ATTACKING BONEH *ET AL.*
(WORK IN PROGRESS)

Peter Nordholt

Claudio Orlandi

Aarhus University, Denmark

RUMP SESSION ASIACRYPT 2012

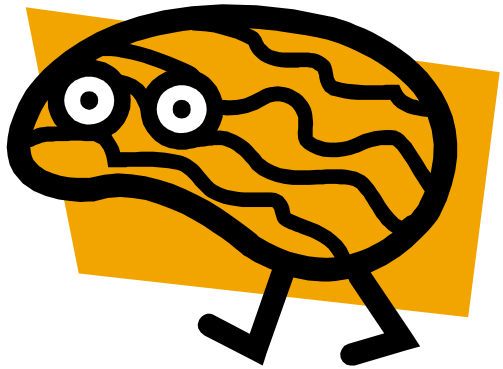
Identification

- Known identification schemes are vulnerable to so called "*rubber hose*" attacks

- This is a knowledge extractor!

New era for crypto?

- Neuroscience tells us that your brain knows things you don't!
  - How to ride a bike…
  - How to play Guitar Hero…
  - …



- **Embed information in your motory skills!**

But where??

Legs?

- Bike: Not very effective for identification (but participants lost weight!)

Fingers?

- Guitar Hero

(test subjects did not want to stop identifying)

Full-Body Memory!

The Boneh Crypto Challenge

- How to make sure that this system is secure to rubber hose attack?

"The BONEH Crypto Challenge"

Rules of the challenge

- You can order a challenge on our homepage (shipping fees might apply)
  - 4 kind of challenges:
    - easy,
    - medium,
    - hard,
    - Impossible

- **Goal: ”extract” password from the challenge**

Challenges – Easy (~40 bits security)

(...or other cryptographers
of equivalent weight class...)

Challenges – Medium (~80 bits security)

Challenges – Hard (~160 bits security)

Challenge – Impossible (~∞ bits security)

THANK YOU!

- Disclaimer 1: No cryptographers (including Dan Boneh) were harmed in the making of this presentation!
- Disclaimer 2: we are not responsible if you get hurt while trying to extract Chuck Norris' password!