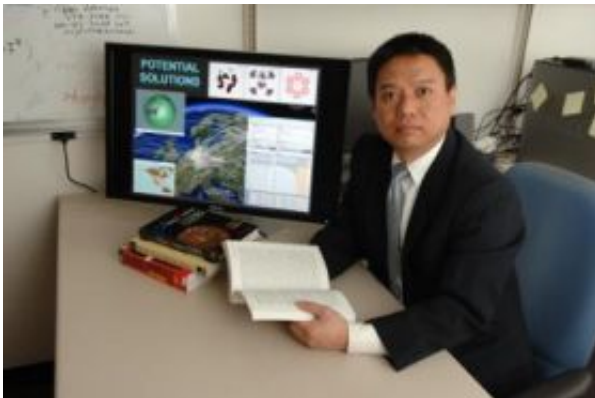


# Fraudsters beware: Iowa State engineer is developing cyber technology to find you

January 7 2008

---



Yong Guan, Iowa State University's Litton Assistant Professor of Electrical and Computer Engineering, is developing technologies to track down cyber criminals and make Web transactions more secure. Credit: Photo by Bob Elbert/Iowa State University

Yong Guan had scribbled 12 arrows across his office whiteboard, each black line going from one little box he had drawn to another little box. He had written five long formulas up there, too. And that was bad news for cyber criminals.

Guan, the Litton Assistant Professor of Electrical and Computer Engineering at Iowa State University, and his students are developing technologies to fight cyber crime and make online activities such as shopping more secure for everyone.

Guan and the Iowa State University Research Foundation have filed a patent on one technology that detects “click fraud” – falsely driving up hits to ads posted on Web sites. Those false hits result in higher costs for pay-per-click advertising. Guan said the invention will help online advertising companies such as Google and Yahoo reduce click fraud.

He said his research could also help millions of computer users who don’t have the time or expertise to protect their machines with the latest security patches and safeguards.

“There are a lot of security issues and researchers have worked on them from the early 1980s,” Guan said. “And 30 years later we’re still working on them. These are hard problems.”

In that time the nature of cyber crime has changed considerably, Guan said. It used to be hackers attacked systems for the thrill of it. Since the late 1990s, as more and more commerce happens online, he said money has become the major motivation for cyber crime.

And so Guan and his collaborators are working on several projects to make computing more secure and hold cyber criminals accountable:

-- Digital forensics

Guan is developing technology and techniques for extracting criminal evidence from computers, network hardware, cell phones and other electronic devices. The work is focused on three projects: Network attack attribution to help investigators find the real origins of cyber criminals and attackers; click fraud detection to protect Internet advertising; and auction fraud technology to quickly identify the people and their accomplices who run bogus Internet auctions.

Guan is working on the projects with James Davis, Iowa State’s chief

information officer; Doug Jacobson, a professor of electrical and computer engineering; Thomas Daniels, an assistant professor of electrical and computer engineering; and Julie Dickerson, an associate professor of electrical and computer engineering. David Baldwin and Todd Zdorkowski, leaders of the Midwest Forensics Resource Center at the U.S. Department of Energy's Ames Laboratory on the Iowa State campus, have also helped establish collaborative relationships with local and state police agencies.

The projects are supported by a \$1.2 million grant from the U.S. intelligence community's Disruptive Technology Office, a \$220,000 grant from the National Science Foundation and funding from Iowa State.

#### -- Wireless security

Guan is working on three projects to improve the security of working with wireless networks.

The first is looking at how a new secure network coding model can be protected from attacks while it transmits network traffic. The old system sent each individual message hop by hop until it reached its destination. The new way, based on network coding and cooperative relaying schemes, sends and combines messages in groups. Guan said it's like loading up a freight train and sending big loads down the line together. It's a way to increase capacity and save energy. But putting all that network traffic together makes it easier for attackers to hit more targets with a single attack.

The second project will develop location-based security systems for wireless technology. That means a person would have to be working in a specific place before gaining access to documents over a wireless network. That would be useful for government employees who need to

work with classified documents over wireless connections. Guan's security system would only allow those documents to be viewed in designated secure rooms.

The third project will help secure wired and wireless multicasts over the Internet by protecting and managing lists of Internet accounts. It could, for example, help a software company limit the delivery of security patches to paying customers. It could also help webcasters manage and limit access to their content.

Working with Guan on the wireless security projects are Ahmed Kamal, a professor of electrical and computer engineering; and Sang Kim, an associate professor of electrical and computer engineering.

The work is supported by a \$400,000 early career development grant from the National Science Foundation and another \$350,000 grant from the National Science Foundation.

-- Privacy protection

Guan has been working on a project that will help protect the identity of Internet users. One application could protect the identities – and medical records – of people who use online pharmacies. Another application could preserve the anonymity of people using an online voting system.

And what about all those arrows and formulas covering Guan's office whiteboard?

It turns out they're a key to figuring out the reliability of his technology to detect the criminals and their accomplices who run bogus Internet auctions. Before evidence uncovered by his technology can be used in court, Guan said error rates need to be quantified.

Judging by the ink stains Guan has left on the wall next to the whiteboard, he and his students spend a lot of time making those kinds of analyses and calculations.

And that's some more bad news for cyber criminals.

Source: Iowa State University

Citation: Fraudsters beware: Iowa State engineer is developing cyber technology to find you (2008, January 7) retrieved 2 May 2024 from <https://phys.org/news/2008-01-fraudsters-beware-iowa-state-cyber.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.