Inductive Inference of Security Strategies

Dusko Pavlovic and Christian Janson, with B. Fauser, A. Pinto and M. Yahia

ASECOLAB.org, Royal Holloway, University of London

Problem

- the defenders have to defend all attack vectors
- the attackers only need to attack one attack vector

Impact

- strategic inference will mitigate problems of cyber security
- security-as-science will consolidate its methodss

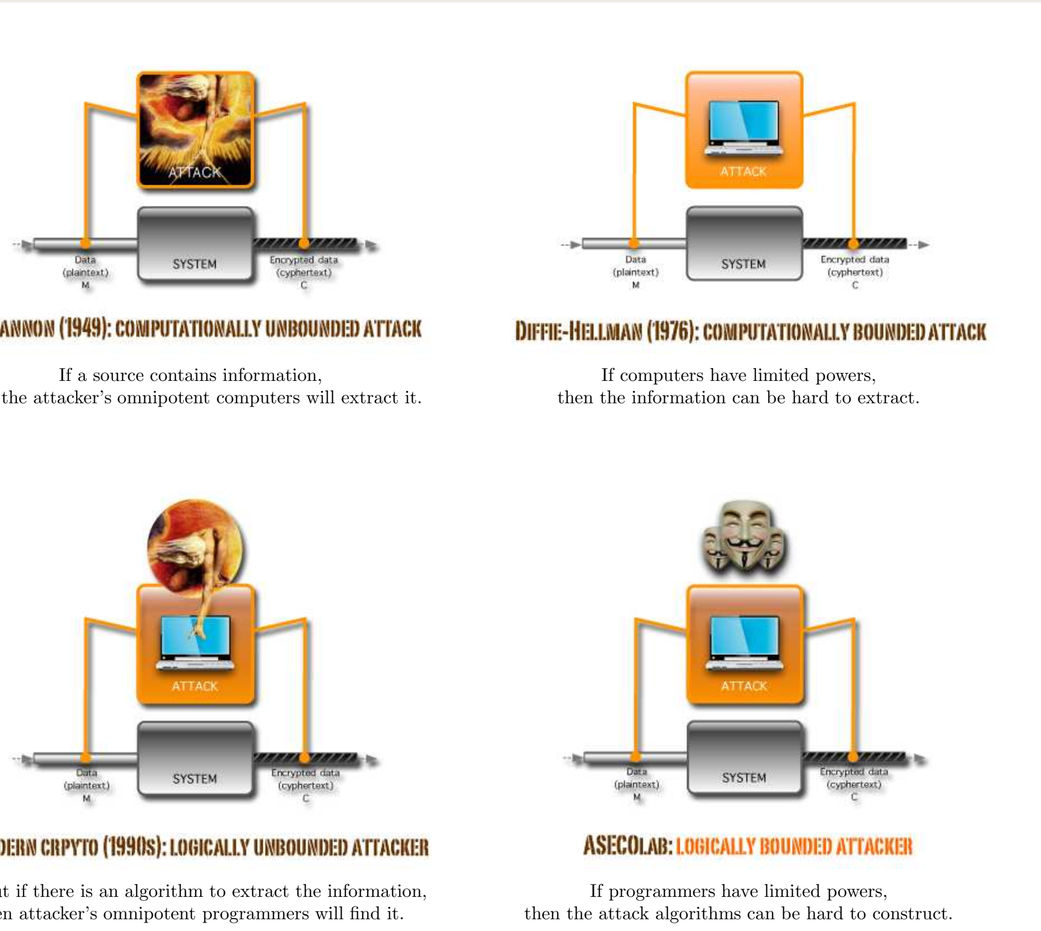
Objective

- build mathematical models to explain this strategic bias
- explore strategies to exploit this bias for defense

Insight:

Security processes follow logics of science

- a design and a security claim can be viewed as a theory
- deployment is an experiment
- an attack disproves the theory
- a theory can never be definitely proved
- a theory can always be disproved by refined experiments



Approach: Epistemic gaming with algorithmic learning

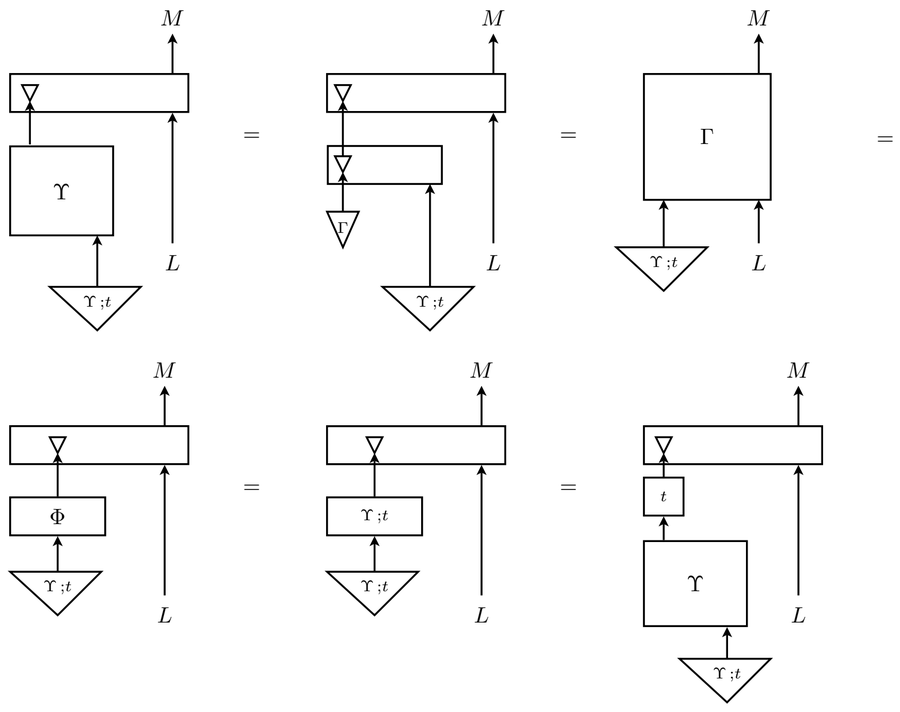
Epistemic game theory of security

- J.Harsanyi, R.Selten, R. Aumann... : games of incomplete information, hierarchies of players' types
- taking into account logical complexity of strategies yields technical simplifications --- and conceptual clarifications

Inductive inference through algorithmic learning

- R. Solomonoff: inductive inference as search for algorithms
- C.H. Bennett: logical depth as time complexity of evolution
- logical complexity = logical depth + Kleene's realizability

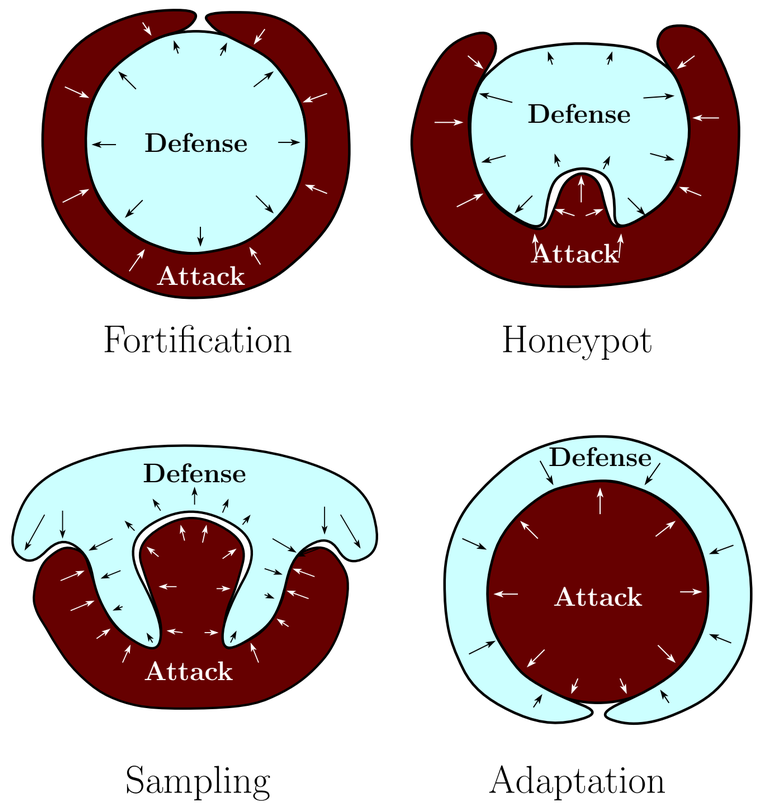
Method: Monoidal computer



Diagrammatic proof of Kleene's Second Recursion Theorem

Paper: Monoidal Computer I, *Information & Computation* (arxiv:1208.5205)

Goal: From static to adaptive security



Paper: Gaming Security by Obscurity, *NSPW 2011, ACM* (arxiv:1109.5542)

2012 Science of Security Community Meeting
Nov. 29-30, 2012
National Harbor, MD
http://cps-vo.org/group/sosmtg

Vote Here