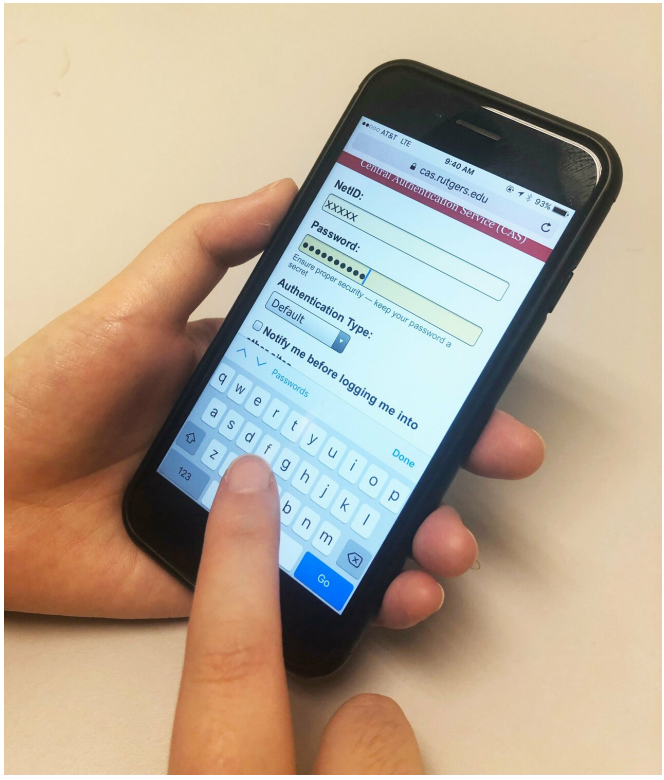
Exposing flaws in metrics for user login systems

26 February 2019



One of the most popular ways to log in involves typing user names and text-based passwords. Credit: Can Liu/Rutgers University-New Brunswick

How good is the research on the success or failure of the system that verifies your identity when you log into a computer, smartphone or other device?

Chances are it's not good, and that's a major security and privacy issue that should be fixed, according to a Rutgers University-New Brunswick study that proposes a novel solution.

"Our paper represents a major advance toward understanding authentication systems," said Janne Lindqvist, senior author and assistant professor in the Department of Electrical and Computer Engineering. "Surprisingly, we found that commonly used metrics in research for reporting the performance of user login systems are flawed. This means the systems may not work well, and that can have serious, real-life consequences for proposed systems that are adopted based on misleading metrics."

User login systems—known as authentication systems—are supposed to ensure that the person who logs into a computer or other device, accesses email or accesses a financial account is who they claim to be. One of the most popular ways to log in involves typing user names and text-based passwords.

Rutgers engineers reviewed 35 recent research papers on authentication systems and found that 33 systems, or 94 percent, had flaws in what they reported. The engineers also found that there is no consistent approach for reporting system performance metrics and the metrics are inadequate.

So they came up with a novel method that gives researchers and others, including government agencies and the public, accurate information on the effectiveness of their authentication systems and how they can be improved, said Lindqvist, who directs the Rutgers Human-Computer Interaction and Security Engineering Laboratory in the School of Engineering.

The Rutgers engineers' solution is to combine the strengths of a commonly used metric from other fields and a rarely used metric. These together can be used to measure the success of user login systems. One provides an overview of how well an authentication system works overall. The second determines whether system performance is measured using misleading data.

"We believe it is crucial for our community to adopt more transparent reporting of metrics and performance," the peer-reviewed study says.

The study will be published in the proceedings of the Network and Distributed System Security Symposium, which is sponsored by the Internet Society and will be held this week in San Diego, California.

More information: DOI: 10.14722/ndss.2019.23351

Provided by Rutgers University