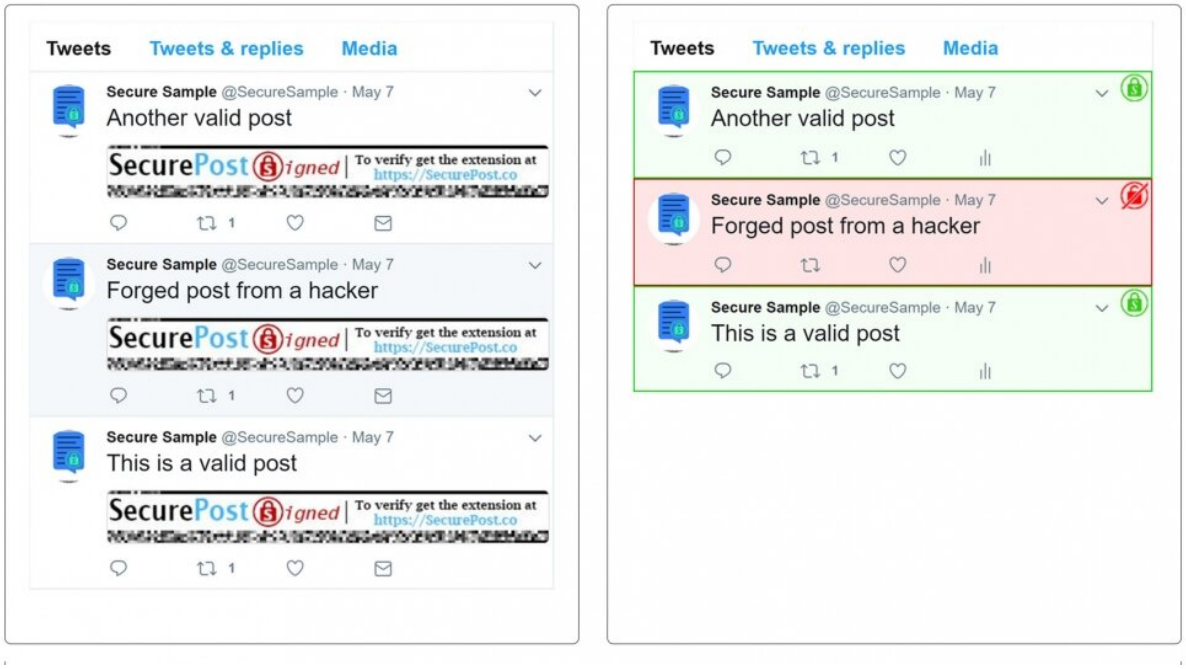
Researchers create an application that ensures anonymity and trustworthiness

January 15 2019, by Harrison Tasoff



The researchers created an internet browser extension that automatically verifies posts' authenticity. The cryptographic signature, visible under each post on the left, is hidden when running the extension on the right. Credit: Michael Nekrasov

Minority and dissident communities face a perplexing challenge in countries with authoritarian governments. They need to remain anonymous to avoid persecution, but also must establish a trustworthy identity in their communications. An interdisciplinary group of

researchers at UC Santa Barbara has designed an application to meet both of these requirements.

Computer science and communication researchers affiliated with the university's Center for Information Technology & Society traveled to three countries to assess the challenges minority groups face in maintaining a secure, trustworthy social media presence. Based on the communities' feedback, the team designed an app for the Android operating system that would safeguard group members' anonymity as well as verify the reliability of posts coming from the group. A paper detailing the technology appeared in the *Journal of Internet Services and Applications*.

The team, led by computer science professor Elizabeth Belding, traveled to Mongolia, Zambia and Turkey, where colleagues at local institutions connected them with members of marginalized communities. At the time, these countries offered a relatively safe alternative to other nations with restricted speech, like Russia, China and Egypt. About two weeks after the group visited Turkey, however, an attempted coup d'état prompted the government to clamp down on political dissidence.

Interviews and surveys with the general public and with members of marginalized groups in these countries confirmed that maintaining anonymity is crucial for protection. But it comes with drawbacks, as the team soon learned. "The problem with anonymous communication is you don't know if it's credible," said Miriam Metzger, a professor in the department of communication, and one of the paper's coauthors. "If you're just getting a message and you don't know who it's coming from, you're probably not going to do what that message tells you to do. Especially if it's risky."

This is where SecurePost comes in. The app allows communities to create secure groups on Twitter and Facebook that let them maintain a

consistent, visible presence on social media. This enables them to build up trust with their readership over time, explained Michael Nekrasov, a computer science doctoral student and lead author of the paper.

What's revolutionary is that SecurePost allows a group to operate without any roster of its individual members. Additionally, the app checks the group's posts, flagging any content that lacks the proper credentials. In this way, each member is protected by their anonymity even if the group is infiltrated or hacked, all while communications from the group itself are verified as trustworthy.

Naturally, these communities want a convenient, yet secure way to extend membership invitations. The research team learned that many groups used passwords for this, however sharing a password always puts the account at risk. "What we found was, people wouldn't just tell someone the password," said Nekrasov. "What they'd do is write it down or send it in a message, and that's incredibly unsafe."

Instead the team developed a much more secure method for inviting a new member to the group. The process involves exchanging secure QR codes visually or over a trusted connection, a technique that uses a pair of visible, public keys and a second pair of hidden, private keys to send and receive encrypted information. This ensures the security of the invite even if a third party was witnessing the exchange, said Nekrasov, because the private key is hidden on the device of the person joining the group.

Once the new member joins the group, they receive a new key pair. The private key enables them to sign posts on behalf of the group. The public key, which anyone can see and use, enables any social media user—including those not in the group—to verify posts. This ensures that if a post is forged or modified by a social network or government, any user will be able to identify it as a forgery.

Content uploaded from an account through SecurePost appears as if it had a single author with no way of identifying individual posters or a group's membership roster. It accomplishes this by hosting the group on a third-party proxy server, which masks the individual's IP address from the social network. "This means you don't have to trust some outside party," said Nekrasov. "A group can run its own server and verify everything that is going on."

What's more, SecurePost attaches a cryptographic signature to the post, generated from the group member's private key. The application then automatically verifies the authenticity of this signature for anyone else running the program, regardless of their membership status in a particular group. Because the proxy server never actually receives the users' private key, the verification feature can flag content such as posts made by an impostor or someone who hacked the proxy.

The team designed SecurePost with the realities of its users in mind. They produced the application for the Android operating system, which made up 86 percent of the global market share at the time. They also made it compatible with older devices, so that as of October 2017, 99.9 percent of Android devices registered with Google could run the application. This is important because many individuals in the targeted user groups use phones with older operating systems, which are cheaper to purchase.

SecurePost can also operate without a continuous internet connection, a necessity in many regions where it will find use. Instead of immediately uploading content, the app stores it on the device and posts it when internet connectivity resumes. To circumvent the vulnerability this creates if authorities confiscate the device, SecurePost also encrypts all data with an application-wide password. If the user is under duress, he or she can provide a false password that wipes the app's data, including the group keys.

The team hopes the software ultimately gets developed into a full-fledged product with a wider reach. "At the end of the day, we're not a company, we're researchers," said Metzger. "We can develop apps, and we can put them in the app store, but we don't have a budget for marketing them."

"But we can create new systems that a company could build a business around and market," she added. "And that's the way these technologies can have a big impact."

More information: Michael Nekrasov et al, A user-driven free speech application for anonymous and verified online, public group discourse, *Journal of Internet Services and Applications* (2018). DOI: 10.1186/s13174-018-0093-4

Provided by University of California - Santa Barbara