SaTC: CORE: Small: API-centric Cryptography

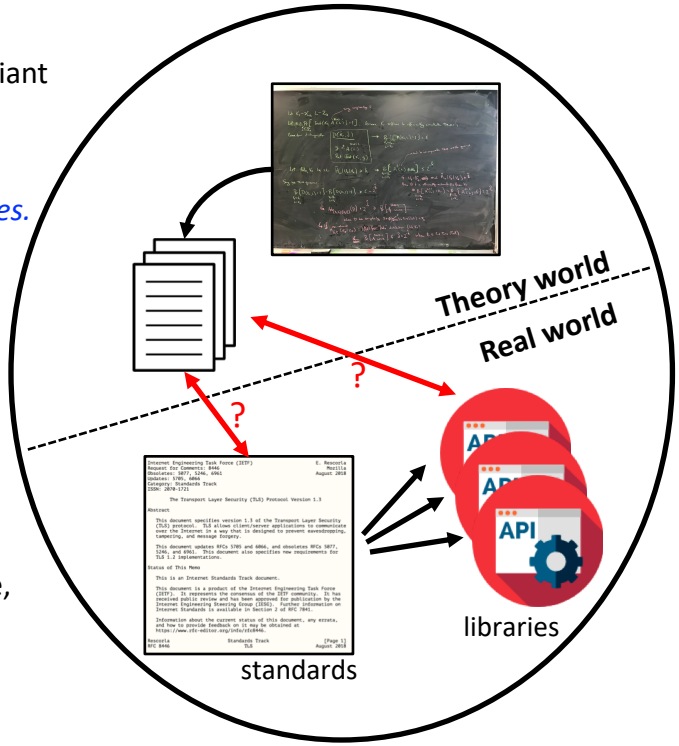
Challenge:

Cryptographic “syntax” ≠ real-world API.

Real-world standards only *partially* specify compliant implementations.

APIs have long lifetimes, can’t be changed easily.

Crypto theory largely fails to address these realities.



Scientific Impact:

Increased confidence in connection between theory and what’s actually being implemented.

More API-like syntax may lead to fewer misunderstandings, mistakes translation to practice.

Raise awareness among theoreticians of implicit biases (“just change the API”) and interesting/impactful new directions.

Solution:

Study real APIs/standards to surface, characterize, quantify mismatches with theory.

Revisit crypto theory with mindset that theory is flexible, APIs aren’t.

Try to make cryptographic syntax ≈ real APIs.

Formalize security notions for “partially specified” protocols/primitives, and for attacks that may use a shared underlying API.

Broader Impact:

Easier to implement and use correctly, smaller attack surface.

Help standard-writers to identify what is safe(r) to leave unspecified.

Theory may be easier for students to grasp, if it looks more like real code/libraries

NSF award 1816375
Thomas Shrimpton
teshrim@ufl.edu