Email security improving, but far from perfect

November 19 2015

Country	
Tunisia	96.1%
Iraq	25.6%
Papua New Guinea	25.0%
Nepal	24.3%
Kenya	24.1%
Uganda	23.3%
Lesotho	20.3%
Sierra Leone	13.4%
New Caledonia	10.1%
Zambia	10.0%

This graph shows the countries with the highest percentage of emails that were intentionally downgraded by STARTTLS modification during April 20-27, 2015. Credit: University of Illinois

Email security helps protect some of our most sensitive data: password recovery confirmations, financial data, confidential correspondences, and more. According to a new report, published by Michael Bailey, an

associate professor of computer science at the University of Illinois at Urbana-Champaign in collaboration with colleagues at the University of Michigan and Google, email security is significantly better than it was two years ago, but still has widespread issues. The full report is published in the *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*.

The networking protocols that underlie today's Internet were not originally built to be secure—it was only years later that security protocols were "bolted on" to the existing systems. However, despite there being measures in place to solve these security issues, each individual email server has the choice whether to adopt these protocols. Email security in the past two years has improved because companies like Google now use these protocols, but there are many other servers that do not.

"Much of the measurement work done in my lab is focused on how we can incentivize an individual or an organization to make a right decision—to adopt these security protocols," said Bailey, a member of the research faculty at Illinois' Coordinated Science Lab. "A lot of the interesting work in security goes beyond not only modeling the technology, but modeling the organizations that use that technology and how they choose to use it."

In addition to measuring the adoption of email security protocols at scale, Bailey and his team also highlighted some of the implications of "bolted on security" in today's email. For example, because the protocols that govern email-server-to-email-server communication were originally not designed to support encryption, a command called STARTTLS was later added that allowed two email servers to negotiate a secure connection. However, because this command can only be issued after two email servers begin communicating in an insecure fashion, an attacker can corrupt the STARTTLS command, forcing the email

exchange to continue without encryption.

"We found that there's a significant number of email exchanges in which there's an adversary between two mail servers who's trying to intentionally downgrade the communication," said Bailey. "For example, pretty much every email server in Tunisia is not safe. In other countries, like Iraq and Nepal, it's close to 1 in 4 servers that are actively being downgraded."

While the report provides encouraging news that email security continues to strengthen, the report also serves to remind users that it remains important to understand the limits of privacy in email and on the Internet as a whole.

"I work under the assumption that any email I send without special care has an Internet-wide distribution list," says Bailey. "If you want to send a secure email, you must either trust every computer and network your email traverses, or make sure that the email contents are encrypted before it ever leaves your computer."

Provided by University of Illinois at Urbana-Champaign