Match me if you can: Cryptographic breakthrough helps spies to shake hands

April 30 2019

Credit: Stevens Institute of Technology

When spies meet, they use secret handshakes to confirm their identities, ensuring they are who they say they are. Now, researchers at Stevens Institute of Technology, and colleagues, have solved a 15-year-old problem that allows handshake-style encryption to be used for time-delayed digital communications such as email—a challenge once thought to be impossible.

The work, led by Giuseppe Ateniese, David and GG Farber Endowed Chair in Computer Science, dramatically expands the technology's utility not just for intelligence agencies and Web-savvy spies, but for anyone with an interest in secure online communication, including journalists, financial workers, lawyers, medical professionals, and others for whom security and privacy are key priorities.

"The demand for tools like this is incredible," said Ateniese, whose work will be presented at Crypto 2019, one of the most competitive conferences in this research area. "Privacy is growing more and more important, and encryption is essential for almost everyone."

Digital handshakes, like in-person handshakes, use real-time interactions to verify participants' identities. That's fine for live communication like online chats, explained Ateniese. But it's a deal breaker for email-style communications, in which messages may need to be decoded long after they were originally sent.

Ateniese and his team, including Danilo Francati, a doctoral student at Stevens, as well as Daniele Venturi from Sapienza University of Rome and David Nuñez from Nucypher, a cryptography company, combined existing key-based cryptographic algorithms in a novel arrangement to create a system called matchmaking encryption, which simultaneously checks the identities of both sender and receiver before decrypting a message. Crucially, matchmaking encryption does away with the need for real-time interactions, allowing messages to be sent on a "dead drop" basis and read at a later date.

"A dead drop is like when a spy leaves a message behind a rock," said Ateniese. "It can be used when you need to send a message to someone who's not there at the moment, but will find it if he or she is the intended recipient.

To use matchmaking encryption, both sender and receiver create policies, or lists of traits, that describe the people with whom they are willing to communicate. Only when both policies are satisfied will a message actually be delivered and decrypted, ensuring that only the intended recipients can read the message without anyone else knowing they are communicating.

Matchmaking encryption can be used for individual-to-individual communication, but also allows users to designate classes of people with whom they are willing to communicate. An FBI agent in Philadelphia could make their messages accessible only to CIA agents in New York, for example; while CIA agents in New York could refuse to accept messages from anyone other than Philadelphia-based FBI agents. "It's a way to combine these two requests, from sender and receiver, into a single system," said Ateniese.

Messages that don't satisfy both users' policies aren't decrypted, with neither sender nor receiver receiving information about the other party. "This is important for intelligence—I don't want to reveal to you that I'm an FBI agent, so I want assurances that you are who you say you are," said Francati. "Matchmaking encryption provides that assurance as well as a level of privacy that's stronger than anything else that's available."

As a proof of concept, Ateniese and his team created a matchmaking encryption bulletin board accessible via the Tor Browser, a web browser that anonymizes one's web traffic, making it easy to protect one's identity online. Users can scan the bulletin board for messages that match their policies and for which they match the sender's policy, and decrypt them in just a few milliseconds—a sign that the matchmaking encryption system doesn't unduly strain computing resources, suggesting it is both effective and efficient.

Ateniese predicts that additional applications will quickly emerge as

researchers explore the new technology, and find ways to make matchmaking encryption even more powerful for professions where security and privacy are key priorities.

"The work opens up new frontiers in secure communication, said Ateniese. "A very important result—a real and long-awaited breakthrough."

More information: Match Me if You Can: Matchmaking Encryption and its Applications , www.semanticscholar.org/paper/Match-Me-if-You-Can%3A-Matchmaking-Encryption-and-its-Ateniese-Francati/14d3f74b8b9baa8a586f7477da19b9c621e90fb3

Provided by Stevens Institute of Technology