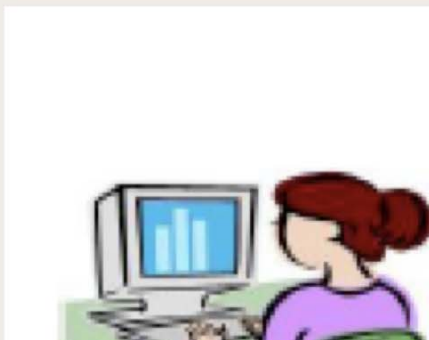


of Protocol

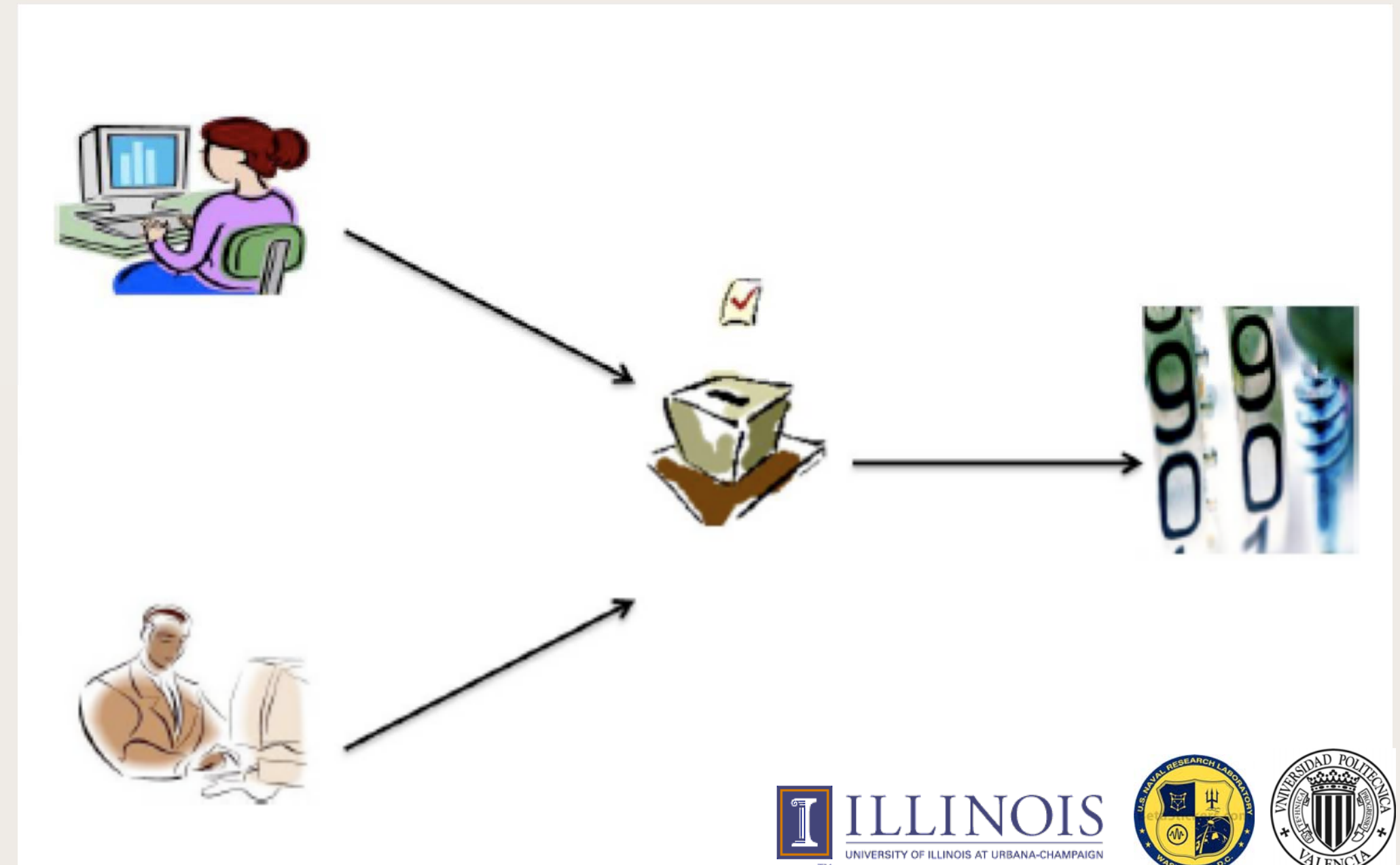
Collaborators: C. Meadows (NRL), and S. Escobar, (UPV)

(expected project start: January 2013)

Project Goals

- Develop the mathematical foundations of protocol indistinguishability, and new methods to automatically analyze indistinguishability properties of privacy-preserving protocols modulo their algebraic theories.
 - Two protocols are *indistinguishable* if an attacker interacting with them is unable to tell the difference.
 - Important for: strong security, resilience against password guessing, privacy preservation, secure cloud computing.
- 

- Indistinguishability *not* a reachability property implies: hard to analyze in Dolev-Yao model.
- **Key insight:** Indistinguishability properties of protocols P_1, P_2 can be reduced to *reachability* properties in the *synchronous product* $P_1 \otimes P_2$ and can be analyzed in Maude-NPA.



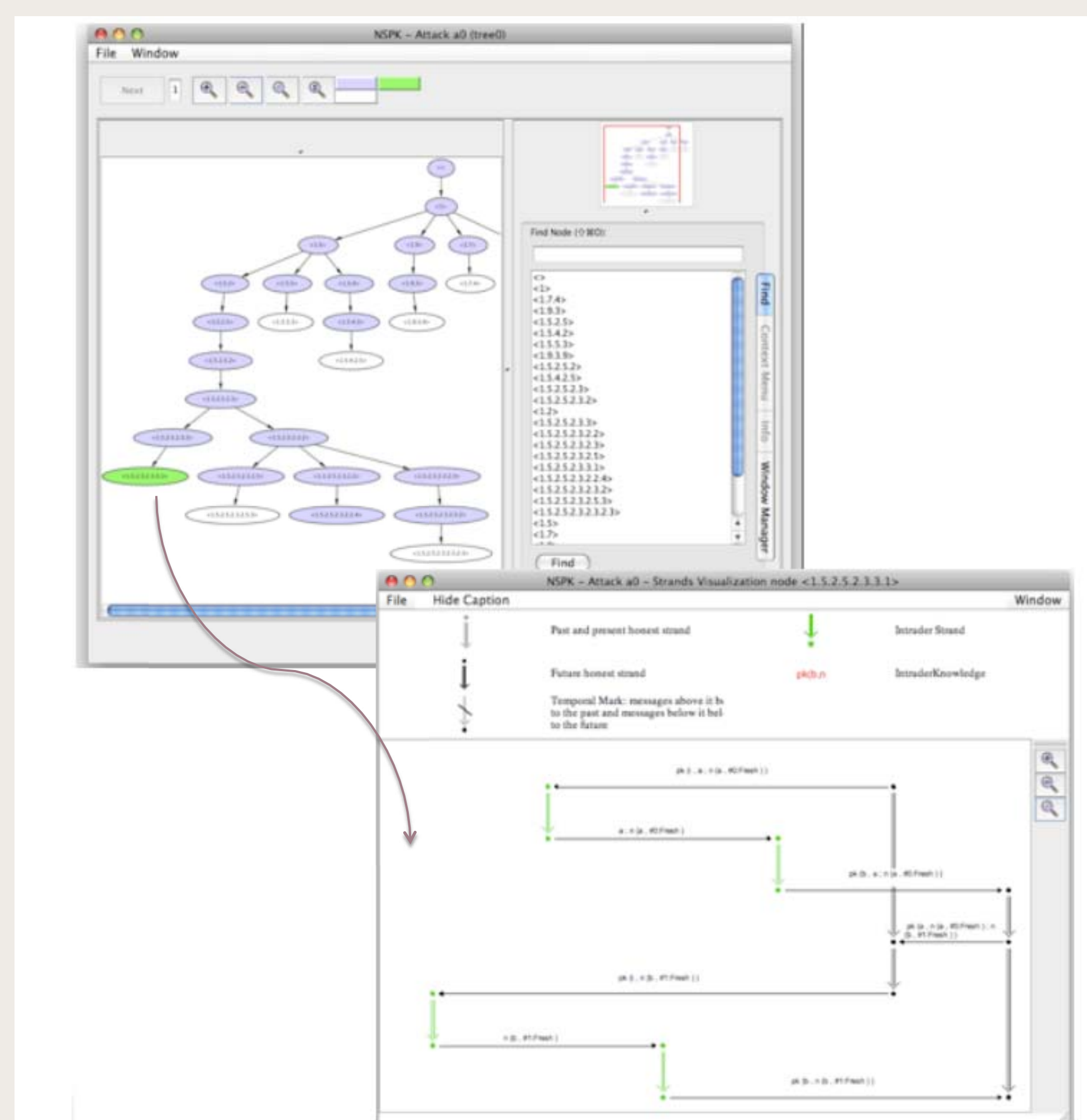
Approach

- Characterize indistinguishability as conjunction of:
 - (i) indistinguishable messages (IM); and
 - (ii) indistinguishable attacker event sequences (IAES).
 - Use synchronous product $P_1 \otimes P_2$ to reduce indistinguishability properties to reachability ones.
 - Relate algebraic properties of protocols P_1, P_2 to those $P_1 \otimes P_2$.
 - First, symbolically analyze failure of IM in Maude-NPA as existence of an attack state.
 - If IM holds, reduce failure of IAES to existence of attack state found by Maude-NPA.
 - Challenge: develop new state-space reduction techniques.

Progress

In current seedling project have:

- Defined synchronous product $P_1 \otimes P_2$.
- Characterized indistinguishability as conjunction of IM and IAES properties.
- Proved that if the algebraic theory of P_1, P_2 has the Finite Variant Property, then that of $P_1 \otimes P_2$ does too.
- Proved that failures of IM or IAES can be characterized as attack states in Maude-NPA.
- Carried out indistinguishability analyses for simple examples.
- Started investigating new state space reduction techniques.



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

