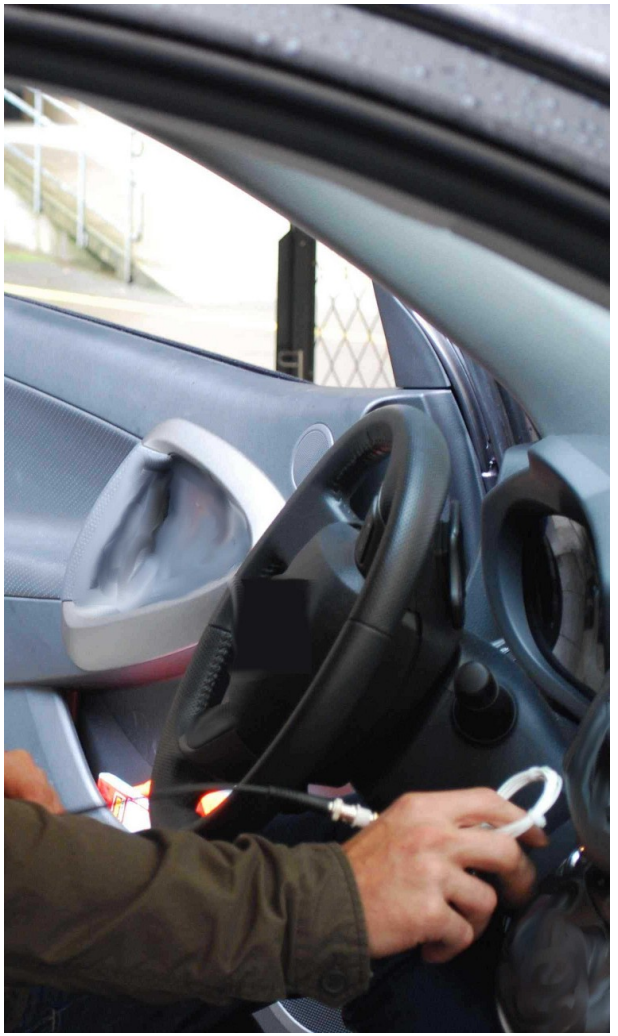
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distance Hijacking Attacks on Distance Bounding Protocols

Cas Cremers
ETH Zurich

Distance Bounding

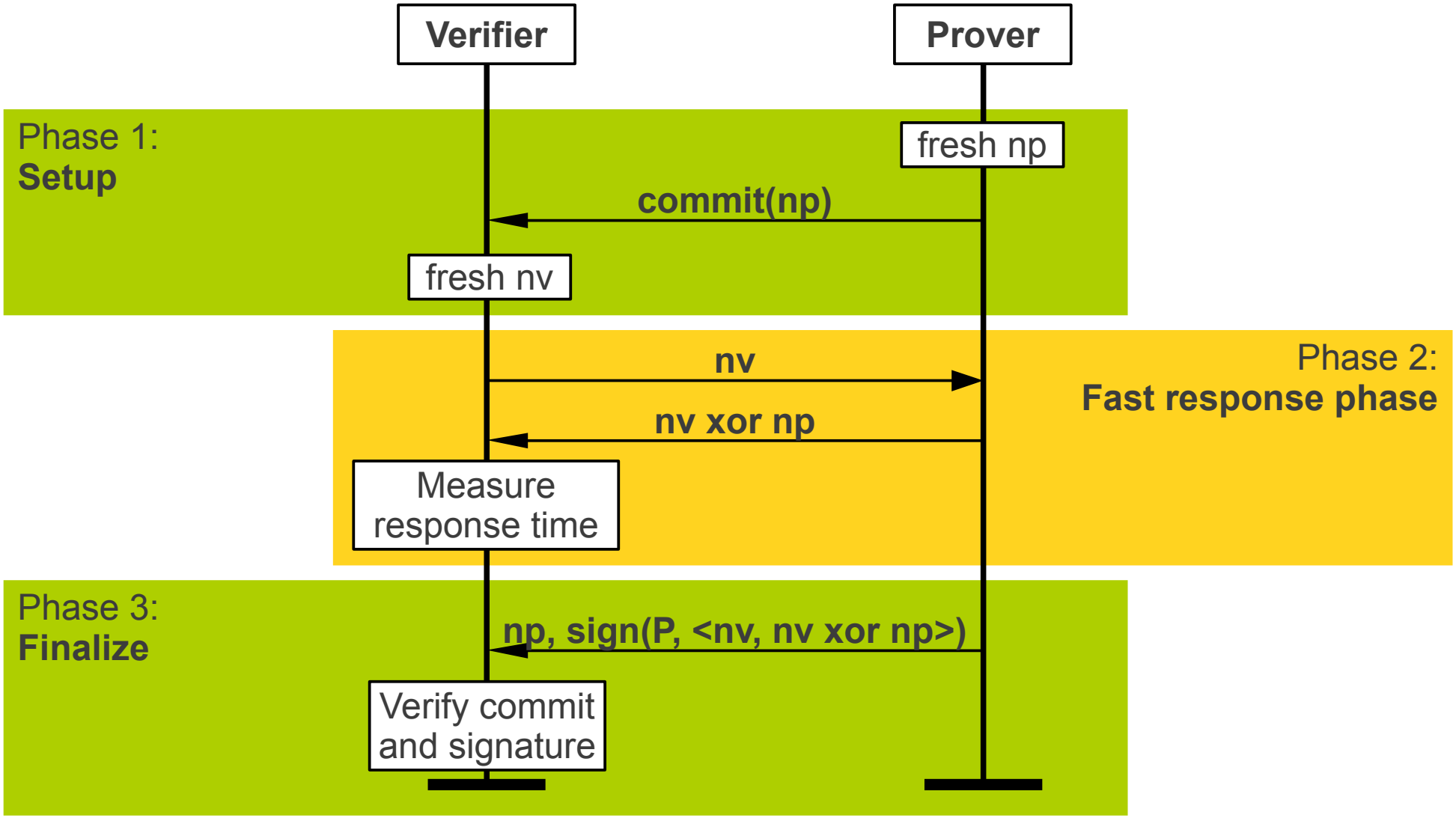


Distance Bounding Protocols

- Objective: **ensure proximity**
- Protocol with two roles: **Prover** and **Verifier**
- **Verifier obtains an upper bound** on the distance to the prover
- Guarantee also holds if the prover is malicious

Distance bounding for network access

Brands and Chaum protocol (1993)

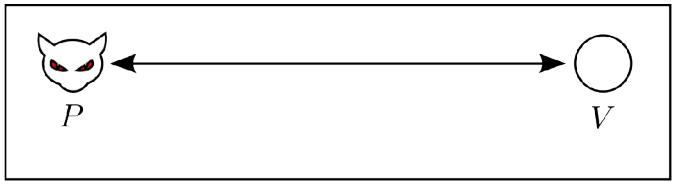


Threats considered in protocol proposals

Mafia Fraud

- **External attacker** modifies distance of **honest prover**

Distance Fraud



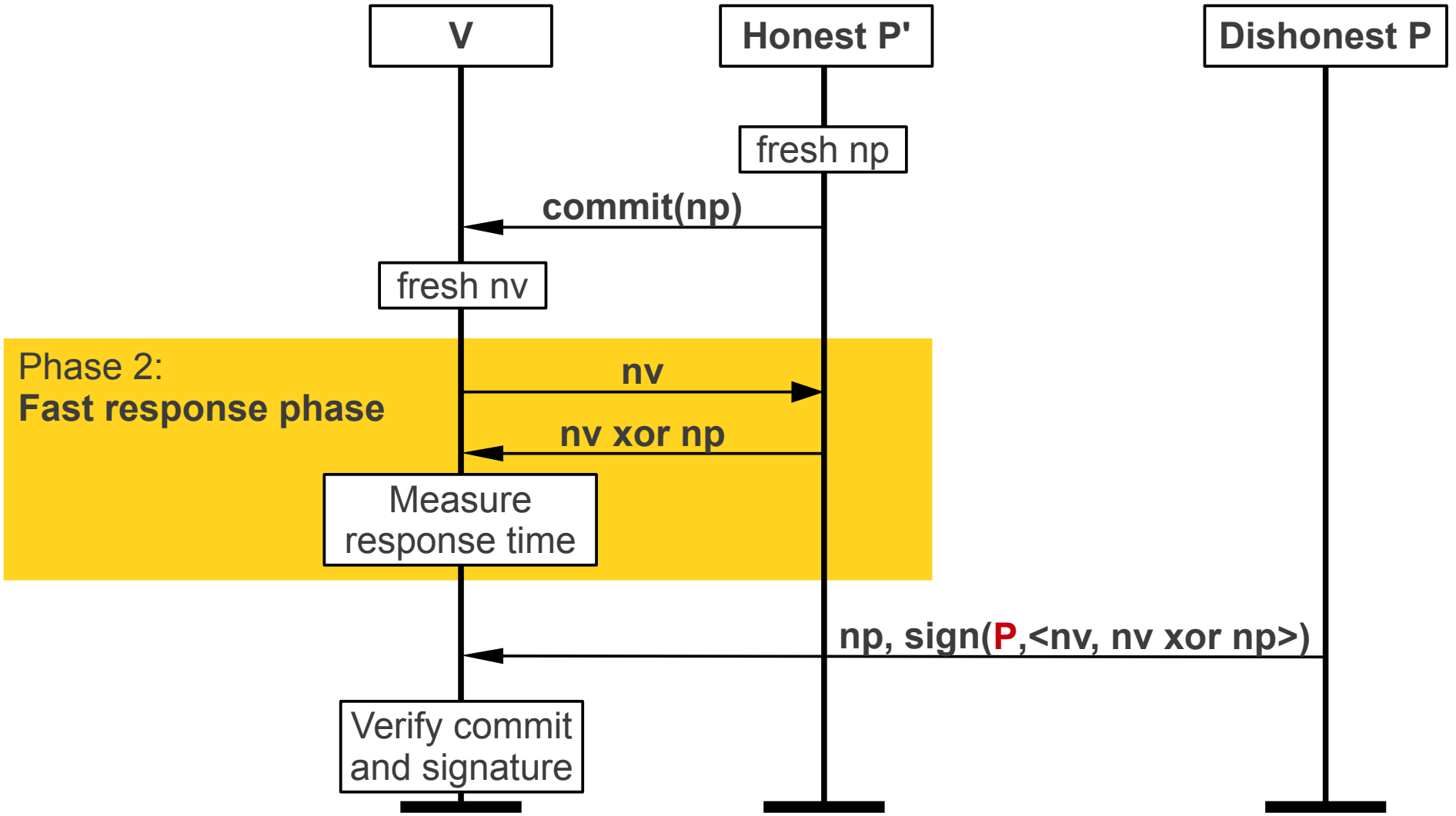
- **Dishonest prover** modifies his own distance

Terrorist Fraud

- **Dishonest prover** collaborates with **closer attacker** to modify his distance

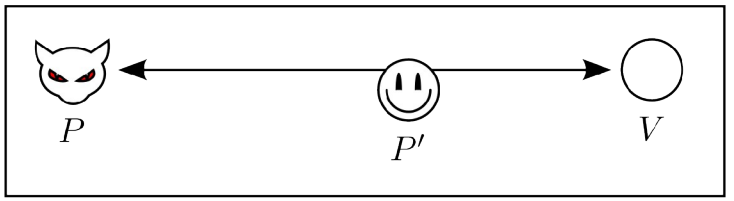
What about other provers?

Distance Hijacking attack on B&C



Distance Hijacking

A **Distance Hijacking attack** is an attack in which a **dishonest prover P exploits** one or more **honest parties** to provide a verifier V with false information about the distance between P and V.



Scope

Protocol	DH-attack?
Brands and Chaum (Fiat-Shamir)	**Yes**
Brands and Chaum (Schnorr)	**Yes**
Brands and Chaum (signature)	**Yes**
Bussard and Bagga	**-**
CRCS	**Yes**
Hancke and Kuhn	**-**
Hitomi	**-**
KA2	**-**
Kuhn, Luecken, Tippenhauer	**Yes**
MAD	**Yes**
Meadows et al for F(..) = <NV,NP xor P>	**Yes**
Munilla and Peinado	**-**
Noise resilient MAD	**Yes**
Poulidor	**-**
Reid et al.	**-**
Swiss-knife	**-**
Tree	**-**
WSBC+DB	**Yes**
WSBC+DB Noent	**Yes**

About half of the investigated protocols vulnerable

- Brands and Chaum based designs usually vulnerable
- Hancke & Kuhn based designs seem okay

Fixing the problem

- **Secure channel** (TLS) **does not help here**
  - Cannot use cryptography during fast response
  - Protocols that use secure channels in the other phases may still be vulnerable
- Fixes **logically bind fast response** to other phases
  - Involve identity in response
  - Bind identity to nonce in Phase 1
  - **Fixes do not require additional cryptography**

Phase 1:
Setup

Phase 2:
Fast response phase

Phase 3:
Finalize

Formal model

- We extended Basin et al. [TPHOLs'09]
- **Hybrid symbolic model**
  - Also captures bit-level overshadowing attacks
    - adversary flips some bits of an unknown message
  - Formalization in Isabelle/HOL
- Used to show that our fixes prevent the found attacks

  (Details in the paper; theory files publicly available)

Multiple protocols

Interaction between protocols with similar fast response hardware **can lead to attacks**

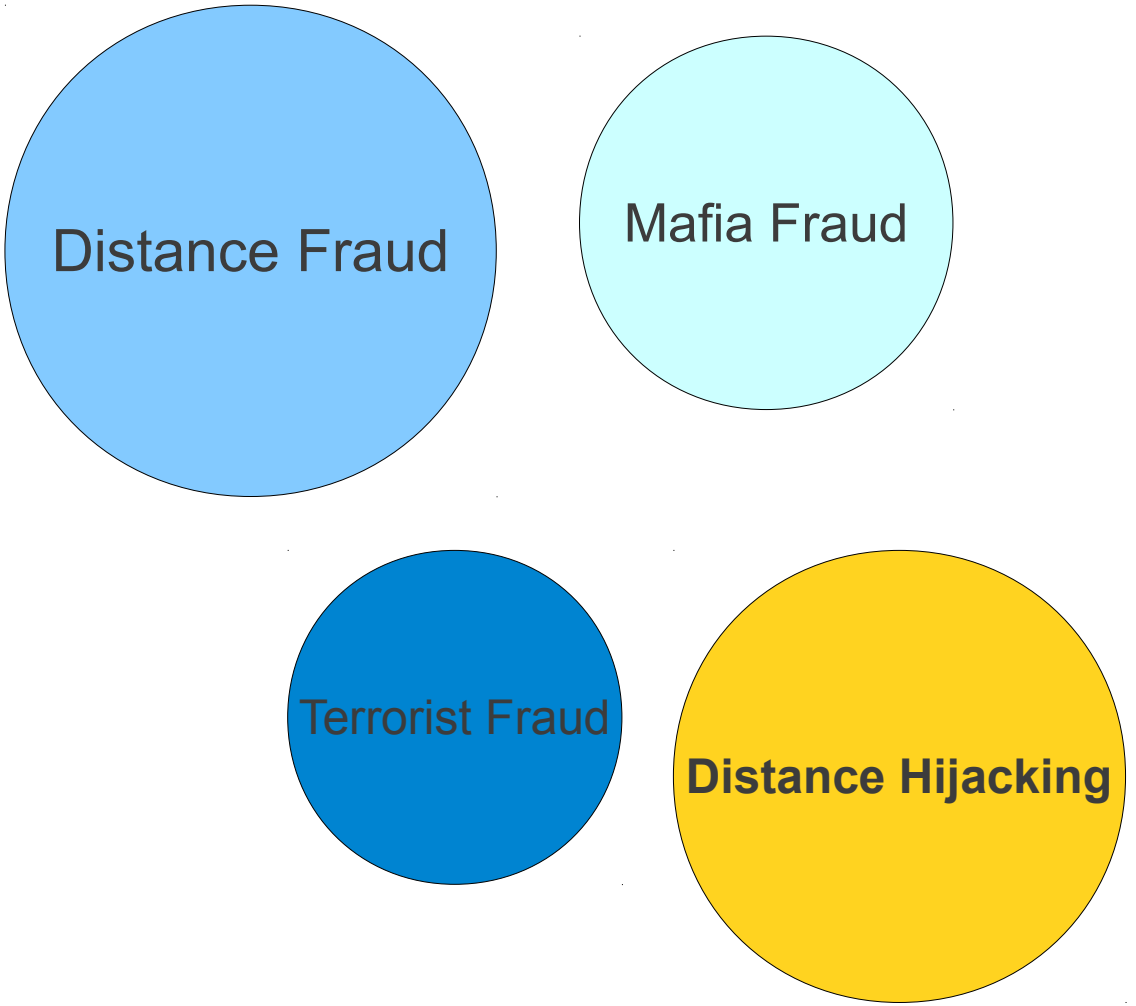
- Similar to "chosen protocol" or "multi-protocol" attacks"
- ALL protocols vulnerable

Honest P' card with bad protocol

Server runs good protocol

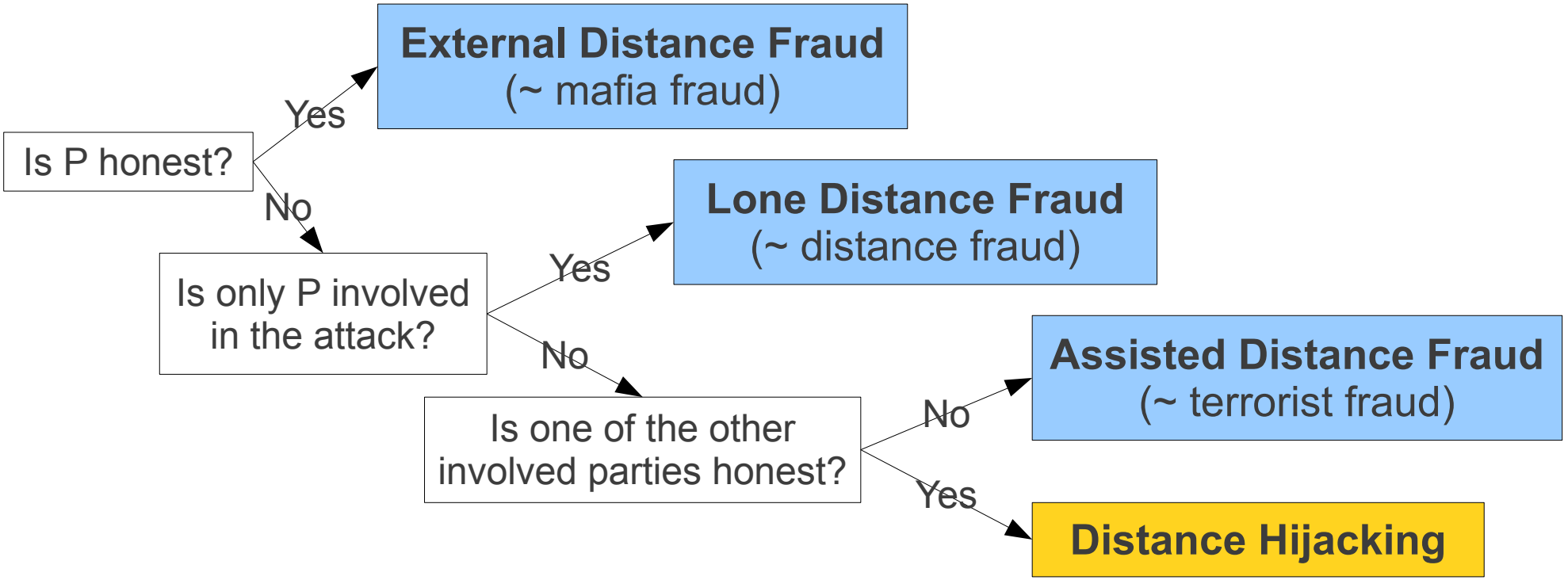
Attacker uses P card with good protocol

Are all attacks now covered?



Restructuring attacks on DB protocols

Assume an attack trace where V computes incorrect distance for P



A **Distance Hijacking attack** is an attack in which a **dishonest prover P exploits** one or more **honest parties** to provide a verifier V with false information about the distance between P and V.

Conclusions

- Many protocols vulnerable to **Distance Hijacking**
  - Fixes do not introduce significant overhead
  - Just-in-time: distance bounding implementations starting to be produced
- Distance Hijacking is a **relevant threat** in many cases
- Cannot afford to ignore multiple provers/verifiers during analysis
- Interaction between different DB-protocols still possible...