The Ada Lovelace Bicentenary Lectures on Computability, December 2015 – January 2016

Radia Perlman (EMC Corporation)

How to Build an Insecure System out of Perfectly Good Cryptography

Thursday, 28 January, 11:00-12:30

Academics tend to focus on subtle properties of the mathematical tools in cryptography. Industry standards bodies tend to fight over the syntax of messages. Although both of these are important, this talk focuses on broader system design issues that tend to get neglected. Examples will show deployed systems and standards that use perfectly good cryptography, but are insecure in practice, as well as lessons to be learned from these examples.

Watch the video