IOWA STATE UNIVERSITY

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

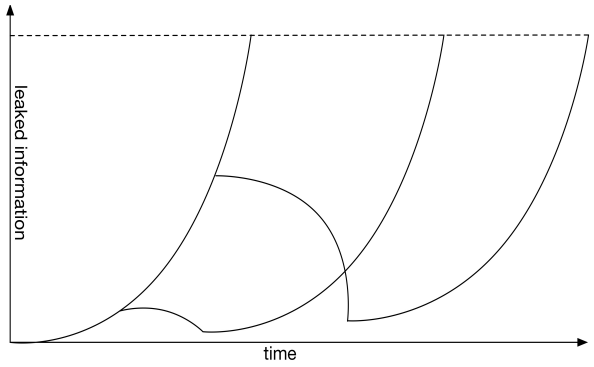
Challenge:

- Use long and uninterrupted time intervals spent in secure environments to create or complement secure key-establishment protocols for low-cost wireless consumer electronics.

Solution:

Puzzle-based approach:

- One party produces a (time-varying) secret, and emits clues.
- If other party gathers enough consecutive clues, it can determine the most recent state of the secret.



Information leakage over time and penalty for missed time intervals

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.

Broader Impact:

- Will apply to a broader spectrum of applications, from military to consumer electronics.
- Direct impact on two graduate courses at ISU.
- ISU's Security Summer Camp for teachers.

CNS 1527579
Iowa State University
George T Amariucai, gamari@iastate.edu
Yong Guan, guan@iastate.edu