# Better Privacy for Trusted Computing Platforms (Extended Abstract)

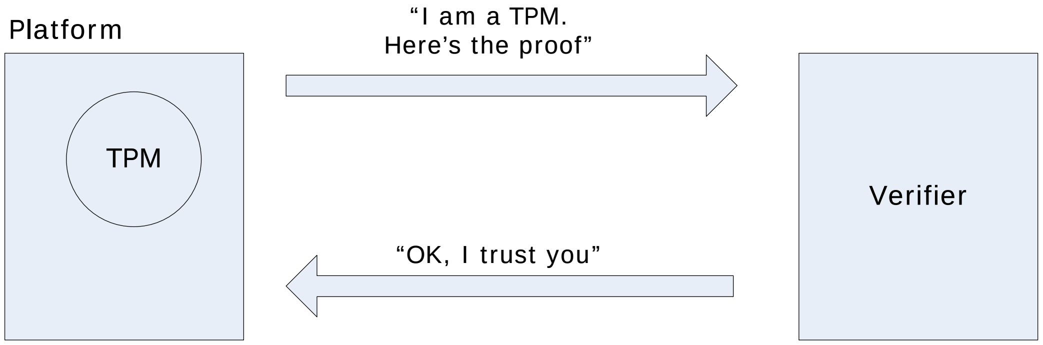
Jan Camenisch, “Better Privacy for Trusted Computing Platforms,” to appear in *ESORICS 2004*. Preprint provided in email by J.Camenisch, July 2004.

Presented by Ron (Seong Min) Kim

skim093@ec.auckland.ac.nz

# Overview

- Trusted Platform Module (TPM)
  - Trusted hardware device integrated into a platform
- TPM authentication protocol
  - Remotely convince other party it is a TPM, hence safe
- Existing protocols
  - Hard to implement
  - Less "privacy"
- Proposed protocol
  - Easy to implement
  - Better "privacy"

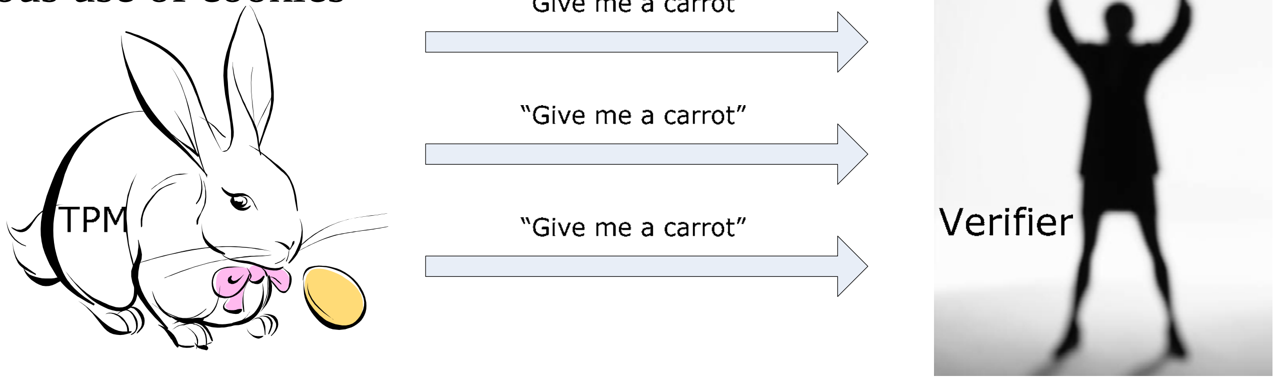


# Key Concepts

- Verifier
  - Party on the other side of channel who detects rogues and provides service
- Privacy
  - Inability of verifiers to uniquely identify a TPM
- Less privacy
  - Verifiers can uniquely identify a TPM
  - Transactions are linkable → profiling possible

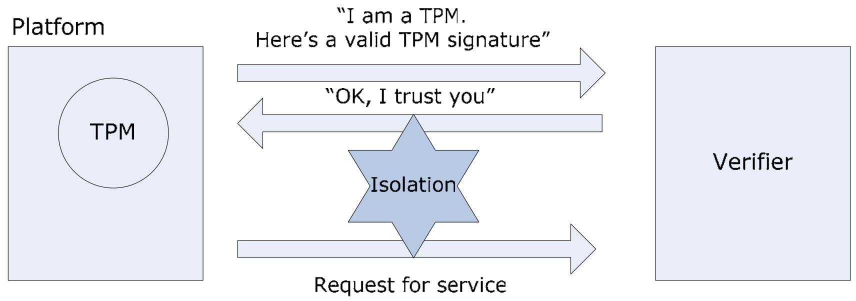
  E.g. Malicious use of cookies

“Now I know that rabbit likes carrots!”



# Appreciative Comment

- Identifies the cause for less privacy
  - Lies in detection mechanism for "rogue TPM"
  - To detect rogues, some privacy is sacrificed
    - I.e. some transactions can be linkable
- Ingenious idea
  - "Let's isolate the problem area from service of request!"
    - I.e. separate detection for rogues and service of request
  - Their premise: it provides a "better privacy"



# Critical Comments

- Not an introductory paper for lay persons

  “The author assumes audiences are knowledgeable in the field and agree with the author’s definition of terms”

  - Gory details
    - Can any of us approve or disapprove their proof?
  - Not self-contained
    - No definition or justification of major concepts

# Not Self-Contained

- Missing definitions
  - Attester
    - What does it exactly mean?
  - Privacy
    - It can mean lots of things!
  - RSA keys
    - What does that do? Is it any good?

# Not Self-Contained II

- Missing definitions and justifications
  - TPM
    - What is a TPM?
    - Why do we need one?
    - Why do we want a new protocol if we don’t need a TPM?
  - Rogue TPM
    - What is a rogue TPM?
    - What harm does it do?
    - Why do we want to detect them when we are not sure what harm it can inflict?

# Question

- A question for you..

  “How would you define what a rogue TPM is that the author implied? Do you see any problem with the definition and would you have used a different term if you were the author?”