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

Quantified Information Flow

Pasquale Malacaria
(Queen Mary, London)

State-of-the-art

Two main quantitative techniques:

1-Information Theory: *How much information is leaked*.

2-Measuring bisimulation: *How bisimilar two systems are (e.g. DiPierro-Hankin-Wikickli)*.

This talk will expand on Information Theory

State-of-the-art

- How confidentiality is quantified using Information theory: Shannon's Mutual Information *I(A;B)* measure the dependency between r.v. *A* and *B*
- *I(A;B|C)* (conditional Mutual Information) measures the dependency between *A* and *B* given knowledge of *C*
- *I(Secret;Process|Public Input)*=measure of the dependency between the process and the secret given knowledge of the public input = leakage

How Information Theory works

- *P= if (h=0) access else deny*,
- *h* boolean var (uniform distribution). Then 1 bit is leaked:
- *P(h=0) Info(access) + P(h=1) Info(deny)= Entropy(P)= I(h,P|low)*=0.5 1 + 0.5 1 = *1*
- Notice: *P* is not secure (motivation for quantitative analysis)

- *I(Secret;Process|Public Input)* pop out in different contexts to quantify interference (or related notions):
- Gray, Millen, (Abstract Machines)
- Clark-Hunt-Malacaria (Programming Languages),
- Boreale (Process Calculi)
- Chatzikokolakis-Palamidessi-Panangedan (Anonymity Protocols)

- The definition is supported by a "Non interference" theorem:
- *I(Secret;Process|Public Input)=0* ***IFF*** the system is "secure": proved by
- Millen (Abstract machines, 1987)
- Clark-Hunt-Malacaria (programming languages, 2002) ~ Classical non Interference
- Boreale (process algebra, 2006) ~ Abadi Gordon Secrecy

Challenges

- How do we compute leakage in big real world programs?
- How do we integrate quantitative and qualitative security?
- How do we integrate quantitative and databases security (statistical inference)?
- Do quantitative bisimulation and Information Theory measure the same?