Encryption made easier: Just talk like a parent

July 3 2015

Eric Gilbert, Assistant Professor of Interactive Computing

Encrypting emails can be tedious, difficult and very confusing. And even

for those who have mastered the process, it's useless unless the intended recipient has the correct software to decode the message. A Georgia Institute of Technology researcher has created an easier method – one that sounds familiar to parents who try to outsmart their 8-year-old child. The new technique gets rid of the complicated, mathematically generated messages that are typical of encryption software. Instead, the method transforms specific emails into ones that are vague by leaving out key words.

"It's kind of like when mom and dad are talking about potential vacation spots while the kids are nearby," said Eric Gilbert, the Georgia Tech assistant professor who developed the software. "They can't say or spell 'Disney,' or the children will get too excited. So they use other words and the meaning is implied. Instead of 'Disney,' they could say 'have you bought tickets to the place yet.'"

Gilbert's Open Book system, a prototype that uses a Google Mail plug-in called Read Me, works the same way by substituting specific words with ambiguous ones. If the above example was an email conversation, the sender would write, "Have you bought tickets to Disney yet?" Open Book would change the message when it was sent. The other person would see, "Have you bought tickets to (place) yet?"

The process reduces the information disclosed to eavesdroppers or computer systems that monitor online communications, while taking advantage of common ground between the participants.

"As people react more with each other, they don't have to say as much to understand what is being said," said Gilbert. "Open Book uses the same technique. Even though the messages resemble typical email conversations, they're lost in the background noise of the Internet."

To test the reliability, Gilbert put together a small study of 10 people

who each wrote emails to five friends, which were then transformed by Open Book. The recipients correctly deciphered the missing words or phrases 95 percent of the time. When the same vague emails were shown to strangers, only 2 percent were interpreted correctly.

The system, which isn't commercially available yet, is tailored for people who know each other. Readers cannot transform the vague email back into specific terms if they're confused and unsure of its meaning.

Gilbert says he's noticed more interest in encryption since Edward Snowden leaked documents about government surveillance. He thinks Open Book could be beneficial for anyone who cares to hide information online, whether it's from the government, a nosy employer or from search engines that use communications for marketing purposes.

The system was presented at the ACM Conference on Human Factors in Computing Systems (CHI 2015) in Seoul, South Korea, April 18-23 (Open Book: A Socially Inspired Cloaking Technique that Uses Lexical Abstraction to Transform Messages).

Provided by Georgia Institute of Technology