 22-42). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)

Wu, Y.-S., Modelo-Howard, G., Foo, B., Bagchi, S., & Spafford, E. H. (2008, 6-8 Oct.). *The search for efficiency in automated intrusion response for distributed applications.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Naples.
(Author affiliation: Purdue University)
We acknowledge partial support of this work by CERIAS at Purdue.

Zhang, F., Papatriantafilou, M., & Tsigas, P. (2008, 6-8 Oct.). *Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS).
(Author affiliation: Chalmers University of Technology - Sweden)

Zonouz, S. A., Khurana, H., Sanders, W. H., & Yardley, T. M. (2009, June 29 - July 2). *RRE: A game-theoretic intrusion Response and Recovery Engine.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: University of Illinois at Urbana-Champaign)
This material is based upon work supported by the National Science Foundation under grant no. CNS-0524695, as part of the NSF/DOE/DHS Trustworthy Cyber Infrastructure for Power Center.

I.2 Cross-area

Resilience-building technologies: State of knowledge (2006). Toulouse, France: ReSIST: Resilience for Survivability in IST. http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledge.pdf
See also Appendices - Papers produced by ReSIST partners since January 2006: http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledgeAppend.pdf

National Cyber Defense Financial Services Workshop Report: Helping Form a Sound Investment Strategy to Defend against Strategic Attack on Financial Services, October 28-29, 2009 (2010). National Cyber Defense Initiative. http://www.cyber.st.dhs.gov/docs/NCDI_FI_Workshop_Report.pdf
Research note: NSF/DHS-funded National Cyber Defense Initiative workshop to better understand the nature of high-impact, large-scale attacks on the banking and finance sector, approaches to addressing those classes of attacks, and ways that industry, academia, and government can work together on such approaches. One of the key recommended research areas resulting from this conference involved resiliency. Appendix 5 of report contains specific research challenge.

Askoxylakis, I., Belimpasakis, P., Bencsath, B., Broda, M., Buttyan, L., Clemo, G., et al. (2010). *Priorities for research on current and emerging network technologies*. Heraklion, Greece: European Network and Information Security Agency (ENISA).
http://www.enisa.europa.eu/act/it/library/deliverables/procent/at_download/fullReport

Axelrod, C. W. (2009). Investing in software resiliency. *CrossTalk, 22*(6), 20-25.
http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-0-Issue.pdf
(Author affiliation: U.S. Cyber Consequences Unit)

Baecher, P., Koetter, M., Holz, T., Dornseif, M., & Freiling, F. (2006). The Nepenthes platform: An efficient approach to collect malware. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 165-184). Berlin / Heidelberg: Springer.
(Author affiliation - Nepenthes Development Team and University of Mannheim)

Basin, D., & Cremers, C. (2010). Modeling and analyzing security in the presence of compromising adversaries. In D. Gritzalis, B. Preneel & M. Theoharidou (Eds.), *Lecture Notes in Computer Science No. 6345: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2010* (pp. 340-356). Berlin / Heidelberg: Springer
(Author affiliation: Swiss Federal Institute of Technology, Zurich)
This work is supported by ETH Research Grant ETH-30 09-3 and the FP7-ICT-2007-1 Project no. 216471 (ADVANTSSAR).

Berthier, R., Arjona, J., & Cukier, M. (2009, June 29 - July 2). *Analyzing the process of installing rogue software.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: University of Maryland, College Park and Universidad Politecnica of Valencia, Spain)

Cappello, F., Geist, A., Gropp, B., Kale, L., Kramer, B., & Snir, M. (2009). Toward Exascale Resilience.

International Journal of High Performance Computing Applications, 23(4), 374-388.
(Author affiliation: Inria, Laboratoire en Recherche Informatique - France, Oak Ridge National Laboratory, University of Illinois at Urbana-Champaign, and Lawrence Berkeley National Laboratory)
Also published as a technical report of the INRIA-Illinois Joint Laboratory on PetaScale Computing.

Castain, Ralph H., & Squyres, J. (2007). Creating a transparent, distributed, and resilient computing environment: The OpenRTE project. *The Journal of Supercomputing, 42*(1), 107-123.
(Author affiliation: Los Alamos National Laboratory and Cisco)

Chung, S., & Mok, A. (2006). Allergy attack against automatic signature generation. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 61-80). Berlin / Heidelberg: Springer
(Author affiliation: University of Texas at Austin)
The research reported here is supported partially by a grant from the Office of Naval Research under contract number N00014-03-1-0705.

Conrad, S. H., Brodsky, N. S., Beyeler, W. E., Brown, T. J., LaViolette, R. A., Glass, L., et al. (2005, April 26-28). *Simulation and analysis of cascading failure in critical infrastructure infrastructure (Slides).* Paper presented at the Working Together: Research and Development Partnerships for Homeland Security, Boston, MA.
(Author affiliation: Sandia National Laboratories)
DOE contract no. AC04-94AL85000

DeBardeleben, N., Laros, J., Daly, J., Scott, S., Engelmann, C., & Harrod, B. (2009). *High End Computing Resilience: Analysis of Issues Facing the HEC Community and Path Forward for Research and Development*: Los Alamos National Laboratory Technical Paper.
(Author affiliation: Los Alamos National Laboratory, Sandia National Laboratories, Department of Defense, Oak Ridge National Laboratory, and DARPA)

DHS Cyber Security Research and Development Center Technical Topic Areas 11-13. [Presentation]. https://www.fbo.gov/download/ad4/ad4190e6bd8f158f3850288824ea9d12/14-DHS_ST_Cyber_Security_Industry_Day_TTA_11-13.pdf
Research wish list for hardware-enabled trust mechanisms, moving target defenses and nature-inspired cyber health for an upcoming DHS S&T HSARPA CSD BAA.

ENISA Virtual Working Group on Network Providers' Resilience Measures (2009). *Network resilience and security: Challenges and measures - Report of the ENISA Virtual Working Group on Network Providers' Resilience Measures*. Heraklion, Greece: European Network and Information Security Agency (ENISA). http://www.epractice.eu/files/Network%20Resilience%20and%20Security%20-%20Challenges%20and%20Measures%20-%20Report%20of%20the%20ENISA%20Virtual%20Working%20Group%20on%20Network%20Providers%20Resilience%20Measures.pdf

Federal Networking and Information Technology Research and Development (NITRD) (2009). *National Cyber Leap Year Summit 2009 Co-chairs' Report*. http://www.qinetiq-na.com/Collateral/Documents/English-

US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf

Gagnon, M., Truelove, J., Kapadia, A., Haines, J., & Huang, O. (2010). Towards net-centric cyber survivability for ballistic missile defense. In H. Giese (Ed.), *Lecture Notes in Computer Science No. 6150: Architecting Critical Systems* (pp. 125-141). Berlin / Heidelberg: Springer
This work was sponsored by the DoD under Air Force contract FA8721-05-C-0002.

Goldman, H. G. (2010, October 29). *Building Secure, Resilient Architectures for Cyber Mission Assurance.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA.
http://www.mitre.org/work/tech_papers/2010/10_3301/
This paper offers ideas along the full spectrum of cyber security, but concentrates on architectural resilience against the upper end of the spectrum, where the stakes are high, the mission or business is critical, and the adversary is sophisticated, motivated, and persistent.

Gorniak, S., Ikonomou, D., Tirtea, R., Cadzow, S., Gierszal, H., Sutton, D., et al. (2011). *Enabling and managing end-to-end resilience*. Heraklion, Greece: European Network and Information Security Agency (ENISA).
http://www.enisa.europa.eu/act/it/library/deliverables/e2eres/at_download/fullReport

Hadley, M. D., & McBride, J. B. (2006, November 12-16). *Cyber Security Vulnerability Impact on I&C Reliability.* Paper presented at the International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology, Albuquerque, NM.
(Author affiliation: Pacific Northwest National Laboratory)

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29*(4), 498-501.
(Author affiliation: University of Virginia.)

Hall, C., Clayton, R., Anderson, R., & Ouzounis, E. (2011). *Inter-X: Resilience of the Internet Interconnection Ecosystem*. Heraklion, Greece: European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/act/res/other-areas/inter-x/report
(Author affiliation: ENISA, Highwayman Associates, and Cambridge University)

Iliasov, A. (2007, September 4). *Refinement patterns for rapid development of dependable systems.* Paper presented at the Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia.
(Author affiliation: Newcastle University)

Jiang, X., Xu, D., Wang, H., & Spafford, E. (2006). Virtual playgrounds for worm behavior investigation. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 1-21). Berlin / Heidelberg: Springer
(Author affiliation: Purdue University and Microsoft Research)

Khalil, Y., Sheta, W., & Elmaghraby, A. (2010). Improved Computer Networks Resilience Using Social Behavior. *International Journal of Computer Science and Information Security, 8*(7).
(Author affiliation: Mubarak City for Scientific Research and Technology Applications (MuCSAT) - Egypt and University of Louisville)

Laprie, J.-C. (2005). *Resilience for the scalability of dependability.* Paper presented at the International Symposium on Network Computing and Applications, Cambridge, MA.

(Author affiliation: LAAS-CNRS, France)

Ma, Z., Krings, A. W., & Sheldon, F. T. (2009). *An outline of the three-layer survivability analysis architecture for strategic information warfare research.* Paper presented at the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee.
(Author affiliation: University of Idaho and Oak Ridge National Laboratory)

Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal, 3*(2), 181-191.
(Author affiliation: Intelligent Systems Technology, Inc and the University of Southern California)

Mehta, V., Bartzis, C., Zhu, H., Clarke, E., & Wing, J. (2006). Ranking attack graphs. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 127-144). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)
This research was sponsored by the Office of Naval Research under grant no. N00014-01-1-0796, the Army Research Office under grant no. DAAD19-01-1-0485, and the National Science Foundation under grant nos. CNS-0411152, CCF-0429120, and 0433540.

Mohamed, A., & Zulkernine, M. (2010). Architectural design decisions for achieving reliable software systems. In H. Giese (Ed.), *Lecture Notes in Computer Science No. 6150: Architecting Critical Systems* (pp. 19-32). Berlin / Heidelberg: Springer.
(Author affiliation: Queen's University, Ontario, Canada)

Muoio, P. (2010). *Research Priorities: Tailored Spaces, Moving Target, Cyber Economics* (Presentation). Washington, DC: Office of the Director of National Intelligence.
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2010-11/Muoio_P_themes-ISPAB.pdf
Research note: ODNI research thrusts (see last slide); high level and of limited utility.

Newsome, J., Karp, B., & Song, D. (2006). Paragraph: Thwarting signature learning by training maliciously. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 81-105). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University and University College London)

O'Neill, D. (2009). Meeting the challenge of assuring resiliency under stress. *CrossTalk, 22*(6), 27-36.
http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-0-Issue.pdf

Pal, P., Schantz, R., Atighetchi, M., Loyall, J., & Webber, F. (2009, June 29). *What next in intrusion tolerance.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: BBN Technologies)

Pal, P., Webber, F., Atighetchi, M., Rubel, P., & Benjamin, P. (2008, April 1). *Automating cyber-defense management.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Glasgow, United Kingdom.
(Author affiliation: BBN Technologies and Pace University)

This research was funded by DARPA under Navy Contract No. N00178-07-C-2003.

Peake, C., & Williams, D. (2010, October 29). *An Integrative Framework for Secure and Resilient Mission Assurance.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Rieger, C. G., Gertman, D. I., & McQueen, M. A. (2009). *Resilient control systems: Next generation design research.* Paper presented at the Conference on Human System Interactions (HSI), Catania, Italy.
(Author affiliation: Idaho National Laboratory)
Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory.

Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., et al. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, 54*(8), 1245-1265.
(Author affiliation: University of Kansas, Lancaster University - UK, and NEC Laboratories Europe.) See also: ResiliNets Wiki https://wiki.ittc.ku.edu/resilinets/
This research was supported in part by the National Science Foundation FIND (Future Internet Design) Program under Grant CNS-0626918 (Postmodern Internet Architecture) and the European Commission under Grants EU FP6- IST-27489 (Autonomic Network Architecture) and FP7- 224619 (ResumeNet).

Strassner, J., Betser, J., Ewart, R., & Belz, F. (2010, October 29). *A Semantic Architecture for Enhanced Cyber Situational Awareness.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Ulieru, M. (2007). *Design for resilience of networked critical infrastructures.* Paper presented at the IEEE-IES Digital EcoSystems and Technologies Conference, Cairns, Australia.
(Author affiliation: University of New Brunswick, Canada)

Xiapu, L., & Chang, R. K. C. (2005, June 28 - July 1). *Optimizing the pulsing denial-of-service attacks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Hong Kong Polytechnic University)
The work described in this paper was partially supported by a grant from the Research Grant Council of the Hong Kong Special Administrative Region, China (Project No. PolyU 5080/02E) and a grant from the Areas of Excellence Scheme established under the University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-01/99).

Xu, C., Andersen, J., Mao, Z. M., Bailey, M., & Nazario, J. (2008, 24-27 June). *Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: University of Michigan, Ann Arbor and Arbor Networks)

Zhang, W. J., & Lin, Y. (2010). On the principle of design of resilient systems - application to enterprise information systems. *Enterprise Information Systems, 4*(2), 99-110.
(Author affiliation: University of Saskatchewan, Canada)

I.3 Deception

DoD SBIR Award: Spoofing Network Architectures in Response to Hostile Reconnaissance (2010). from http://www.dodsbir.net/sitis/archives_display_topic.asp?Bookmark=37704
(PIs affiliated with DataSoft Corp.)

Alata, E., Nicomette, V., Kaaniche, M., Dacier, M., & Herrb, M. (2006, 18-20 October). *Lessons learned from the deployment of a high-interaction honeypot.* Paper presented at the European Dependable Computing Conference (EDCC), Coimbra, Portugal.
(Author affiliation: University of Toulouse - France and Eurécom - France)
This work has been partially supported by: 1) CADHo, a research action funded by the French ACI "Securité & Informatique" (www.cadho.org), 2) the CRUTIAL IST-027513 project (crutial.cesiricerca.it), and 3) the ReSIST IST- 026764 project (www.resist-noe.org).

Bowen, B., Prabhu, P., Kemerlis, V., Sidiroglou, S., Keromytis, A., & Stolfo, S. (2010). BotSwindler: Tamper resistant injection of believable decoys in VM-based hosts for crimeware detection. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 118-137). Berlin / Heidelberg: Springer.
(Author affiliation: Columbia University and the Massachusetts Institute of Technology)
This work was partly supported by the National Science Foundation through grants CNS-07-14647 and CNS-09-14312.

Cohen, F. (2001). Should we use deception as an InfoSec defence? *Network Security, 2001*(11), 18-19.
(Author affiliation: Sandia National Laboratories)

Cohen, F. (2002). Protection by deception. *Network Security, 2002*(9), 17-19.
(Author affiliation: Sandia National Laboratories)

Leita, C., & Dacier, M. (2008, 7-9 May). *SGNET: A worldwide deployable framework to support the analysis of malware threat models.* Paper presented at the European Dependable Computing Conference (EDCC), Kaunas, Lithuania.
(Author affiliation: Institute Eurecom)
This work has been partially supported by the RNTR ACES project (contract number ANR05RNRT00103) and by the ReSIST Network of Excellence (contract number 026764). This work has been partially supported by the European Commissions through project FP7-ICT-216026- WOMBAT funded by the 7th framework program.

Leita, C., Dacier, M., & Massicotte, F. (2006). Automatic handling of protocol dependencies and reaction to 0-day attacks with ScriptGen based honeypots. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 185-205). Berlin / Heidelberg: Springer
(Author affliliation: Institute Eurecom - France and Communications Research Centre - Canada)

McQueen, M. A., & Boyer, W. F. (2009, May 21-23). *Deception used for cyber defense of control systems.* Paper presented at the Conference on Human System Interactions (HSI), Catania, Italy.
(Author affiliation: Idaho National Laboratory)

Research note: Defines two classes of deception (dissimulation and simulation) and three types of deception for each class, and then gives examples of each type of deception. Little in the way of detail.
Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory.

Rowe, N. (2007, March 8-9). *Planning cost-effective deceptive resource denial in defense to cyber-attacks.* Paper presented at the International Conference on Information Warfare & Security, Monterey, CA.
(Author affiliation: Naval Postgraduate School)
This work was supported by the U.S. National Science Foundation under the Cyber Trust Program.

Rowe, N., Goh, H., Lim, S., & Duong, B. (2007, March 8-9). *Experiments with a Testbed for Automated Defensive Deception Planning for Cyber-Attacks.* Paper presented at the International Conference on I-Warfare and Security (ICIW), Monterey, CA.
(Author affiliation: Naval Postgraduate School)
Research note: Description of testbed for conducting defensive deception experiments.
This work was supported by the U.S. National Science Foundation under the Cyber Trust Program.

Rowe, N. C. (2003, June 18-20). *Counterplanning deceptions to foil cyber-attack plans.* Paper presented at the IEEE Information Assurance Workshop, West Point, NY.
(Author affiliation: Naval Postgraduate School)
This work is part of the Homeland Security Leadership Development Program supported by the U.S. Department of Justice Office of Justice Programs and Office for Domestic Preparedness.

Ryu, C., Sharman, R., Rao, H., & Upadhyaya, S. (2010). Security protection design for deception and real system regimes: A model and analysis. *European Journal of Operational Research, 201*(2), 545-556.
(Author affiliation: Kookmin University - Korea and SUNY at Buffalo)
This research has been funded in part by NSF under grant 0417095, and Research program 2006 of Kookmin University in Korea.

Tan, K. L. G. (2003). *Confronting cyberterrorism with cyber deception.* Unpublished Master's Thesis, Naval Postgraduate School, Monterey, CA.
http://www.au.af.mil/au/awc/awcgate/nps/cyberterr_cyberdecep.pdf
(Author affiliation: Naval Postgraduate School)

Van-Hau, P., & Dacier, M. (2009, 19-21 Oct. 2009). *Honeypot traces forensics: The observation viewpoint matters.* Paper presented at the International Conference on Network and System Security, Gold Coast, Australia.
(Author affiliation: EURECOM, France Symantec)
This work has been partially supported by the European Commissions through project FP7-ICT-216026-WOMBAT funded by the 7th framework program.

Zou, C. C., & Cunningham, R. (2006, 25-28 June). *Honeypot-aware advanced botnet construction and*

maintenance. Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: University of Central Florida)

I.4 Detection

DoD SBIR Award: Protecting IT Systems from Cyber Attacks (2005). from https://sba-sbir-qa.reisys.com/sbirsearch/detail/139826
(PI affiliated with CYBER SPK, LLC.)

DoD SBIR Award: Formal Methods for Malware Detection (2006). from https://sba-sbir-qa.reisys.com/sbirsearch/detail/97149
(PI affiliated with Aries Design Automation, LLC)

National Science Foundation Cyber Trust Award: Automatic Generation of High-Quality Attack Signatures and Patches (2006). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0627672
(PI affiliated with National Science Foundation.)

DoD SBIR Award: Impact Modeling and Prediction of Attacks on Cyber Targets (IMPACT) (2007). from https://sba-sbir-qa.reisys.com/sbirsearch/detail/67761
(PI is affiliated 21st Century Technologies, Inc.)

National Science Foundation CAREER Award: Introspective Computing: A Multicore Approach to Availability, Reliability and Security (2007). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0644096
(PI affiliated with Georgia Institute of Technology.)

National Science Foundation CAREER Award: A Networking Approach to Host-based Intrusion Detection (2009). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0844144

Almgren, M., Lindqvist, U., & Jonsson, E. (2008). A multi-sensor model to improve automated attack detection. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 291-310). Berlin / Heidelberg: Springer
(Author affiliation: Chalmers University of Technology - Sweden and SRI International)

Antonakakis, M., Dagon, D., Luo, X., Perdisci, R., Lee, W., & Bellmor, J. (2010). A centralized monitoring infrastructure for improving DNS security. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 18-37). Berlin / Heidelberg: Springer
(Author affiliation: Georgia Institute of Technology)

Basile, C., Meeta, G., Kalbarczyk, Z., & Iyer, R. K. (2006, 25-28 June). *An approach for detecting and distinguishing errors versus attacks in sensor networks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.

(Author affiliation: University of Illinois at Urbana-Champaign)
This work is supported in part by MURI grant N00014-01-1-0576, the Gigascale Systems Research Center (GSRC/MARCO), and the Motorola Corporation as part of Motorola Center.

Best, D. M., Bohn, S., Love, D., Wynne, A., & Pike, W. A. (2010). *Real-time visualization of network behaviors for situational awareness.* Paper presented at the Seventh International Symposium on Visualization for Cyber Security, Ottawa, Ontario, Canada.
(Author affiliation: Pacific Northwest National Laboratory)
This research was supported by the U.S. Department of Homeland Security Science and Technology Directorate.

Bolzoni, D., Etalle, S., & Hartel, P. (2009). Panacea: Automating attack classification for anomaly-based network intrusion detection systems. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 1-20). Berlin / Heidelberg: Springer
(Author affiliation: University of Twente, The Netherlands and Eindhoven Technical University, The Netherlands)

Caffrey, J. M. (2008). The resiliency challenge presented by soft failure incidents. *IBM Systems Journal, 47*(4), 641-652.
(Author affiliation: IBM)

Campo-Giralte, L., Jimenez-Peris, R., & Patino-Martinez, M. (2009, 27-30 Sept.). *PolyVaccine: Protecting web servers against zero-day, polymorphic and metamorphic exploits.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Niagara Falls, NY.
(Author affiliation: Universidad Politecnica de Madrid)
This research has been partially funded by the Spanish National Science Foundation (MICINN) under grant TIN2007-67353-C02, the Madrid Regional Research Council (CAM) under the AUTONOMIC project (S- 0505/TIC/000285), and the European Commission under the NEXOF-RA project (FP7-216446).

Chinchani, R., & van den Berg, E. (2006). A fast static analysis approach to detect exploit code inside network flows. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 284-308). Berlin / Heidelberg: Springer
(Author affiliation: University at Buffalo and Telcordia Technologies)
This material is based upon work supported by the Air Force Research Laboratory – Rome Labs under Contract No. FA8750-04-C-0249.

Chung, S., & Mok, A. (2006). On random-inspection-based intrusion detection. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 165-184). Berlin / Heidelberg: Springer
(Author affiliation: University of Texas at Austin)

Chung, S., & Mok, A. (2007). Advanced allergy attacks: Does a corpus really help? In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 236-255). Berlin / Heidelberg: Springer
(Author affiliation: University of Texas at Austin)
The research reported here is supported partially by a grant from the Office of Naval Research

under contract number N00014-03-1-0705.

Co, M., Coleman, C. L., Davidson, J. W., Ghosh, S., Hiser, J. D., Knight, J. C., et al. (2009). *A lightweight software control system for cyber awareness and security.* Paper presented at the International Symposium on Resilient Control Systems (ISRCS), Idaho Falls, ID.
(Author affiliation: University of Virginia)
This material is based on research sponsored by the Air Force Research Laboratory under award number FA8750- 07-2-0029. This work was also supported in part by the National Science Foundation under awards CNS-0551560, CNS-0716446, CCF-0811689 and the US Department of Defense under grant FA9550-07-1-0532.

Collins, M., & Reiter, M. (2006). Finding peer-to-peer file-sharing using coarse network behaviors. In D. Gollmann, J. Meier & A. Sabelfeld (Eds.), *Lecture Notes in Computer Science No. 4189: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2006* (pp. 1-17). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)
This work was partially supported by NSF award CNS-0433540, and by KISA and MIC of Korea.

Collins, M., & Reiter, M. (2007). Hit-list worm detection and bot identification in large networks using protocol graphs. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 276-295). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon Software Engineering Institute and University of North Carolina at Chapel Hill)

Cova, M., Balzarotti, D., Felmetsger, V., & Vigna, G. (2007). Swaddler: An approach for the anomaly-based detection of state violations in web applications. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 63-86). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Santa Barbara)

Cretu-Ciocarlie, G., Stavrou, A., Locasto, M., & Stolfo, S. (2009). Adaptive anomaly detection via self-calibration and dynamic updating. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 41-60). Berlin / Heidelberg: Springer
(Author affiliation: Columbia University and George Mason University)

Cucurull, J., Asplund, M., & Nadjm-Tehrani, S. (2010). Anomaly detection and mitigation for disaster area networks. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 339-359). Berlin / Heidelberg: Springer
(Author affiliation: Linkoping University - Sweden)

de Bruijn, W., Slowinska, A., van Reeuwijk, K., Hruby, T., Xu, L., & Bos, H. (2006). SafeCard: A gigabit IPS on the network card. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 311-330). Berlin / Heidelberg: Springer
(Author affiliation: Vrije Universiteit, The Netherlands and Universiteit van Amsterdam)

Di Crescenzo, G., Ghosh, A., & Talpade, R. (2005). Towards a theory of intrusion detection. In S. di

Vimercati, P. Syverson & D. Gollmann (Eds.), *Lecture Notes in Computer Science No. 3679: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2005* (pp. 267-286). Berlin / Heidelberg: Springer
(Author affiliation: Telcordia Technologies)
The research was supported by Telcordia and NSA/ARDA under AFRL Contract F30602-03-C-0239.

Du, X., Shayman, M. A., & Skoog, R. A. (2008). Designing fault tolerant networks to prevent poison message failure. *Security and Communication Networks, 1*(2), 161-177.
(Author affiliation: North Dakota State University, University of Maryland - College Park, and Telcordia Technologies)
This work was partially supported by U.S. DARPA under contract N66001-00-C-8037.

Freiling, F., Holz, T., & Wicherski, G. (2005). Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. In S. di Vimercati, P. Syverson & D. Gollmann (Eds.), *Lecture Notes in Computer Science No. 3679: Computer Security – European Symposium on Research In Computer Security (ESORICS) 2005* (pp. 319-335). Berlin / Heidelberg: Springer
(Author affiliation: Aachen University - Germany)
Thorsten Holz was supported by Deutsche Forschungsgemeinshaft (DFG) as part of the Graduiertenkolleg "Software for mobile communication systems" at RWTH Aachen University.

Gao, D., Reiter, M., & Song, D. (2006). Behavioral distance for intrusion detection. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 63-81). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)

Gao, D., Reiter, M., & Song, D. (2006). Behavioral distance measurement using hidden markov models. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 19-40). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)

Giffin, J., Dagon, D., Jha, S., Lee, W., & Miller, B. (2006). Environment-sensitive intrusion detection. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 185-206). Berlin / Heidelberg: Springer
(Author affiliation: University of Wisconsin and Georgia Institute of Technology)

Giffin, J., Jha, S., & Miller, B. (2006). Automated discovery of mimicry attacks. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 41-60). Berlin / Heidelberg: Springer
(Author affiliation: University of Wisconsin)

Giroire, F., Chandrashekar, J., Taft, N., Schooler, E., & Papagiannaki, D. (2009). Exploiting temporal persistence to detect covert botnet channels. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 326-345). Berlin / Heidelberg: Springer
(Author affiliation: I3S (CNRS/UNS)/INRIA and Intel Research)

Gonzalez, J., & Paxson, V. (2006). Enhancing network intrusion detection with integrated sampling and

filtering. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 272-289). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Berkeley)

Griffin, K., Schneider, S., Hu, X., & Chiueh, T.-c. (2009). Automatic generation of string signatures for malware detection. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 101-120). Berlin / Heidelberg: Springer
(Author affiliation: Symantec)

Guanhua, Y., Cuellar, L., Eidenbenz, S., & Hengartner, N. (2009, June 29 - July 2). *Blue-Watchdog: Detecting Bluetooth worm propagation in public areas.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: Los Alamos National Laboratory)

Guo, F., Ferrie, P., & Chiueh, T.-c. (2008). A study of the packer problem and its solutions. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 98-115). Berlin / Heidelberg: Springer
(Author affiliation: Symantec)

Hansen, J., Tan, K., & Maxion, R. (2006). Anomaly detector performance evaluation using a parameterized environment. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 106-126). Berlin / Heidelberg: Springer
(Author affiliation: Carnegie Mellon University)

Hsu, C.-H., Huang, C.-Y., & Chen, K.-T. (2010). Fast-flux bot detection in real time. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 464-483). Berlin / Heidelberg: Springer
(Academic affiliation: National Taiwan Ocean University)

Jacob, G., Debar, H., & Filiol, E. (2009). Malware behavioral detection by attribute-automata using abstraction from platform and language. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 81-100). Berlin / Heidelberg: Springer
(Author affiliation: France Telecom R&D and ESIEA Laval - France)
This work has been partially supported by the European Commission through project FP7-ICT-216026-WOMBAT funded by the 7th framework program.

Katipally, R., Gasior, W., Cui, X., & Yang, L. (2010). *Multistage attack detection system for network administrators using data mining.* Paper presented at the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee.
(Author affiliation: University of Tennessee at Chattanooga and Oak Ridge National Laboratory)
This work is partially supported by grants from Tennessee Higher Education Commission's Center of Excellence in Applied Computational Science and Engineering and Oak Ridge National Laboratory.

Ke, W., Parekh, J. J., & Stolfo, S. J. (2006). Anagram: A content anomaly detector resistant to mimicry

attack *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 226-248). Berlin / Heidelberg: Springer.
(Author affiliation: Columbia University)

Kreidl, O. P., & Willsky, A. S. (2009, June 29). *Network intrusion detection with minimal communication overhead.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: MIT)

Kruegel, C., Kirda, E., Mutz, D., Robertson, W., & Vigna, G. (2006). Polymorphic worm detection using structural information of executables. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (Vol. 3858, pp. 207-226). Berlin / Heidelberg: Springer
(Author affiliation: Technical University of Vienna and the University of California, Santa Barbara)

Lap Chung, L., Wei, L., & Tzi-cker, C. (2006, 25-28 June). *Accurate and automated system call policy-based intrusion prevention.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: Stony Brook University)

Leita, C., Bayer, U., & Kirda, E. (2010, June 28 - July 1). *Exploiting diverse observation perspectives to get insights on the malware landscape.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: Symantec Research Labs, Technical University Vienna, and Institute Eurecom - France)
This work has been partially supported by the European Commission through project FP7-ICT-216026-WOMBAT funded by the 7th framework program.

Li, P., Gao, D., & Reiter, M. (2009). Automatically adapting a trained anomaly detector to software patches. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 142-160). Berlin / Heidelberg: Springer
(Author affiliation: University of North Carolina at Chapel Hill and Singapore Management University)

Li, Z., Gao, Y., & Chen, Y. (2010). HiFIND: A high-speed flow-level intrusion detection approach with DoS resiliency. *Computer Networks, 54*(8), 1282-1299.
(Author affiliation: Northwestern University)

Luchaup, D., Smith, R., & Estan, C. (2009). Multi-byte regular expression matching with speculation. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 284-303). Berlin / Heidelberg: Springer
(Author affiliation: University of Wisconsin-Madison and NetLogic Microsystems)

Maggi, F., Robertson, W., Kruegel, C., & Vigna, G. (2009). Protecting a moving target: addressing web application concept drift. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 21-40). Berlin / Heidelberg: Springer

(Author affiliation: University of California, Santa Barbara)

Martignoni, L., Stinson, E., Fredrikson, M., Jha, S., & Mitchell, J. (2008). A layered architecture for detecting malicious behaviors. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 78-97). Berlin / Heidelberg: Springer
(Author affiliation: Universita degli Studi di Milano, Stanford University, and University of Wisconsin)

Mathew, S., Petropoulos, M., Ngo, H., & Upadhyaya, S. (2010). A data-centric approach to insider attack detection in database systems. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 382-401). Berlin / Heidelberg: Springer
(Author affiliation: Amazon.com Inc. and University at Buffalo)

Mizrak, A. T., Cheng, Y. C., Marzullo, K., & Savage, S. (2005, June 28 - July 1). *Fatih: Detecting and isolating malicious routers.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: University of California, San Diego)

Modelo-Howard, G., Bagchi, S., & Lebanon, G. (2008). Determining placement of intrusion detectors for a distributed application through Bayesian network modeling. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 271-290). Berlin / Heidelberg: Springer
(Author affiliation: Purdue University)

Muelder, C., Ma, K.-L., & Bartoletti, T. (2006). Interactive visualization for network and port scan detection. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 265-283). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Davis and Lawrence Berkeley National Laboratory)

Mutz, D., Robertson, W., Vigna, G., & Kemmerer, R. (2007). Exploiting execution context for the detection of anomalous system calls. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 1-20). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Santa Barbara)

Neves, N., Antunes, J., Correia, M., Verissimo, P., & Neves, R. (2006, 25-28 June). *Using attack injection to discover new vulnerabilities.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: University of Lisbon and Technical University of Lisbon)
This work was partially supported by the EC through project IST-2004-27513 (CRUTIAL), and by the FCT through projects POSC/EIA/61643/2004 (AJECT) and the Large-Scale Informatic Systems Laboratory (LASIGE).

Oliner, A., Kulkarni, A., & Aiken, A. (2010). Community epidemic detection using time-correlated anomalies. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 360-381). Berlin / Heidelberg: Springer

(Author affiliation: Stanford University)

Pacific Northwest National Laboratory. Research Project: Adaptive Cyber-defense using an Auto-associative Memory Paradigm (ACAMP), from http://i4.pnl.gov/focusareas/acamp.stm
Research note: PNNL research to design, develop, and test an adaptive attack recognition system that transcends current approaches by using an auto-associative memory paradigm. The system will be self-instructive of new variants based on similarities to past experiences.

Panjwani, S., Tan, S., Jarrin, K. M., & Cukier, M. (2005, June 28 - July 1). *An experimental evaluation to determine if port scans are precursors to an attack.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: University of Maryland, College Park)
This research was supported by NSF CAREER award 0237493.

Peng, Y., Zhang, L., Chang, J., & Guan, Y. (2009). An effective method for combating malicious scripts clickbots. In M. Backes & P. Ning (Eds.), *Lecture Notes in Computer Science No. 5789: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2009* (pp. 523-538). Berlin / Heidelberg: Springer
(Author affiliation: Iowa State University)

Pietraszek, T., & Berghe, C. (2006). Defending against injection attacks through context-sensitive string evaluation. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 124-145). Berlin / Heidelberg: Springer
(Author affiliation: IBM Research and Katholieke Universiteit Leuven - Belgium)

Polychronakis, M., Anagnostakis, K., & Markatos, E. (2007). Emulation-based detection of non-self-contained polymorphic shellcode. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 87-106). Berlin / Heidelberg: Springer
(Author affiliation: Institute for Computer Science, Foundation for Research & Technology - Greece and Institute for Infocomm Research - Singapore)

Rajab, M., Monrose, F., & Terzis, A. (2006). Fast and evasive attacks: Highlighting the challenges ahead. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 206-225). Berlin / Heidelberg: Springer
(Author affiliation: Johns Hopkins University)

Ramsbrock, D., Wang, X., & Jiang, X. (2008). A first step towards live botmaster traceback. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 59-77). Berlin / Heidelberg: Springer.
(Author affiliation: George Mason University and the University of North Carolina Raleigh)

Ray, I., & Poolsapassit, N. (2005). Using attack trees to identify malicious attacks from authorized insiders. In S. di Vimercati, P. Syverson & D. Gollmann (Eds.), *Lecture Notes in Computer Science No. 3679: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2005* (pp. 231-246). Berlin / Heidelberg: Springer
(Author affiliation: Colorado State University)

Rehák, M., Staab, E., Fusenig, V., Pěchouček, M., Grill, M., Stiborek, J., et al. (2009). Runtime monitoring and dynamic reconfiguration for intrusion detection systems. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 61-80). Berlin / Heidelberg: Springer
(Author affiliation: Czech Technical University in Prague, University of Luxembourg, and CESNET - Czech Republic)

Schear, N., Albrecht, D., & Borisov, N. (2008). High-speed matching of vulnerability signatures. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 155-174). Berlin / Heidelberg: Springer
(Author affiliation: University of Illinois at Urbana-Champaign)

Sengar, H., Wijesekera, D., Wang, H., & Jajodia, S. (2006, 25-28 June). *VoIP intrusion detection through interacting protocol state machines.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: George Mason University and the College of William and Mary)

Shafiq, M., Tabish, S., Mirza, F., & Farooq, M. (2009). PE-Miner: Mining structural information to detect malicious executables in realtime. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 121-141). Berlin / Heidelberg: Springer
(Author affiliation: National University of Computer & Engineering Sciences - Pakistan and National University of Sciences & Technology - Pakistan)

Sharif, M., Singh, K., Giffin, J., & Lee, W. (2007). Understanding precision in host based intrusion detection: Formal analysis and practical models. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 21-41). Berlin / Heidelberg: Springer
(Author affiliation: Georgia Institute of Technology)

Sihyungo, L., Wong, T., & Kim, H. S. (2006, 25-28 June). *Secure split assignment trajectory sampling: A malicious router detection system.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: Carnegie Mellon University)
This work was funded in part by KISA, MIC, Samsung and Carnegie Mellon CyLab.

Silva, C., Sousa, P., & Veríssimo, P. (2010, June 28). *RAVE: Replicated AntiVirus Engine.* Paper presented at the Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS), Chicago.
(Author affiliation: Portugal Telecom and LaSIGE, Faculty of Sciences, University of Lisbon)

Singh, K., Srivastava, A., Giffin, J., & Lee, W. (2008, 24-27 June). *Evaluating email's feasibility for botnet command and control.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: Georgia Institute of Technology)
This material is based upon work supported in part by the NSF under grants CCR-0133629, CNS-0627477, and CNS-0716570, and by the U.S. Army Research Office under grant W911NF061 0042.

Sinha, S., Jahanian, F., & Patel, J. (2006). WIND: Workload-Aware INtrusion Detection. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 290-310). Berlin / Heidelberg: Springer
(Author affiliation: University of Michigan, Ann Arbor)

Srivastava, A., & Giffin, J. (2010). Automatic discovery of parasitic malware. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 97-117). Berlin / Heidelberg: Springer
(Author affiliation: Georgia Institute of Technology)

Sufatrio, & Yap, R. (2006). Improving host-based ids with argument abstraction to prevent mimicry attacks. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (Vol. 3858, pp. 146-164). Berlin / Heidelberg: Springer
(Author affiliation: National University of Singapore

Sun, F., Xu, L., & Su, Z. (2009). Client-side detection of XSS worms by monitoring payload propagation. In M. Backes & P. Ning (Eds.), *Lecture Notes in Computer Science No. 5789: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2009* (pp. 539-554). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Davis)

Thonnard, O., Mees, W., & Dacier, M. (2009). *Addressing the attack attribution problem using knowledge discovery and multi-criteria fuzzy decision-making.* Paper presented at the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics, Paris, France.

Todd, A., Raines, R., Baldwin, R., Mullins, B., & Rogers, S. (2007). Alert verification evasion through server response forging. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 256-275). Berlin / Heidelberg: Springer
(Author affiliation: Air Force Institute of Technology and Air Force Research Laboratory)

Treinen, J., & Thurimella, R. (2006). A framework for the application of association rule mining in large intrusion detection infrastructures. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 1-18). Berlin / Heidelberg: Springer
(Author affiliation: IBM Global Services and University of Denver)

Tseng, C., Wang, S.-H., Ko, C., & Levitt, K. (2006). DEMEM: Distributed evidence-driven message exchange intrusion detection model for MANET. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 249-271). Berlin / Heidelberg: Springer
(Author affiliation: University of California, Davis)

Vallentin, M., Sommer, R., Lee, J., Leres, C., Paxson, V., & Tierney, B. (2007). The NIDS cluster: Scalable, stateful network intrusion detection on commodity hardware. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (Vol. 4637, pp. 107-126). Berlin / Heidelberg: Springer
(Author affiliation: International Computer Science Institute, Lawrence Berkeley National

Laboratory, and Technische Universitaet Muenchen, Germany)

Vasiliadis, G., Antonatos, S., Polychronakis, M., Markatos, E., & Ioannidis, S. (2008). Gnort: high performance network intrusion detection using graphics processors. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 116-134). Berlin / Heidelberg: Springer
(Author affiliation: Foundation for Research & Technology - Greece)

Wang, K., Cretu, G., & Stolfo, S. (2006). Anomalous payload-based worm detection and signature generation. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 227-246). Berlin / Heidelberg: Springer
(Author affiliation: Columbia University)
This work has been partially supported by a grant with the Army Research Office/DHS, No. DA W911NF-04-1-0442 and an SBIR subcontract with the HS ARPA division of the Department of Homeland Security.

Wang, L., Liu, A., & Jajodia, S. (2005). An efficient and unified approach to correlating, hypothesizing, and predicting intrusion alerts. In S. di Vimercati, P. Syverson & D. Gollmann (Eds.), *Lecture Notes in Computer Science No. 3679: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2005* (pp. 247-266). Berlin / Heidelberg: Springer
(Author affiliation: George Mason University)
This work was partially supported by the National Science Foundation under grant CCR-0113515, by the Air Force Research Laboratory, Rome under the contract F30602-00-2-0512, and by Army Research Office under the grant DAAD19-03-1-0257.

Wang, Y. M., Beck, D., Vo, B., Roussev, R., & Verbowski, C. (2005, June 28 -July 1). *Detecting stealth software with Strider GhostBuster.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Microsoft Research)

Wei, Y., Nan, Z., Xinwen, F., Bettati, R., & Wei, Z. (2008, 24-27 June). *On localization attacks to Internet Threat Monitors: An information-theoretic framework.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: Texas A&M University, University of Texas at Arlington, Dakota State University, and Rensselaer Polytechnic Institute)
This work was supported in part by the National Science Foundation under grants 0808419, 0324988, 0721571, 0329181, 0721783, 0747150, 0721766 and 0722856.

Woo, H., Yi, J., Browne, J. C., Mok, A. K., Atkins, E., & Xie, F. (2008, June 17-20). *Design and development methodology for resilient cyber-physical systems.* Paper presented at the International Conference on Distributed Computing Systems, Beijing, China.
(Author affiliation: University of Texas at Austin, University of Michigan, and Portland State University)
This research was supported in part by NSF Grant 0613665 to the University of Texas at Austin, Grant 0650049 to the University of Michigan and Grant 0613930 to Portland State University.

Wurzinger, P., Bilge, L., Holz, T., Goebel, J., Kruegel, C., & Kirda, E. (2009). Automatically generating models for botnet detection. In M. Backes & P. Ning (Eds.), *Lecture Notes in Computer Science*

No. 5789: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2009 (pp. 232-249). Berlin / Heidelberg: Springer
(Author affiliation: Vienna University of Technology, Institute Eurecom - France, University of Mannheim, and University of California, Santa Barbara)

Ying, Z., Mao, Z. M., & Jia, W. (2007, 25-28 June). *A firewall for routers: Protecting against routing misbehavior.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: University of Michigan and AT&T Labs)

Yuanyuan, Z., Xin, H., & Shin, K. G. (2010, June 28 - July 1). *Detection of botnets using combined host- and network-level information.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: University of Michigan, Ann Arbor)
The work reported in this paper was supported in part by NSF under Grant CNS 0905143 and ONR under Grant No. N000140911042.

Yu-Sung, W., Bagchi, S., Singh, N., & Wita, R. (2009, June 29 - July 2). *Spam detection in voice-over-IP calls through semi-supervised clustering.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: Purdue University, Avaya Labs, and Chulalongkorn University, Thailand)

Zhang, Z., & Shen, H. (2005, June 28 -July 1). *Constructing multi-layered boundary to defend against intrusive anomalies: An autonomic detection coordinator.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Japan Advanced Institute of Science and Technology)
This research is conducted as a program for the ”Fostering Talent in Emergent Research Fields” in Special Coordination Funds for Promoting Science and Technology by Ministry of Education, Culture, Sports, Science and Technology.

Zhiqiang, L., Xiangyu, Z., & Dongyan, X. (2010, June 28 - July 1). *Reuse-oriented camouflaging trojan: Vulnerability detection and attack construction.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: Purdue University)
This research is supported, in part, by the Office of Naval Research (ONR) under grant N00014-09-1-0776 and by the National Science Foundation (NSF) under grants 0716444, 0720516 and 0845870.

Zhuowei, L., XiaoFeng, W., Zhenkai, L., & Reiter, M. K. (2008, 24-27 June). *AGIS: Towards automatic generation of infection signatures.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: Indiana University at Bloomington, Carnegie Mellon University, and the University of North Carolina at Chapel Hill)
This work was supported in part by the National Science Foundation Cyber Trust program under Grant No. CNS-0716292.

I.5 Dynamic

DoD SBIR Award: Software Protection to Fight through an Attack (2009). from https://sba-sbir-qa.reisys.com/sbirsearch/detail/112414
(PI affiliated with BlueRISC Inc.)

European 6th Framework Program: HIDENETS (2009). from http://www.hidenets.aau.dk/
Research note: EU-funded IP resilience research related to automobile communication, but appears to be generally applicable.

National Science Foundation Award: Collaborative Research - Automated and Adaptive Diversity for Improving Computer Systems Security (2010). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0832943&WT.z_pims_id=6191
(PI is affiliated with University of California, Berkeley.)
Research note: NSF award focusing on the development of methods for diversifying computer systems automatically and systematically -- exploring diversity at various levels of a system and for various purposes, e.g., to make a system more difficult to compromise, to make a system more difficult to damage even after a successful compromise, and to make it more difficult for a successful compromise to evade detection.

Allan, B. A., Armstrong, R. C., Mayo, J. R., Pierson, L. G., Torgerson, M. D., & Walker, A. M. (2010). *The theory of diversity and redundancy in information system security: LDRD final report*. Albuquerque, NM; Livermore, CA: Sandia National Laboratories. http://prod.sandia.gov/techlib/access-control.cgi/2010/107055.pdf
(Author affiliation: Sandia National Laboratories)

Amir, Y., Danilov, C., Dolev, D., Kirsch, J., Lane, J., Nita-Rotaru, C., et al. (2006, 25-28 June). *Scaling Byzantine fault-tolerant replication to wide area networks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliations: Johns Hopkins University, Hebrew University of Jerusalem, and Purdue University)
This work was partially funded by DARPA grant FA8750-04-2-0232, and by NSF grants 0430271 and 0430276.

Anh, N.-T., Evans, D., Knight, J. C., Cox, B., & Davidson, J. W. (2008, 24-27 June). *Security through redundant data diversity.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: University of Virginia)
We gratefully acknowledge support from the National Science Foundation through awards CNS-0524432 and CNS-0627523.

Antonatos, S., Akritidis, P., Markatos, E., & Anagnostakis, K. (2005, November 11). *Defending against hitlist worms using network address space randomization.* Paper presented at the WORMS, Alexandria, VA.
(Author affiliation: Institute of Computer Science, Foundation for Research and Technology - Greece and Institute for Infocomm Research - Singapore.)
This work was supported in part by the IST project LOB- STER funded by the European Union

under Contract No. 004336, and the GSRT project EAR (USA-022) funded by the Greek Secretariat for Research and Technology.

Bangalore, A. K., & Sood, A. K. (2009, June 18-23). *Securing web servers using Self Cleansing Intrusion Tolerance (SCIT).* Paper presented at the International Conference on Dependability, Athens, Greece.
(Author affiliation: George Mason University)
This research was partially supported by a contract from Lockheed Martin and a contract from Virginia Center for Innovative Technologies.

Bessani, A., Daidone, A., Gashi, I., Obelheiro, R., Sousa, P., & Stankovic, V. (2009, June 29). *Enhancing fault / intrusion tolerance through design and configuration diversity.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: University of Florence, University of Lisbon, City University London, and Universidade do Estado de Santa Catarina, Brazil)
This work was partially supported by the EC through project IST-2004-27513 (CRUTIAL) and NoE IST-4- 026764-NOE (RESIST), and by the FCT through the Multiannual Funding and the CMU-Portugal Programs.

Cheng, X., Bi, J., & Li, X. (2008). *Swing - A novel mechanism inspired by Shim6 address-switch conception to limit the effectiveness of DoS attacks.* Paper presented at the International Conference on Networking, Cancun, Mexico.
(Author affiliation: Tsinghua University, Beijing)

Clarke, D., & Ezhilchelvan, P. (2010, June 28). *Assessing the attack resilience capabilities of a fortified primary-backup system.* Paper presented at the Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS), Chicago.
(Author affiliation: Newcastle University)

Cohen, F. (2010). *Moving Target Defenses with and without Cover Deception*. Livermore, CA: Fred Cohen & Associates. http://all.net/Analyst/2010-10.pdf
Research note: Paper introduces moving target defenses with cover deception. Deceptive cover involves inducing and suppressing return signals from an attacker's acts. The paper claims success in deceiving attackers, in some cases greatly increasing the amount of work or time for an attacker to achieve a successful penetration.

Distler, T., Kapitza, R., & Reiser, H. P. (2008, April 1). *Efficient state transfer for hypervisor-based proactive recovery.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Glasgow, United Kingdom.
(Author affiliation: University of Erlangen and University of Lisbon)
This work was partially supported by the EU through NoE IST-4-026764-NOE (RESIST/FOREVER) and project IST- 4-027513-STP (CRUTIAL), and by the FCT through the Multiannual Programme.

Federal Networking and Information Technology Research and Development (NITRD). Federal Cybersecurity Game-change R&D, from http://cybersecurity.nitrd.gov/page/moving-target

Fu, X., & Crowcroft, J. (2006). *GONE: An infrastructure overlay for resilient, DoS-limiting networking.* Paper presented at the International Workshop on Network and Operating System Support for

Digital Audio and Video, Newport, RI.
(Author affiliation: University of Cambridge, UK and University of Göttingen, Germany)

Gallos, L. K., & Argyrakis, P. (2007). Scale-free networks resistant to intentional attacks. *Europhysics Letters, 80*(5), 58002 (58005pp.).
(Author affiliation: University of Thessaloniki, Greece)
This work was supported by a NEST/PATHFINDER project DYSONET/012911 of the EC, and also by a project of the Greek GGET in conjunction with ESF in the frame of international organizations.

Gallos, L. K., Cohen, R., Liljeros, F., Argyrakis, P., Bunde, A., & Havlin, S. (2006). Attack strategies on complex networks *Lecture Notes in Computer Science No. 3993: Computational Science* (pp. 1048-1055): Springer-Verlag.
(Author affiliation: University of Thessaloniki - Greece, Bar-Ilan University - Israel, Stockholm University - Sweden, and Justus-Liebig-Universität Giessen, Germany)
This work was supported by a European research NEST/PATHFINDER project DYSONET 012911 (European Commission).

Guerraoui, R., & Vukolic, M. (2007, March 23). *Refined quorum systems.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: École Polytechnique Fédérale de Lausanne (EPFL))

Hansen, A. F., Kvalbein, A., Cicic, T., Gjessing, S., & Lysne, O. (2005, June 28 - July 1). *Resilient routing layers for recovery in packet networks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Simula Research Laboratory, Norway and Telenor R&D, Norway)

Herder, J. N., Bos, H., Gras, B., Homburg, P., & Tanenbaum, A. S. (2007, 25-28 June). *Failure resilience for device drivers.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: Vrije Universiteit, Amsterdam, The Netherlands)
This work was supported by Netherlands Organization for Scientific Research (NWO) under grant 612-060-420.

Huang, Y., Arsenault, D., & Sood, A. (2006). *Securing DNS services through system self cleansing and hardware enhancements.* Paper presented at the International Conference on Availability, Reliability and Security, Vienna, Austria.
(Author affiliation: George Mason University)
This research is part of the Critical Infrastructure Protection Project funded by the National Institute of Standards and Technology.

Huang, Y., Ghosh, A. K., Bracewell, T., & Mastropietro, B. (2010). *A security evaluation of a novel Resilient Web Serving architecture: Lessons learned through industry/academia collaboration.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: George Mason University and the Raytheon Company)
This work was partially under Air Force Office of Scientific Research (AFOSR) grant # FA9550-07-1- 0527 and DARPA contract # N66001-06-C-2050.

Huang, Y., Ghosh, A. K., Bracewell, T., & Mastropietro, B. (2010, June 28). *A security evaluation of a novel resilient web serving architecture: Lessons learned through industry/academia collaboration.* Paper presented at the Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS), Chicago.
(Author affiliation: George Mason University and Raytheon Company)
This work was partially under AFOSR grant # FA9550-07-1-0527 and DARPA contract # N66001-06-C-2050.

Kewley, D., Fink, R., Lowry, J., & Dean, M. (2001, June 12-14). *Dynamic approaches to thwart adversary intelligence gathering.* Paper presented at the DARPA Information Survivability Conference & Exposition II, Anaheim, CA.
(Author affiliation: BBN Technologies)

Kourai, K., & Chiba, S. (2007, 25-28 June). *A fast rejuvenation technique for server consolidation with virtual machines.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: Tokyo Institute of Technology)

Laranjeiro, N., & Vieira, M. (2007, September 4). *Towards fault tolerance in web services compositions.* Paper presented at the Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia.
(Author affiliation: University of Coimbra - Portugal)

Lee, P. P. C., Misra, V., & Rubenstein, D. (2007). Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking, 15*(6), 1490-1501.
(Author affiliation: Columbia University)

Littlewood, B., & Strigini, L. (2004). Redundancy and diversity in security. In P. Samarati, P. Ryan, D. Gollmann & R. Molva (Eds.), *Lecture Notes in Computer Science No. 3193: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2004* (pp. 423-438): Springer Verlag.
(Author affiliation: City University, London)
Supported by the UK Engineering and Physical Sciences Research Council.

Majorczyk, F., Totel, E., & Mé, L. (2007, March 23). *Experiments on COTS diversity as an intrusion detection and tolerance mechanism.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisboa, Portugal.
(Author affiliation: Supélec, France)

Michalski, J., Price, C., Stanton, E., Lee, E., Chua, K. S., Wong, Y. H., et al. (2002). *Final Report for the Network Security Mechanisms Utilizing Network Address Translation LDRD Project*. Albuquerque, NM: Sandia National Laboratories. http://prod.sandia.gov/techlib/access-control.cgi/2002/023613.pdf
(Author affiliation: Sandia National Laboratories and DSO National Laboratories, Singapore.)

Moniz, H., Neves, N. F., Correia, M., & Verissimo, P. (2006, 25-28 June). *Randomized intrusion-tolerant asynchronous services.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.

(Author affiliation: University of Lisbon)
This work was partially supported by the EU through NoE IST-4- 026764-NOE (RESIST) and project IST-4-027513-STP (CRUTIAL), and by the FCT through project POSI/EIA/60334/2004 (RITAS) and the Large-Scale Informatic Systems Laboratory (LASIGE).

Morehead, R., & Noore, A. (2007). Novel hybrid mitigation strategy for improving the resiliency of hierarchical networks subjected to attacks. *Physica A: Statistical Mechanics and its Applications, 378*(2), 603-612.
(Author affiliation: West Virginia University)

Nai Fovino, I., Carcano, A., & Masera, M. (2009). *A secure and survivable architecture for SCADA systems.* Paper presented at the International Conference on Dependability, Athens, Glyfada, Greece.
(Author affiliation: Institute for the Protection and Security of the Citizen Joint Research Centre, EU Commission)

Okhravi, H., Robinson, E. I., Yannalfo, S., Michaleas, P. W., & Haines, J. (2010, October 29). *TALENT: Dynamic Platform Heterogeneity for Cyber Survivability of Mission Critical Applications.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Ranjan, S. a., Swaminathan, R., Uysal, M., Nucci, A., & Knightly, E. (2009). DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. *IEEE/ACM Transactions on Networking, 17*(1), 26-39.
(Author affiliation: HP Laboratories, Rice University, and Narus Inc)
The work of S. Ranjan and E. Knightly was supported by HP Laboratories and NSF Grant ANI-0331620.

Sampaio, L., & Brasileiro, F. (2005, June 28 - July 1). *Adaptive indulgent consensus.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Universidade Federal de Campina Grande)
Financial support from CAPES/Brazil (grant 478.752/01) and CNPq/Brazil (grant 300.646/96).
This work was partially developed in collaboration with HP Brazil R&D.

Shmatikov, V., & Wang, M.-H. (2006). Timing analysis in low-latency mix networks: Attacks and defenses. In D. Gollmann, J. Meier & A. Sabelfeld (Eds.), *Lecture Notes in Computer Science No. 4189: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2006* (pp. 18-33). Berlin / Heidelberg: Springer
(Author affiliation: University of Texas at Austin)
This work was partially supported by NSF grants CNS-0509033 and IIS-0534198.

Sousa, P., Bessani, A. N., Correia, M., Neves, N. F., & Verissimo, P. (2007, December 17-19). *Resilient Intrusion Tolerance through Proactive and Reactive Recovery.* Paper presented at the Pacific Rim International Symposium on Dependable Computing, Melbourne, Qld.
(Author affiliation: University of Lisbon)
Research note: Research topic detailing a proactive-reactive recovery service that guarantees the availability of the minimum number of system replicas necessary to sustain a system's correct operation.
This work was partially supported by the EC through project IST-2004- 27513 (CRUTIAL) and NoE IST-4-026764-NOE (RESIST), and by the FCT through project POSI/EIA/60334/2004 (RITAS) and

the Large-Scale Informatic Systems Laboratory (LaSIGE).

Sousa, P., Neves, N. F., & Verissimo, P. (2005, June 28 - July 1). *How resilient are distributed f fault/intrusion-tolerant systems?* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: University of Lisbon)
This work was partially supported by the FCT, through the Large- Scale Informatic Systems Laboratory (LaSIGE).

Srivatsa, M., Iyengar, A., Yin, J., & Liu, L. (2006). A middleware system for protecting against application level denial of service attacks *Lecture Notes in Computer Science No. 4290: Middleware 2006* (pp. 260-280): Springer Verlag.
(Author affiliation: Georgia Institute of Technology and IBM T.J. Watson Research Center)
Most of this work was done while Mudhakar Srivatsa was a summer intern at IBM Research. At Georgia Tech, Mudhakar Srivatsa and Ling Liu were partially supported by NSF ITR, NSF CyberTrust and NSF CSR.

Totel, E., Majorczyk, F., & Mé, L. (2006). COTS diversity based intrusion detection and application to web servers. In A. Valdes & D. Zamboni (Eds.), *Lecture Notes in Computer Science No. 3858: Recent Advances in Intrusion Detection (RAID)* (pp. 43-62). Berlin / Heidelberg: Springer
(Author affiliation: Supélec)

Xuxian, J., Wang, H. J., Dongyan, X., & Yi-Min, W. (2007, 10-12 Oct.). *RandSys: Thwarting code injection attacks with system service interface randomization.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Beijing.
(Author affiliation: George Mason University, Microsoft Research, and Purdue University)
This work was supported in part by a gift from Microsoft Research and grants from the National Science Foundation (OCI- 0438246, OCI-0504261, CNS-0546173).

Yakymets, N., & Kharchenko, V. (2007, September 4). *Fault-tolerant digital systems implemented with partially definite and partially correct automata.* Paper presented at the Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia.
(Author affiliation: Universität Stuttgart and National Aerospace University "KhAI", Kharkiv, Ukraine)

Zamboni, D., Bhatkar, S., & Sekar, R. (2008). Data Space Randomization *Lecture Notes in Computer Science No. 5137: Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 1-22). Berlin / Heidelberg: Springer.
(Author affiliation: Symantec and Stony Brook University)
This research is supported in part by an ONR grant N000140710928 and an NSF grant CNS-0627687. This work was part of the first author's Ph.D. work completed at Stony Brook University.

I.6 Integrity

National Science Foundation Cyber Trust Award: Well-Typed Trustworthy Computing in the Presence of

Transient Faults (2009). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0627650&WT.z_pims_id=6191
Research note: NSF award focusing on the question of how to build software systems that operate on faulty hardware, yet provide ironclad reliability guarantees. The goal of the project is to produce a trustworthy, flexible and efficient computing platform that tolerates transient faults.

National Science Foundation Software and Hardware Foundations Award: Rethinking Computer Architecture for Secure and Resilient Systems (2009). from http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0917134
(PI affiliation: Princeton University.)

Amir, Y., Coan, B., Kirsch, J., & Lane, J. (2008, 24-27 June). *Byzantine replication under attack.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: Johns Hopkins University and Telcordia Technologies)
This publication was supported by grants 0430271 and 0716620 from the National Science Foundation.

Barcellos, M. P., Bauermann, D., Sant'Anna, H., Lehmann, M., & Mansilha, R. (2008, 6-8 Oct.). *Protecting BitTorrent: Design and evaluation of effective countermeasures against DoS attacks.* Paper presented at the Symposium on Reliable Distributed Systems (SRDS), Naples.
(Author affiliation: Pontifical Catholic University of Rio Grande do Sul - Brazil and Universidade do Vale do Rio dos Sinos - Brazil)
Funded by grants from Brazilian National Research Agency CNPq.

Basile, C., Kalbarczyk, Z., & Iyer, R. K. (2005, June 28 - July 1). *Neutralization of errors and attacks in wireless ad hoc networks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: University of Illinois at Urbana-Champaign)
This work is supported in part by NSF grant CCR 00- 86096 ITR, MURI grant N00014-01-1-0576, the Gigascale Systems Research Center (GSRC/MARCO), and the Motorola Corporation as part of Motorola Center.

Bessani, A. N., Alchieri, E. P., Fraga, J. d. S., & Lung, L. C. (2007, March 23). *Design and implementation of an intrusion-tolerant tuple space.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: Pontificia Universidade Catolica do Parana – Brazil and Universidade Federal de Santa Catarina - Brazil)
This work was supported by CNPq (Brazilian National Research Council) through process 550114/2005-0 and CAPES/GRICES (project TISD).

Bortnikov, E., Gurevich, M., Keidar, I., Kliot, G., & Shraer, A. (2009). Brahms: Byzantine resilient random membership sampling. *Computer Networks, 53*(13), 2340-2359.
(Author affiliation: Yahoo! Research, The Technion – Israel Institute of Technology, and Microsoft Research)

Carter, N. P., Naeimi, H., & Gardner, D. S. (2010, 8-12 March 2010). *Design techniques for cross-layer resilience.* Paper presented at the Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany.
(Author affiliation: Intel)
This material is based upon work supported by the National Science Foundation under Grant No. 0637190 to the Computing Research Association.

Chun-Ying, H., Kuan-Ta, C., & Chin-Laung, L. (2006, 25-28 June). *Mitigating active attacks towards client networks using the bitmap filter.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: National Taiwan University)
This work was supported in part by the Ministry of Economic Affairs under the Grants 94-EC-17-A-02-S1-049, and by the Taiwan Information Security Center (TWISC), National Science Council under the Grants No. NSC 94-3114-P-001-001Y and NSC 94-3114-P-011-001.

Cunha, J. C., Medeiros, P. D., Kola, G., Kosar, T., & Livny, M. (2005). Faults in Large Distributed Systems and What We Can Do About Them *Lecture Notes in Computer Science No. 3648: Euro-Par 2005 Parallel Processing* (pp. 442-453): Springer.
(Author affiliation: University of Wisconsin-Madison)

Děcký, M. (2010). A road to a formally verified general-purpose operating system. In H. Giese (Ed.), *Lecture Notes in Computer Science No. 6150: Architecting Critical Systems* (pp. 72-88). Berlin / Heidelberg: Springer.
(Author affiliation: Charles University - Czech Republic)

Dueñas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural Safety, 31*(2), 157-167.
(Author affiliation: Rice University)
The work reported here has been funded in part by the National Science Foundation grant CMMI-0728040.

Edge, C., & Mitropoulos, F. (2009, December 14). *Aspectization of the secure communication pattern for data integrity.* Paper presented at the Workshop on Information Security & Privacy (WISP), Pheonix, AZ.
(Author affiliation: Coastal Carolina University and Nova Southeastern University)

Gennaro, R., Halevi, S., Krawczyk, H., Rabin, T., Reidt, S., & Wolthusen, S. (2008). Strongly-resilient and non-interactive hierarchical key-agreement in MANETs. In S. Jajodia & J. Lopez (Eds.), *Lecture Notes in Computer Science No. 5283: Computer Security - European Symposium on Research in Computer Security (ESORICS) 2008* (pp. 49-65). Berlin / Heidelberg: Springer
(Author affiliation: IBM Research and University of London)
Research was sponsored by US Army Research laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001.

Guanglei, L., & Chuanyi, J. (2006). *Resilient architecture of all-optical networks: Probabilistic graphical models for crosstalk attack propagation.* Paper presented at the IEEE International Symposium on Information Theory.
(Author affiliation: Georgia Institute of Technology)

Gutfraind, A. (2010). Optimizing Topological Cascade Resilience Based on the Structure of Terrorist Networks. *PLoS ONE, 5*(11), e13448.
(Author affiliation: Los Alamos National Laboratory)
This work was supported by the Department of Energy at the Los Alamos National Laboratory (LA-UR 10-01563) under contract DE-AC52-06NA25396 through the Laboratory Directed Research and Development program, and by the Defense Threat Reduction Agency.

Jaggi, S., Langberg, M., Katti, S., Ho, T., Katabi, D., Medard, M., et al. (2008). Resilient network coding in the presence of byzantine adversaries. *IEEE Transactions on Information Theory, 54*(6), 2596-2603.
(Author affiliation: Chinese University of Hong Kong, The Open University of Israel
This material is based upon work supported by the Air Force Office of Scientific Research under Grant FA9550-06-1-0155, the National Science Foundation under Grants CCR-0325496 and CCF-0325324, the Chinese University of Hong Kong under Direct Grant 2050394, and Caltech's Lee Center for Advanced Networking.

Lee, K.-W., Chari, S., Shaikh, A., Sahu, S., & Cheng, P.-C. (2007). Improving the resilience of content distribution networks to large scale distributed denial of service attacks. *Computer Networks, 51*(10), 2753-2770.
(Author affiliation: IBM T.J. Watson Research Center)

Leem, L., Hyungmin, C., Bau, J., Jacobson, Q. A., & Mitra, S. (2010, 8-12 March 2010). *ERSA: Error Resilient System Architecture for probabilistic applications.* Paper presented at the Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany.
(Author affiliation: Stanford University and Nokia Research Center)
This work was supported in part by the Focus Center Research Program (FCRP) Gigascale Systems Research Center (GSRC) and the National Science Foundation.

Li, Z., Wang, L., Chen, Y., & Fu, Z. (2007). *Network-based and attack-resilient length signature generation for zero-day polymorphic worms.* Paper presented at the International Conference on Network Protocols, Beijing, China.
Support for this work was provided by the NSF grant CNS-0627751.

Maffeis, S., Mitchell, J., & Taly, A. (2009). Isolating JavaScript with filters, rewriting, and wrappers. In M. Backes & P. Ning (Eds.), *Lecture Notes in Computer Science No. 5789: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2009* (pp. 505-522). Berlin / Heidelberg: Springer.
(Author affiliation: Imperial College London and Stanford University)

Mondal, A., & Kuzmanovic, A. (2007). *A poisoning-resilient TCP stack.* Paper presented at the International Conference on Network Protocols
(Author affiliation: Northwestern University)
This work is supported by NSF CT grant ANI-0627715.

Pappas, V., Massey, D., & Lixia, Z. (2007, 25-28 June). *Enhancing DNS resilience against denial of service attacks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.

(Author affiliation: IBM Research, Colorado State University, and University of California, Los Angeles)

Rajagopalan, M., Hiltunen, M., Jim, T., & Schlichting, R. (2005, June 28 - July 1). *Authenticated system calls.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: University of Arizona and AT&T Labs-Research)
This work was supported in part by NSF under grants EIA-0080123, CCR-0113633, and CNS-0410918.

Ramasamy, H. V., & Schunter, M. (2007, June 27). *Architecting dependable systems using virtualization.* Paper presented at the Workshop on Architecting Dependable Systems, Edinburgh, Scotland.
(Author affiliation: IBM Zurich Research.)

Reiser, H. P., & Kapitza, R. (2007, March 23). *VM-FIT: Supporting intrusion tolerance with virtualisation technology.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Lisbon.
(Author affiliation: University of Erlangen and University of Lisbon)
This work has been supported by the DAAD.

Riley, R., Xuxian, J., & Dongyan, X. (2007, 25-28 June). *An architectural approach to preventing code injection attacks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: Purdue University and George Mason University)
This work was supported in part by NSF Grants OCI-0438246, OCI-0504261, and CNS-0546173.

Rodríguez, R., & Merseguer, J. (2010). Integrating fault-tolerant techniques into the design of critical systems. In H. Giese (Ed.), *Lecture Notes in Computer Science No. 6150: Architecting Critical Systems* (pp. 33-51). Berlin / Heidelberg: Springer.
(Author affiliation: Universidad de Zaragoza, Spain)

Sousa, P., Bessani, A. N., Dantas, W. S., Souto, F., Correia, M., & Neves, N. F. (2009, June 29 - July 2). *Intrusion-tolerant self-healing devices for critical infrastructure protection.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: University of Lisbon)
Supported by the EU through project IST-4-027513-STP (CRUTIAL) and the FCT through the Multiannual and CMU-Portugal Programmes.

Sousa, P., Bessani, A. N., & Obelheiro, R. R. (2008, April 1). *The FOREVER service for fault/intrusion removal.* Paper presented at the Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS), Glasgow, United Kingdom.
(Author affiliation: University of Lisbon and Universidade do Estado de Santa Catarina)
This work was partially supported by the EC through project IST-2004-27513 (CRUTIAL) and NoE IST-4-026764- NOE (RESIST/FOREVER), and by the FCT, through the Multiannual and the CMU-Portugal Programmes.

Wang, J., Stavrou, A., & Ghosh, A. (2010). HyperCheck: A hardware-assisted integrity monitor. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in*

Intrusion Detection (RAID) (pp. 158-177). Berlin / Heidelberg: Springer
(Author affiliation: George Mason University)

Wang, Z., & Zhang, W. (2010). A new construction of leakage-resilient signature. *Journal of Computational Information Systems, 6*(2), 387-394.
(Author affiliation: Nanjing University of Posts and Telecommunications, China)

Xu, Y., Bailey, M., Vander Weele, E., & Jahanian, F. (2010). CANVuS: Context-aware network vulnerability scanning. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection (RAID)* (pp. 138-157). Berlin / Heidelberg: Springer
(Author affiliation: University of Michigan, Ann Arbor)

Yixin, S., & Gyungho, L. (2007, 25-28 June). *Augmenting branch predictor to secure program execution.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: University of Illinois at Chicago)
This work was supported in part by a grant from the US National Science Foundation (CNS-0627431).

Yuanbo, G., Jianfeng, M., & Yadi, W. (2005). An intrusion-resilient authorization and authentication framework for grid computing infrastructure *Lecture Notes in Computer Science No. 3516: Computational Science* (pp. 229-236): Springer-Verlag.
(Author affiliation: School of Electronic Technology, Information Engineering, University, Zhengzhou, Henan, China; and Xidian University, China)

Zhiqiang, L., Xiangyu, Z., & Dongyan, X. (2008, 24-27 June). *Convicting exploitable software vulnerabilities: An efficient input provenance based approach.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: Purdue University)
This work is supported in part by NSF grants CNS-0720516, CNS-0708464 and CNS-0716444.

I.7 Isolation

Baliga, A., Iftode, L., & Chen, X. (2008). Automated containment of rootkits attacks. *Computers & Security, 27*(7-8), 323-334.
(Author affiliation: Rutgers University and VMware)

Batsell, S. G., Rao, N. S., & Shankar, M. (2003). *Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security*. Oak Ridge, TN: Oak Ridge National Laboratory.
http://www.ioc.ornl.gov/projects/documents/containment.pdf
Research note: ORNL developed an integrated cyber security framework for identifying and containing attacks within an organizational network domain. This framework is distributed, autonomous, and capable of detecting new attacks.

Foo, B., Wu, Y. S., Mao, Y. C., Bagchi, S., & Spafford, E. (2005, June 28 - July 1). *ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment.* Paper presented at the

International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Purdue University)

Hansen, A. F., Kvalbein, A., Cicic, T., & Gjessing, S. (2005). Resilient routing layers for network disaster planning *Lecture Notes in Computer Science No. 3420: Networking* (Vol. vol.2, pp. 9 pp.): Springer-Verlag.
(Author affiliation: Simula Research Laboratory, Norway and Telenor R&D, Norway)

Hoang, N., & Nahrstedt, K. (2007). *Attack containment framework for large-scale critical infrastructures.* Paper presented at the International Conference on Computer Communications and Networks.
(Author affiliation: University of Illinois at Urbana-Champaign)
This material is based upon work supported by the National Science Foundation under Grant CNS-0524695.

Khalil, I., Saurabh, B., & Shroff, N. B. (2005, June 28 - July 1). *LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Purdue University)

Liu, P., Wang, H., & Li, L. (2006). Real-time data attack isolation for commercial database applications. *Journal of Network and Computer Applications, 29*(4), 294-320.
(Author affiliation: Pennsylvania State University.)
Research note: Database attack isolation algorithm and prototype.

Rahimi, S., & Zargham, M. (2010, October 29). *Security Implications of Different Virtualization Approaches for Secure Cyber Architectures.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Sekar, V., Xie, Y., Reiter, M. K., & Zhang, H. (2006, 25-28 June). *A multi-resolution approach for worm detection and containment.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: Carnegie Mellon University)
This work was partially supported by NSF grant number CNS- 0433540, and by KISA and MIC of Korea.

Sellke, S., Shroff, N. B., & Bagchi, S. (2005, June 28 - July 1). *Modeling and automated containment of worms.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Purdue University)
This work is partially supported by the National Science Foundation grant 0335247-ANI and an NSF Graduate Fellowship.

Soo Bum, L., Gligor, V. D., & Perrig, A. (2010, June 28 - July 1). *Dependable connection setup for network capabilities.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: Carnegie Mellon University)
This research was supported in part by US Army Research Laboratory and the UK Ministry of Defence under Agreement Number W911NF-06-3-0001 and by the US Army Research Office

under Contract W911 NF-07 -1-0287 at the University of Maryland.

Srivastava, A., & Giffin, J. (2008). Tamper-resistant, application-aware blocking of malicious network connections. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 39-58). Berlin / Heidelberg: Springer.
(Author affiliation: Georgia Institute of Technology)

Wai-Leong, Y., Westphal, C., & Kozat, U. C. (2010). *A resilient architecture for automated fault tolerance in virtualized data centers.* Paper presented at the IEEE/IFIP Network Operations and Management Symposium
(Author affiliation: DoCoMo USA Labs)

Wilder, M. D., Rinker, R. E., & Alves-Foss., J. (2010, October 29). *Automated Preemptive Hardware Isolation of High-Risk Computing Applications.* Paper presented at the Secure & Resilient Cyber Architectures Conference, McLean, VA, 29 Oct 2011.

Yu, Y., Wei, Y., Yi, Y., & Yong, L. (2010). *A switch-based ARP attack containment strategy.* Paper presented at the International Conference on Communication Systems, Networks and Applications.
(Author affiliation: Northeastern University - China)
This work is supported by the National Natural Science Foundation of China under No. 60803132.

I.8 Metrics

Measurement Frameworks and Metrics for Resilient Networks and Services - Technical report (2011). (Discussion Draft). Heraklion, Greece: European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report

Resilience Metrics and Measurements: Challenges and Recommendations (2011). Heraklion, Greece: European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-survey

Anwar, Z., Shankesi, R., & Campbell, R. H. (2008, 24-27 June). *Automatic security assessment of critical cyber-infrastructures.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: University of Illinois at Urbana-Champaign)
This work was funded by the UIUC TCIP Project NSF CNS 05-24695

Årnes, A., Valeur, F., Vigna, G., & Kemmerer, R. (2006). Using Hidden Markov models to evaluate the risks of intrusions. In D. Zamboni & C. Kruegel (Eds.), *Lecture Notes in Computer Science No. 4219: Recent Advances in Intrusion Detection (RAID)* (pp. 145-164). Berlin / Heidelberg: Springer
(Author affiliation: Norwegian University of Science and Technology and University of California, Santa Barbara)

Bondavalli, A. (2008, 7-9 May). *How hard is assessing and measuring resilience? [Panel].* Paper presented at the European Dependable Computing Conference (EDCC), Kaunas, Lithuania. (Author affiliation: University of Firenze)

Bondavalli, A., Lollini, P., Barbosa, R., Ceccarelli, A., Falai, L., Karlsson, J., et al. (2009). *Assessing, Measuring, and Benchmarking Resilience (AMBER): Final research roadmap*: AMBER Consortium. http://www.amber-project.eu/documents/md_279_amber_d3.2_finalresearchroadmap_v1.0.pdf

Carnegie Mellon Software Engineering Institute (2010, November 19). CERT Resilience Management, from http://www.cert.org/resilience/
Research note: A process improvement approach to enable an organization to ensure that its important assets stay productive in supporting business processes and services. An important component of this approach is resilience measurement and analysis.
Key references: CERT Resilience Management Model, Version 1.0. (2010): http://www.cert.org/archive/pdf/10tr012.pdf; Measuring operational resilience using the CERT Resilience Management Model. (2010): http://www.cert.org/archive/pdf/10tn030.pdf; Caralli, R A. (2006). Sustaining operational resilience: A process improvement approach to security management: http://www.cert.org/archive/pdf/sustainoperresil0604.pdf; and Merrell, S. A., Moore, A. P., & Stevens, J. P. (2010, November 8-10). *Goal-based assessment for the cybersecurity of critical infrastructure*. Paper presented at the IEEE International Conference on Technologies for Homeland Security, Waltham, MA.

Chołda, P., Jajszczyk, A., & Wajda, K. (2008). A unified quality of recovery (QoR) measure. *International Journal of Communication Systems, 21*(5), 525-548.
(Author affiliation: AGH University of Science and Technology, Krakow, Poland.)
Contract/grant sponsor: Polish Ministry of Science and Higher Education.

Cholda, P., Tapolcai, J., Cinkler, T., Wajda, K., & Jajszczyk, A. (2009). Quality of resilience as a network reliability characterization tool. *IEEE Network, 23*(2), 11-19.
(Author affiliations: AGH University of Science and Technology and Budapest University of Technology and Economics.)
Supported by the Polish Ministry of Science and Higher Education; the High Speed Network Laboratory (HSNLab) at the Budapest University of Technology and Economics; the Hungarian National Research Fund; the National Office for Research and Technology; and the Hungarian Academy of Sciences.

Collins, M., & Reiter, M. (2008). On the limits of payload-oblivious network attack detection. In R. Lippmann, E. Kirda & A. Trachtenberg (Eds.), *Lecture Notes in Computer Science No. 5230: Recent Advances in Intrusion Detection (RAID)* (pp. 251-270). Berlin / Heidelberg: Springer
(Author affiliation: RedJack and the University of North Carolina at Chapel Hill)
This work was done while the author was listed with the CERT/NetSA group at the Software Engineering Institute, Carnegie Mellon University.

Cooke, E., Mao, Z. M., & Jahanian, F. (2006, 25-28 June). *Hotspots: The root causes of non-uniformity in self-propagating malware.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: University of Michigan)

This work was supported by the Department of Homeland Security (DHS) under contract number NBCHC040146, and by corporate gifts from Intel Corporation and Cisco Corporation.

Cukier, M., Berthier, R., Panjwani, S., & Tan, S. (2006, 25-28 June). *A statistical analysis of attack data to separate attacks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Philadelphia, PA.
(Author affiliation: University of Maryland, College Park)
This research has been supported by NSF CAREER award 0237493.

Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T., & Beitollahi, H. (2009, June 29 - July 2). *ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: CESI RICERCA - Italy and Katholieke Universiteit Leuven - Belgium)

Fonseca, J., & Vieira, M. (2008, 24-27 June). *Mapping software faults with web security vulnerabilities.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Anchorage, Alaska.
(Author affiliation: University of Coimbra - Portugal)

Gu, G., Fogla, P., Dagon, D., Lee, W., & Skoric, B. (2006). Towards an information-theoretic framework for analyzing intrusion detection systems. In D. Gollmann, J. Meier & A. Sabelfeld (Eds.), *Lecture Notes in Computer Science No. 4189: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2006* (pp. 527-546). Berlin / Heidelberg: Springer.
(Author affiliation: Georgia Institute of Technology and Philips Research Laboratories - the Netherlands)

Ha, D. T., Guanhua, Y., Eidenbenz, S., & Ngo, H. Q. (2009, June 29 - July 2). *On the effectiveness of structural detection and defense against P2P-based botnets.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: University at Buffalo and Los Alamos National Laboratory)
Hung Ngo and Duc Ha were supported in part by NSF CAREER Award CCF-0347565

Ingham, K., & Inoue, H. (2007). Comparing anomaly detection techniques for HTTP. In C. Kruegel, R. Lippmann & A. Clark (Eds.), *Lecture Notes in Computer Science No. 4637: Recent Advances in Intrusion Detection (RAID)* (pp. 42-62). Berlin / Heidelberg: Springer
(Author affiliation: University of New Mexico and Carleton University - Canada)

Jajodia, S., & Lopez, J. (2008). Identifying critical attack assets in dependency attack graphs. In R. Sawilla & X. Ou (Eds.), *Lecture Notes in Computer Science No. 5283: Computer Security - European Symposium on Research in Computer Security (ESORICS) 2008* (pp. 18-34). Berlin / Heidelberg: Springer
(Author affiliation: Defence Research and Development Canada and Kansas State University)
This author was partially supported by the US National Science Foundation under grant No. 0716665 and the US Department of Energy.

Jie, W., Phan, R. C. W., Whitley, J. N., & Parish, D. J. (2010, November 8-11). *Quality of detectability (QoD) and QoD-aware AAT-based attack detection.* Paper presented at the International

Conference for Internet Technology and Secured Transactions (ICITST), London.
(Author affiliation: Loughborough University)

Jing, J., & Xinyuan, W. (2009, June 29 - July 2). *On the effectiveness of low latency anonymous network in the presence of timing attack.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Lisbon, Portugal.
(Author affiliation: George Mason University)
This work was partially supported by NSF Grants CNS-0524286 and CT-0627493.

Kheir, N., Cuppens-Boulahia, N., Cuppens, F., & Debar, H. (2010). A service dependency model for cost-sensitive intrusion response. In D. Gritzalis, B. Preneel & M. Theoharidou (Eds.), *Lecture Notes in Computer Science No. 6345: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2010* (pp. 626-642). Berlin / Heidelberg: Springer
(Author affiliation: Telecom Bretagne - France, France Telecom R&D, and Telecom SudParis)

Kim, S., Lee, H., & Lee, W. Y. (2006). *Improving resiliency of network topology with enhanced evolving strategies.* Paper presented at the IEEE International Conference on Computer and Information Technology, Seoul, Korea.
(Author affiliation: Korea University and Hallym University)
This work was supported in part by the ITRC program of the Korea Ministry of Information & Communications under the grant IITA-2005-(C1090-0502-0020) and the BK21 program of the Korea Ministry of Education.

Kocsis, I., Csertan, G., Pasztor, P. L., & Pataricza, A. (2008, August 25-31). *Dependability and security metrics in controlling infrastructure.* Paper presented at the International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Cap Esterel.
(Author affiliation: Budapest University of Technology and Economics)

Kreidl, O. P. (2010, June 28). *Analysis of a Markov decision process model for intrusion tolerance.* Paper presented at the Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS), Chicago.
(Author affiliation: MIT Laboratory for Information and Decision Systems)

Lad, M., Oliveira, R., Beichuan, Z., & Lixia, Z. (2007, 25-28 June). *Understanding resiliency of internet topology against prefix hijack attacks.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: University of California, Los Angeles and University of Arizona)
This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) under Contract No N66001-04-1- 8926 and by National Science Foundation(NSF) under Contract No ANI- 0221453.

Marnerides, A., Pezaros, D. P., & Hutchison, D. (2008). *Detection and mitigation of abnormal traffic behaviour in autonomic networked environments.* Paper presented at the ACM CoNEXT Conference, Madrid, Spain.
(Author affiliation: Lancaster University, UK)

Martin, R. A. (2009). Making security measurable and manageable. *CrossTalk, 22*(6), 27-36.
http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-0-Issue.pdf

(Author affiliation: MITRE Corporation)

Meyer, J. F. (2009, September 17). *Defining and evaluating resilience: A performability perspective.* Paper presented at the International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS), Eger, Hungary.
(Author affiliation: University of Michigan, Ann Arbor.) See also Presentation slides: ftp://www.eecs.umich.edu/people/jfm/PMCCS-9_Slides.pdf.

Mu, C., Li, X., Huang, H., & Tian, S. (2008). Online risk assessment of intrusion scenarios using D-S evidence theory. In S. Jajodia & J. Lopez (Eds.), *Lecture Notes in Computer Science No. 5283: Computer Security - European Symposium on Research in Computer Security (ESORICS) 2008* (pp. 35-48). Berlin / Heidelberg: Springer
(Author affiliation: Beijing Institute of Technology, Beijing Jiaotong University, and NanChang University - China)
Supported by the Annual Proposed Sci-tech Project of 2008 of Jiangxi Education Bureau (GJJ08036).

Oehmen, C., Peterson, E., & Dowson, S. (2010). *An organic model for detecting cyber-events.* Paper presented at the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee.
(Author affiliation: Pacific Northwest National Laboratory)
Work presented herein was partly funded by the Laboratory Directed Research and Development (LDRD) at Pacific Northwest National Laboratory (PNNL).

Peng, X., Li, J. H., Xinming, O., Peng, L., & Levy, R. (2010, June 28 - July 1). *Using Bayesian networks for cyber security analysis.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Chicago, IL.
(Author affiliation: Intelligent Automation Inc., Kansas State University, and Pennsylvania State University)
This work was partially supported by Army Research Office contract W911NF-07-C-0101. Xinming Ou was partially supported by U.S. NSF under Grant No.0716665, and U.S. AFOSR under contract FA9550-09-1-0138. Peng Liu was supported by ARO MURI on Computer-aided Human Centric Cyber Situation Awareness, AFOSR MURI FA9550-07-1-0527, NSF CNS-0905131, NSF CNS-0916469, and AFRL FA8750-08-C-0137.

Potyra, S., Sieh, V., & Cin, M. D. (2007, September 4). *Evaluating fault-tolerant system designs using FAUmachine.* Paper presented at the Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia.
(Author affiliation: University of Erlangen)

Rosenkrantz, D. J., Goel, S., Ravi, S. S., & Gangolly, J. (2005). Structure-based resilience metrics for service-oriented networks. In M. Dal Cin, M. Kaâniche & A. Pataricza (Eds.), *Lecture Notes in Computer Science No. 3463: Dependable Computing - Proceedings of the 2005 European Dependable Computing Conference* (pp. 345-362): Springer Verlag.
(Author affiliation: University of Albany)

Stafford, S., & Li, J. (2010). Behavior-based worm detectors compared. In S. Jha, R. Sommer & C. Kreibich (Eds.), *Lecture Notes in Computer Science No. 6307: Recent Advances in Intrusion Detection*

(RAID) (pp. 38-57). Berlin / Heidelberg: Springer
(Author affiliation: University of Oregon)
This material is based upon work supported by the United States National Science Foundation under Grant No. CNS-0644434.

van Moorsel, A., Alberdi, E., Barbosa, R., Bloomfield, R., Bondavalli, A., Durães, J., et al. (2009). *Assessing, Measuring, and Benchmarking Resilience (AMBER): State of the art*: AMBER Consortium. http://www.amber-project.eu/documents/md_242_amber_d2.2_stateoftheart_v2.0final_submit.pdf

Vieira, M., Laranjeiro, N., & Madeira, H. (2007, 25-28 June). *Assessing robustness of web-services infrastructures.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK.
(Author affiliation: University of Coimbra - Portugal)

Vieira, M., & Madeira, H. (2005, June 28 - July 1). *Towards a security benchmark for database management systems.* Paper presented at the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan.
(Author affiliation: Coimbra University, Portugal)

Wang, H., & Liu, P. (2006). Modeling and evaluating the survivability of an intrusion tolerant database system. In D. Gollmann, J. Meier & A. Sabelfeld (Eds.), *Lecture Notes in Computer Science No. 4189: Computer Security – European Symposium on Research in Computer Science (ESORICS) 2006* (pp. 207-224). Berlin / Heidelberg: Springer
(Author affiliation: Pennsylvania State University)

Wang, L., Jajodia, S., Singhal, A., & Noel, S. (2010). *K*-zero day safety: Measuring the security risk of networks against unknown attacks. In D. Gritzalis, B. Preneel & M. Theoharidou (Eds.), *Lecture Notes in Computer Science No. 6345: Computer Security – European Symposium on Research in Computer Security (ESORICS) 2010* (pp. 573-587). Berlin / Heidelberg: Springer
(Author affiliation: Concordia University, George Mason University, and NIST)

Xuan, C., Copeland, J., & Beyah, R. (2009). Toward revealing kernel malware behavior in virtual execution environments. In E. Kirda, S. Jha & D. Balzarotti (Eds.), *Lecture Notes in Computer Science No. 5758: Recent Advances in Intrusion Detection (RAID)* (pp. 304-325). Berlin / Heidelberg: Springer.
(Author affiliation: Georgia Institute of Technology and Georgia State University)

Appendix II: Commercial Organizations Performing Resiliency Research

The commercial organizations below are a few of the companies that had specific, published resiliency research efforts showing in the search results for this report. They are listed with a short description of the research noted and a web address to additional information about their research.

CA

Research area: Security management.
http://www.ca.com/us/about-us/ca-labs/research-areas/security-management.aspx

Cisco

Research areas: Software vulnerability mitigation and information protection.
http://www.cisco.com/web/about/ac50/ac207/crc_new/ciscoarea/virtualization.html

Core Labs

Research areas: Attack attribution, vulnerability analysis, and source code auditing.
http://www.coresecurity.com/content/corelabs-projects-index

HP Laboratories

Research areas: Cyber risk, security automation, trusted infrastructure, and sophisticated attack mitigation.

http://www.hpl.hp.com/research/cloud_security/

IBM Research

Research areas: Software static analysis and network intrusion.
https://researcher.ibm.com/researcher/view_project.php?id=151

Intel

Research area: Cyber attack defense.
http://techresearch.intel.com/projecthome.aspx?ResearchAreaId=7

Mcafee Labs

Research areas: Malware research and threat protection.
http://www.mcafee.com/apps/view-all/publications.aspx?tf=mcafee_labs&sz=10&region=us

Microsoft Research

Research areas: Automated software testing, provable security guarantees, software static analysis, software vulnerability mitigation, software reliability, and systems dependability.
http://tinyurl.com/4wcxmh9

PARC

Research areas: General security/privacy research.
http://www.parc.com/work/focus-area/security-and-privacy/

RSA Laboratories

Research areas: Authentication technologies and high integrity solutions.
http://www.rsa.com/rsalabs/node.asp?id=3121

Symantec

Research areas: Attack attribution, high-availability systems, malware analysis, vulnerability analysis, and software reliability.

http://www.symantec.com/about/profile/researchlabs.jsp

Appendix III: Matrix of Institutions by Category

Table 2 presents a quick view of all institutions associated with the resiliency references listed in Appendix I, and their noted resiliency categories.

Table 2: Matrix of institutions by category

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
21st Century Technologies, Inc.	US				1					1
2LRESEARCH	US	1								1
Aachen University - Germany	EU				1					1
Aalborg University	EU					1				1
Aerospace Corporation	US		1							1
AFCO Systems Development, Inc	US	1								1
AGH University of Science and Technology	EU								2	2
Air Force	US		1							1
Air Force Institute of Technology	US				1					1
Air Force Office of Scientific Research	US		1			2	1		1	5
Air Force Research Laboratory	US	2			5				1	8
Alphatech Inc	US	1								1
Amazon.com Inc.	US				1					1
AMBER	EU								2	2
Arbor Networks	US		1							1
Aries Design Automation, LLC	US				1					1
Army Research Laboratory	US						1			1
Army Research Office	US		1		3			1	1	6

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
AT&T Labs	US				1					1
AT&T Labs-Research	US						1			1
Avaya Labs	US				1					1
Bar-Ilan University, Israel	IS	1				1				2
BBN Technologies	US	3	2			1				6
Beijing Institute of Technology	CH								1	1
Beijing Jiaotong University	CH								1	1
Bell Labs/Lucent Technologies	US	1								1
BlueRISC Inc	US					1				1
Boeing Company	US	1								1
Brazilian Ministry of Education	SA					1				1
Brazilian Ministry of Science and Technology	SA					1				1
Brazilian National Research Agency CNPq	SA						1			1
Brazilian National Research Council	SA						1			1
Budapest University of Technology and Economics	EU								2	2
California Institute of Technology	US						1			1
Cambridge University	EU		1							1
Carleton University - Canada	CA								1	1
Carnegie Mellon Software Engineering Institute	US				1				2	3
Carnegie Mellon University	US	1	2		6			2		11

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
CESI RICERCA	EU								1	1
CESNET - Czech Republic	EU				1					1
Chalmers University of Technology - Sweden	EU	1			1					2
Charles University - Czech Republic	EU						1			1
Chinese Ministry of Economic Affairs	CH						1			1
Chinese University of Hong Kong	CH						1			1
Chulalongkorn University, Thailand	AS				1					1
Cisco	US		1						1	2
City University London	EU					2				2
CNIT - Italy	EU	1								1
Coastal Carolina University	US						1			1
Coimbra University, Portugal	EU								1	1
College of William and Mary	US				1					1
Colorado State University	US				1		1			2
Columbia University	US	2		1	3	1				7
Communications Research Centre - Canada	CA			1						1
Concordia University	US								1	1
CYBER SPK, LLC	US				1					1
Czech Technical University in Prague	EU				1					1
Dakota State University	US				1					1
DARPA	US	7	2		1	4			1	15
DataSoft Corp.	US			1						1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Defence Research and Development Canada	CA								1	1
Defense Threat Reduction Agency	US						1			1
Dell	US	1								1
DENSoft Corporation	X		1							1
Department of Defense	US	2	1	1	5	1	1		1	12
Department of Energy	US	1	2	1			1		1	6
Department of Homeland Security	US	1	1		2				1	5
Deutsche Forschungsgemeinshaft (DFG)	EU				1					1
DoCoMo USA Labs	AS							1		1
DSO National Laboratories (Singapore)	AS					1				1
École Polytechnique Fédérale de Lausanne (EPFL)	EU					1				1
Eindhoven Technical University, The Netherlands	EU				1					1
ENISA	EU		4						2	6
ESF	EU					1				1
ESIEA Laval - France	EU				1					1
European Commission	EU	1	1	3	4	8	1			18
European Union	EU			1			1			2
Federal Networking and Information Technology Research and Development (NITRD)	US		2			1				3
Foundation for Research & Technology - Greece	EU				2					2

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
France Telecom R&D	EU				1				1	2
Fred Cohen & Associates	US					1				1
French Ministry of Research.	EU			1						1
George Mason University	US	2			4	4	2		2	14
George Washington University	US	1								1
Georgia Institute of Technology	US				6	1	1	1	2	11
Georgia State University	US				1				1	2
Gigascale Systems Research Center	US				1		1			2
Global InfoTek, Inc	US	1								1
Government of South Korea	AS								1	1
Greek GGET	EU					1				1
Greek Secretariat for Research and Technology	EU					1				1
Hallym University, Korea	AS								1	1
Hebrew University of Jerusalem	IS					1				1
Hewlett Packard	US					1				1
Highwayman Associates	EU		1							1
Hong Kong Polytechnic University	AS		1							1
Hong Kong Special Administrative Region, China	CH		1							1
HP Laboratories	US					1				1
Hungarian Academy of Sciences	EU								1	1
Hungarian National Research Fund	EU								1	1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
I3S (CNRS/UNS)/INRIA	EU				1					1
IBM	US				1					1
IBM Global Services	US				1					1
IBM Research	US	1			1		2			4
IBM T.J. Watson Research Center	US					1	1			2
Idaho National Laboratory	US		1	1						2
Imperial College London	EU						1			1
Indiana University	US		1							1
Inria, Laboratoire en Recherche Informatique, France	EU		1							1
Institute Eurecom	EU			1						1
Institute Eurecom - France	EU			4	2					6
Institute for Human and Machine Cognition	US	1								1
Institute for Infocomm Research - Singapore	AS				1	1				2
Institute of Computer Science, Foundation for Research and Technology - Greece	EU					1				1
Intel	US	1			1		1		1	4
Intelligent Automation Inc	US								1	1
Intelligent Systems Technology, Inc	US		1							1
International Computer Science Institute	US				1					1
Iowa State University	US				1					1
Israeli Ministry of Science	IS	1								1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Japan Advanced Institute of Science and Technology	AS				1					1
Japanese Ministry of Education, Culture, Sports, Science and Technology	AS				1					1
Jiangxi Education Bureau	CH								1	1
Johns Hopkins University	US				1	1	1			3
Justus-Liebig-Universit¨at Giessen, Germany	EU					1				1
Kansas State University	US								2	2
Katholieke Universiteit Leuven - Belgium	EU				1				1	2
Korea Information Security Agency	AS				2			1		3
Korea Ministry of Education	AS								1	1
Korea Ministry of Information & Communications	AS								1	1
Korea Science and Engineering Foundation	AS	1								1
Korea University	AS								1	1
Korean Ministry of Information and Communications	AS				2			1		3
LAAS-CNRS - France	EU		1							1
Lancaster University, UK	EU	1	1						1	3
Lawrence Berkeley National Laboratory	US		1		2					3
Linkoping University - Sweden	EU				1					1
Indiana University at Bloomington	US				1					1
Lockheed Martin	US	1								1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Los Alamos National Laboratory	US		2		1		1		1	5
Loughborough University	EU								1	1
Madrid Regional Research Council	EU				1					1
MADYNES - INRIA - France	EU	1								1
Massachusetts Institute of Technology	US		1	1	1		1		1	5
Microsoft Research	US		1		1	1	1			4
MIT Lincoln Laboratory	US					1				1
MITRE Corporation	US	1	1						1	3
Motorola	US				1		1			2
Motorola Labs	US						1			1
Mubarak City for Scientific Research and Technology Applications (MuCSAT), Egypt	AF		1							1
NanChang University - China	CH								1	1
Nanjing University of Posts and Telecommunications, China	CH						1			1
Narus Inc	US					1				1
National Aerospace University "KhAI", Kharkiv, Ukraine	EU					1				1
National Cyber Defense Initiative	US		1							1
National Institute of Standards and Technology	US					1				1
National Natural Science Foundation of China	AS							1		1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
National Office for Research and Technology	X								1	1
National Science Council, Taiwan	AS						1			1
National Science Foundation	US	7	2	2	13	8	14	3	8	57
National Taiwan Ocean University	AS				1					1
National Taiwan University	AS						1			1
National University of Computer & Engineering Sciences - Pakistan	AS				1					1
National University of Sciences & Technology - Pakistan	AS				1					1
National University of Singapore	AS				1					1
Natural Science and Engineering Council of Canada	CA	1								1
Naval Postgraduate School	US			1						1
NEC Laboratories Europe	EU		1							1
NEC Labs America	AS	1								1
Nepenthes Development Team	EU		1							1
Netherlands Organization for Scientific Research	EU					1				1
NetLogic Microsystems	EU				1					1
Newcastle University	EU		1			1				2
NIST	US								1	1
Nokia Research Center	EU						1			1
North Dakota State University	US				1					1
Northeastern University - China	CH							1		1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Northwestern University	US				1		2			3
Norwegian Computing Center - Norway	EU	1								1
Norwegian University of Science and Technology	EU								1	1
Nova Southeastern University	US						1			1
Oak Ridge National Laboratory	US	1	3		1			1		6
Office of Naval Research	US	1	2		3	1				7
Office of the Director of National Intelligence	US		1							1
Pace University	US		1							1
Pacific Northwest National Laboratory	US		1		2				1	4
Pennsylvania State University	US							1	2	3
Philips Research Laboratories - the Netherlands	EU								1	1
Polish Ministry of Science and Higher Education	EU								2	2
Pontifical Catholic University of Rio Grande do Sul - Brazil	SA						1			1
Pontificia Universidade Catolica do Parana – Brazil	SA						1			1
Portland State University	US				1					1
Portugal Telecom	EU				1					1
Princeton University	US						2			2
Puerto Rico Industrial Development Company	US	1								1
Purdue University	US	1	1		3	2	2	3		12
Q-Sphere Ltd - UK	EU	1								1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Queen Mary University of London	EU	1								1
Queen's University, Ontario, Canada	CA		1							1
Raytheon Company	US					2				2
RedJack	US								1	1
Rensselaer Polytechnic Institute	US				1	1				2
ReSIST	X		1							1
Rice University	US					1	1			2
Royal Military Academy, Belgium	EU				1					1
Rutgers University	US	1						1		2
Samsung	AS				1					1
Sandia National Laboratories	US		2			2				4
School of Electronic Technology, Information Engineering, University, Zhengzhou, Henan, China	CH						1			1
SCIT Labs	US	1								1
Sentar, Inc.	US		1							1
Simula Research Laboratory, Norway	EU					1		1		2
Singapore Management University	AS				1					1
Smart Information Flow Technologies (SIFT)	US	1								1
Southern Illinois University	US							1		1
Spanish National Science Foundation	EU				1					1
SRI International	US				1					1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Stanford University	US				2		2			4
Stockholm University, Sweden	EU					1				1
Stony Brook University	US	1			2	1				4
Supélec	EU					2				2
Swiss Federal Institute of Technology, Zurich	EU		1							1
Symantec	US	1		1	3	1				6
Symantec Research Labs	US				1					1
Taiwan Information Security Center	AS						1			1
Technical University of Lisbon	EU				1					1
Technical University of Vienna	EU				2					2
Technion – Israel Institute of Technology	IS	2								2
Technische Universitaet Muenchen, Germany	EU				1					1
Telcordia Technologies	US				3		1			4
Telecom Bretagne - France	EU								1	1
Telecom SudParis	EU								1	1
Telekom Austria AG	EU	1								1
Telenor R&D, Norway	EU					1		1		2
Tennessee Higher Education Commission	US				1					1
Texas A&M University	US				1					1
The Open University of Israel	IS						1			1
The Technion – Israel Institute of Technology	IS						1			1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
Tokyo Institute of Technology	AS					1				1
Tsinghua University, Beijing, China	CH					1	1			2
TXT e-solutions SpA - Italy	EU	1								1
U.S. Cyber Consequences Unit	US		1							1
UK Engineering and Physical Sciences Research Council	EU					1				1
UK Ministry of Defence	EU						1	1		2
Universidad de Zaragoza, Spain	EU						1			1
Universidad Politecnica de Madrid	EU				1					1
Universidad Politecnica of Valencia, Spain	EU		1							1
Universidade do Estado de Santa Catarina	SA					1	1			2
Universidade do Vale do Rio dos Sinos - Brazil	SA						1			1
Universidade Federal de Campina Grande	SA					1				1
Universidade Federal de Santa Catarina - Brazil	SA						1			1
Universita degli Studi di Milano	EU				1					1
Universität Stuttgart	EU					1				1
Universiteit van Amsterdam	EU				1					1
University at Buffalo	US				2				1	3
University College London	EU		1							1
University of Albany	US								1	1
University of Arizona	US						1		1	2

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
University of California, Berkeley	US				1	1				2
University of California, Davis	US	2			3					5
University of California, Los Angeles	US						1		1	2
University of California, San Diego	US				1					1
University of California, Santa Barbara	US				5				1	6
University of Cambridge (UK)	EU					1				1
University of Central Florida	US			1						1
University of Coimbra - Portugal	EU					1			2	3
University of Denver	EU				1					1
University of Erlangen	EU					1	1		1	3
University of Firenze	EU								1	1
University of Florence	EU					1				1
University of Göttingen (Germany)	EU					1				1
University of Idaho	US		1					1		2
University of Illinois at Chicago	US						1			1
University of Illinois at Urbana-Champaign	US	2	1		2		1	1	1	8
University of Kansas	US	1	1							2
University of Lisbon	EU				2	5	3			10
University of London	EU						1			1
University of Louisville	US		1							1
University of Luxembourg	EU				1					1
University of Mannheim	EU		1		1					2

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
University of Maryland, College Park	US	1	1		2				1	5
University of Memphis	US	1								1
University of Michigan	US				2				1	3
University of Michigan, Ann Arbor	US		1		2		1		1	5
University of New Brunswick, Canada	CA		1							1
University of New Mexico	US								1	1
University of North Carolina at Chapel Hill	US				3				1	4
University of North Carolina Raleigh	US				1					1
University of Notre Dame	US	1								1
University of Oregon	US								1	1
University of Saskatchewan, Canada	CA		1							1
University of Southern California	US	1	1							2
University of Tennessee at Chattanooga	US				1					1
University of Texas at Arlington	US				1					1
University of Texas at Austin	US		1		3	1				5
University of Thessaloniki, Greece	EU					2				2
University of Toulouse - France	EU			1						1
University of Turabo, Puerto Rico	US	1								1
University of Twente, The Netherlands	EU				1					1
University of Virginia	US				1	1				2
University of Waterloo, Canada	CA	1								1

Institutions	Region Code	Adaptive	Cross-Area	Deception	Detection	Dynamic	Integrity	Isolation	Metrics	Total
University of Wisconsin	US				3					3
University of Wisconsin-Madison	US				1		1			2
USAF Space and Missile Systems Center	US		1							1
Vienna University of Technology	EU				1					1
VMware	US	1						1		2
Vrije Universiteit, The Netherlands	EU				1	1				2
VTT Technical Research Centre - Finland	EU	1								1
West Virginia University	US					1				1
Xidian University, China	CH						1			1
Yahoo! Research	US						1			1
(discarded)										3
Total (duplicated count)		**80**	**77**	**23**	**189**	**98**	**85**	**25**	**86**	**666**

	Region Codes
AS	Asia-other
CA	Canada
CH	China
AF	Africa
EU	Europe
IS	Israel
SA	South America
US	USA