Thesis topics

Paul Walther

07.02.2020
General scope: Physical Layer Security

- Wireless Network Security
  - Classical Encryption (Computational Security)
    - Symmetric Encryption
    - Asymmetric Encryption
  - Physical Layer Security (Information-Theoretic Security)
    - Keyless Security
    - Secret Key-Based Secrecy
General scope: Physical Layer Security
Channel Reciprocity based Key Generation

Wireless Network Security

Classical Encryption (Computational Security)
- Symmetric Encryption
- Asymmetric Encryption

Physical Layer Security (Information-Theoretic Security)
- Keyless Security
- Secret Key-Based Secrecy
Soft decision ECC for Information Reconciliation
PLS/CRKG

**Reciprocal measurements** do have **slight differences**
Currently removed in Information Reconciliation after Quantization

**ECC codes** can work with **real valued data**

**Tasks:**
- Implement appropriate soft decision ECC code
- Realize reconciliation with existing measurements
- Compare metrics against hard decision baseline
Secure Key Bit Analysis for Channel Model Attack

**PLS/CRKG**

**Attack CRKG** by *precalculation* of transmission properties

**Analysis** regarding *impact* on resulting key material

**Analytical approach:**
- Calculate Mutual Information

**Tasks:**
- Select appropriate feature extraction approach
- Apply to measurements and simulation data
- Evaluate regarding Mutual Information
Secure Key Bit Analysis for Channel Model Attack
PLS/CRKG

**Attack CRKG** by **precalculation** of transmission properties

**Analysis** regarding **impact** on resulting key material

**Practical approach:**

Compare resulting keys

**Tasks:**

- Select and implement processing steps
- Apply to measurements and simulation data
- Compare resulting key material
Attacking CRKG with Machine Learning

PLS/CRKG

Use ML to represent **room structure**

**Regression to mean** of AB/BA

Input passive measurements

Only „rough“ matches needed for success

**Tasks:**

- Design appropriate learning model
- Train with synthetic data and/or measurements
- Evaluate with measurements regarding reciprocity/secure key bits
EVK measurements
PLS/CRKG

Impulse Responses deliver more entropy than RSSI
UWB development platform to gather reciprocal measurements

Tasks:
- Modify SDK examples for CRKG protocol
- Perform measurements
- Evaluate regarding reciprocity
Implementing/Evaluating the Whips MAC scheme

**Stateful MAC** scheme based on PRF
Increasing security, varying security levels and resynchronization capabilities

**Tasks:**
- Design evaluation of varying security levels
- Implement MAC scheme in defined use cases
- Evaluate performance and security guarantees