Aalto University

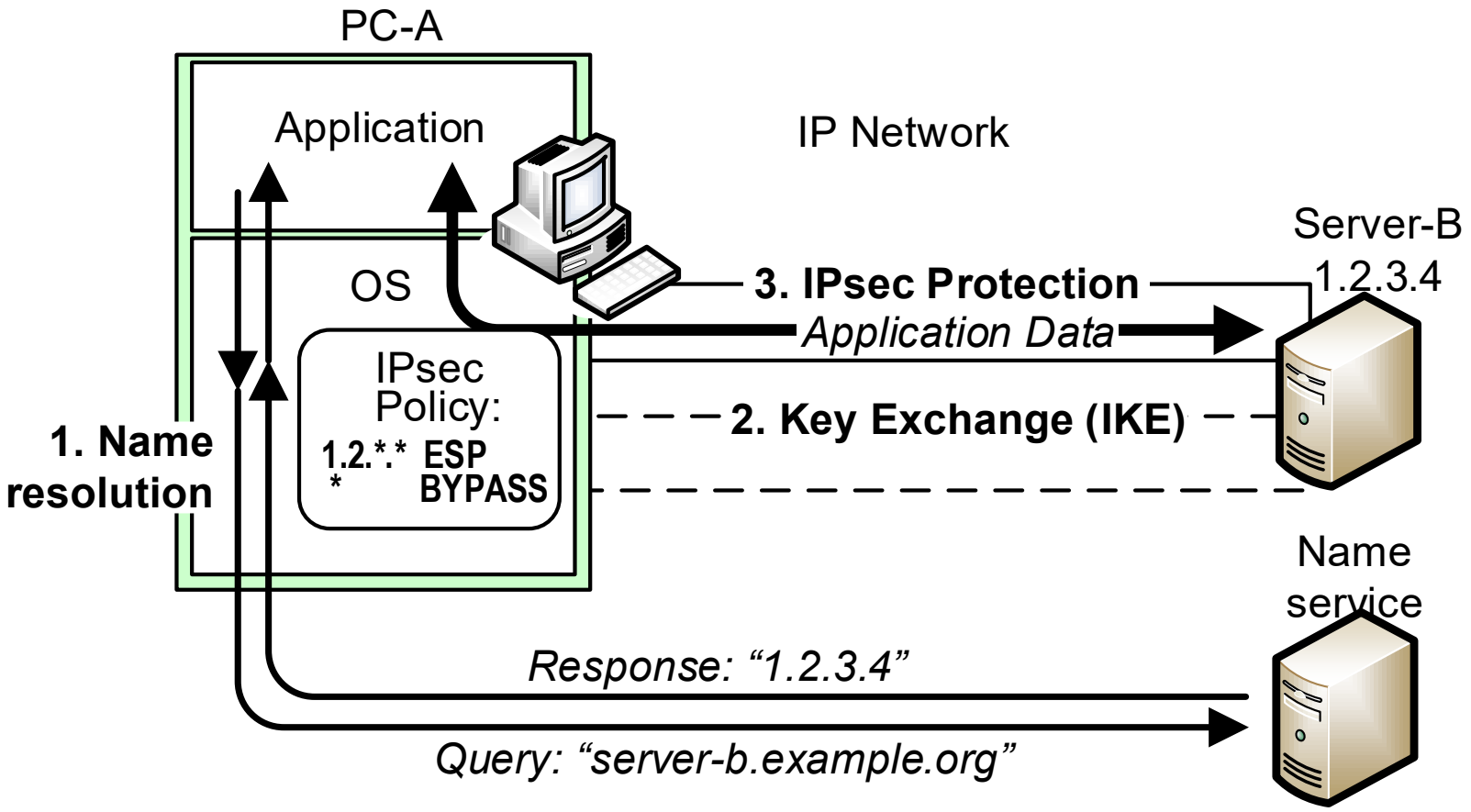
Network Security: Issues with host-to-host IPsec

Tuomas Aura

CS-E4300 Network security

Aalto University

IPsec and name resolution



- TCP socket API: resolve name into an IP address; then connect to it
- TCP SYN to the address triggers IKEv2 (if the ESP SA does not yet exist)

IPsec and identifiers

1. Application opens a connection to an IP address. IPsec uses the IP addresses as policy selector
2. Application actually wants to connect to a specific name, and IKE usually authenticates the remote node by its DNS name

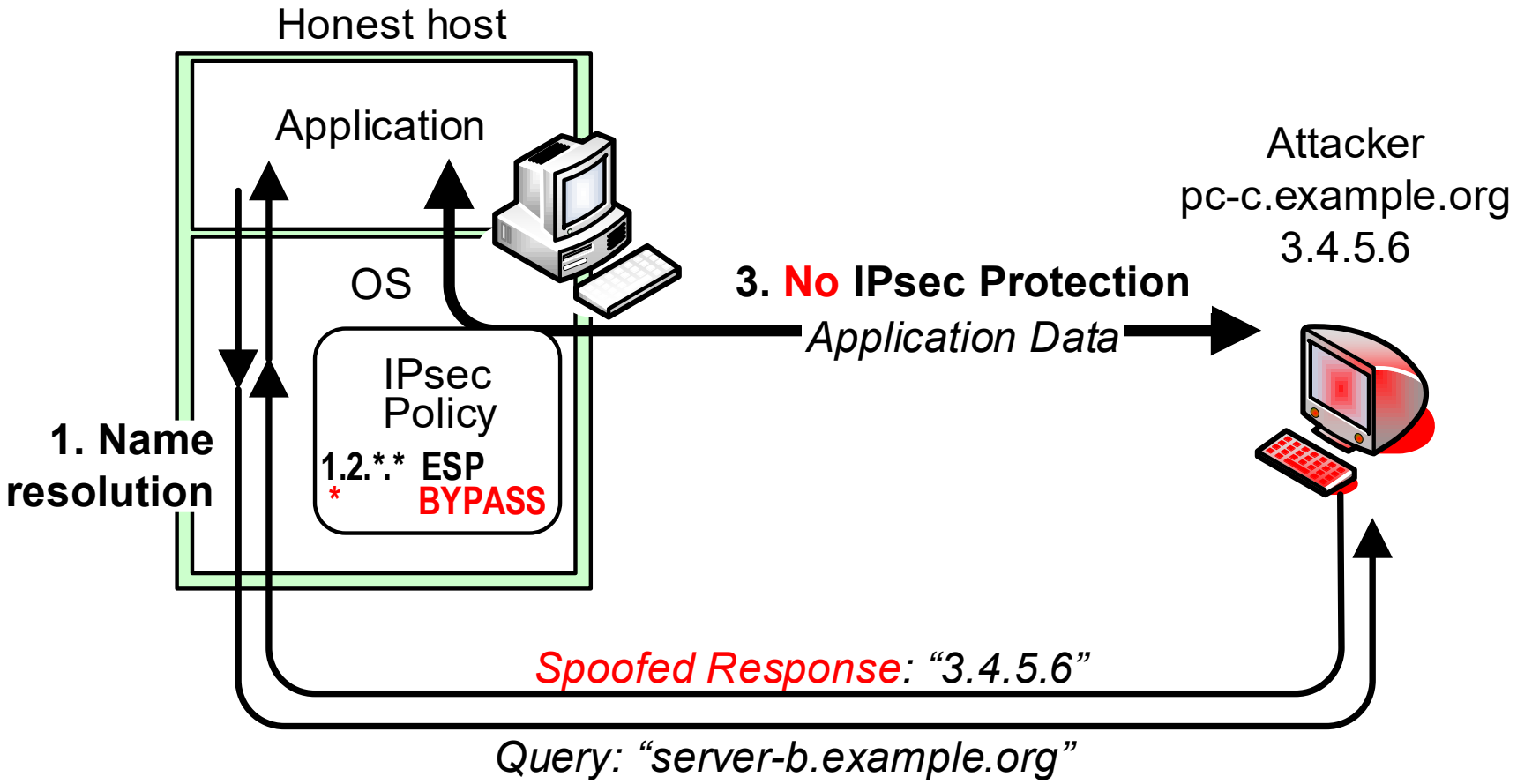
- Problem: No secure mapping between the two identifier spaces: DNS names and IP addresses

IPsec and DNS spoofing

- Practically all host-to-host IPsec policies have BYPASS action for some remote addresses
  - Internet outside the intranet, e.g., web servers
  - Devices that do not support IPsec, e.g., printers, sensors

  → Spoofed DNS response can cause any hostname to map to a BYPASS action
- Thus, IPsec policy selection depends on secure name resolution

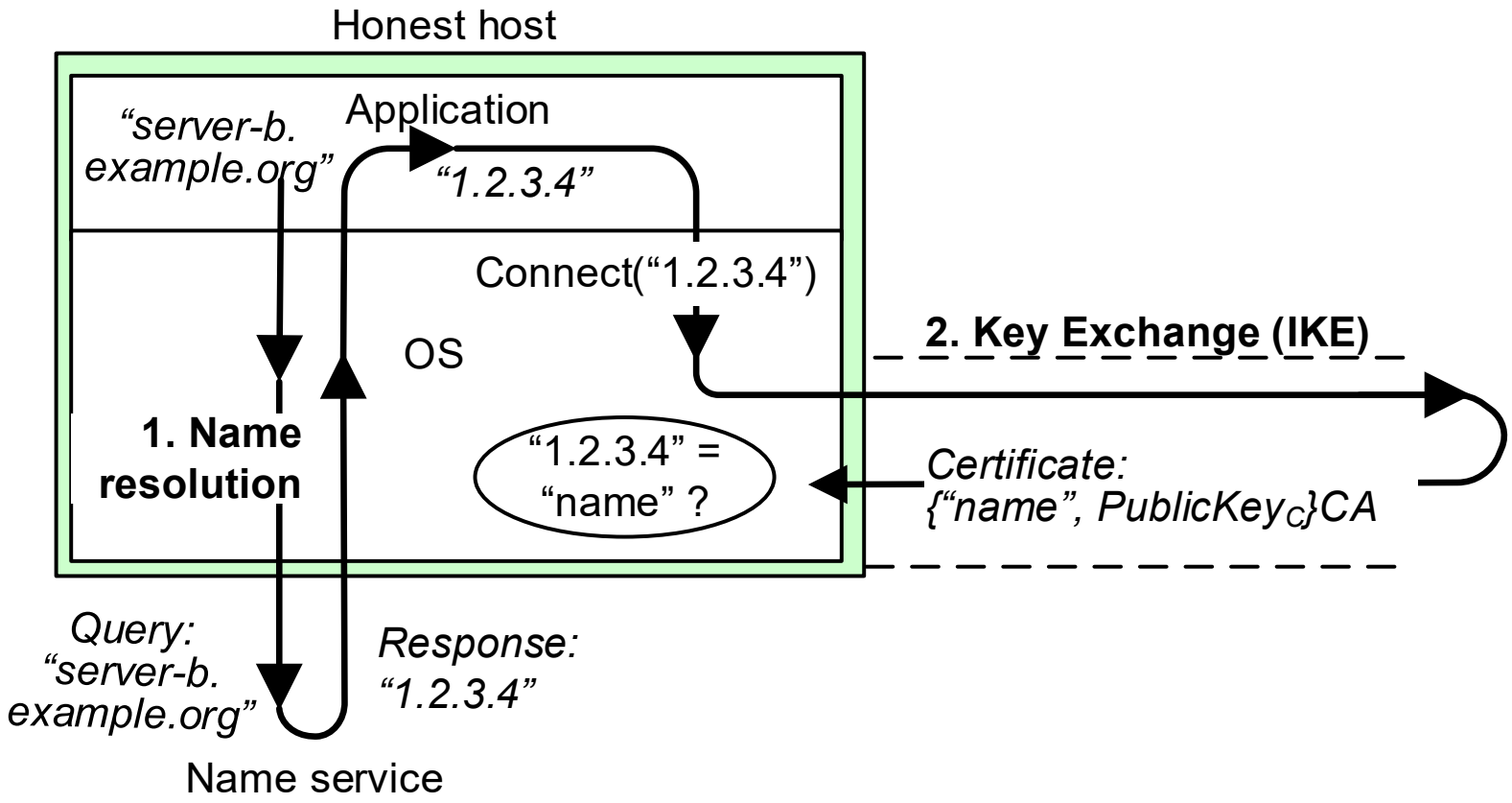
Classic IPsec/DNS Vulnerability



- Attacker spoofs DNS response to circumvent the IPsec policy

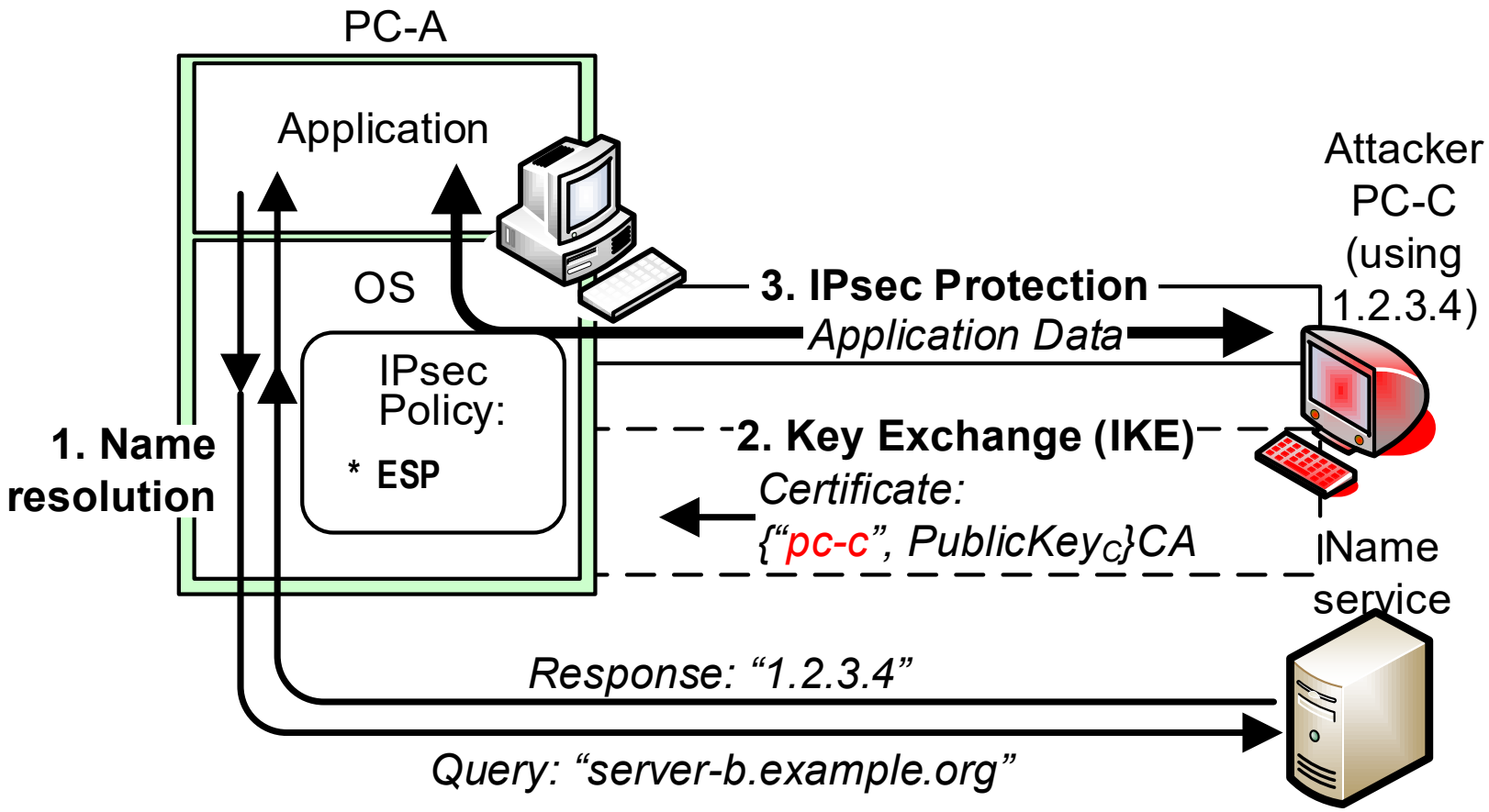
Let's assume secure DNS. Does it solve the problems?

Further problem: IPsec and Certificates



- Name resolution is done in a separate step. IKE knows the peer's IP address, not its name. The certificate, on the other hand, only contains the name. How does IKE know if the certificate is ok? No obvious solution.

Further problem: IPsec and Certificates



- IKE knows the peer's IP address, not its name. The certificate only contains the name. How does IKE know if the certificate is ok? No obvious solution.

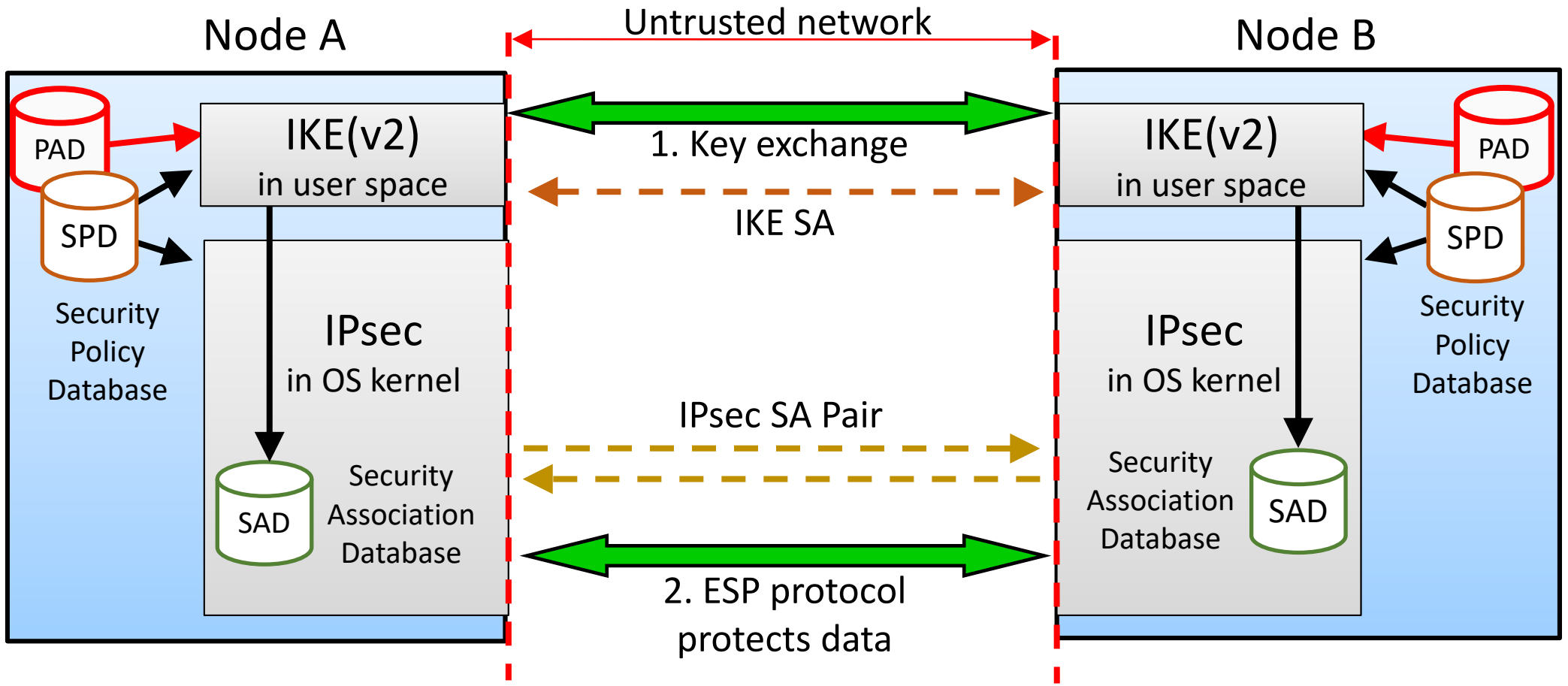
IPsec and Certificates – solutions?

- Secure DNS (forward lookup) does not help — why?
- Secure reverse DNS would be a solution — but it does not exist

Other solutions:

- Connect by name — change the socket API so that the connect() call specifies the host name, not the IP address
- Give up IPsec transparency: applications query the socket API for the authenticated name
  - VPN applications do this to check the VPN gateway name from the certificate
- Ignore the hostname: use IPsec only to isolate certified intranet hosts from outsiders/intruders
  - Example: NAP in a Windows domain uses IPsec for network access control and not for end-to-end authentication of the individual host identities

IPsec architecture [RFC 4301]



Peer authorization database (PAD)

- IPsec specification [RFC4301] defines a database that maps authenticated names to allowed IP addresses
- How is PAD implemented?
  - VPN applications check that the name on the certificate matches a known VPN gateway
  - For host-to-host IPsec in a closed domain, such as intranet, PAD could theoretically be implemented – but it has not been
  - No solution for general host-to-host IPsec in the open Internet

This is why IPsec is really only used for VPN and *not* host-to-host