PKI Revealed
1:56

Hi, I'm Wes Kussmaul. On behalf of my PKI colleagues, please accept our apologies for trying to explain PKI using the language of mathematics and cryptography. You don't need to know any of that confusing stuff to understand the incredible power of the puzzle kit infrastructure.

In PKI, your phone or other device generates two very big numbers. One of the numbers is public, while the other is secret and never leaves your device.

For logins, instead of using a password, your username is accompanied by your public number. Using that number, the server makes a puzzle and sends it back. Using the secret number, your device solves the puzzle and sends the solution back to the server. That solution proves that you have the secret number that goes with your public number, and so the server believes your identity claim.

Note that if a hacker captures every bit going back and forth – the identity, the public number, the puzzle, the solution to the puzzle – they'll end up with nothing of value. That's because every puzzle made with that public number is different. A solution to a previous puzzle is useless.

Besides secure logins with no passwords, PKI gives you true digital signatures. Using the reverse of the login procedure, you make a puzzle out of your document using your secret number. After that, anyone who has your public number can solve the puzzle and know that it was really you who signed it and that not a single comma has been changed since you signed it.

Lastly, PKI makes encryption practical, by ensuring that only authorized people have the decryption key that turns your encrypted document from gibberish back into the original.

PKI means rock-solid security for password-free login, true digital signatures, and control of decryption keys.