



**SPOTTING DANGERS:** "We explore different means for an adversary to compromise one's privacy, and how to counteract these dangers," says Professor Nan Zhang.

## Minimizing Trade-Offs

Life is full of trade-offs: we give something up to get something else. In the world of wireless devices and networks, sometimes the trade-off is giving up a bit of privacy in exchange for the convenience of using your cell phone, PDA, or other wireless device. That trade-off is what Professor Nan Zhang of the Department of Computer Science is working to minimize.

Zhang currently works on three projects that fit under the common theme of information security and privacy. Two of the projects—location privacy for wireless networks and privacy-preserving data mining—research and identify the threats to an individual person's privacy and aim to develop methods to protect them and counteract the threats.

The first step to combating the threats to privacy is to identify them. That is what Zhang and his colleagues, Professor Xinwen Fu of the University of Massachusetts-Lowell and Professor Wei Zhao of the University of Macau, have been doing. They were the first to discover that an adversary can set up a large antenna on the top of a building and very accurately estimate the location of all wireless devices operating in the area. "Most people," says Zhang, "don't know that whenever they have their cell phones with Wi-Fi open, this allows someone to know exactly where they are, even if they are not talking." Zhang and his colleagues also have discovered a system that allows people to use location-based services like Google maps to find points-of-interest, yet automatically hide their location from Google and still get very accurate location-based information. In fact, Zhang's doctoral student, Aniket Pingley, is currently working to publish the system on the Web and make it available to the public.

Likewise, Zhang and doctoral student Xin Jin are exploring ways to protect the privacy of individual information during data mining, a process that extracts information from databases for use in marketing, weather forecasting, medical diagnosis, and national security. Practical privacy-preserving data mining systems are largely in the research and prototyping stages, and Zhang is trying to explore possible solutions that would lead to guidelines for building these systems. Zhang explains, "We want to allow everyone to be able to get knowledge from the data, but we don't want individual people's information—like their age, occupation, salary—to be disclosed."

Zhang's third project considers privacy from the perspective of a company, government organization, or other large information provider. These organizations need to publish large amounts of information, either to provide services to their customers or for the benefit of society, but they need to keep the data from being exploited by competitors, adversaries, or terrorists. Zhang and his colleague, Professor Gautam Das of the University of Texas at Arlington, defined the problem of privacy protection in hidden Web databases. Says Zhang, "We basically discovered for the first time that the hidden database is also subject to significant privacy concerns, and we provided the first solution to help protect privacy in hidden databases."

### PROFILE

**Chair:** Abdou S. Youssef  
202-994-7181

**www.cs.gwu.edu**

**Full-time faculty:** 18

**Undergraduate students:** 102

**Graduate students:** 310

**Annual research expenditures:**  
\$2.2 million

### FACULTY

Abdelghani Bellaachia, **ASSOCIATE PROFESSOR**

Simon Berkovich, **PROFESSOR**

Peter Bock, **PROFESSOR**

Matthew Burke, **ASSISTANT PROFESSOR**

Xiuchen "Susan" Cheng, **ASSOCIATE PROFESSOR**

Hyeong-Ah Choi, **PROFESSOR**

James K. Hahn, **PROFESSOR**

Rachelle S. Heller, **PROFESSOR**

Lance J. Hoffman, **DISTINGUISHED RESEARCH PROFESSOR**

#### AND ACM FELLOW

C. Dianne Martin, **PROFESSOR AND ACM FELLOW**

Bhagirath Narahari, **PROFESSOR**

Rhys Price Jones, **PROFESSOR**

Shmuel Rotenstreich, **ASSOCIATE PROFESSOR**

John L. Sibert, **PROFESSOR**

Rahul Simha, **PROFESSOR**

Poorvi Vora, **ASSISTANT PROFESSOR**

Abdou S. Youssef, **PROFESSOR**

Nan Zhang, **ASSISTANT PROFESSOR**

### RESEARCH AREAS

#### ALGORITHMS AND THEORY

Bellaachia, Berkovich, Cheng, Choi, Price Jones, Youssef, Zhang

#### BIOINFORMATICS AND BIOMEDICAL COMPUTING

Bellaachia, Berkovich, Cheng, Hahn, Price Jones, Rotenstreich, Simha

#### COMPUTER SECURITY AND INFORMATION ASSURANCE

Hoffman, Martin, Simha, Vora, Zhang

#### DIGITAL MEDIA

Hahn, Heller, Martin, Sibert, Youssef

#### MACHINE INTELLIGENCE AND COGNITION

Bock

#### NETWORKING AND MOBILE COMPUTING

Cheng, Choi, Narahari, Rotenstreich, Simha

#### PERVASIVE COMPUTING AND EMBEDDED SYSTEMS

Cheng, Narahari, Simha

#### SOFTWARE ENGINEERING AND SYSTEMS

Narahari, Rotenstreich

#### SEARCH AND DATA MINING

Bellaachia, Berkovich, Youssef, Zhang