Security levels and deliberate/indeliberate protocol attacks

Is the attacker the only trouble?

Stefano Bistarelli

Consiglio Nazionale delle Ricerche - Pisa

Istituto per l'Informatica e la Telematica

Giampaolo Bella

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Lowe attack to the NSPK protocol

Alice

Who is the enemy?

Bob

$1.\ e_{Kc}(Alice, Na)$

$1'.\ e_{Kb}(Alice, Na)$

$2'.\ e_{Ka}(Na, Nb)$

$2'.\ e_{Ka}(Na, Nb)$

$2.\ e_{Ka}(Na, Nb)$

$3'.e_{Kb}(Nb)$

$3.\ e_{Kc}(Nb)$

Yve

Lowe attack to the NSPK protocol

$e_{Kb}(Na, Nb,$ Transfer \$1000 from Alices account to Yve's)

Lowe attack to the NSPK protocol

$e_{Ka}(Na, Nb$, Transfer $1000 from Yves account to Bobs)

Classical view

- The Spy is a specific agent with specific abilities implicitely/explicitely represented

- Tools/Methodologies
  - check the knowledge of the spy at the end of (all) possible protocol sessions

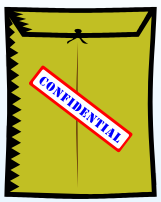
  - Equivalence between systems with/without a spy

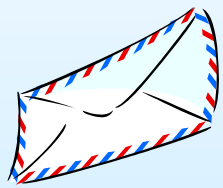
Our view

- All agents involved in the protocol are potential attackers
  - Matching **Imputable** network with the **Policy** Network

Protocol goals with levels

- Confidentiality
- Nonces, Session keys, Private keys, shared keys, …
- each level represents the "cost of loss" of the information
  - Private-confidentiality vs traded-confidentiality
- Authentication
- Usually performed by exchanging secrets
  - Private-authentication vs public-authentication

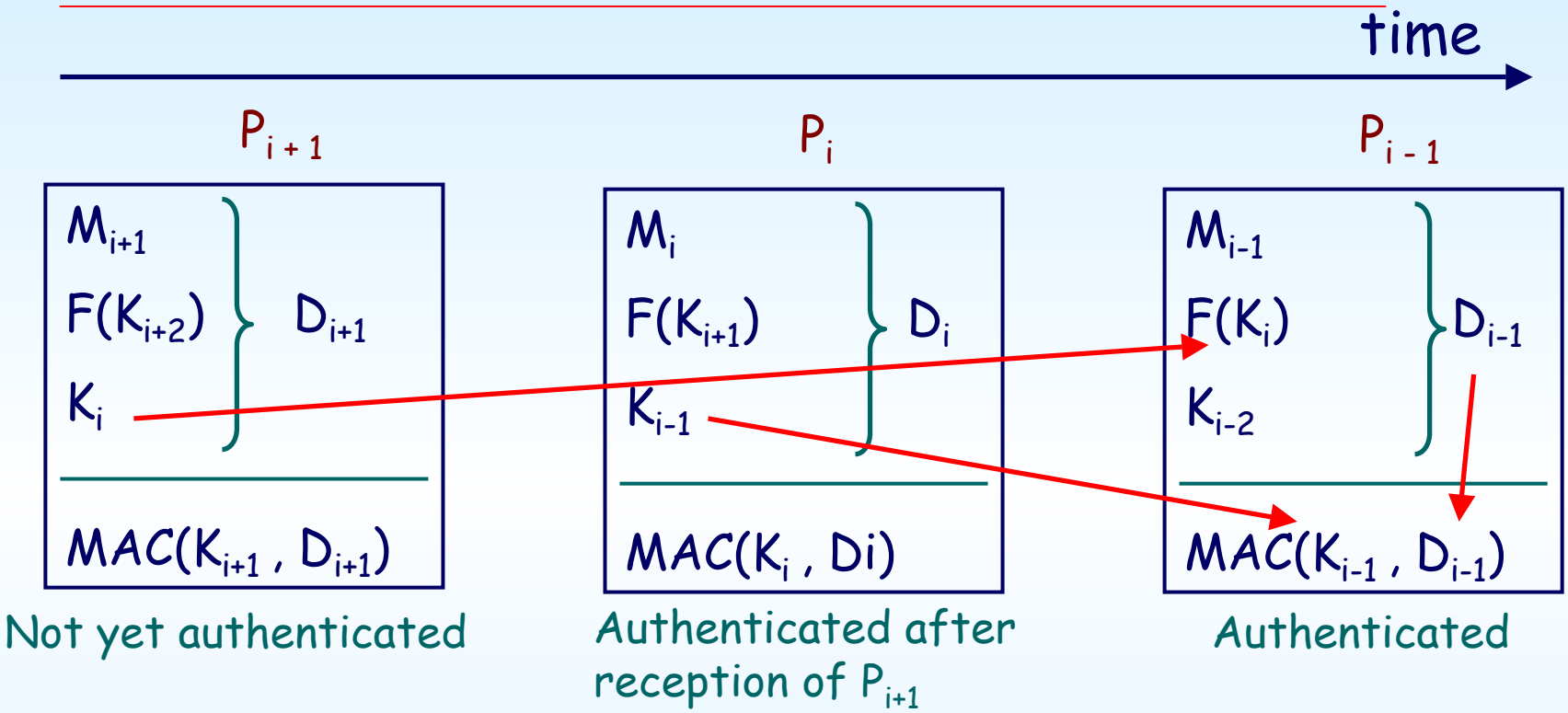




Experience

- Variable security-level encryption
  - Digital cellular telephone encryption (Alanara, Berson US Patent 1997)
- Chaining
  - Kerberos
  - Yahalom
  - TESLA (Multicast authentication over Lossy Channels - Perrig, Canetti, Song, Tygar – 2001)

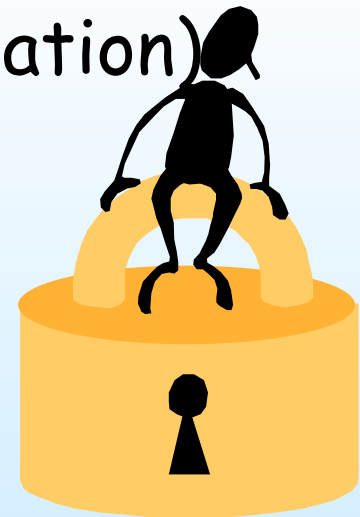
Basic TESLA


time
P_{i+1}
P_i
P_{i-1}
M_{i+1}
$F(K_{i+2})$
K_i
D_{i+1}
$MAC(K_{i+1}, D_{i+1})$
M_i
$F(K_{i+1})$
K_{i-1}
D_i
$MAC(K_i, Di)$
M_{i-1}
$F(K_i)$
K_{i-2}
D_{i-1}
$MAC(K_{i-1}, D_{i-1})$
Not yet authenticated
Authenticated after reception of P_{i+1}
Authenticated

Security levels history

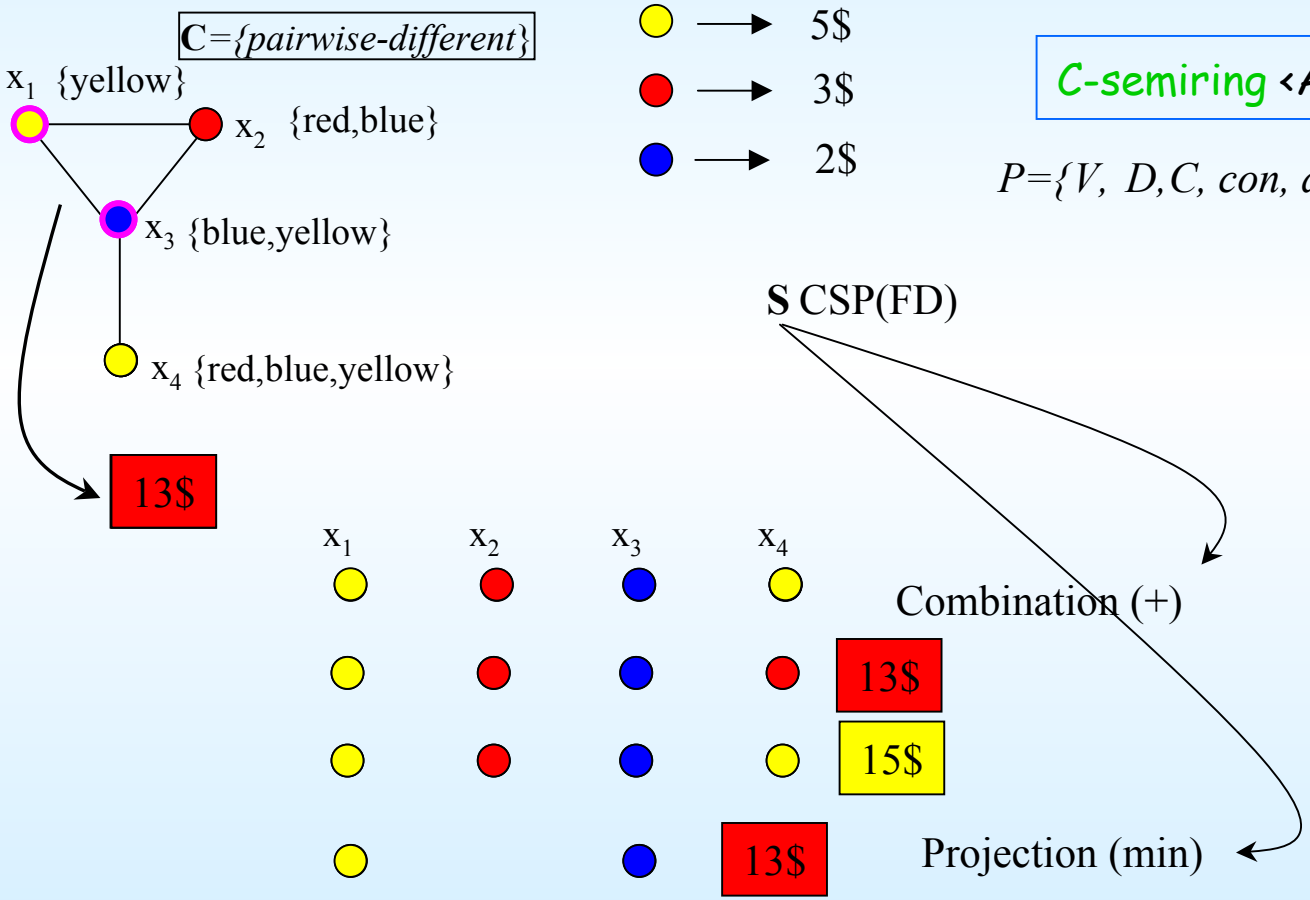
- Bell-LaPadula 1973
- Denning 1976
  - Information Flow (Confidentiality= improper disclosure)
- Biba 1977
  - Data Integrity (improper modification)
- Volpano 1996
  - Information Flow as type system

No explicit notion of cryptography



Check configurations by SCSPs

- SCSP



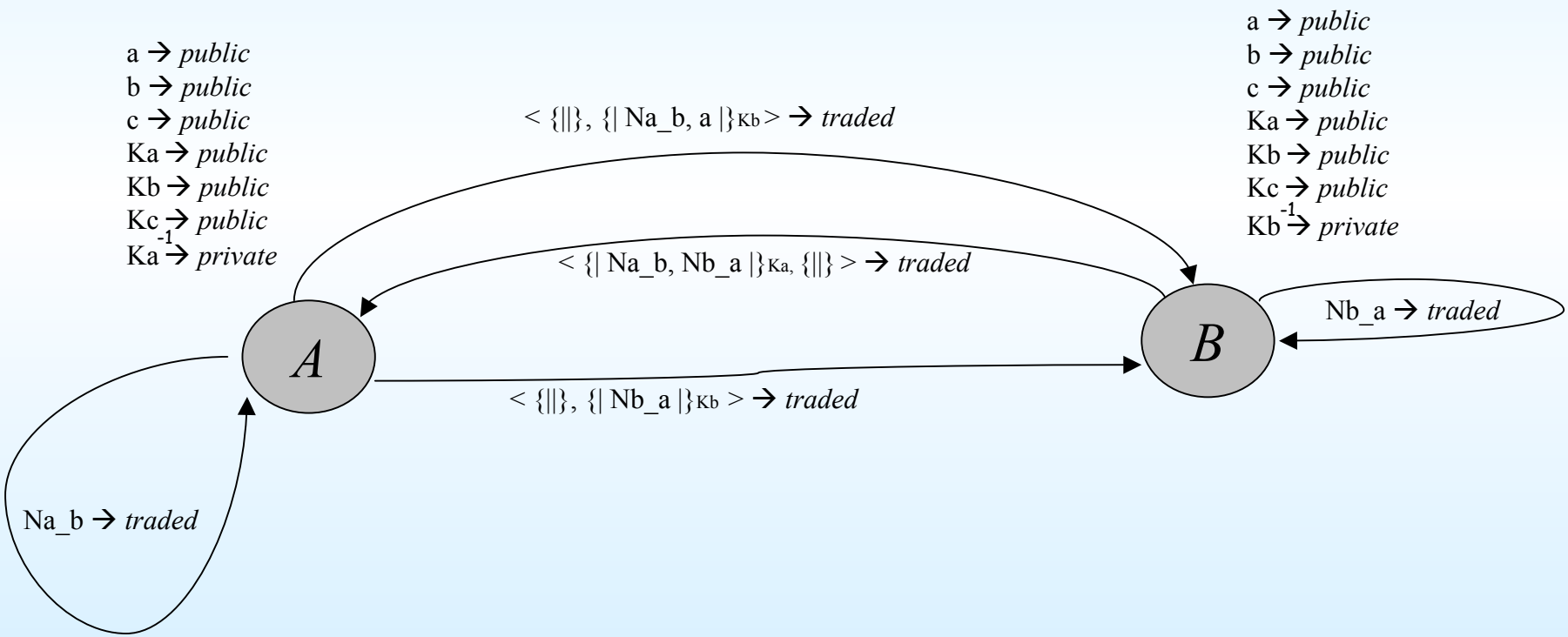
Check configurations by SCSPs

- Network-SCSP
  - V variables (agents)
  - D domain values (messages)
    - represents all agents' knowledge
  - S_{sec} = {L, $+_{sec}$, $\times_{sec}$, *public, unknown*} the security semiring
    - L = {*unknown, private, traded, public*}, set of "*security levels*"
    - $+_{sec}$ yields the *best* and $\times_{sec}$ the *worst* element

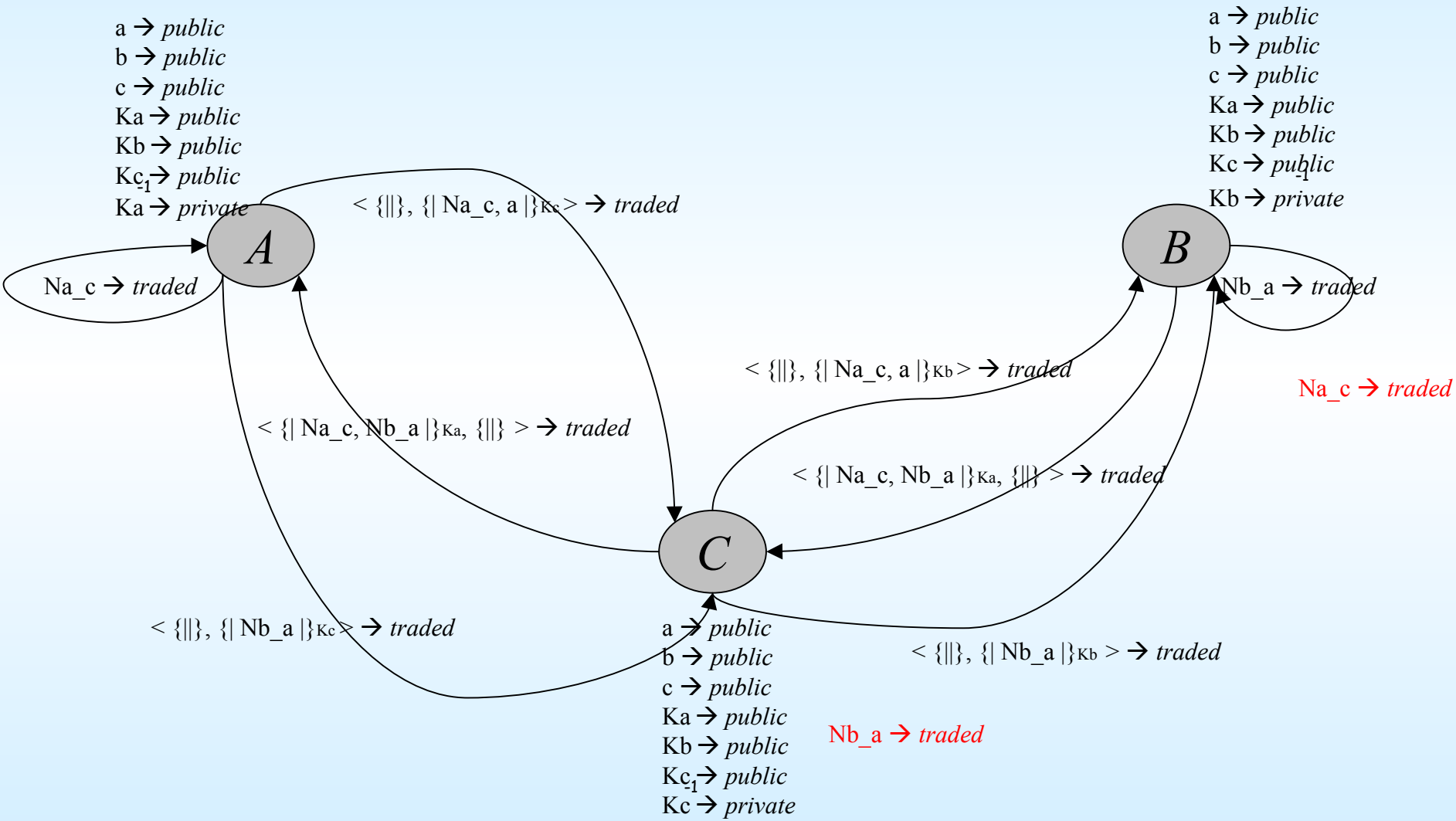
Check configurations by SCSPs

- C Set of constraints defining the
  - Policy CSP
- C' Set of constraints defining the network configuration you want to analyze
  - Imputable CSP
- Attack if the solution of C and C' differ

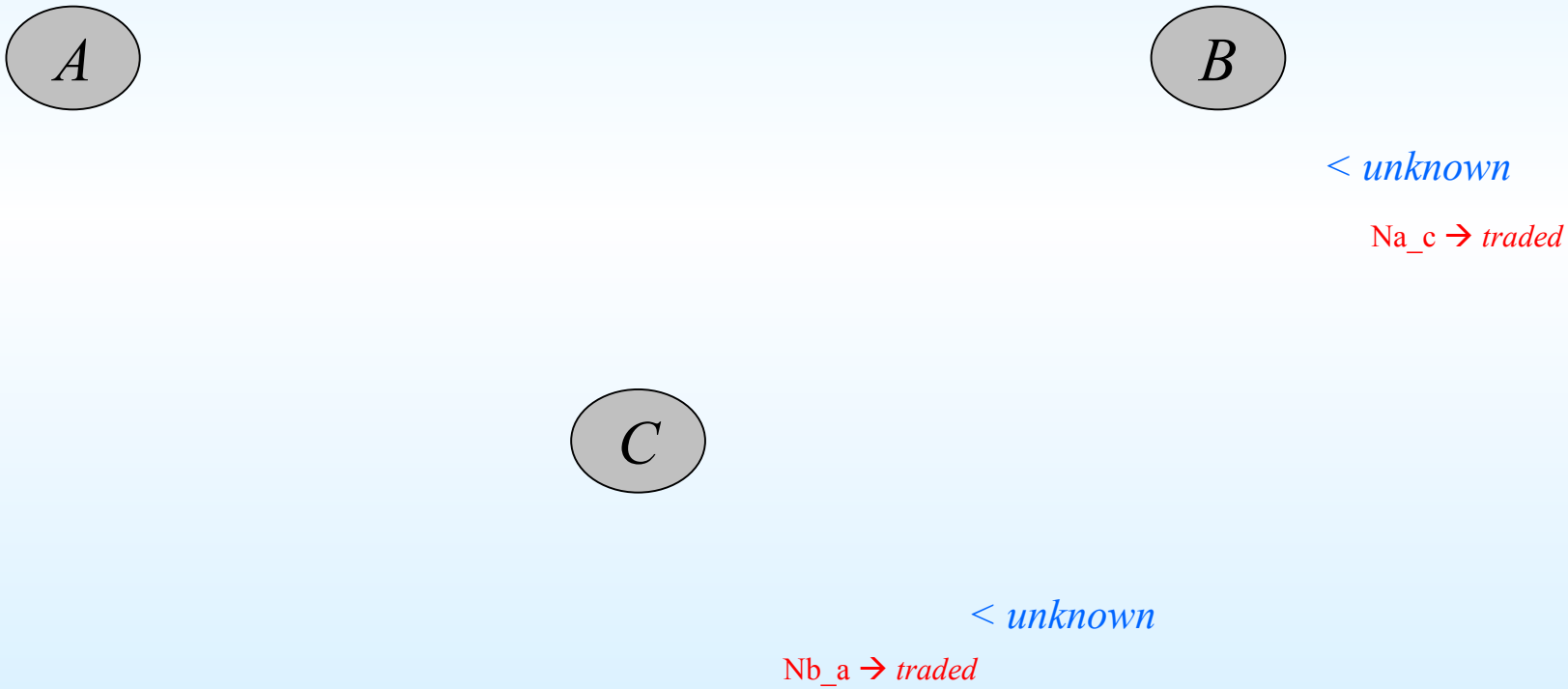
Encoding in SCSP



The configuration corresponding to Lowe's attack



The configuration corresponding to Lowe's attack



"Soft goals" for each agent

- *l-confidentiality*
  - Message *m* is *l-confidential* in *p* iff *def_p(m)* = *l*.
- *confidentiality attack*
  - There is a confidentiality attack on *m* in *p* iff *def_p (m)* < *def_policy (m)*.
- *comparing attacks on m*
  - *Configuration p* bears a *worse* confidentiality attack than configuration *q* on *m* iff *def_p(m)* < *def_q(m)*.
- *comparing protocols with the same aims*

- *A suitable entailment relation* allows message encryption, decryption, concatenation and splitting.
  - Splitting
    - $def(m_1,m_2)=v \mid\!- def(m_1)=v$
  - Concatenation
    - $def(m_1)=v_1, def(m_2)=v_2 \mid\!- def(m_1,m_2)=max(v_1,v_2)$
- relations among levels.
  - Can represent encryption chaining
  - Encryption
    - $def(k)=v_1, def(m)=v_2 \mid\!- def(e(k,m)=max(next(v_1),v_2)$

- Must upgrade security semiring:

  L = {*unknown*, *private*, *traded*$_1$, …, *traded*$_n$, *public*}

- Must upgrade rules for building Policy SCSP

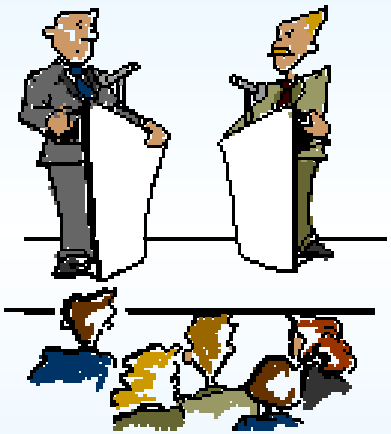
Building the Policy SCSP shows that *A* knows *authK* as *traded*$_1$ and *servK* as *traded*$_3$.

Conclusions and future work

- All the users can deliberately or indeliberately violate the policy
- The danger of each attack is represented as a level
  - Levels for a preliminary analysis
    - Match between protocols with the same aims
- Express more protocol goals
- Interface to model checker
- Improve the solver built in CHR

Questions?

Security levels and deliberate/indeliberate protocol attacks



Is the attacker the only trouble?

Stefano Bistarelli

Consiglio Nazionale delle Ricerche - Pisa

Istituto per l'Informatica e la Telematica

Giampaolo Bella

UNIVERSITY OF CAMBRIDGE

Computer Laboratory