9-May: Source: [Galois]

Who is verifying their cryptographic protocols?..

Computational Model

→ Limited adversary.

→ Involves translating English proofs to something a machine can understand.

→ Lot of work needs to be done by humans.

Symbolic Model:

→ Limits the adversary to a Dolev-Yao attacker.

→ Leverages full automation.

(Not convinced by this.)

Challenges.

→ Mostly an academic pursuit.

→ If it isn't the backbone of an industrial standard or a novel piece of open source crypto it isn't getting verified.

1. Understanding and operating the tools

2. Demonstrating the RoI compared to the cost of verification.

   ↳ Protocol verification has had a big impact on improving security.
   How? References? Examples?

⟹ Each tool does something different, and the devil is in the details.

→ Reconciling Formal Models and Implementation.

Typo:

The nauce comes ----

↓

nuance?