

Hardware-Based Security (Author Workshop)

Institute for Security Technology Studies

Dartmouth College

(Revised agenda of September 12, 2005)

<http://www.cs.dartmouth.edu/~hardsec/>

Research into computer security and privacy typically focuses on computation. However, since computation ultimately requires computer hardware at its base, the structure and behavior of this hardware can fundamentally shape properties of the computation it hosts. This anthology will collect a set of invited papers that depict the state of the art in research into the design, use, and evaluation of hardware techniques to achieve security and privacy properties in higher-level computation.

The approach we will take is to look *forward* at the ideas and trends emerging here, and to portray the *diversity* of ideas and work: from architectural, application, and even programming languages perspectives, and from both academic as well as industrial areas. We want the text to reflect the dynamic state of this promising and emerging field.

Monday, September 12

Reception 6:00-8:00pm. Morrison Common, in Rockefeller Center (the same building as the meeting).

Tuesday, September 13 *Continental breakfast, outside Room 02*

- 8:45-9:15. *Welcome*. Ruby Lee and Sean Smith.

Processor-Level Projects (I)

- 9:15-10:00. *Cell Broadband Engine Security Architecture*. Kanna Shimizu (IBM Austin).
- 10:00-10:45. *LaGrande*. David Grawrock (Intel) (via telephone).
- 10:45-11:00. *Break*.
- 11:00-11:45. *Security and Hardware-Assisted Virtualization*. Leendert van Doorn, Ron Perez, Reiner Sailer (IBM Watson).

Baseline

- 11:45-12:30 *TCPA, TCG, TPMs, and TSSs*. Dave Challener (Lenovo) (via telephone)

Lunch (provided)

Processor-Level Projects (II)

- 1:30-2:15. *Architecture Support for Copy and Tamper-Resistant Software*. David Lie (University of Toronto).
- 2:15-3:00. *Minimalist Security Architecture in SP-processors*. Peter Kwan and Ruby Lee (Princeton University).
- 3:00-3:45. *Building Reliable and Secure Systems: from Measurements to Design*. Ravi Iyer and Zbigniew Kalbarczyk (University of Illinois at Urbana-Champagne).
- 3:45-4:00. *Break*.

Attestation

- 4:00-4:45. *Property-based Attestation*. Ahmad-Reza Sadeghi and Christian Stübke (Ruhr-University Bochum).
- 4:45-5:30. *Semantic Remote Attestation: Attesting Behavior, not Binaries*. Vivek Haldar, Deepak Chandra, and Michael Franz (University of California, Irvine).

Dinner (provided)

6:00-7:30pm, at *Jesse's Restaurant & Tavern*. <http://www.jesses.com/>

Wednesday, September 14 *Continental breakfast, outside Room 02*

- 8:45-9:00. *Re-orienting*. Ruby Lee and Sean Smith.

Application Frameworks

- 9:00-9:45. *Hardware Countermeasures for Malware*. David Kaeli (Northeastern University).
- 9:45-10:30. *Computer Architecture Countermeasures against Zombie Recruitment in DDoS Attacks*. David Champagne and Ruby Lee (Princeton University).
- 10:30-10:45. *Break*.
- 10:45-11:30, *Tiny Trusted Third Parties*. Alex Iliev and Sean Smith (Dartmouth College).

Wrap-up

- 11:30-1pm. *Discussion, and lunch (provided)*

Walking tour of Dartmouth Campus (optional)

Meeting Location

We've placed a marked-up campus map at <http://www.cs.dartmouth.edu/~hardsec/map.pdf>.

The meeting will be in Room 002, Rockefeller Center (D/E4 on the map).

All participants should try to park in the Dewey Lot (G/H 1/2 on the map). It's a short walk to Rockefeller Center; also a campus shuttle bus starts running in the parking lot at 7am (every 10 minutes).

Dartmouth features an open wireless network.

Hotels:

- Chieftain Motor Inn, Rte. 10 North, Hanover (approximately 2 miles from Dartmouth campus).
Telephone: (603) 643-2550 <http://www.chieftaininn.com/>
- Hampton Inn, 104 Ballardvale Drive, White River Junction, Vermont (approximately 5 miles from Dartmouth campus).
Telephone: (802) 296-2800 <http://www.whiteriverhampton.com/>

For More Information

Nicole Hall Hewett
Communication and Events Manager
Institute for Security Technology Studies
Dartmouth College
Phone: (603) 646-0714
Fax: (603) 646-0660
Nicole.Hall.Hewett@dartmouth.edu

Sean Smith
Department of Computer Science
Dartmouth College
Phone: (603) 646-1618
Fax: (603) 646-1672
sws@cs.dartmouth.edu