

DISTANCE BOUNDING PROTOCOLS: AUTHENTICATION LOGIC ANALYSIS

Catherine Meadows
Center for High Assurance Computer Systems
Naval Research Laboratory
meadows@itd.nrl.navy.mil

ITI Workshop on Dependability and Security
Dec. 5, 2006

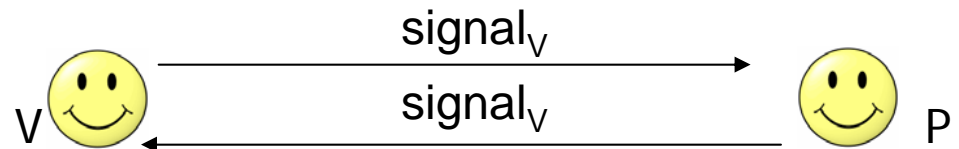
WHAT THIS TALK IS ABOUT

- Authenticating time of flight ranging
 - Measuring distance using round trip of a signal
- Time of Flight useful and accurate method of
 - for location computation in sensor networks
 - Measure your distance from nodes that know their own locations
 - Use multilateration to figure out your own location
 - Finding nearest neighbor
- But, securing it is tricky, since authentication mechanisms can interfere with timing
 - Class of protocols called “distance bounding protocols” achieves this, but is not that well understood
- We have been using formal methods to improve and validate distance bounding and related protocols

Securing Time of Flight

- Basic ToF

- $d = v(t_2 - t_1)/2$



- Potential Attacks on TOF

- Attacker can take on another node's identity

- Attacker can “hijack” another node's response

- Attacker can delay response and pretend to be further away than it is

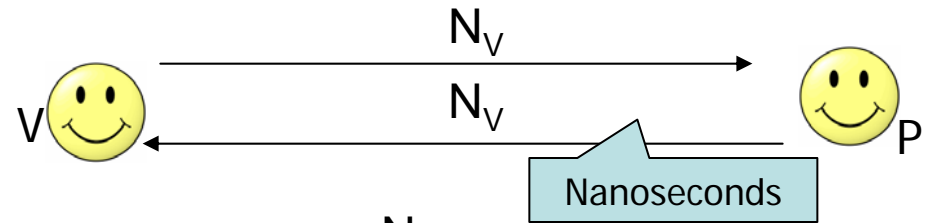
- Attacker can respond prematurely and pretend to be closer than it is

- Question: How do you secure time of flight?

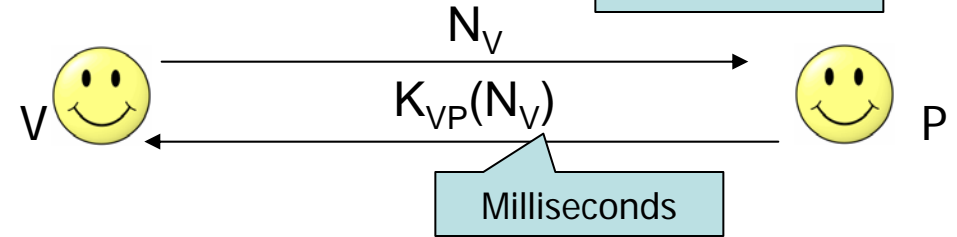
- You need to secure not only the value of the data, but the time it takes to arrive

SOME POSSIBLE SOLUTIONS

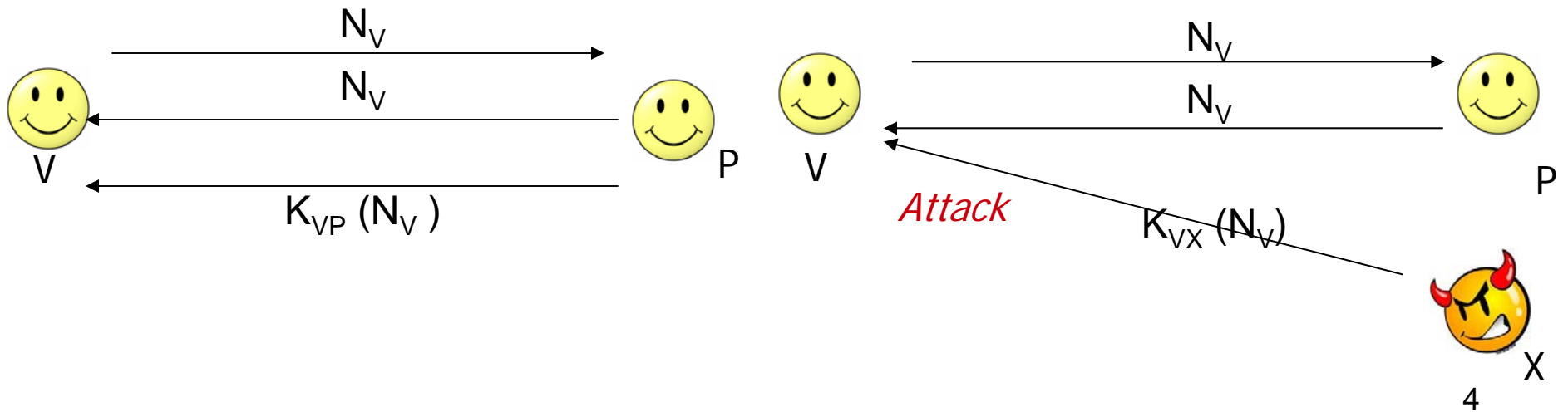
Echo Protocol (Sastry et al.)



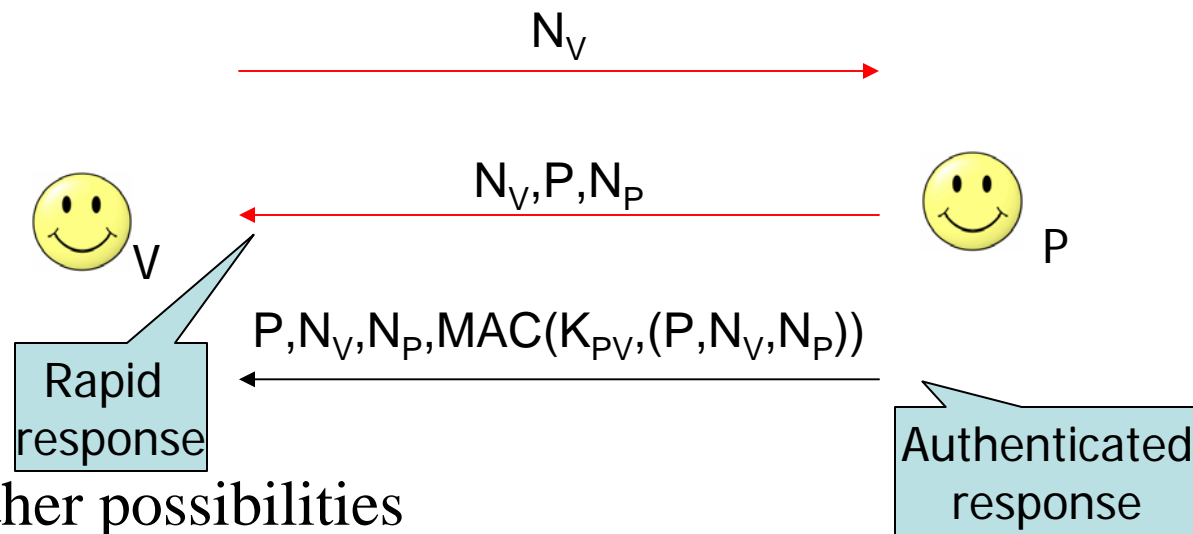
Adding Authentication
Crypto adds latency



Separating authenticated response from timed response



One of Our Solutions



- Many other possibilities
 - Do authentication before rapid exchange (Hancke-Kuhn)
 - Distribute authentication before and after rapid exchange (Brands-Chaum)
 - Replace single rapid exchanges by multiple single bit exchanges (Brands-Chaum, others)
 - Develop lighter-weight protocol with weaker threat model
 - E.g. don't defend against prover trying to appear closer than it is, protect info of honest provers only (Capkun-Hubeaux, Meadows)

WHAT WE ARE DOING

- Developing formal framework for distance bounding protocols, based on techniques for formal crypto protocol analysis
- Allows us to specify desired properties at a high level
- Instantiate with different protocols and provide security proofs at the same time
- Security proofs based upon assumptions about physical medium which must be verified empirically

CHALLENGES FACED

- How do we integrate physical properties into formal model?
 - Have done this with with time and distance
 - Distance defined in terms of minimum time for round trip
 - Working on
 - Latency-introducing implementation details
 - Signal processing attacks
- How do we deal with probabilistic properties and probabilistic guarantees?
- How do we formulate guarantees so they can be used by other parts of the system?
 - In this case, by a secure localization algorithm
 - Which in turn is used by other secure applications