CYBERCRIME FIGHTERS

The internet is a boon for business, communication and access to information – but also to cyber criminals and hackers. Researchers in the Computer Security Laboratory of the Concordia Institute for Information Systems Engineering are working diligently, and successfully, at beefing up security.

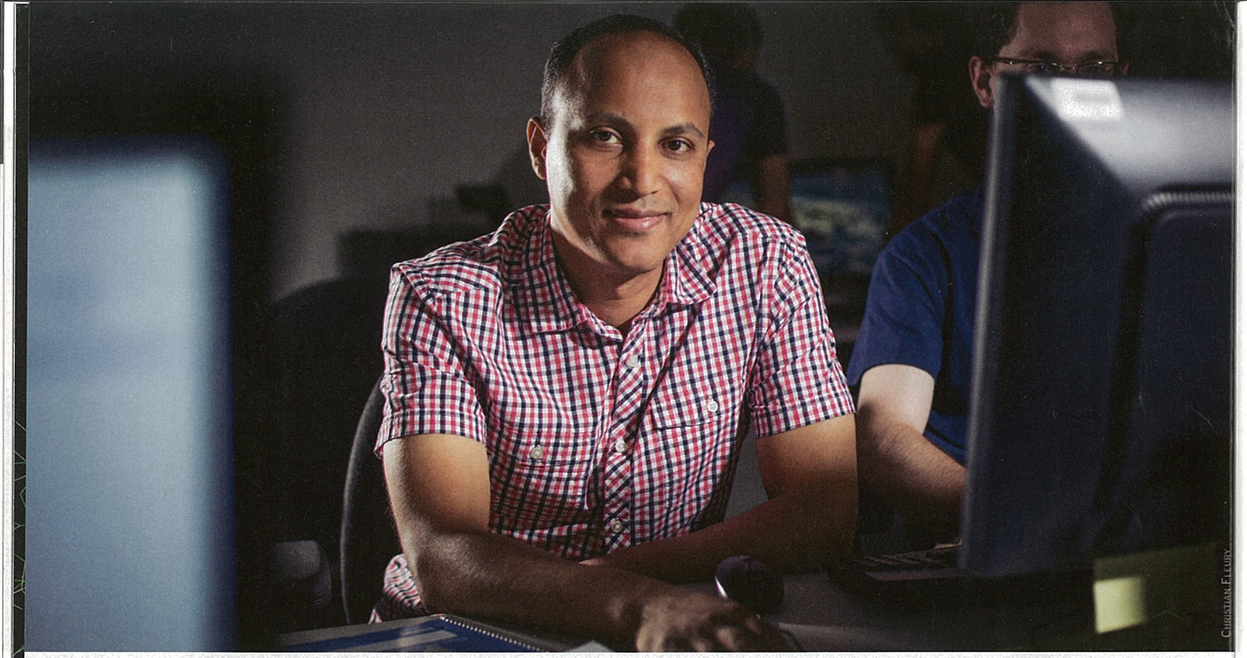
By Jake Brennan

In the late 1960s, a small group of American researchers developed a system to share information remotely via a network of computers. The individuals knew and could trust each other and therefore weren't very concerned with security issues. Twenty-five years later, when the network — now known as the internet — was commercialized, suddenly anyone with a modem could join.

Fast forward to today: the internet now features 340 billion websites and traffic of 300 billion emails daily, allowing users to instantly communicate, access information and do business in ways inconceivable just a few years back. The explosion changed the game — and escalated opportunities for nefarious activity.

Cybercrime, estimated in 2011 at $114 billion globally, now costs most businesses more than conventional, physical crime. The United States Department of Defense regularly wards off cyber-attacks from viruses and other malware being created at nearly one new piece per second. In 2011, former CIA director Leon Panetta warned, "The next Pearl Harbour we confront could very well be a cyber-attack."

Since 2002, faculty and researchers at the Concordia Institute for Information Systems Engineering (CIISE), housed in the Faculty of Engineering and Computer Science, have been on the case to tackle such security and theft issues and threats. These include professional hacking gangs stealing identities, governments attacking their enemies or spying on their own citizens, and friends and ourselves divulging too much on social media.



MOHAMMAD MANNAN IN CONCORDIA'S COMPUTER SECURITY LABORATORY. THE ASSISTANT PROFESSOR CONDUCTS RESEARCH ON AUTHENTICATION AND PASSWORDS.

CONCORDIA'S EXPERTISE

Mourad Debbabi, who became the CIISE's first hired faculty member in 2002 and then its director from 2007 to 2013, recalls receiving a recruitment email while sitting in Panasonic's Atlanta, Ga., research department, where he worked. "It is very rare to have an opportunity to create a department, rather than join one," he explains. "I was also charmed by the fact that it would be research intensive and interdisciplinary around information and systems engineering. I thought, 'This is an opportunity not to be missed.'"

Students agreed. With few other institutions offering graduate programs in information and systems engineering, enrolment in CIISE's PhD, two masters and two graduate-certificate programs was up to full capacity at 100 entrants per year a few cycles after its founding.

Eleven years later, the 19 full-time faculty — computer scientists and electrical and mechanical engineers — work in three primary research areas. One of them, the Computer Security Laboratory (CSL), is home to six professors and more than 60 graduate students. This makes the CSL the country's largest concentration of information systems security researchers. Rachida Dssouli, a professor and CIISE's founding and current director, says it also has "the highest impact in terms of reputation, research grants attracted, industrial collaborations and publications" of any comparable lab in Canada. "It constitutes not only a signature area for the university but helped put Concordia on the world map. The CSL is a brand name now."

> If I send you an email, I think I'm just sending you an email, as if it's a letter. But all these emails are just sitting in a server, so they're absolutely not private.

The CSL's expertise and unique setup have brought in more than $4.2 million in external research funding in the past six years alone. Its researchers include those looking to detect and prevent malfeasance, as well as faculty such as Benjamin C.M. Fung, a former assistant professor who specializes in data mining, hoping to track down bad guys. (See the sidebar on page 40, "Forensics: Tools to bring criminals to justice.")

Part of the magnetic attraction for money and students is the CSL's integral role in the National Cyber-Forensics and Training Alliance Canada (NCFTA). The non-profit organization brings together academic institutions, government and law enforcement, and private companies to share resources, intelligence and expertise to stop emerging cybercrime threats and mitigate existing ones. Since it started in 2008, NCFTA has been headquartered at the CSL, ensuring Concordia scholars work on the latest, most relevant topics — a fast-moving target in the cyber world.

Debbabi's many research interests include network security, cyber-forensics and malicious code detection. "To design less vulnerable systems, you need to detect problems as they occur, prevent them, and also perform more in-depth detection research after the fact — forensics," he explains.

DETECTION: ROOTING OUT ATTACKERS

As president of NCFTA, Debbabi can access information feeds that monitor a wide variety of malfeasance — malicious Internet Protocols (IPs) and domains, reconnaissance and intrusion attempts, and dedicated denial-of-service (DDOS) attacks, a major threat with an interesting local connection.

Back in 2000, a high-school student from Montreal's West Island made history. Like most hackers of the era, Michael Calce — internet alias: Mafiaboy — was a young man who wanted to show off to other hackers. He had figured out how to control computers remotely by installing viruses via the internet, to link these compromised machines together into powerful networks called "botnets," and to instruct the linked computers to send packets of information to a receiving server simultaneously, thereby overloading that server and crashing it. Testing his method in February 2000, in the space of a week he took down the websites of Yahoo, eBay, E*Trade, Amazon and Dell, plus CNN and its 1,200 auxiliary sites. The stunts caused an estimated $1.7 billion in damage and sent the stock market for a ride by demonstrating that in the dot-com boom, the new emperor, online commerce, was not just exposing a little midriff; completely unprotected from unsavoury elements, it was stark naked.

Hacker groups worldwide took note: Calce had perfected the DDOS attack, a powerful cyber weapon that renders one's opponent inoperable. Anything online — military, banks, utilities — could be compromised by hacktivist groups like today's Anonymous or even by governments. It is widely believed that Russian hackers protested Estonia's decision to move a Soviet war memorial by unleashing just such an attack in 2007. The Estonian government, media and financial institutions' sites all went down, virtually incapacitating a country which, like Canada, is one of the planet's most wired.

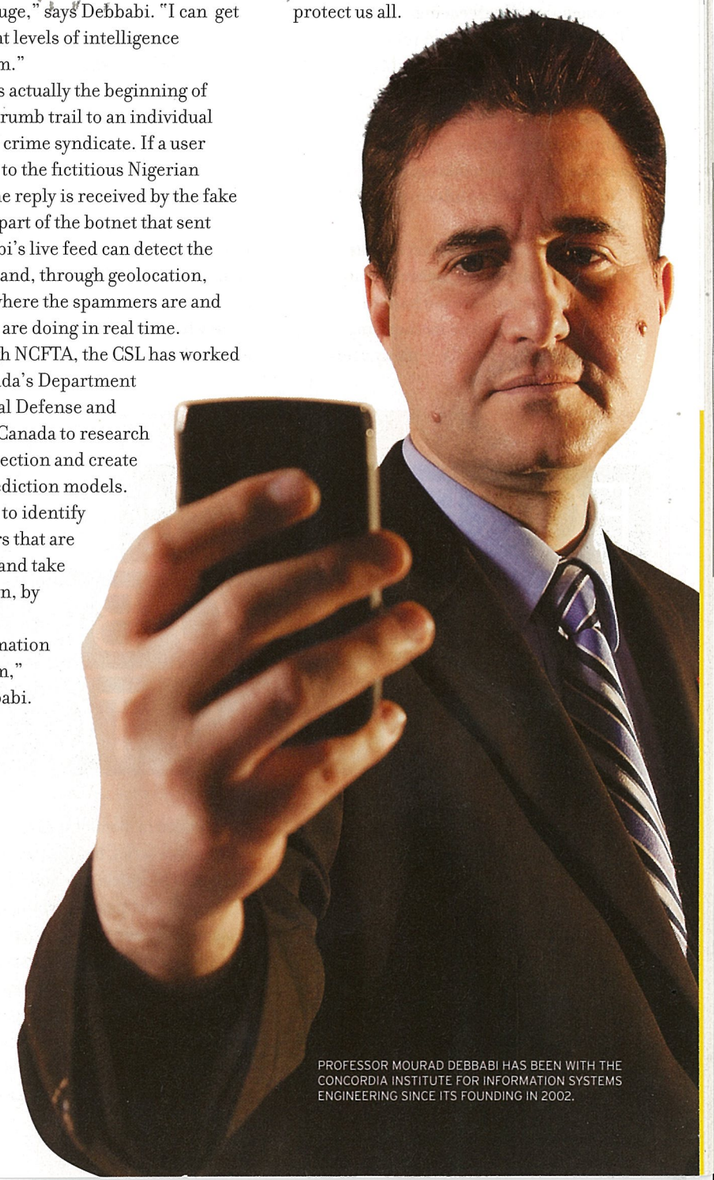
As the CSL's Mohammad Mannan says, early hacker groups running botnets "were flashy and showing off — 'look, I infected millions of machines in 15 minutes!' " Yet as the technology matured, professional gangs monetized it. They shrunk botnets to avoid detection, and now rent them out by the hour to groups attempting DDOS attacks and phishing schemes, who spam to sell real or counterfeit products or spread propaganda, adds Debbabi.

Most users automatically delete any spam that slips through the email service's spam filter — an ad for cheap Viagra, or an ungrammatical help request from a "Nigerian prince" trying to move his money overseas. "But for me, it's huge," says Debbabi. "I can get significant levels of intelligence from spam."

Spam is actually the beginning of a bread-crumb trail to an individual hacker or crime syndicate. If a user responds to the fictitious Nigerian prince, the reply is received by the fake IP that is part of the botnet that sent it. Debbabi's live feed can detect the response and, through geolocation, identify where the spammers are and what they are doing in real time.

Through NCFTA, the CSL has worked with Canada's Department of National Defense and Ericsson Canada to research attack detection and create attack prediction models. "We need to identify the servers that are phishing and take them down, by deriving the information from spam," says Debbabi.

With so many working credit card numbers available that hacker groups sell them to fraudsters for as low as $1 each, and a full ID — date of birth, social insurance number, driver's licence and photo — for only $5, this is a societal problem. Yet Canada lags behind the U.S. in information sharing for cybercrime mitigation purposes, says Debbabi. That's why this summer the CSL increased its capacity to become a U.S.-style data hub for information that carries little privacy value — spam and viruses — but can help protect us all.



PROFESSOR MOURAD DEBBABI HAS BEEN WITH THE CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING SINCE ITS FOUNDING IN 2002.

PREVENTION: PLAYING DEFENSE

It is no surprise the first major cyber war was launched from Russia, home to much cyber criminality. Mannan suggests that, like tax havens, botnet location is merely a case of lowest legal resistance. "The attackers are dynamic. If they have, in the Russian or now the Chinese legal system, better opportunities to hide, they will exploit that system."

With our information under constant threat from hackers, we need armour. The assistant professor holds a Natural Sciences and Engineering Research Council Discovery Grant to improve the security and privacy of high-impact applications, such as email and online banking, "to benefit society and average citizens."

A major means to thwart threats is improved passwords. Because truly secure passwords are too hard to remember — imagine memorizing X@h6y3i89B9*4no3!k — many users employ simpler ones that include real words and reuse them on multiple accounts. "I can't really blame people," says Mannan. "We are pattern-based animals."

Mannan has devised a few password-generation techniques to circumvent these problems. With his master's degree student, Adam Skillen, Mannan recently released Myphrase, software that generates a "passphrase": six words long. To ensure the words themselves are familiar to the user, a 1,024-word dictionary is devised from the user's own writing, such as sent emails. But, as a compromise between security and memorability, "I do not let you choose which words, or their order, because I know what you will do — make a coherent phrase that is more easily hacked," says Mannan. The generated passphrase can be a random sequence of words, like "purple monkey dishwasher move seem wish," or, by using a part-of-speech engine and sentence templates, the connected discourse option gives the passphrase the slightly more memorable ring of semantic sense: "They traced again and loudly radiant."

> I think those who post everything on Facebook now will learn and advise their children differently.

For the less linguistically inclined, Mannan's object-based password (ObPwd) requires a user to select any file from his or her computer or an online location. The software will generate a strong password from the binary code underlying that file. Rather than memorizing a password, all the user has to do is remember where he has stored the file.

Both ObPwd and Myphrase have proven robust to attacks. The greatest risk to the average user, says Mannan, is actually the user her- or himself.

Since companies like Google and Facebook don't want to exclude potential customers, they suggest but don't enforce using strong passwords. Worse, through social media, people unwittingly reveal password and security-question information — your date and place of birth, siblings' names, high school and so on. "If I have access to your Facebook account, I can customize the attack," says Mannan. "You think, 'Who will guess that my password is my wife's name when there are so many possibilities?' " But hackers' powerful computer algorithms render random guessing attacks quickly, and targeted attacks quicker.

"Even by not using Facebook, your privacy may be leaked," says Mannan. Tagging friends in a photo confirms their identity, like a photo ID. We are effectively spying on each other.

Our failure to account for both computers' computational power and the transparency of online communication is what Mannan calls our "mental model problem" with digital technology. "If I send you an email, I think I'm just sending you an email, as if it's a letter. But all these emails are just sitting in a server, so they're absolutely not private."

One possible solution would be to pass more stringent privacy laws. However, Mannan points out, "Government is an interested party. If we disallow Facebook to collect all this information, then the government also has no access to it [through a court order], so there is a conflict."

And the conflict exists at all levels. While President Obama hosted Chinese President Xi Jinping in June for a friendly yet face-saving summit to discuss the problem of Chinese cyber-espionage stealing U.S. state and corporate secrets, Stuxnet, the U.S.-Israeli cyber worm allegedly deployed in 2010 with Obama's blessing to cripple Iran's nuclear centrifuges, was hailed as a low-cost, 21st-century warfare solution. At all levels, "Everyone is targeting and exploiting everyone else," says Mannan.

The combination of its traceless transparency and the government's interest make surveillance a given, with most people believing that they're law-abiding citizens and have nothing to hide. Yet Mannan asks, "Why do you lock your door when you're home? Would you accept a web cam in your home so that the whole world can see?" He believes attitudes towards discretion will eventually change. "Most people just don't understand the privacy implications of online services. I think those who post everything on Facebook now will learn and advise their children differently."

THE STRUGGLE CONTINUES

Gangs and governments will always do battle, in the virtual world as in the physical. While great progress has been made on virus and Wi-Fi security, email, a longstanding communications medium and the basis for business today, is still not secure, Mannan warns. "I am a very optimistic person — I believe there must be usable solutions out there. As academics, we have to do what is best for citizens. These are difficult problems, but they're not insoluble." ■

— Jake Brennan is a Montreal writer.

FORENSICS: _TOOLS TO BRING CRIMINALS TO JUSTICE_

While citizens may be wary of their government snooping online into their affairs, there are many cases where governments, or at least law enforcement, should and must intervene.

For example, forensic detectives used to need to spend months poring over emails, chat logs and text messages to amass evidence against child pornographers. In an age when keyboards have replaced pens, police hoped to identify suspects not by their written script, but their writing style. That's why Benjamin C.M. Fung, formerly a Concordia Institute for Information Systems Engineering assistant professor who specialized in data mining, and his former PhD student, Farkhund Iqbal, MCSc 06, PhD 11, partnered with Mourad Debbabi and the National Cyber-Forensics and Training Alliance Canada to develop digital authorship identification software.

Police can use an IP address to determine the physical address from which electronic communications were sent. But what if several people live there? To determine who has authored a particular, felonious message from a pool of known authors, Fung and Iqbal's software first identifies the features and patterns found in other messages known to be written by the suspect. Repeated grammatical mistakes, punctuation patterns, commonly used words, and spacing between paragraphs are all examples — thousands of unconscious writing habits. Then, they filter out any of these features also found in the emails of other suspects. The combination of remaining features is unique to the author of the messages being analyzed. For example, while all suspects may always type "%" instead of "per cent," only one will type "%," habitually use commas instead of periods and think "none" takes a plural verb. Fung calls this combination the suspect's Writeprint.

They tested their software on Enron's real email data set — 200,000 emails from 158 users — that was made public when the American company went bankrupt in 2001 after its corporate fraud scandal. Fung and Iqbal achieved an authorship accuracy of 80 to 90 per cent, a rate highly valuable to law enforcement, which is already using the tool. And analysis that used to take months now takes mere hours. The next stage of research will be to apply the data-mining method to the even shorter texts of instant messaging, chat rooms and social media.

This summer, Fung co-published with his PhD student, Gaby Dagher, a time-saving variant. "Out of all the types of available data in cybercrime investigation, text data is the most common medium used by scammers, identity thieves and child exploitation criminals," says Fung. "But this type of data is also the most challenging to analyze." So, when a suspect's computer is seized, months may pass before sufficient information to press charges can be extracted from documents and messages in the hard drive.

As Dagher explains, "In a normal search engine, a user enters some keywords and results can vary — widely." Fung and Dagher's search engine, in contrast, captures the suspects' vocabulary — learns their slang — and then uses it to improve the speed and accuracy of the search results. The researchers' new methods automatically identify the criminal topics discussed in the textual conversation, show which participants are most active with respect to the identified criminal topics, and then provide a visualization of the social networks among the participants. What took months now takes mere hours.

The search engine can even help uncover hidden topics. Dagher recalls a recent case where the hard drive of a suspect arrested for sexual harassment was found also to contain thousands of stolen credit card numbers.

Dagher, a self-described "theoretical guy" who normally works on data mining, encryption and the security of storing information through cloud computing, admits, "Getting real data from real cases from the law enforcement agencies and helping them catch these people is very satisfying."