The Quaternion

Volume 31: Number 1; Fall, 2016
The Newsletter of the Department of Mathematics and Statistics

Mathematics and Cybersecurity at USF

The Internet may have been a curiosity in the Twentieth century, but now it's a major part of the economy. According to the McKinsey Global Institute, in 2009 the Internet accounted for 3.4 % of the world's economic activity, more than education or agriculture. According to the Boston Consulting Group, in 2010 the Internet accounted for 4.7 % of the US economy, more than the federal government. The Internet is growing about 10 % a year, and that attracts a wide variety of entrepreneurs. That includes criminals.

As the old line goes, Willie Sutton robbed banks because that's where the money was. Now the money's on the net, so that's where robbers go. And spies, saboteurs, and vandals. In 2014, McAffee estimated that "cybercrime" costs the world economy about half a trillion dollars a year. Hence the demand for "cybersecurity."

The Florida state government responded by creating the *Florida Center for Cybersecurity* (fc^2), based at the University of South Florida, with supporting programs throughout the State University System. The USF program is a *National Center for Academic Excellence in Cyber Defense*, with baccalaureate and masters' programs certified by the National Security Agency. It includes a program for preparation for *the Certified Information Systems Security Professional* (CISSP) certificate.

This is an interdisciplinary program, spanning the colleges of Arts & Sciences, Behavioral & Community Sciences, Business, Education, and Engineering. "Demand is so large that there will be two hundred thousand positions that will go unfilled" this year, said fc^2 Managing Director **Sri Sridharan**, who anticipates one to two million new cybersecurity jobs during the next three years. That includes jobs in law enforcement, from local police to the FBI and Secret Service, to IT jobs in corporations and institutions.

Mathematics is a source of much of the cybersecurity toolkit. And USF is developing the next generation of tools.

Kaiqi Xiong works on securing networks - networks of computers that are invisible to the user. This is convenient for users who want to avoid the machine-dependent details. One such convenience is the *Software Defined Network* (SDN), which is a system pretending to be the network that the user desires. The system mimics the desired network, handling the details itself. Possible applications range from airline traffic to currency transactions; the former application shows the stakes in getting the programming right - and the latter shows the opportunities for spies and saboteurs.

For example, machines in the SDN system communicate by sending messages, and the virtual machines that they mimic communicate by sending messages. A hacker might gain access by tricking a participating machine to open and act on a spurious message.

This happens in email all the time: a criminal sends a legitimate-looking email with a "Trojan" - a piece of code that sneaks in with the email. The Trojan might steal secrets, sabotage or take over the computer, or even hold it for ransom. There is no absolute test to check if an email contains a Trojan: in 1989, William Dowling observed that from Rice's Theorem it follows that no such absolute test can exist. We are stuck in a perpetual arms race with the hackers.

Professor Xiong works on the question: upon receipt of a message allegedly sent by

The Quaternion is an annual publication of the USF Department of Mathematics & Statistics, which can be visited on the web at <http://www.math.usf.edu/>. Our our snail-mail address is Department of Mathematics and Statistics, University of South Florida, 4202 E. Fowler Ave., CMC342, Tampa, FL 33620-5700. Our phone number is (813) 974-2643, and our fax number is (813) 974-2700.

goodmachine.org, what does one do with it? Servers handling messages need increasingly sophisticated tests to detect increasingly sophisticated hacks, while not blocking legitimate messages needed to keep the network running. That's why servers encrypt their messages so that legitimate messages are accepted while illegitimate messages are not.

Encryption is part of cryptography, the mathematical foundation for engineering secure computing and communications systems and protecting them from hacks. The underlying model of encryption is to allow two people to communicate over a possibly compromised channel, but so that a third party would not be able to decode an intercepted message (or create a usable spurious message). The Department of Mathematics & Statistics has an active cryptography group.

Jean-François Biasse and **Dima Savchuk** use groups to encode messages. A *group* is a collection of objects, like numbers, matrices or permutations, which can be combined to get other objects of the group. (A group also has an identity and inverses.) The set of all positive fractions using multiplication is a group; the set of all real numbers under addition is a group.

Groups have been used in encryption for some time. For example, the Diffie-Hellman-Merkle "open key" method for two people to openly agree to a code while frustrating spies. Let G be a group, and let $g \in G$. Jack chooses a secret number x and sends the power g^x to Jill; the spy might intercept g^x but would have difficulty computing x. Meanwhile, Jill chooses a secret y and sends g^y to Jill. Jack can compute $(g^y)^x = g^{yx}$ and Jill can compute $(g^x)^y = g^{xy}$ and if $g^{xy} = g^{yx}$, Jack and Jill have a shared key that a spy cannot readily get from the intercepted g^x and g^y.

But many experts, including the U. S. Department of Commerce, anticipate a quantum leap in the arms race with hackers. Quantum computers - computers whose circuits can be in "mixed" states (partially OFF and partially ON) rather than current computers (whose circuits are either in state OFF or state ON) - are moving off the drawing board and into the laboratory. Some experts anticipate commercially viable quantum computers within five to fifteen years. And it looks like quantum computers will be able to readily crack our favorite cryptographic systems.

Professors Biasse and Savchuk are working on cryptographic systems that should be less vulnerable to quantum computing attacks. For example, one kind of commutative group Professor Biasse has worked with is a *geometric lattice*. Suppose you wanted to send a message consisting of the list (4, 11, -3, 9, 0, 2). If you had a *basis* of six-dimensional vectors - say, $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6\}$ - you could transmit the sum $4\mathbf{b}_1 + 11\mathbf{b}_2 - 3\mathbf{b}_3 + 9\mathbf{b}_4 + 0\mathbf{b}_5 + 2\mathbf{b}_6$, and the recipient could readily decode the message if the recipient had that basis. A spy who intercepted the message but did not have the basis would have difficulty decoding the message - even with a quantum computer.

On the other hand, Professor Savchuk has been working with *noncommutative* groups. Addition and multiplication are *commutative* in the sense that $A + B = B + A$ and $A \times B = B \times A$. But the set of all one-to-one and onto functions of the real numbers under composition is a noncommutative group. For example, if $f(x) = x^3$ and $g(x) = x+1$, then $(f \circ g)(x) = f(g(x)) = (x+1)^3 \neq x^3+1 = g(f(x)) = (g \circ f)(x)$. Then using noncommutative groups, Jack and Jill could send (carefully selected) elements $x^{-1}gx$ and $y^{-1}gy$ back and forth, again presenting difficulties for a hacker armed with a quantum computer.

Biasse and Savchuk also teach a course, *Introduction to Cryptography and Coding Theory*, recently launched at USF. Coding theory is different form cryptography: how to handle messages that have been degraded by interference. (Coding theory is of great interest to NASA, which has to communicate with robots billions of miles from Earth.) Meanwhile, they are developing the foundations for securing keys and keeping ahead in the arms race with the hackers.

The demand for cybersecurity is only going to increase, and USF will be at the forefront of meeting this demand.