

CYBERSECURITY

James G. Hook, Associate Professor
Department of Computer Science
Maseeh College of Engineering and Computer Science
Portland State University
PO Box 751
Portland, OR 97207
(503)725-5540
hook@cs.pdx.edu

Summary of Research

A dozen faculty in the Computer Science department at PSU collaborate on a broad array of cybersecurity efforts that include: proactive techniques to build systems immune from attack, defensive techniques to protect systems from attack, forensic tools to analyze how a system was attacked, and offensive techniques that actively respond to cyberattacks. These efforts, some of which are in partnership with other institutions (most notably OGI), are funded by the Department of Defense, the National Science Foundation, and by industrial and regional sponsors.

Potential for Commercialization and Job Creation

There is an emerging business cluster in the Portland area that focuses on cybersecurity. The RAINS organization, in which PSU has taken a lead role, has been actively promoting the development of this cluster. Prior to moving to PSU, the systems and languages groups at OGI each launched successful spin-off companies. Galois Connections and Immunix maintain active relationships with PSU faculty. Cybersecurity research at PSU is generating patent applications, particularly for Dr. Wu-chang Feng's novel offensive techniques for response to denial of service attacks. In general, the prospects of new companies, and of growth in existing companies, are excellent.

Total Research Funding

Cybersecurity projects are funded from a variety of sources. The DOD awarded over \$6M to a joint project with OGI that began in 2000 and is funded to continue until 2008. The National Science Foundation has awarded over \$750,000,000. Industry and regional government have invested over \$350k.

Student Involvement

Students are involved in research all levels. Pre-college students serve as interns in the research programs. Undergraduate students participate in intensive summer internship programs. Over eight graduate students work on these projects full time.

Websites

Programatica

<http://www.cse.ogi.edu/PacSoft/projects/programatica/default.htm>

Forensix

<http://www.thefengs.com/wuchang/work/4N6>

<http://sourceforge.net/projects/forensix/>

IP Puzzles

<http://www.thefengs.com/wuchang/work/puzzles/>

Ourmon

Ourmon is open source and is also deployed in the center of PSU's network. The official ourmon link is: <http://ourmon.cat.pdx.edu/ourmon> The latest release is ourmon 2.4 which includes significant anomaly detection capabilities.