

Quantum attacks worry computer scientists

Robert Lemos, SecurityFocus 2006-10-31

Today's network administrators have it easy.

In the weird world of quantum computing, the state of computer systems networked together is so fragile that a read access to a single quantum bit, or qubit, on one machine would require a network-wide reset. It's no wonder, then, that two researchers who are working on ways of defending against the future possibility of malicious attack assume that any unauthorized access to a quantum computer constitutes a catastrophic failure.

For that reason, their defense resembles the communications protocol for a paranoid spy: Only send out messages at prearranged and seemingly random intervals, have long average wait times between legitimate network connections, and fill all the unused network time with decoy transmissions. By spreading out network connections over random intervals in time, the researchers--Daniel Lidar, an associate professor in electrical engineering, chemistry and physics at the University of Southern California and Lian-Ao Wu, a research associate in the Chemical Physics Theory Group at the University of Toronto--have shown quantum computer scientists can reduce the chance of a successful attack but still keep the performance advantages promised by quantum computing.

"We would not want to use this method against any threat beside malware, because it is inefficient," Lidar said in an interview with SecurityFocus. "We are taking the network down for a long period of time."

Quantum computers are only taking their first toddler steps in the world of computer science. While a research topic in physics for more than 20 years, quantum computing has only recently moved from its theoretical underpinnings to actually being demonstrated in the lab.

The promise of such computers, however, is nothing short of astonishing. Many problems that "blow up" on a classical computer system, such as finding the prime factors of a large number, can theoretically be easily solved on a quantum computer. Other aspects of a quantum information system allow for more interesting possibilities, such as the [secure transmission of encryption keys](#) over quantum networks.

For example, in conjunction with Harvard University and Boston University, Internet service provider BBN Technologies built the [DARPA Quantum Network](#), billed as the world's first quantum key distribution (QKD) network. The project, funded by the Defense Advanced Research Projects Agency (DARPA), uses light particles, or photons, that are linked over a distance through the quantum mechanical property of entanglement to transmit key information in a way that any eavesdropping can be detected.

Yet, as such technologies mature and greater access is granted to researchers outside the core group of quantum computer scientists, the probability that such computers and systems will be attacked increases. The computers already have to be hardened against any interaction with the environment, to ward off the impact of even a single cosmic ray, which could pollute an ongoing quantum process and affect the outcome of an operation. The impact of an intelligent attacker is a more difficult problem.

"I want to maintain the quantum computer in a good state until, magically, the answers appear," said John Lowry, a principal scientist at Internet service provider BBN Technologies and a member of that company's research team working on the DARPA Quantum Network. "Stray cosmic rays and things like that--if they interact with this stuff, then something changes and the computer crashes. The thought is that people

could do that on purpose."

Classical computers as formalized by the early giants of computer science consist, at the most basic level, of a processor, memory and a program. The processor acts on data in a predictable way and the state of the system is easily determined. (This is a simplification from the original five elements--a controller, an mathematical unit, memory, and input and output units--proposed by John von Neumann in the early 1940s, while Alan Turing used four--a tape, a head to read or write to the tape, a table of inputs and outputs, and a state register--in his work during the 1930s.)

Quantum computers make use of quantum physics, the rules of subatomic particles and light, to create a computing system. Where a classical computers uses binary values of 0 and 1, a quantum system can be in a state that represents either 0 or 1, or a probabilistic blend of both states, known as a "superposition," so that it has the potential to be either 0 or 1 with its value only be determined at time of measurement. These quantum bits of information, or qubits, essentially take on all possibilities until measured, when the state of the qubits collapse to an actual value.

The science behind quantum computing gets even weirder. Two particles that represents qubits in a quantum computer system--say two electrons with their up and down spin representing 0 and 1, respectively--can be entangled. That is, the states of the two particles rely on each other irrespective of the distance between them. When one electron is measured and collapses to a value, its entangled partner--whether a meter away or a light year--reacts as well. Such entanglement is a key factor in the computations that can be achieved with a quantum system.

Finally, a quantum calculation done with a certain number of qubits in essence performs the calculation on all combinations of those bits, a property that, some physicists have theorized, can only happen because the subatomic particles exist in multiple dimensions. The ability of quantum computing to attempt every possibility to a solution at the same time makes classically difficult problems, such as factoring, a snap.

However, the other side of quantum computing is that the physics makes reliable computation technically difficult. The quantum state of a particle can not be copied, a property formalized as the No-Cloning Theorem, which means that two registers in a quantum computer cannot hold copies of the same values. Measuring the state of a register also causes the value to collapse to 0 or 1, and if the qubit is entangled, means the value of the qubit's partner also becomes determined.

Such fragility makes a quantum computer a hard system in which to guarantee integrity and an easy system to corrupt through malicious attack.

Today, quantum computers are essentially at the same stage as conventional computers were at during the first half of the 20th century, with some theoretical foundations and rudimentary working hardware. Current experiments involved manipulating anywhere from 2 qubits to 13 qubits of information and working systems mainly focus on quantum key distribution for otherwise classically implemented encryption systems.

Worrying about malicious software may be premature for a technology so young. The first digital electronic computer, ENIAC, went online in 1946 and the first known attacks against computer systems occurred about two decades later. Yet, in all likelihood, such attacks will become a reality, and that's reason enough to worry now, said USC's Lidar.

There is no telling what such an attack might look like. Destroying data or circumventing a calculation on a quantum computer is the easiest course. Attackers could operate a rogue computer on the quantum network or coopt the communications

line, he said.

"We deliberately stay away from specifics of malware, such as Trojan horses, et cetera," Lidar said. "So, quantum malware to us just looks like any malicious instruction set sent to an attacker."

The defense proposed by Lidar and Wu is to give each legitimate node on the network a list of times distributed over a long period, during which the quantum computers can exchange information and possibly entangle qubits across the network. All other times, a set of decoy qubits are sending data on the network to mimic legitimate traffic flow. When not connected, the networked qubits transfer data back to a third set of qubits, known as the ancillary, or ancilla, qubits. Those registers are never connected to the network, so quantum computations can be carried out without worry of attack.

"As long as we can keep the local nodes free from malicious intruders and build a heavily fortified castle around them, we can assume the ancilla qubits are malware free," Lidar said.

Lidar and Wu found in a paper published earlier this year ([PDF](#)) that the number of network connections can never exceed the ratio of the average time between attacks over the length of time it takes to complete an attack.

In classical computing the result would be a poor tradeoff. Only connecting for one second out of every hundred or thousand would unacceptably slow down the calculation speed of, say, a grid computing system. However, in a quantum computing system, such a slowdown does not appreciably affect the speed gains of the system.

"The protocol shuts down the network for a certain period of time, say 99 percent," Lidar said. "While that's a factor of 100, it doesn't matter, because it doesn't change the complexity of the problem."

In other words, for a computer that exists in multiple dimensions and uses a form of teleportation in its calculations, taking a hundred, or even a thousand, times longer means little.

[Privacy Statement](#)

Copyright 2006, SecurityFocus