For honest voting, write a message the 'man in the middle' can't intercept

11 December 2012, by Bill Steele

(Phys.org)—In the run-up to the last election warnings about computer hacking were rampant. Experts demonstrated how the hardware in voting machines could be modified. Touch-screen machines visibly changed votes. One possibility that wasn't mentioned was the "man in the middle" who might change totals as they are sent in.

Cornell computer scientists have developed a new way to send a "non-malleable" message—one that cannot be altered by a third party—over a computer network. It's as if the message were engraved on a stone tablet, and any further chiseling would cause the tablet to crumble.

Rafael Pass, associate professor of computer science, and Ph.D. student Huijia Lin reported their work at the 43rd Association for Computing Machinery Symposium on the Theory of Computing last summer in San Jose, Calif. They worked in the context of what computer scientists call "commitment schemes," such as might be used in online bidding for a contract, but their methods could be applied to other computer communications, including stock trading and online voting, Pass said.

Pass and Lin supply a mathematical proof that their protocol is secure. The man in the middle must pass the message unchanged or the system will fail. That proof is the most important step, Pass said. "Everything I do I prove secure," he said.

Most computer security is reactive, he explained. We trust a system until someone breaks it, then patch the vulnerability and wait. "For the last 2,000 years cryptography has been a game between artist and attacker," Pass said. "We've used it in critical situations like war, and now the Internet relies on it. It should have a scientific basis. We must rigorously model what we want to do and specify our assumptions, and if it breaks, the assumptions are broken."

The man-in-the-middle attack is a classic problem in computer security. The attacker slips into the communications channel between two parties and relays their messages back and forth, letting them think they are talking directly to one another. By monitoring many repetitions, the interloper might pick up enough clues to break whatever encryption the parties are using. It's not even necessary to read the messages. A hacker might be able to change the value of a vote or a competitive bid, even without knowing what the actual value was.

In the system proposed by the Cornell researchers, the content of the message is intimately intertwined with digital signatures of each party, encoded by a system such as public-key cryptography, where the message is enciphered using a key that is the product of two large prime numbers. The sender and receiver exchange several messages to create a "chain of signatures" that depends on the identities of the senders. To disentangle the signature chain from the message an attacker would have to break the keys back into their two primes, which might require a computer the size of the universe. If any of this content is altered by the man in the middle, the system will detect it.

Other methods of creating non-malleable messages have been put forth, the researchers noted, but they require either thousands of rounds back and forth or that the sender and receiver agree to send messages at prearranged times. The new protocol works with perhaps 15 rounds or less and requires no "trusted infrastructure" set up in advance.

"I wouldn't say the problem of man-in-the-middle attacks is solved," Pass noted, "but a minimal number of communications rounds is now possible. And it doesn't mean we have practical solutions yet." The present work is theoretical, he pointed out, and someone has yet to write applications to put it into practice.

Provided by Cornell University