Towards Stronger and Verified Security for Real-World Cryptography

Challenge:

- Many real-world cryptographic schemes only have weak or no security guarantees.
- This either indicates a limitation of analysis, or suggests an actual vulnerability.

Solution:

- Break NIST standards for encrypting credit card numbers.
- Develop better analysis:
  - GCM encryption in TLS.
  - NIST standard CTR-DRBG.
  - Streaming encryption in Google's Tink library.

NSF CRII 1755539
Viet Tung Hoang, Florida State University
tvhoang@cs.fsu.edu

Attacks on NIST encryption standards

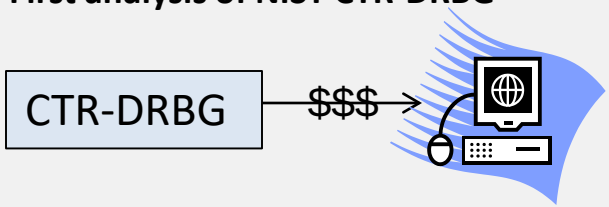
FF1

FF3

Better bounds on encryption in TLS

GCM

First analysis of NIST CTR-DRBG



Scientific Impact:

- The FF1/FF3 standards were revised due to our attacks.
- The analysis of GCM, Google's Tink library, and CTR-DRBG give theoretical assurance to their widespread usage.

Broader Impact:

- Several companies have been patching their products due to our attacks.
- The crypto course at FSU has been revised to have both theoretical rigor and practical skills to break bad designs.