CAREER: Lightweight and Fast Authentication for Internet of Things – CNS 1652389 (2017-2022)

PI: Dr. Attila A. Yavuz, **Email:** attilaayavuz@usf.edu
Webpage: http://www.csee.usf.edu/~attilaayavuz/

Research Challenges

(I) Resource-limited IoTs need low crypto overhead, scalability and non-repudiation, but existing methods are unscalable or costly. **How to *create lightweight digital signatures for resource-limited IoTs?***

(II) Delay-aware IoTs (e.g., smart-grid) need real-time authentication, but existing methods might be slow. ***How to create fast digital signatures for delay-aware IoTs?***

(III) ***How to efficiently enhance the privacy in IoTs with authentication and integrity?***

Scientific Impact

20 intellectual merits and several open-source cryptographic framework:

- **4** delay-aware signatures
- **2** lightweight PKC frameworks
- **2** signer near-optimal signature schemes
- **2** lattice-based public key searchable enc.
- **3** symmetric searchable enc. schemes
- **2** ORAM schemes
- **2** location-privacy frameworks
- **3** patents
- **10+** open-source cryptographic frameworks

Solutions

New Delay-Aware Signatures

- Create fast signatures by exploiting special encodings, homomorphic one-way functions and pre-computation techniques

- **~100x** faster signing
- Improved side-channel resiliency

- Intellectual Merit:
  - CEDA [IEEE CNS'18],
  - Tachyon [ACM CCS'18],
  - ARIS [IEEE ICC'19],
  - FAAS [FC'19]

New Lightweight Signatures and PKC Frameworks

- Algorithmic improvements, pre-computation and optimized EEC-based techniques for minimum energy consumption

- **~7x-35x** less energy usage
- High scalability

- Intellectual Merit:
  - Dronecrypt [Milcom'18]
  - PKCFramework [IoT Wkps'18]
  - ESEM [IEEE CNS'19]
  - SEMECS [IEEE TSC'19]

New Privacy Enhancing Technologies

- Novel PEKS, searchable encryption, ORAM and location privacy methods with authentication and integrity

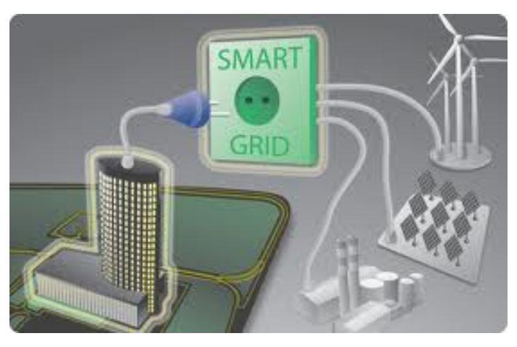
- **10x-200x** lower delay
- High-security and access control

- Intellectual Merit:
  - S3ORAM [ACM CCS'17],
  - PEKS [DBSec'17, IEEE TDSC'18],
  - DSSE [IEEE ICC'18]
  - TrustSAS [IEEE INFOCOM'19]
  - IM-DSSE [IEEE TSC'19]
  - OMAT/OTREE [IEEE TCC'18]
  - Loc-PIR [IEEE TCCN'19]

Broader Impact

- Improving national security by enhancing the security of Internet of Things
- Broader impact on a vast range of application domains:

Energy Delivery Systems



Cloud Computing

Wireless Systems

Autonomous Vehicles

Medical IoTs

- Educational and Outreach Activities
  - The research has been integrated into course modules with 4 different cyber-security courses
  - REU research activities for underrepresented students
    - NSF Bulls-EYE (2 students), USF WICSE (1 student), FG-LSAMP (1 student)
    - CodeBreakHERS STEM Summer Camp for high-school students
      - https://www.codebreakhers.org

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting) October 25-29, 2019 I Alexandria Virginia