Scott A. Craver

Assistant professor,
Electrical and Computer Engineering
Binghamton University
Binghamton, NY 13902-6000
phone: 607.777.7238
scraver@binghamton.edu

Education

Princeton University, Princeton, NJ
Ph.D. in Electrical Engineering, November 2004
Dissertation Title: "Problems in Steganography and Watermarking."

Northern Illinois University, DeKalb, IL
M.S. in Computer Science: August 1995
B.S. in Computer Science and Mathematics: June 1994

Employment History

Binghamton University, Assistant Professor
Binghamton, NY, 8/04-present
TeraCentral Corporation, Software Engineer
Cupertino, CA, 6/01-9/01
Intel Microprocessor Research Lab, Research Assistant
Santa Clara, CA, 1/98-9/98, 6/99-9/99, 6/00-9/00
IBM T.J. Watson Research Center, Research Assistant
Hawthorne, NY, 6/97-12/97

Citation counts ISI Web of Science: 225 citations, H-index=4
Google Scholar[1]: 1163 citations, H-index=12

Research areas Steganalysis, security of DRM systems, cryptographic protocols, multimedia security, adversarial detection and estimation.

Key inventions, discoveries, and problems solved (in chronological order of ideas)[2]:

Ambiguity attacks (w/ Nasir Memon, Boon-Lock Yeo and Minerva Yeung.) Technique for forging evidence of watermarks, either by inversion or inspection of watermark embedding algorithms. Also called inversion attacks, "Craver attacks," "IBM attacks" and protocol attacks in the literature.

---

[1] This excludes the citation count for a book chapter, because citation counts are only available for the entire book, with 12 authors. Including this book gives a citation count of 2120, with an H-index of 13.

[2] Collaborators are explicitly named except in the case of my advisors or my students.

Supraliminal channels. Robust broadcast channel that permits public key exchange in censored environments.

Zero-knowledge watermark detection. Various techniques allow an adversary to directly verify a watermark signal's presence without enough information to damage or remove it.

PHOOSballs (w/ Boon-Lock Yeo.) Data structures derived from mutually incompatible space-filling curves, used to flatten a high-dimensional search space into two relational tables.

Breaking SDMI (w/ Ed Felten, Patrick McGregor, Bede Liu, Min Wu, Drew Dean, Ben Swartzlander and Adam Stubblefield.) Reverse-engineered and broke four unknown audio watermarks and one unknown CD signature algorithm. Under legal threat, filed declaratory judgment to establish that publishing such results do not violate federal law, with inconclusive results.

Histo-cepstral estimation. Technique to visualize the pdf of an unknown watermark signal by graphing a liftered folded cepstrum of a sample histogram. While useful for detection, its primary application is visualization for reverse-engineering.

Wow embedding. Imperceptible spatial/temporal warping of media that causes a compressed media file, taken as a binary string, to hash to a desired message.

Privacy ceilings (w/ Janice Tsai and Lorrie Cranor.) An hypothesized economic limit of privacy violation, caused by the increased liability of possessing too much control over, and information about, users.

BOWS-I. Led effort with students to win first stage of contest to defeat unknown image watermark. Attack strategies led to noise calipers technique.

Noise calipers. A method of reverse-engineering an unknown detection region with an oracle by randomly growing high-magnitude false alarms. Also called the "snakes on a cone" attack (or "snakes on a hyperplane" in the case of unnormalized correlation.)

Stego-contaminated animations. Computer animations and special effects for videoconferencing and wireless phone applications, whose pseudo-random behavior betrays ciphertext, estimable by a recipient with high robustness and bitrate.

Limits of coin-flip channels. Limiting results show that supraliminal channels can be derailed by an active warden with vanishingly small attack rates. This is due to the inability to overtly employ error correction in a censored environment.

Self-destructing unforwardable unprintable email (w/ Yu Chen.) Using an FPGA-augmented video cable, we can identify and decrypt encrypted images between a computer and display, preventing any in-computer leakage and allowing the enforcement of fine-grained usage rules.

Journal Articles:

1. **S.A. Craver, I.M. Atakli, and J. Yu**, "Reverse-Engineering a Watermark Detector Using an Oracle" *EURASIP Journal on Information Security*, vol. 2007, Article ID 43034, 7 pages, 2007. doi:10.1155/2007/43034.

2. **S.A. Craver, N. Memon, B-L. Yeo, and M. Yeung**, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications." In *IEEE Journal of Selected Areas in Communications*, special issue on Copyright and Privacy Protection, May 1998. 573-586.

3. **S.A. Craver, B-L. Yeo, and M. Yeung**, "Technical Trials and Legal Tribulations." In *Communications of the ACM*, July 1998. 44-54.

LNCS Articles[3]:

1. **S. Craver, E. Li, J. Yu, and I. Atakli.** "A supraliminal channel in a videoconferencing application." *Information Hiding*: 10th International Workshop, IH 2008, Santa Barbara, CA, USA, May 19-21, 2008. Revised Selected Papers. LNCS vol 5284/2008, pp 283–293.

2. **S.A. Craver**, "An Improved Asymmetric Watermarking System using Matrix Embedding," *Information Hiding*, 8th International Workshop, IH 2006, Alexandria, VA, USA, July 10-12, 2006. Revised Selected Papers. LNCS vol 4437/2007, pp 15-25

3. **S.A. Craver, B. Liu, and W. Wolf,** "An Implementation of, and Attacks on, Zero-knowledge watermarking." *Information Hiding*, 6th International Workshop, IH 2004, Toronto, Canada, May 23-25, 2004, Revised Selected Papers. LNCS 3200/2005 pp 1-12.

4. **S.A. Craver, B. Liu, and W. Wolf**, "Detectors for Echo-Hiding Systems." *Information Hiding*, 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7-9, 2002, Revised Papers. LNCS vol 2578/2003 pp 247-257.

---

[3] Articles in Springer *Lecture Notes in Computer Science* are sometimes cited as journal articles, sometimes conference publications. LNCS volumes are typically conference proceedings; however, LNCS has its own editorial board which exerts control over conference selection, and enforces stricter editorial rules. Articles in the *Information Hiding* series require revision after presentation.

To further complicate matters, LNCS volumes published prior to October 2006 are indexed as articles in *ISI Web of Science.* Volumes after this date appear in *ISI Proceedings* index.

5. **S.A. Craver**, "Zero-Knowledge Watermark Detection." *Information Hiding*, Third International Workshop, IH'99, Dresden, Germany, September 29 - October 1, 1999. LNCS vol 1768/2000 pp 101-116.

6. **S.A. Craver**, "On Public-Key Steganography in the Presence of an Active Warden." *Information Hiding*, Second International Workshop, Portland, Oregon, USA, April 14-17, 1998, Proceedings. LNCS vol 1525/1998 pp 355-368.

Conference Publications:

1. **E. Li and S.A. Craver**, "A Supraliminal Channel in a Wireless Phone Application." in 11th proc. ACM Multimedia and Security Workshop, NJ USA, Sept 7-8 2009. pp 151-154.

2. **I. Atakli, Y. Chen, Q. Wu and S.A. Craver**, "BLINK: Pixel-Domain Encryption for Secure Document Management." in 11th proc. ACM Multimedia and Security Workshop, NJ USA, Sept 7-8 2009, pp 171-175.

3. **S.A. Craver, E. Li and J. Yu**, "Protocols for Data Hiding in Pseudo Random State." in Proc. SPIE, Media Forensics and Security, Jan 19 2009, San Jose, CA. Vol. 7254, 72540W.

4. **S.A. Craver, Y. Chen, H. Chen, J. Yu, and I.M. Atakli,** "BLINK: Securing Information to the Last Connection." 6th IEEE Consumer Communications and Networking Conference, Jan 10-13 2009, Las Vegas NV.

5. **S. Zahorian, R. Belohlavek, S. A. Craver, R. McGrann, and L. Yu**, Work in progress - bringing SOCRATES into computer-assisted instruction." Frontiers in Education Conference, 2008. FIE 2008. 38th Annual, Saratoga Springs, NY

6. **S. Craver, E. Li, J. Yu, and I. Atakli.** A supraliminal channel in a videoconferencing application. In Information Hiding: 10th International Workshop, IH 2008, Santa Barbara, CA, USA, May19-21, 2008, pages283–293.

7. **S.A. Craver, J. Yu and I. Atakli,** "How We Broke the BOWS Watermark." In Proceedings of The International Society for Optical Engineering, E. J. Delp III and P. W. Wong, Eds., vol. 6505 of Proceedings of SPIE, San Jose, Calif, USA, January 2007.

8. **S.A. Craver and J. Yu,** "Reverse-engineering a Watermark with False Alarms." To appear, ." In Proceedings of SPIE, Security and Watermarking of Multimedia Contents IX, January 2007.

9. **J. Y. Tsai, L. Cranor and S. Craver**, "Vicarious Infringement Creates a Privacy Ceiling." In Proceedings of DRM 2006, the Sixth ACM Workshop on Digital Rights Management. October 2006.

10. **S.A. Craver and J. Yu**, "Fingerprinting with Wow." In Proceedings of SPIE, Security and Watermarking of Multimedia Contents VIII, January 2006.

11. **S.A. Craver, B. Liu, and W. Wolf**, "Histo-Cepstral Analysis for Reverse-Engineering Watermarks." In Proceedings of the 38th Conference on Information Sciences and Systems (CISS '04), Princeton, New Jersey: March 2004.

12. **S.A. Craver, M. Wu, B. Liu, and E. Felten**, "Analysis of Attacks on SDMI Audio Watermarks." In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Salt Lake City, Utah: May 1369-1372.

13. **S.A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.S. Dean, and E. Felten**, "Reading Between the Lines: Lessons Learned from the SDMI Challenge." In Proceedings of the Usenix Security Symposium, Washington D.C.: August 2001. 353-363.

14. **S.A. Craver and S. Katzenbeisser**, "Security Analysis of Public-Key Watermarking Schemes." In Proceedings of SPIE, Mathematics of Data/Image Coding, Compression and Encryption IV with Applications, July 2001. 172-182.

15. **S.A. Craver**, "The Return of Ambiguity Attacks." In Proceedings of SPIE, Security and Watermarking of Multimedia Contents IV, January 2002. 252-259.

16. **S.A. Craver, J.P. Stern,** "Lessons learned from SDMI," In Proceedings of the IEEE Fourth Workshop on Multimedia Signal Processing (2001) 213-218.

17. **S.A. Craver and S. Katzenbeisser**, "Copyright Protection Protocols Based on Asymmetric Watermarking: The Ticket Concept." *Communications and Multimedia Security Issues of the New Century*. From the Joint Working Conference on Communications and Multimedia Security, held May 21-22, 2001. Edited by R. Steinmetz, J. Dittmann, and M. Steinebach. Boston: Kluwer Academic Publishers, 2001. 159-170.

18. **S.A. Craver, B-L. Yeo, and M. Yeung**, "Multi-Linearization Data Structure for Browsing." In Proceedings of SPIE, Storage and Retrieval of Image and Video Databases, San Jose: CA: January 1999. 155-166.

19. **S.A. Craver, N. Memon, B-L. Yeo, and M. Yeung**, "On the Invertibility of Invisible Watermarking Techniques." In Proceedings of the IEEE International Conference on Image Processing (ICIP '97), Santa Barbara, CA: 1997. 540-543.

20. **S.A. Craver, N. Memon, B-L. Yeo, and M. Yeung**, "Can Digital Watermarks Resolve Rightful Ownerships?" In Proceedings of SPIE, Storage and Retrieval of Image and Video Databases, San Jose, CA: 1997. 310-321.

Invited Talks:

S.A. Craver, "Noise Calipers: a Technique for Reverse-Engineering Watermarks." In WaCha, The 2nd Wavila Challenge Workshop, Geneva, Switzerland, Nov 2006

S.A. Craver, M. Wu, and B. Liu, "What can we Reasonably Expect from Watermarks?" In Proceedings of the IEEE Workshop on Applications of Signal Processing to Audio and Acoustics 2001, Mohonk, NY: October 2001. 223-226.

Book Chapter:

S.A. Craver, A. Perrig, and F.A.P. Petitcolas. "Robustness of Copyright Marking Systems." *Information Hiding Techniques for Steganography and Digital Watermarking*. Edited by S. Katzenbeisser and F.A.P. Peticolas. Norwood, MA: Artech House, 2000. 149-174.

Patents:

S.A. Craver, B-L Yeo, and M. Yeung. "Multi-Linearization Data Structure for Image Browsing." U.S. Patent no. 6,233,367. May 2001.

S.A. Craver, B-L Yeo, and M. Yeung. "Displaying ordered images based on a linearized data structure." U.S. Patent no. 6,556,723. April 2003.

S.A. Craver, B-L Yeo, and M. Yeung. "Creating a linearized data structure for ordering images based on their attributes." U.S. Patent no. 6,628,846. September 2003.

S.A. Craver, B-L Yeo, and M. Yeung. "Linearized data structure ordering images based on their attributes." U.S. Patent no. 7,016,553. March 2006.

Courses Designed and Taught:

EECE 560 – Cryptology (Fall 2004-2009)
EECE 405 – Cryptography and Information Security (Spring 2005, Fall 2006-2009)
EECE 457 – Security Engineering (Fall 2005, Spring 2007-2009)
EECE 527 – Information Theory (Spring 2006-2009)

Awards and Research Grants:

Presidential Early Career (PECASE) award:
"Towards a General Theory of Counterdeception." $1,000,000, Sept 2009-Aug 2014. S. Craver, Principal Investigator.

AFOSR Young Investigator Award FA9550-07-1-0044:
"Identification of Secret Algorithms Using Oracle Attacks." $300,000, Jan 2007-Dec 2009. S. Craver, Principal Investigator.

AFOSR award FA9550-95-1-0440. "Estimation of Information Hiding Algorithms and Parameters." $150,000, June 2005-Nov 2006. S. Craver, Principal Investigator.

AFRL Grant FA8750-1-05-0235.
"Estimation of Hidden Signal Distributions and Reverse Engineering of Embedding Algorithms." $21,004, May-Aug 2005.

Activities:
Creator and organizer, **Annual Underhanded C Contest**.
http://underhanded.xcott.com/

Deputy Director, **Center for Advanced Information Technologies**.

Co-chair, **2009 ACM Multimedia and Security Workshop, Princeton NJ**

Session chair, **2006 ACM Multimedia and Security Workshop, Alexandria VA**
Session chair, **2006 SPIE Security and Watermarking of Multimedia Contents VIII**
Session chair, **2005 ACM Multimedia Security Workshop in New York, NY, Aug 2005.**
Session chair, **1999 Information Hiding Workshop, Dresden, Germany**

Nominated to attend National Academy of Engineering 2005 **US Frontiers of Engineering Symposium** in Niskayuna, NY, Sept 22-24, 2005.