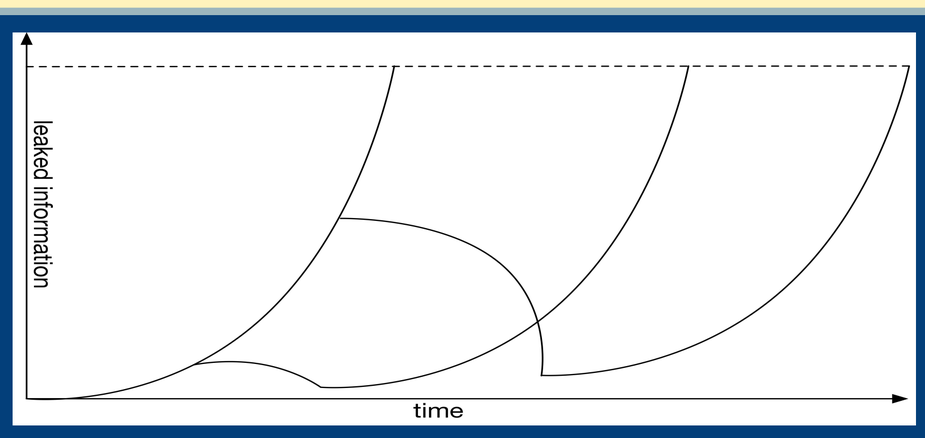
Time-Advantage-Based Key Establishment for Low-Cost Wireless Systems

PIs: Yong Guan and George T. Amariucai (Iowa State University)

The project investigates how the long and uninterrupted time intervals spent in secure environments can be used to create or complement secure key-establishment protocols for low-cost wireless consumer electronics. Such protocols will be used in the absence of a trusted security infrastructure.

The protocols have to

1. Stand alone (not rely on the security of other protocols, like user or machine authentication)
2. Be automatic (not require human intervention).



Information leakage over time and penalty for missed time intervals

Technical Challenges

- Devices have no secure notion of "secure location" − since protocols have to be stand-alone, external notification cannot be used
- Lightweight devices, such as RFID tags, do not have an absolute notion of time.
- Quantifying the information leakage over time not straightforward in the case of standard cryptographic constructs.

Scientific Impact

- Introduces a new paradigm in the context of key establishment: using time as a resource and an advantage;
- Establishes a theoretical framework for the construction and evaluation of general time-based key-establishment protocols.
- Introduces an alternative to physical-channel-based key establishment.
- Creates a building block for the engineering of practical security solutions for low-cost wireless devices.

Approach

Puzzle-based implementation

- Upon key-establishment request, one of the parties produces a (time-varying) secret, and emits clues at regular time intervals.
- If the requestor gathers consecutive clues over a time interval of length ***n***, it can determine the most recent state of the secret.

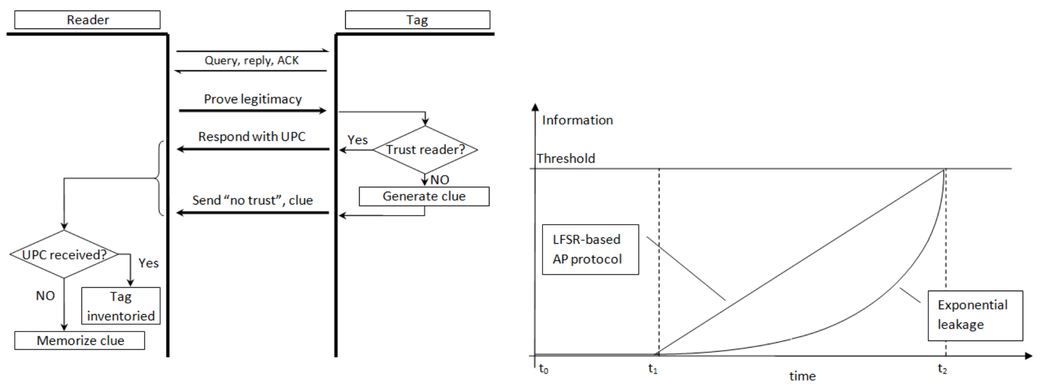
Security

- The protocol has to leak little or no information to an attacker who gathers consecutive clues over many time intervals of length at most ***m***, separated by breaks of length at least ***t*** – we call this (***m***,***t***)-security.

Robustness

- Legitimate requestor is allowed to miss a few clues (small penalty incurred).

An LFSR-based first-order approximation



The Adopted-Pet Protocol for RFID:

- RFID tag runs internal LFSR
- Tag's secret formed by LFSR coefficients
- Clues are emitted upng request
- Tag's responses are throttled
- Implemented using nonlinear combination generator, or shrinking generator

Theoretical requirements:

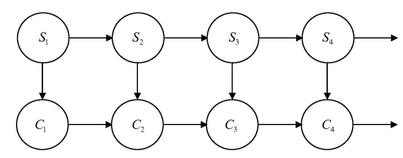
1. Same information leakage profile regardless of starting point: H(S|C1)=H(S|C2)=⋯
2. Super-linear leakage:

   H(S|C1)-H(S|C1,C2)>H(S)-H(S|C1)

This implies that P(c2|s,c1) is not multiplicative, i.e. one cannot write P(c2|s,c1)=R(c2,s)Q(c2,c1). So every new clue has to depend both on secret and on old clues

Current directions

1. An algebraic approach based on clues and masks shared between multiple clues
2. A statistical approach based on a general Hidden Markov Model.



Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

IOWA STATE UNIVERSITY