Message Quality for Ambient System Security

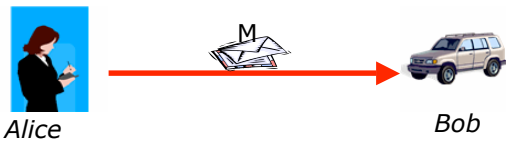
Ciarán Bryce

INRIA-France

The Security Challenge

- Theft, viruses, bugs
  - 200 000 phone thefts in France each year
  - 2004: Cabir virus on Symbian, Duts virus on PocketPC
- SPAM and i-waste
- Spoofing attacks
- *And to complicate matters*
  - Scale of system precludes centralised authority to store principal information

The Meaning of Principal

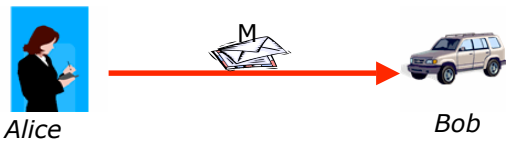


- A principal is an entity that undertakes actions in the system
  - E.g., *devices, services, servers*, etc.
  - Entity in which one needs to place trust
- The population of principals can be extremely large
  - Most principals do not know each other
- The identity of a principal may convey little security information
  - *E.g., knowledge of a soda machine's serial number does not permit its trustworthiness to be established.*

The Meaning of Principal

- For principals, we need to care less about who they are but by what they do, e.g.,
  - Principal coffee machine returns coffee in return for coin
- Identity might not change; but ability to service a request can, e.g.,
  - Hardware and software system ware, devices become infected, users become malicious
- Principal Attestation
  - The onus is on Alice to demonstrate to Bob what it claims to be
    - *E.g., Coffee machine demonstrates that it returns coffee*

The Security Properties



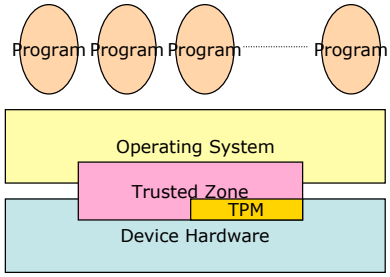
- Fidelity
  - M is a message that Alice is likely to utter
  - M is uttered by Alice, and is not being replayed
- Trustworthy
  - M is most likely true
  - Alice provides evidence to Bob to substantiate message
- Utility
  - Bob really needs to hear M

Message Quality

Traditional Security Properties

- Confidentiality and Integrity of M
  - Parties agree on shared key by exchange of public keys
  - Message quality ensures that keys are securely exchanged
- Availability
  - Bob cannot be prevented from reading message;
    - Would need to consider network signal attacks (which we do not)
- Privacy / anonymity
  - 3rd parties cannot learn that Alice sent message or information about Alice
    - Need to deprecate role of identity in security model

Implementing Security: principal profile



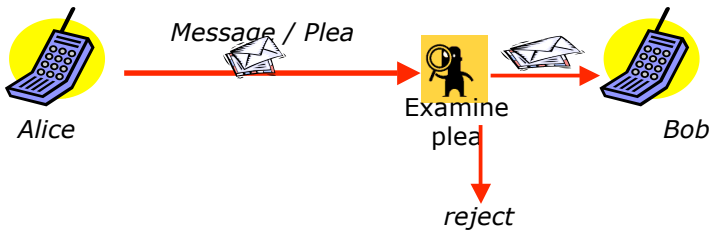
- Principal characterised by what it does
  - I.e., by set of installed programs
- Program qualified by

Principal profile

  - Actions (messages)
  - Certification of code origin
  - Certification of installation
    - How code on device got there
  - Other application, service or user-specific certifications
    - E.g., certification of review, etc.
- Certificates might be signed by well-known principals (e.g., car manufacturer or retailer)
  - But fewer than in systems relying on identity

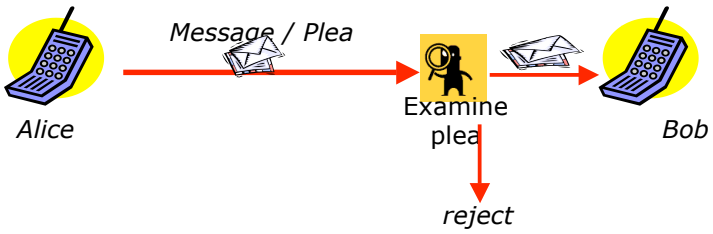
Message Quality Verification

- Profile used to construct plea object that argues for message's quality
  - Uses profile certificates and history of exchanged messages (evidence)



- Authentication and authorization replaced by
  - Principal attestation - verifies that plea is valid
  - Message quality verification

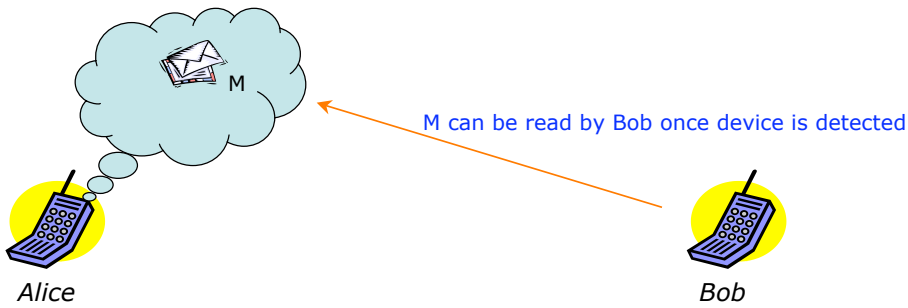
Message Quality Verification



- Verifying message quality
  - Fidelity: message created by a trusted zone with Alice's profile
  - Trustworthy: history of messages constitute evidence
  - Utility: message belongs to Bob's profile

Lana Programming Model

- Based on Linda tuple space model (also, Lime, Spread, etc.)
  - Each device has its own tuple space in which he publishes tuples (using out)
  - A device may read from other devices' tuple spaces



Programming Model

Operation	***Role***
read(Tuple pattern)	Returns a tuple matching pattern from any device in network neighborhood
out(Tuple t)	Publishes t in the local tuple space
remove(Tuple t)	Removes t from local tuple space

- Java-based implementation
- Networking implemented over multicast (sockets) and Bluetooth (BlueZ)

Example

< Please, « Airport » >

Calling cab

<« Airport », 20 Euros>

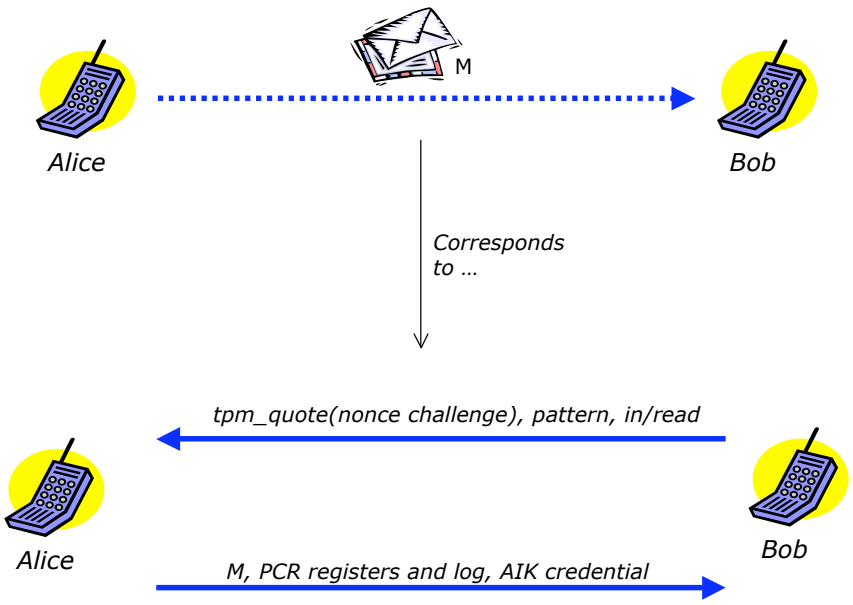
< Stop, « Airport », 20 Euros >

< Arrived, « Airport » >

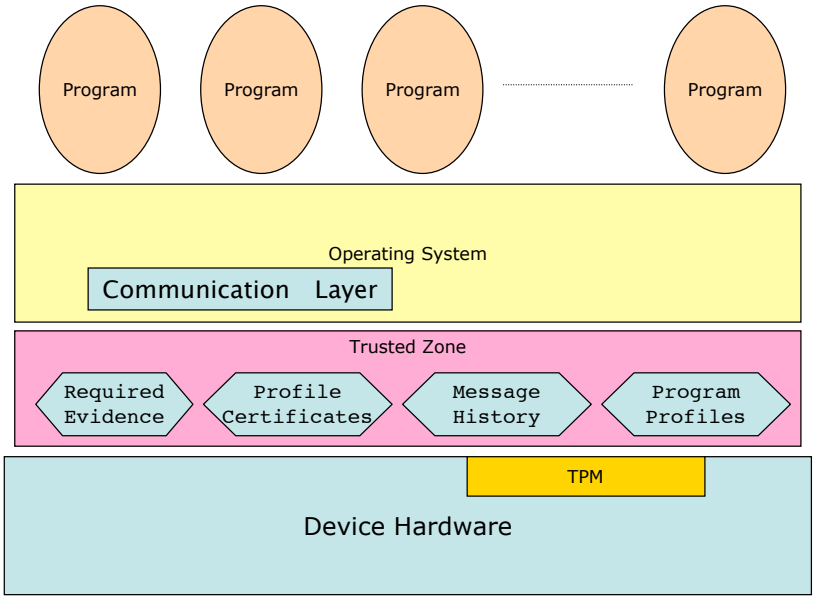
Leaving cab

< Bye >

Implementing Security using TPMs



AiK credential signed by software provider



Constructing Pleas

$M = \{ Data, K, H, P, S, C_k, xBy^* \}$

- K : symmetric key generated by trusted zone
- C_k = trusted zone certificate for K
- S : Signature: { D, H, P, xBy*}K
- xBy : Application-specific certificate: { x, P, sig }K,
  - E.g., { reviewedBy Sam, Profile, Sam_{sig} }K
- P : Profile: $<d^{i/o}>^*$ -- sequence of input/output actions
- H : History: < M >*

Hearing Pleas

- How does a plea for message M succeed?
  - $M = \{ Data, K, H, P, S, C_k, xBy^* \}$
- Bob requires evidence
  - History of Alice's messages he wants to see H_R
- HearPlea(M, H_R, xBy*)
  - M is signed by a trusted zone with profile P : S(M, P)
  - M is in Alice's profile (for fidelity)
  - Selected xBy certificates are valid
  - M is in Bob's profile (for utility)
  - History H in M is complete with respect to H_R

Conclusions

- Aim of work to rethink meaning of security in pervasive system
- Implementation to help experiment scenarios
- Rely on trusted computing unit, e.g., TPM