

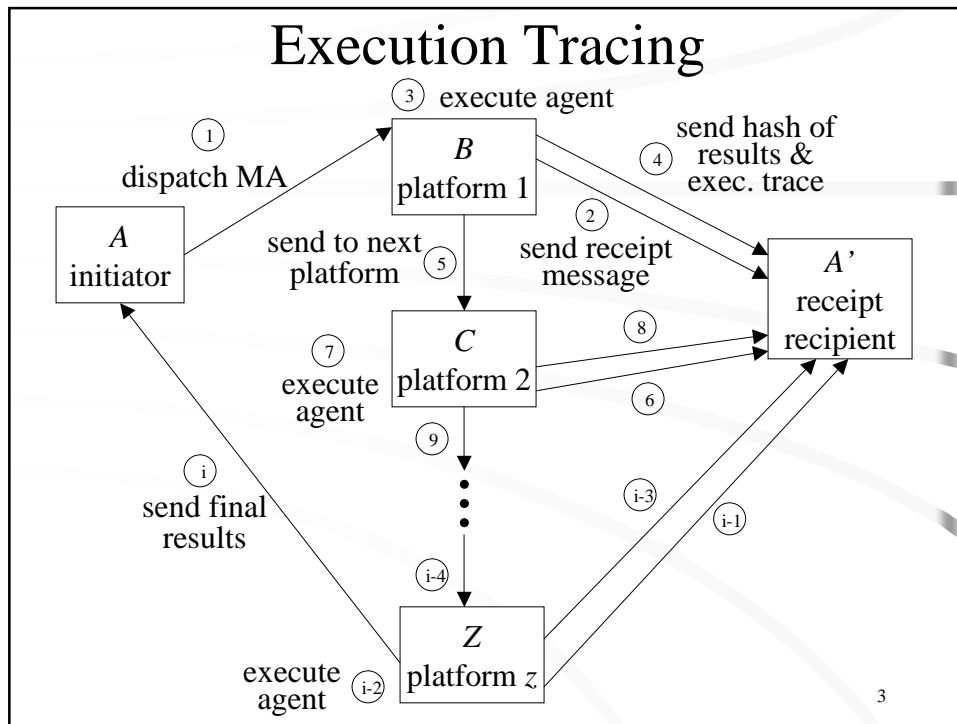
# Data Encapsulation Protocols

Anna Suen  
suen@cs.fsu.edu  
March 5, 2003

## Preview

- Publicly Verifiable Chained Digital Signature Protocol
- Chained Digital Signature Protocol with Forward Privacy
- Chained MAC Protocol
- Data Collection Protocol

2



### Terminology

$P_0$	Originator	creator of mobile agent
$P_{i>0}$	Platform	computational environment for mobile agent
$o_i$	Offer	the data that a platform submits
$O_i$	Encapsulated offer	the offer encrypted or hashed together with some other information

4

## Publicly Verifiable Chained Digital Signature Protocol (PVCDS): Assumptions

- assumes PKI
- each platform has
  - a unique name
  - a public signature verification key
    - issued by certification authority
- there is a directory service to retrieve certificates

5

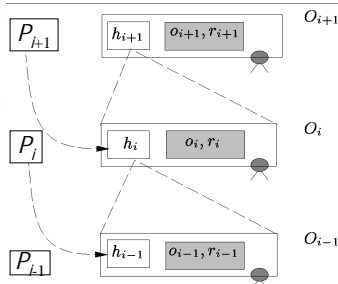
## PVCDS

- each platform signs with secret key
  - non-repudiable & unforgable
- may encrypt offer with public key
  - data confidentiality
- uses hash chain
  - links offer of current platform with identity of next platform

6

## PVCDSP: Protocol

- *Encapsulated Offer:*
  - $O_i = SIG_i(ENC_0(o_i, r_i), h_i), 0 \leq i \leq n$
- *Chaining Relation*
  - $h_0 = \mathcal{H}(r_0, P_1)$
  - $h_i = \mathcal{H}(O_{i-1}, P_{i+1}), 1 \leq i \leq n$
- *Protocol*
  - $P_i \rightarrow P_{i+1}: \{O_k \mid 0 \leq k \leq i\}, 0 \leq i \leq n$

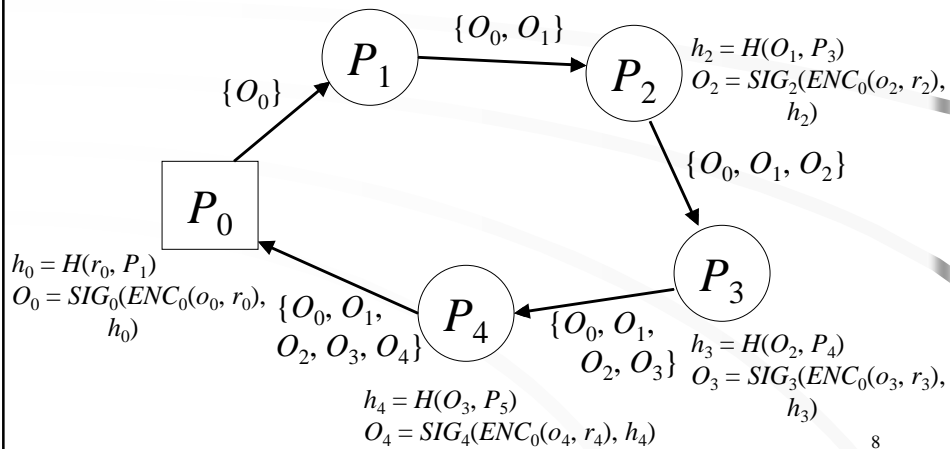


7

## PVCDSP: Protocol

$$h_1 = H(O_0, P_2)$$

$$O_1 = SIG_1(ENC_0(o_1, r_1), h_1)$$



8

## PVCDSF : The Encapsulated Offer $O_i$

- offer  $o_i$ 
  - probabilistically encrypted so only originator can retrieve it
- hash of previous encapsulated offer concatenated with identity of next platform
  - links previous offer with current one
    - can't modify  $O_{i-1}$  without modifying  $O_i$
  - guarantees that only  $P_{i+1}$  can append next offer

9

## Chained Digital Signature Protocol with Forward Privacy (CDSPFP)

- variation of PVCDSF
- change order of signing and encrypting offer
  - hide identity of offer provider (platform)
    - *Encapsulated Offer:*
      - $O_i = \mathcal{ENC}_0(\mathcal{SIG}_i(o_i), r_i), h_i, 0 \leq i \leq n$
    - *Chaining Relation*
      - $h_0 = \mathcal{H}(r_0, \mathbb{P}_1)$
      - $h_i = \mathcal{H}(O_{i-1}, r_i, \mathbb{P}_{i+1}), 1 \leq i \leq n$
    - *Protocol*
      - $\mathbb{P}_i \rightarrow \mathbb{P}_{i+1}: \{O_k \mid 0 \leq k \leq i\}$

10

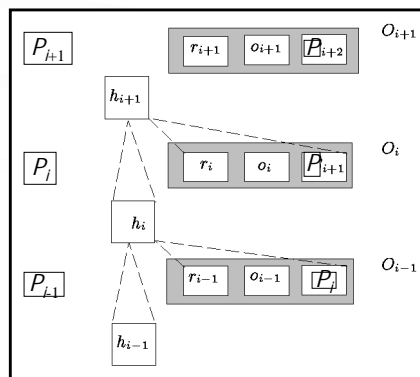
## Chained MAC Protocol: Assumptions

- no PKI
  - each platform know public key of originator
- requires each pair of platforms to be connected via a confidential channel

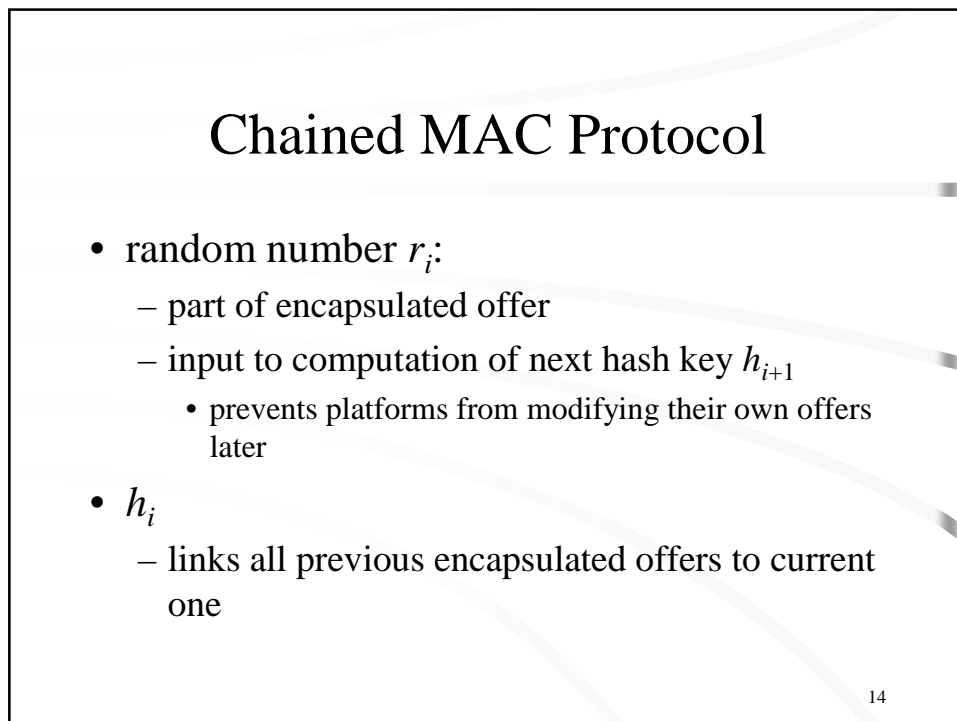
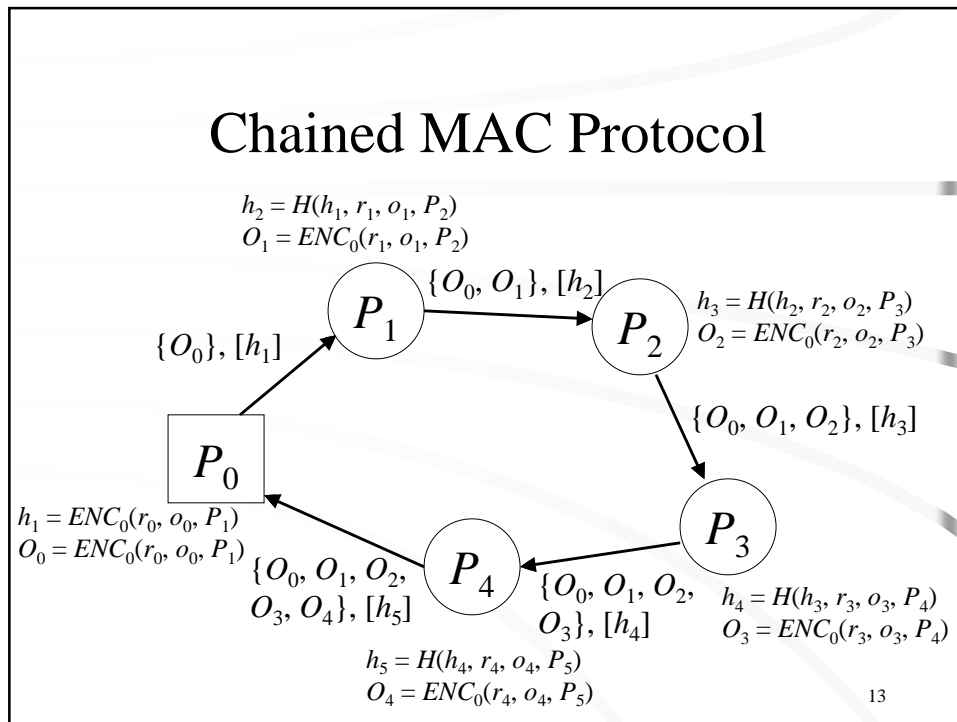
11

## Chained MAC Protocol

- *Encapsulated Offer*:
  - $O_i = \mathcal{ENC}_0(r_i, o_i, \mathcal{P}_{i+1})$ ,  $0 \leq i \leq n$
- *Chaining Relation*:
  - $h_1 = \mathcal{ENC}_0(r_0, o_0, \mathcal{P}_1)$
  - $h_{i+1} = \mathcal{H}(h_i, r_i, o_i, \mathcal{P}_{i+1})$ ,  $1 \leq i \leq n$
- *Protocol*:
  - $\mathcal{P}_j \rightarrow \mathcal{P}_{i+1}: \{O_k \mid 0 \leq k \leq i\}, [h_{i+1}]$ ,  $0 \leq i \leq n$



12



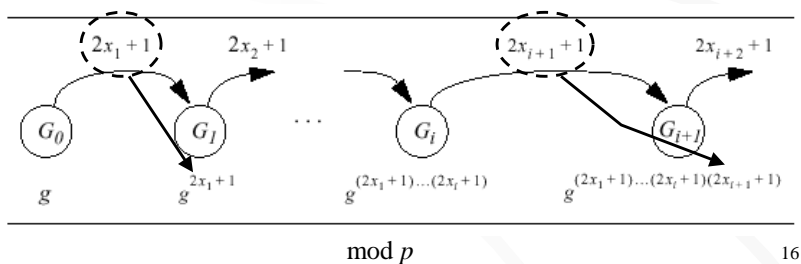
## Data Collection Protocol

- allows multiple offer updating
- does not require
  - data confidentiality
  - platform anonymity
  - (not necessary in all scenarios)
- no PKI
  - secret shared key between originator and each platform

15

## Data Collection Protocol: Set Hashing

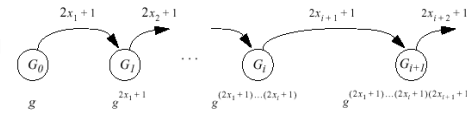
- method to hash together a set of data blocks in an order-independent way
- based on difficulty of solving discrete logarithm problem



16

## Set Hashing Properties

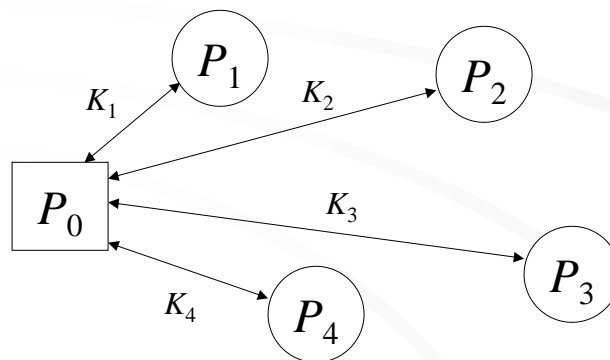
- Security
  - knowing any  $G_i$  and  $G_{i+1}$ , computationally infeasible to compute  $x_{i+1}$
  - discrete logarithm problem
- Commutativity
  - order of  $x$  does not matter
- Cancellation
  - knowing  $G_{i+1}$  and  $x_{i+1}$ , can compute  $G_i$
- Computational Complexity
  - knowing  $x_i$ , computation on  $G_i$  requires
    - $2n$  multiplications
    - $n$  additions
    - 1 exponentiation



17

## Data Collection Protocol – 1

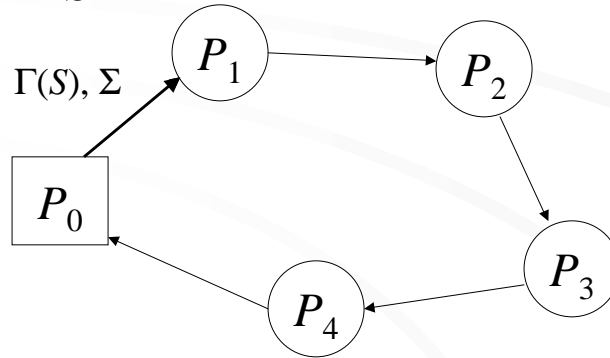
- Each platform  $P_{i>0}$  exchanges secret shared key  $K_i$  with originator  $P_0$



18

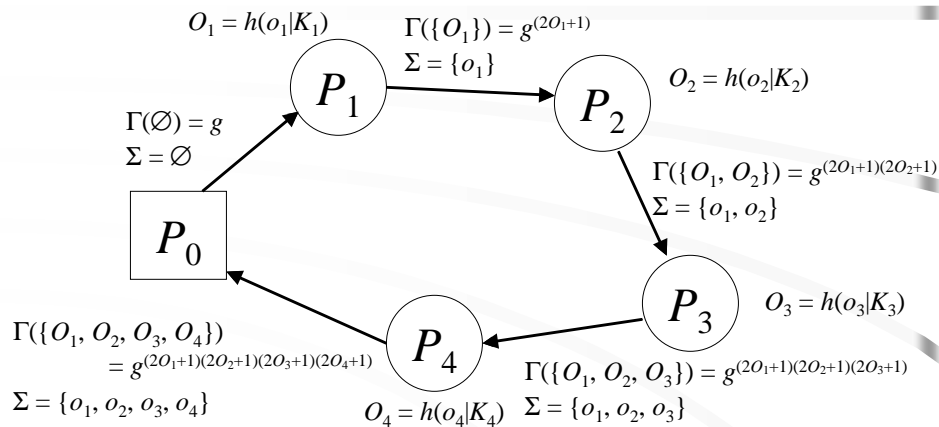
## Data Collection Protocol – 2

- $P_0$  sends MA with
  - set hash value  $\Gamma(S) = \Gamma(\emptyset) = g \text{ mod } p$
  - $\Sigma = \emptyset$



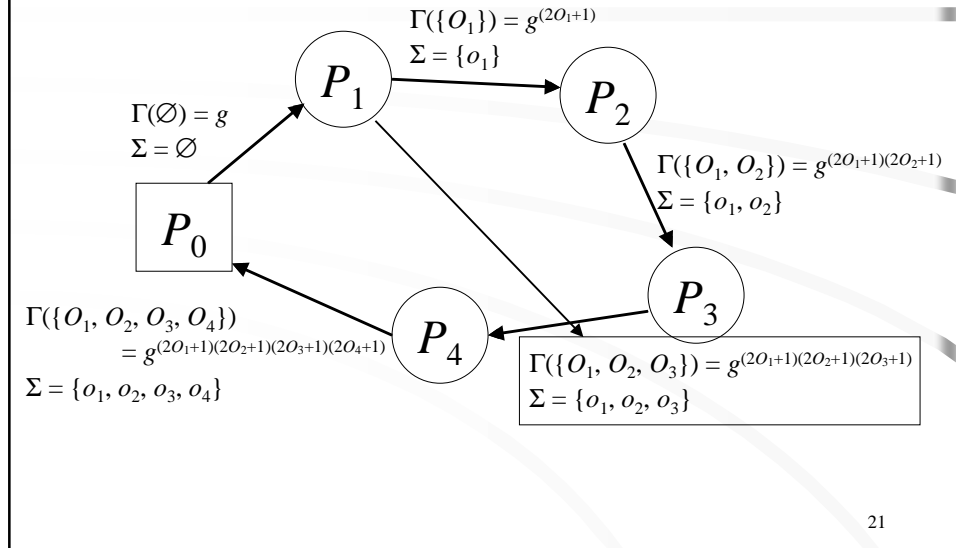
19

## Data Collection Protocol – 3



20

## Data Collection Protocol: Updating



## Data Collection Protocol: Updating

- replace old offer  $o_i$  with new offer  $o_i'$
- cancel out old integrity proof value  $O_i$  from  $\Gamma(S)$
- compute new integrity proof value  $O_i'$
- compute new set hash with  $O_i'$

$P_1$

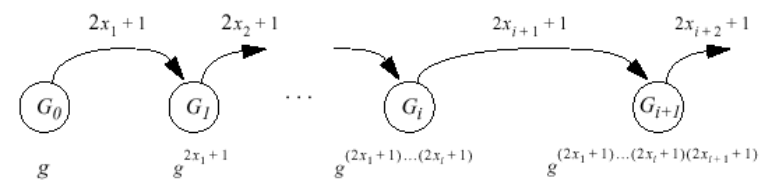
$$\Gamma(\{O_1', O_2, O_3\}) = g^{(2O_1'+1)(2O_2+1)(2O_3+1)}$$

$$\Sigma = \{o_1', o_2, o_3\}$$

22

## Data Collection Protocol: Verification

- check:
  - $\Gamma(S) =? g^{(2O_1+1)(2O_2+1)\dots(2O_n+1)}$
- if fail:
  - no offers are valid

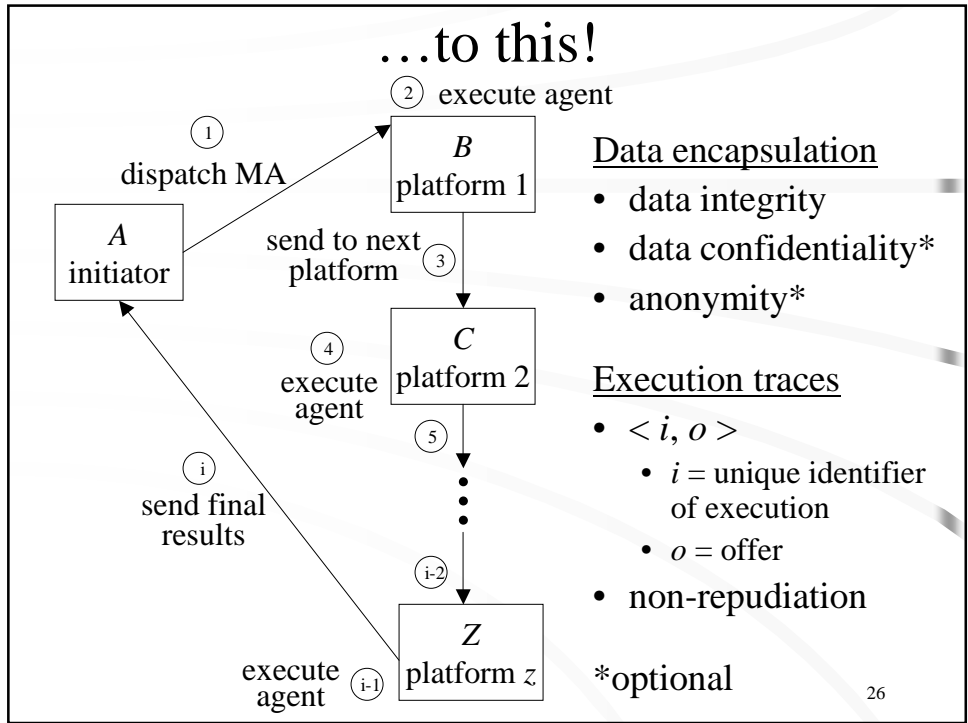
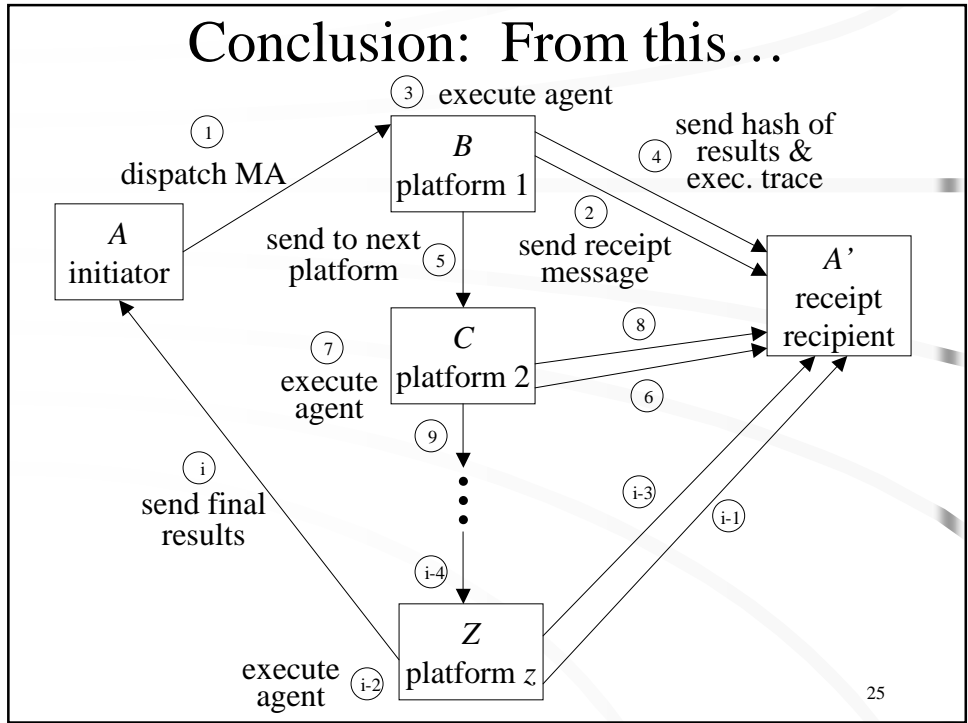


23

## Review

- PVCDSP
  - PKI; data confidentiality; no updating
- CDSFPF
  - PKI; data confidentiality; platform anonymity; no updating
- Chained MAC Protocol
  - no PKI; data confidentiality; no updating
- Data Collection Protocol
  - no PKI; no data confidentiality; no platform anonymity; updating

24



# Questions?

27

## References

- G. Karjoth, N. Asokan, C. Gulcu. "Protecting the computation results of free-roaming agents." *Proceedings of the Second International Workshop, Mobile Agents 98*. Springer-Verlag Lecture Notes in Computer Science 1477, pages 195-207. Springer, 1998.
- Sergio Loureiro, Refik Molva, Alain Pannetrat. "Secure Data Collection with Updates." *Electronic Commerce Research Journal*. 1/2: 119-130. February/March 2001.
- Giovanni Vigna. "Protecting Mobile Agents through Tracing." *Proceedings of the 3<sup>rd</sup> ECOOP Workshop on Mobile Object Systems*. Jyväskylä, Finland. June 1997.

28