Snooping Pay-over-the-Phone Transactions over Encrypted 5G/4G Voice Calls
Jingwen Shi*, Shaan Shekhar*2, Guan-Hua Tu1, Chunyi Peng2
*Equal contribution 1Michigan State University 2Purdue University

**Attack Overview**

Snooping Pay-over-the-phone (PoP) transactions in the air
- **Normal use scenario:** UE (say, a mobile phone) calls an Interactive Voice Response (IVR) system and makes a credit/debit card transaction to pay a bill.
- **Attack:** deploy a **radio sniffer only** to infer such sensitive and confidential payment transactions

---

**Attack Solution**

- **Detecting 5G/4G voice calls over encrypted traffic**
  - **Tiny packets (≤13 bytes) only in voice,** not other traffic
  - **Ironically, due to 5G/4G enhancement techniques**
    - Adaptive speech codec (AWR): lower rate for noise
    - Comfort Noise (CN): background noise in the silence to make the other party hear something and avoid call termination
    - Robust Header Compression (RoHC): compress very small PDCP packets that carry voice calls
  - **Detecting IVR calls using IVR-specific fingerprinting**
    - DTMF-like tone: very brief, different from human speech
    - Primarily one-way traffic: IVR talks and human listens
    - Purpose-specific call patterns: depending on IVR menu
  - **Detecting PoP transactions over payment-specific patterns**
    - Credit/Debit Card Number (15 -- 16 digits)
    - Expiry Date (4 digits)
    - Security Code (CVV) (3 – 4 digits)
    - Zip Code (5 – 9 digits)
    - Note: each digit creates one DTMF tone (one key touch)

---

**Attack Evaluation**

- **Ethics: all in controlled experiment (victims all owed by us)**
- **1000 radio traces from 30 companies**
  - LSTM + CNN: >93% accuracy (except cut-off)

---

**Contact Faculty**

Chunyi Peng (CS)
chunyi@purdue.edu

Know more about the MSSN Lab (Mobile System, Security and Networking)