Department of Computer Science

Bridging the Theory and Practice of Cryptography

Joseph Jaeger
University of Washington

Hosted by Reza Curtmola

DATE: Wednesday, March 10, 2021
TIME: 2:30 PM - 3:30 PM
Webex Link: https://njit.webex.com/njit/j.php?MTID=m0562b146db4d49da5699bfd1834e9dee

https://cs.njit.edu/seminars

Abstract:

Cryptography is deployed at scale to protect data, both in transit and at rest. However, protocols are often designed or even deployed aiming for security that extends beyond what is formally understood. This talk will cover my efforts to narrow this gap and to provide protocols that are both practical and provably secure.

In my talk I will showcase examples of this from my recent and ongoing research, including how the use of cryptography at scale (e.g. in encrypted messaging apps such as WhatsApp) required new models to address unique threats and how a better understanding of the power of computational resources used by attackers (e.g. computation time and memory usage) enabled me to prove stronger security guarantees for important protocols like TLS.

Bio:

Joseph Jaeger is a Postdoctoral Scholar at the University of Washington. He previously received his PhD from UC San Diego. His research interests span a wide range of topics across cryptography and its applications. His work received the Early-Career Best Paper Award at Crypto 2020.