Information hiding: state-of-the-art and emerging trends

Anonymity

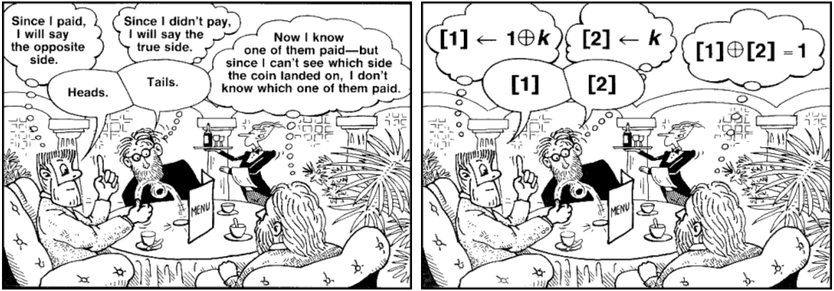
Steve Kremer

LSV, ENS de Cachan, CNRS & INRIA, France

SecCo'07 — Lisboa, Portugal

Introduction: anonymity systems

Classical example: Dining cryptographers (uncondiational anonymity)


Since I paid, I will say the opposite side.
Since I didn't pay, I will say the true side.
Now I know one of them paid—but since I can't see which side the coin landed on, I don't know which one of them paid.
Heads.
Tails.
MENU
$[1] \leftarrow 1 \oplus k$
$[2] \leftarrow k$
$[1] \oplus [2] = 1$
[1]
[2]
MENU

Anonymous channels: MIX-nets, Onion routing/TOR, Crowds, etc.

Idea of a MIX: receive a seqauence of encrypted messages, decrypt and forward a random permutation

Anonymity in applications: anonymous cash, electronic voting

Use of cryptographic primitives such as blind signatures, re-encryption, etc.

Past: definitions based on equivalence

Many informal, natural language definitions

Example: [taken from a classical electronic voting protocol paper]

"Privacy: no participant other than a voter should be able to determine the value of the vote cast by that voter"

First formal definition given in [Schneider, Sidiropoulos 96] (applied to dining cryptographers, possibilistic anonymity)

Idea based on equivalence between processes: permuting identities/actions yields equivalent executions

Process equivalences in other works (modelling cryptographic primitives)

- C. Fournet, M. Abadi: Hiding Names: Private Authentication in the Applied Pi Calculus. ISSS'02.
- S. Mauw, J. Verschuren, E. de Vink: A Formalization of Anonymity and Onion Routing. ESORICS'04.
- S. Kremer, M. Ryan: Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. ESOP'05.

Past: definitions based on knowledge

Use of epistemic logic for defining anonymity

J. Halpern, K. O'Neill: Anonymity and Information Hiding in Multiagent Systems. CSFW'03.

Idea of knowledge: observer has an imperfect view of the system which could correspond to a set of possible executions

An observer knows a property φ if all possible executions consistent with the obervation verify φ

Example of anonymity definition: the attacker does not know that agent A did action c

- Natural, intuitive definitions
- System description less natural than process algebraic approaches
- Cryptographic primitives generally implicit in the notion of imperfect observation
- Tool support?

Past: definitions of probabilistic anonymity

Probabilistic analysis of anonymity

Degrees of anonymity [Reiter & Rubin. Crowds '98]

- Beyond suspicion the real sender appears to be no more likely than any other potential sender in the system
- Probable innocence The real sender appears no more likely to be the originator of the message than to not be the originator, i.e., the probability that the adversary observes the real sender as the source of the message is less than $1/2$
- Possible innocence there is a nontrivial probability that the message was originated by someone other than the real sender

Formal definitions:

- V. Shmatikov: Probabilistic Analysis of Anonymity. CSFW'02.
- J. Halpern, K. O'Neill: Anonymity and Information Hiding in Multiagent Systems. CSFW'03.
- K. Chatzikokolakis, C. Palamidessi: Probable Innocence Revisited. FAST'05.

Past: Measures of probabilistic anonymity

Measuring probabilistic anonymity

Use of information-theoretic measures for probabilistic anonymity

- A. Serjantov, G. Danezis: Towards an Information Theoretic Metric for Anonymity. PET'02
- C. Díaz, S. Seys, J. Claessens, B. Preneel: Towards Measuring Anonymity. PET'02
- K. Chatzikokolakis, C. Palamidessi, P. Panangaden. Anonymity Protocols as Noisy Channels. TGC'06

Present: Application-oriented privacy properties

Application-oriented flavours of anonymity

Example: receipt freeness in electronic voting (the voter cannot break his own anonymity)

- applied pi calculus and observational equivalence: [S. Delaune, S. Kremer, M. Ryan: Coercion-Resistance and Receipt-Freeness in Electronic Voting. CSFW'06]
- definitions based on epistemic logic: [H. Jonker, W. Pieters, Receipt-Freeness as a Special Case of Anonymity in Epistemic Logic, WOTE'06]
- epistemic logic for a simple crypto process langauage and decidability issues: [A. Baskar, R. Ramanujam, S.P. Suresh. Knowledge-based modelling of voting protocols. TARK'07]

Present: Application-oriented privacy properties

Automated verification

Existing state-of-the-art tool: ProVerif (but has limitations)

Symbolic bisimulation techniques for checking observational equivalence (cf talk this morning)

Automated verification of epistemic logics

[A. Baskar, R. Ramanujam, S.P. Suresh. Knowledge-based modelling of voting protocols. TARK'07]

Fundamental issues on probability and non-determinism

Considering both non-determinism and probabilities in a security context may cause problems

[K. Chatzikokolakis, C. Palamidessi. Making Random Choices Invisible to the Scheduler. CONCUR'07]

Future

Languages with tool support for detailed, full-fledged case studies of real systems

- probabilities
- cryptographic primitives (Dolev-Yao style)
- logics for reasoning about anonymity properties

Suggestion: probabilistic applied pi calculus

Suggestions for such case studies:

- MIX-net, onion routing
- Prêt-à-Voter electronic voting protocol

Link with more detailed computational models for anonymity properties