# REPORT DOCUMENTATION PAGE

AFRL-SR-AR-TR-04-

0495



| 1. REPORT DATE *30-8-2004* | 2. REPORT TYPE - Final Project Report | 3. DATES COVERED 9/1/2001 – 4/30/2004 |
|---|---|---|

**4. TITLE AND SUBTITLE**

## Sylvanus Thayer Fellowship

Critical Infrastructure Protection and Information Assurance Fellowship Program

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER** F49620-01-1-0272

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
George Cybenko, Thayer School of Engineering, Dartmouth College, Hanover NH 03755

gvc@dartmouth.edu, 603 646-3843

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Trustees of Dartmouth College
1 Rope Ferry Road
Hanover NH 03755

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

AFOSR
4015 Wilson Blvd., Room 713
Arlington, VA 22203-1954

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Unlimited

PIE

20041008 246

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The Sylvanus Thayer Fellowship project supported two Ph.D. level researchers from technical fields related to Critical Infrastructure Protection and Information Assurance to contribute more centrally to these areas. The fellows have worked in an intense research environment and are now actively engaged in research activities related to information assurance. Their newly acquired expertise is evidenced by their roles in CIPIA activities funded by federal and industrial research projects subsequent to this fellowship. The program has been extremely successful at turning US research scientists towards the nationally important and timely area of Critical Infrastructure Protection and Information Assurance.

**15. SUBJECT TERMS**

Critical information infrastructure information assurance fellows, security cybersleuth, cognitive hacking, semantic interoperability.

| 16. SECURITY CLASSIFICATION OF: Unclassified | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON George Cybenko |
|---|---|---|---|---|---|
| a. REPORT Unclassified | b. ABSTRACT Unclassified | c. THIS PAGE Unclassified | Unclassified | 4 | 19b. TELEPHONE NUMBER 603 646-3843 |

The Sylvanus Thayer Fellowship Project has been extremely successful at retraining two US citizens to contribute to national research priorities in the critical infrastructure protection and information assurance technical areas during the September 2001 to May 2004 duration of the project. The two US scientists were:

- David Koconis, Ph.D. Aeronautics and Astronautics Engineering, Stanford University 1993
- Paul Thompson, Ph.D. Information and Library Systems, University of California, Berkeley, 1986

Both had Ph.D.'s in technical areas tangential to critical infrastructure protection and information assurance (CIPIA) from leading US universities and were well prepared to retool in order to contribute to CIPIA research areas. The project started with a search, in the summer of 2001 for US citizens with Ph.D.'s who were interested in changing their technical research directions. The search identified Koconis and Thompson who both began working under fellowship funding in the fall of 2001.

Koconis has become an expert in UNIX security, to the point that he has contributed to the teaching of SANS courses nationally. He is currently working on an Defense Advanced Research and Development Activity (OARDA) project at Dartmouth funded under subcontract from General Dynamics. That project is developing a state-of-the-art network prediction system based on a large variety of sensor and data fusion technologies. His expertise has successfully leveraged the significant UNIX systems programming experience that he gained during his previous scientific computing work. Koconis has contributed to both Livewire 1 and Livewire 2 exercises.

Thompson has become an expert in electronic information deception techniques, especially as they apply to criminal and other illegal activities. His work has been widely reported in technical conferences, journals and books. He is presently teaching computational linguistics and related courses at Dartmouth and is working at Norwich University's Cyber Security research center as well. Thompson was able to leverage his considerable information retrieval experience successfully and apply that to CIPIA areas. His current areas of interest include information retrieval applications in the intelligence community. Thompson has contributed to both Livewire 1 and Livewire 2 exercises.

In both cases, the fellowship program was largely successful due to mentoring provided by a large and active community of CIPIA practioners at Dartmouth's Thayer School of Engineering and the Institute for Security Technology Studies. The fellowship provided travel resources that allowed the fellows to attend conferences and workshops, initially to learn about CIPIA technologies and problems and eventually to present research results.

Short biographies of the two fellows are included below along with major technical findings summarized as links and abstracts.

**David Koconis** has primary responsibility for managing the information retrieval related subtask of the National Institute of Justice contract. He is also the lead developer on the main project under this task, the Security CyberSleuth, an email subscription service that gathers computer security related information from open sources on the Internet, indexes the documents, and disseminates customized notifications. His current research includes investigating and implementing techniques for automated document clustering, text categorization, and topic tracking. David is also engaged in the SANS community where he serves on the board of advisers for the UNIX security administrator (GCUX) certification track, is the Lead Grader for the track, and is certified in the Windows Security Administrator and Firewall Analyst tracks. He received a B.S. in Aerospace and Ocean Engineering from Virginia Tech in 1987 and an M.S. and Ph.D. in Aeronautics and Astronautics Engineering from Stanford University in 1988 and 1993, respectively.

Koconis' main technical contribution has been the Security Cybersleuth, described below. More details can be found at the website listed below.

**Security Cybersleuth**: Investigating cyber-attacks and related computer crimes requires up-to-date knowledge of current operating-system vulnerabilities, attack tools, intrusion-detection systems, and other security trends, threats, and defensive measures. Many open-source Web sites are dedicated to these topics, but manually monitoring the sites for updated information is costly and time-consuming. The Cyber Sleuth automates this monitoring process, notifying users whenever new relevant information appears on the Web. David Koconis has been the lead developer of the Cybersleuth software and web service. The CyberSleuth is an email subscription service available at

https://www.ists.dartmouth.edu/cybersleuth/

and is currently used by a community of security professionals. Other academic and commercial sites are interested in licensing the software from Dartmouth for related notification services. A screenshot of the CyberSleuth information page is below.

The Security CyberSleuth is a *FREE!* service that will save search engine queries and web site URLs, check them periodically, and send you email whenever a new web page is found or monitored pages are updated.

---

- Tell me more about what the Security CyberSleuth does.
- What search engine does the Security CyberSleuth use?
- Who runs the Security CyberSleuth?

---

**Tell me more about what the Security CyberSleuth does.**

The Security CyberSleuth is a notification service that works in three ways.

- You can enter up to five sets of query keywords. At a periodic interval of 1, 3, 7, 14, or 30 days (which you specify), the Security CyberSleuth submits your keyword queries to the ISTS search engine and collects the ten Web pages that are most relevant to your keywords. The list of ten pages are compared with the ten pages saved from the last time your query was run. If a new page appears in the recent list that was not in the older list, or if one of the marked pages from your previous top ten list has changed, the Security CyberSleuth sends you an e-mail message.
- You can enter up to six web site addresses (URLs) that are of particular interest to you. At a periodic interval of 1, 3, 7, 14, or 30 days (which you specify), the Security CyberSleuth checks these Web pages and sends you e-mail if one or more of them have changed since the last time it was checked.
- You can subscribe to an Interest Profile. The Security CyberSleuth checks profiles daily and sends you e-mail if a new page is discovered that matches the profile.

Once you receive the e-mail, you return to the Security CyberSleuth web page where you will find a table of the URLs that are newly discovered or updated. Or, if you prefer, we can include the URL's of the new or updated web pages in the e-mail you receive.

*Back to Top* *Close Window*

---

**What search engine does the Security CyberSleuth use for queries?**

The ISTS maintains a search engine that is continually updated with documents relevant to computer security. A customized crawler is used to discover new links daily. Each document is screened to ensure that it is relevant to the topic domains supported by the Security CyberSleuth before it is added to our search index. Currently, keyword searches can be submmitted to our collection of Security in the News

articles or to a collection of Linux Security articles.

*Back to Top* *Close Window*

---

**Who runs the Security CyberSleuth?**

The Security CyberSleuth is a software package produced by members of the IRIA at the Dartmouth College Institute for Security Technology Studies.

You can contact the developers at the cybersleuth@ists.dartmouth.edu.

**Paul Thompson** received his Ph.D. from the University of California, Berkeley, in 1986. His graduate research was on probabilistic information retrieval. From 1986-1988, he was an assistant professor at Drexel University's College of Information Studies. Subsequently, from 1988-1993, he was a member of PRC, Inc.'s artificial intelligence development group, where he conducted research in natural language understanding and information retrieval. Then from 1993 until 2001, he worked for West Publishing Company, which later became West Group. At West his research involved natural language understanding, information retrieval, and machine learning / text categorization. At ISTS he leads the Semantic Hacking project. He is currently a lecturer at Dartmouth College's Thayer School of Engineering and Department of Computer Science and research scientist at Norwich University in Vermont.

**Semantic Hacking:** A semantic attack is one in which the attacker modifies electronic information in such a way that the result is incorrect, but looks correct to the casual or perhaps even the attentive viewer. IRIA is developing a categorization of semantic attacks, as well as implementing a set of techniques for detecting semantic attacks.

**Published Papers and Documentation (at** http://www.ists.dartmouth.edu/IRIA/published/

George Cybenko, Annarita Giani, Carey Heckman, and Paul Thompson, "Cognitive Hacking: Technological and Legal Issues", Law Tech 2002 November 7-9, 2002.

George Cybenko, Annarita Giani, and Paul Thompson, "Cognitive Hacking: A Battle for the Mind", IEEE Computer August 2002, vol. 35, no. 8, p. 50-56.

George Cybenko, Annarita Giani, and Paul Thompson, "Cognitive Hacking and the Value of Information", Workshop on Economics and Information Security, May 16-17, 2002, Berkeley, California.

Gabriel Mateescu, Masha Sosonkina, and Paul Thompson, "A New Model for Probabilistic Information Retrieval on the Web", Second SIAM International Conference on Data Mining (SDM 2002) Workshop on Web Analytics.

Paul Thompson, "Semantic Hacking and Intelligence and Security Informatics", NSF / NIJ Symposium on Intelligence and Security Informatics, Lecture Notes in Computer Science, Berlin: Springer-Verlag, June 1-3, 2003, Tucson, Arizona, p. 390.

Paul Thompson, "Names: A New Frontier in Text Mining" NSF / NIJ Symposium on Intelligence and Security Informatics, Lecture Notes in Computer Science, Berlin: Springer-Verlag, June 1-3, 2003, Tucson, Arizona, p. 27-38 (co-authored with Frankie Patman).

Paul Thompson, "Utility - Theoretic Information Retrieval, Cognitive Hacking, and Intelligence and Security Informatics", to be presented at the Seventh International Conference on Computer Science and Informatics, Session on Predictive Modeling Techniques in Cary, North Carolina, on 28 September 2003.

Paul Thompson, "Cognitive Hacking and Digital Government: Digital Identity", presented at the International Conference on Politics and Information Systems: Technologies and Applications in Orlando, Florida, on 2 August 2003.

Paul Thompson and Steven Lulich, "Question Answering in the Infosphere: Semantic Interoperability and Lexicon Development", Language Evaluation Resources Conference Workshop on Question Answering Strategies, May 28, 2002, Las Palmas de Gran Canaria, Spain.