BRAD KING BUSINESS SEP 14, 2001 2:00 AM

Hiding Like Snakes in the E-Grass

Information overload -- including billions of e-mails, instant messages and cell phone minutes -- poses a challenge for law enforcement agencies that monitor communications. By Brad King.

SAVE

THE PROLIFERATION OF cell phones, e-mail and faxes is making the hunt for terrorists increasingly more difficult.

Security agencies have literally billions of messages to sift through every day -- many with encryptions that make it impossible for anyone other than the intended recipient to read.

"If I dump a stack of hundreds of thousands of pages on your desk and tell you one page is a terrorist threat, it would take forever to get through," said Sayan Chakraborty, vice president of engineering at Sigaba, an e-mail encryption company. "Because one person can't read every message, you have to rely on computers to read messages and computers only do what we tell it to do."

So while high-speed computing has made search capability quicker, it hasn't necessarily made it more accurate.

"If you have a computer looking for 'bomb,' you'll get a lot of messages that have nothing to do with terrorist threats, while the terrorists will be using code words."

Americans spent 2.58 billion minutes on their cell phones in 2000, up a remarkable 75 percent from the previous year according to the Cellular Telephone & Internet

Association. That number is expected to continue to grow as high-speed networks become available, making digital communication more effective and efficient.

E-mail and instant messages pose an even larger problem than cell phone use. America Online -- the largest ISP in the country -- handles 225 million e-mails every day and 1.1 billion instant messages.

However, new, smart "data mining" technologies offer listening stations new weapons in the war on terrorism.

With all of that information flowing through the airwaves and phone lines, government agencies have started to build up an infrastructure to handle the crushing weight of the modern communications networks.

At the Echelon listening post in North Yorkshire, England -- an operation the National Security Agency has declined to discuss -- computer experts sift through faxes and phone calls looking for hints about the next possible terrorist attacks.

At the NSA's Fort Meade headquarters in Maryland, teams of experts pore through millions of communications from around the world.

The FBI has deployed teams of agents to ISPs, asking the technology companies to install the e-mail monitoring system Carnivore on the servers.
Congressmen are calling for technology companies to include "back-door" access for government agencies that monitor communications.

Much of the new technology being deployed in the listening posts remains under wraps, leaving industry experts to speculate on what kind of technology could be used.

There are new technologies emerging in the commercial marketplace that some experts believe are being used by the government. Fuzzy computing is high on that list.

Fuzzy computing refers to a computer's ability to interpret data by looking for patterns in problems and using "intuition" while completing its tasks. The technology

is already in use in its simplest form in automobile anti-lock brake systems, which keeps people from swerving out of control when they jam on the brake pedal.

Of course, anti-lock brakes are a long way from breaking complex encryption and intuiting the meaning of secret codes.

"To teach a computer what goes together and what doesn't so it can do a job processing is something that takes a very long time," Chakraborty said. "But these engineers have taken the skill of a high-end race car driver and made it into a computer system, and that's not something to look down upon."

Microsoft Chairman Bill Gates announced his company has been focusing its research on computer software that has problem-solving abilities, to allow the PC to understand what its user wants.

Another aid in breaking encryption technology, which has all but locked down e-mail messages, is parallel computing.

A normal PC comes with one processing chip, such as the Pentium, which handles all of the functions of the computer like a juggling act. Users can open a Word document and Excel document at the same time, giving the illusion that the computer is multi-tasking. However, processors only handle one function at a time. The chips just work at such high speeds it appears as though the computer is completing multiple tasks.

With parallel computing, multiple processors in the computer radically improve the speed at which the equipment works. For security systems attempting to break encryptions with 256 locks, this type of speed and power might be the only way to break the codes, Chakraborty said.

While new technology is being developed for commercial use, a recent government report on terrorism found that most government agencies continue to operate using aging technology.

A report delivered to Congress last year by the National Commission on Terrorism detailed the potential problems government agencies would have in dealing with

modern communication networks that would allow individual cells of terrorist organizations to operate anywhere in the world.

While the Commission recommended traditional sources of gathering information, such as recruiting individuals to infiltrate the inner-circle of terrorist organizations, it also recommended that surveillance technology be made easier for federal agencies.

Even when communications are identified -- either through listening stations or raids -- the information is often encrypted and difficult to break.

"The National Security Agency (NSA) is America's most important asset for technical collection of terrorism information, yet it is losing its capability to target and exploit the modern communications systems used by terrorists, seriously weakening the NSA's ability to warn of possible attacks," the Commission reported to Congress.

The group also detailed the Federal Bureau of Investigation and the Central Intelligence Agency's aging technology as potential problems.

Why It Took Meta 7 Years to Turn on End-to-End Encryption for All Chats

Mark Zuckerberg personally promised that the privacy feature would launch by default on Messenger and Instagram chat. WIRED goes behind the scenes of the company's colossal effort to get it right.

LILY HAY NEWMAN

A New Trick Uses AI to Jailbreak AI Models—Including GPT-4

Adversarial algorithms can systematically probe large language models like OpenAI's GPT-4 for weaknesses that can make them misbehave.

WILL KNIGHT

Anduril's New Drone Killer Is Locked on to AI-Powered Warfare

Autonomous drones are rapidly changing combat. Anduril's new one aims to gain an edge with jet power and AI.

WILL KNIGHT

The EU Just Passed Sweeping New Rules to Regulate AI

The European Union agreed on terms of the AI Act, a major new set of rules that will govern the building and use of AI and have major implications for Google, OpenAI, and others racing to develop AI systems.

MORGAN MEAKER

OpenAI’s Custom Chatbots Are Leaking Their Secrets

Released earlier this month, OpenAI's GPTs let anyone create custom chatbots. But some of the data they're built on is easily exposed.

MATT BURGESS

The Binance Crackdown Will Be an 'Unprecedented' Bonanza for Crypto Surveillance

Binance's settlement requires it to offer years of transaction data to US regulators and cops, exposing the company—and its customers—to a "24/7, 365-days-a-year financial colonoscopy."

ANDY GREENBERG

The Case for Using AI to Log Your Every Living Moment

Sam Liang, CEO of Otter, argues that life would be better if algorithms logged every spoken word so life events past can be lived and explored again.

STEVEN LEVY

Tesla Is Recalling Nearly All Vehicles Sold in US to Fix an Autopilot Fault

The Tesla recall, which affects more than 2 million vehicles, follows a two-year investigation by the US government into a series of crashes linked to the Autopilot system.

JEREMY WHITE