Creating accountable anonymity online

November 12 2013, by Brock Ascher

The World Wide Web is, in many ways, still the Wild West. Though a large portion of internet traffic is monitored and traceable, systems like the Tor Project allow users to post and share anything anonymously. Anonymous systems provide enormous public benefits by helping journalists, activists, and others communicate in private, away from the prying eyes of the Internet at-large.

These systems, however, have been degraded by criminals who use them to support unlawful activities. Tor reportedly has been used to aid in the selling of illegal drugs and in the proliferation of child pornography, among other crimes. With complete anonymity, criminals are often free to do whatever they like with little or no repercussions.

Researchers at Iowa State are working to solve this problem with an approach they call Accountable Anonymity. Yong Guan, associate professor, and his students, have devised a system that offers anonymity for honest users, and accountability for dishonest users.

"The lack of accountability on these anonymous services is easy to exploit," Guan says. "Criminals use anonymous systems to commit crimes against innocent people online and in the real world. I thought there was a real need for accountability within these systems to protect honest users that just wish to exchange lawful information anonymously."

Tor works by sending information through a series of nodes and using layers of encryption at each stop. When the information arrives at its

destination, the encrypted messages are unlocked with a key and the original message becomes readable. The layers of encryption disguise the origin of the message, thus providing anonymity, but at a high computing cost. Bouncing messages around a network, and adding a layer of encryption with each bounce, takes time and computing power. If a criminal uses the service to send a malicious message, the network expends the same computing power to send that message, and the victim has limited ways in which to trace it.

Guan's Accountable Anonymity system, named THEMIS, is designed to minimize the computing power used to send messages and provide a way to track the source of the message, should it be thought of as malicious. By its very design, the system, as a measure for both deterrence and retributivism, avoids expending computing power to send illegal and harmful messages.

"With a level of accountability, criminal activity online will decrease," Guan says. "By that measurement, computing power expended to support criminal activity will also decrease. That's a good thing."

The Accountable Anonymity system aims to offer four features. First and foremost, the system must provide anonymity under normal circumstances. Users looking to exchange information in a lawful manner without being tracked will be able to do so without problems.

"Providing reliable anonymity is the first step," Guan says. "Without it, users won't use the system."

Second, the system must, under certain circumstances, allow for the identification of sources without impairing other users' anonymity. This involves a number of steps, including notifying law enforcement. This feature would be used to find senders of malicious messages, and requires the cooperation of the system's key generator and internet

service provider's registration database.

"Our system provides law enforcement with the means to catch criminals who wish to distribute illegal or harmful messages," Guan says. "Without some kind of accountability, users tend to show an absence of restraint."

Third, the system must be incentive-compatible. This means users must have an incentive to use the system as it is intended to be used. Without incentive-compatibility, users can simply bypass attributes of the system they don't wish to comply with.

Fourth, the system must make framing or impersonating an honest user impossible. THEMIS achieves this by using digital signatures that are computationally infeasible to generate without source keys.

"Forging keys is computationally difficult," Guan says. "If a node wishes to obtain a signing key, or sign a message without the source's signing key, it would have to solve a problem that is incredibly difficult, even for the fastest computers."

THEMIS is comprised of two separate proxy re-encryption based schemes. Scheme one, a multi-hop proxy re-encryption-based scheme, provides an anonymous communication channel between the source of a message and its destination. Much like with Tor, messages in THEMIS are bounced through several proxies. However, instead of adding layers of encryption, THEMIS converts the original message at each stop using XAG encryption. Each proxy along the path knows only its predecessor and successor, and proxy re-encryption keys to corresponding channels are hidden in the message in an onion header. The layers of the onion header contain the information for the corresponding node.

Scheme two provides for accountability when malicious messages are present. As with any encryption system, public keys and private keys are

utilized to ensure that messages arrive where they should and are readable to the intended recipient. However, an AFGH re-encryption key is included with each message and serves as the accountability information which links the destination of the message to its source. Without this AFGH re-encryption key, messages are unreadable.

At the request of the message recipient, law enforcement officials can use the AFGH re-encryption key to track the source of the message. Law enforcement can subpoena data from the key generator and the internet service provider's registration database (both nodes along the path the message follows) and use this data with the message's AFGH re-encryption key to determine the source of the message.

"If no one reports the message as malicious," Guan says, "law enforcement cannot get involved. There would be no way for them to know about it."

Guan envisions his system as a way for law enforcement to track down senders of threatening emails and those who leak important documents. THEMIS represents the first system to provide both anonymity and accountability in an incentive-compatible fashion and the first anonymous network to use multi-hop proxy re-encryption.

"The next step," Guan says, "is to test it on a large scale over the internet. This way, we can really see how well it performs."

Provided by Iowa State University