CERIAS

The Center for Education and Research in Information Assurance and Security

Snooping Pay-over-the-Phone Transactions over Encrypted 5G/4G Voice Calls

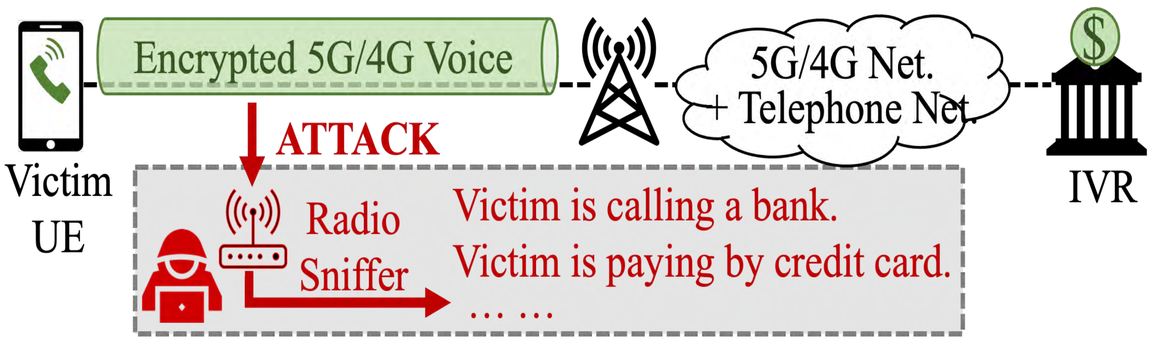
Jingwen Shi*[1], Shaan Shekhar*[2], Guan-Hua Tu[1], Chunyi Peng[2]

*Equal contribution [1] Michigan State University [2] Purdue University

Attack Overview

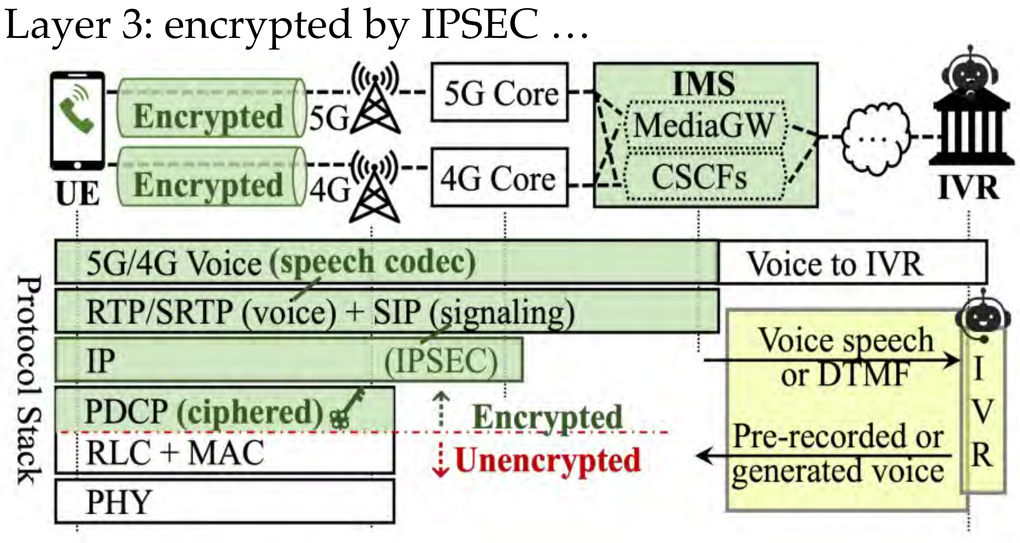
Snooping Pay-over-the-phone (PoP) transactions in the air

- **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

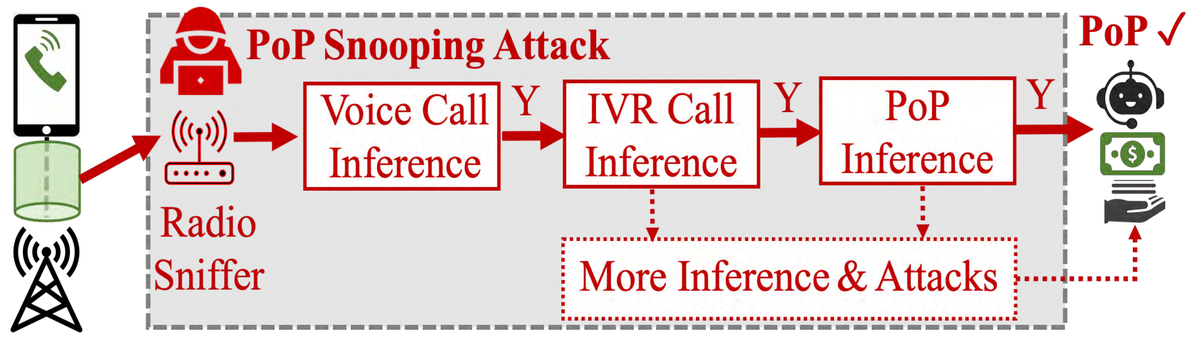


Not far from real threats …

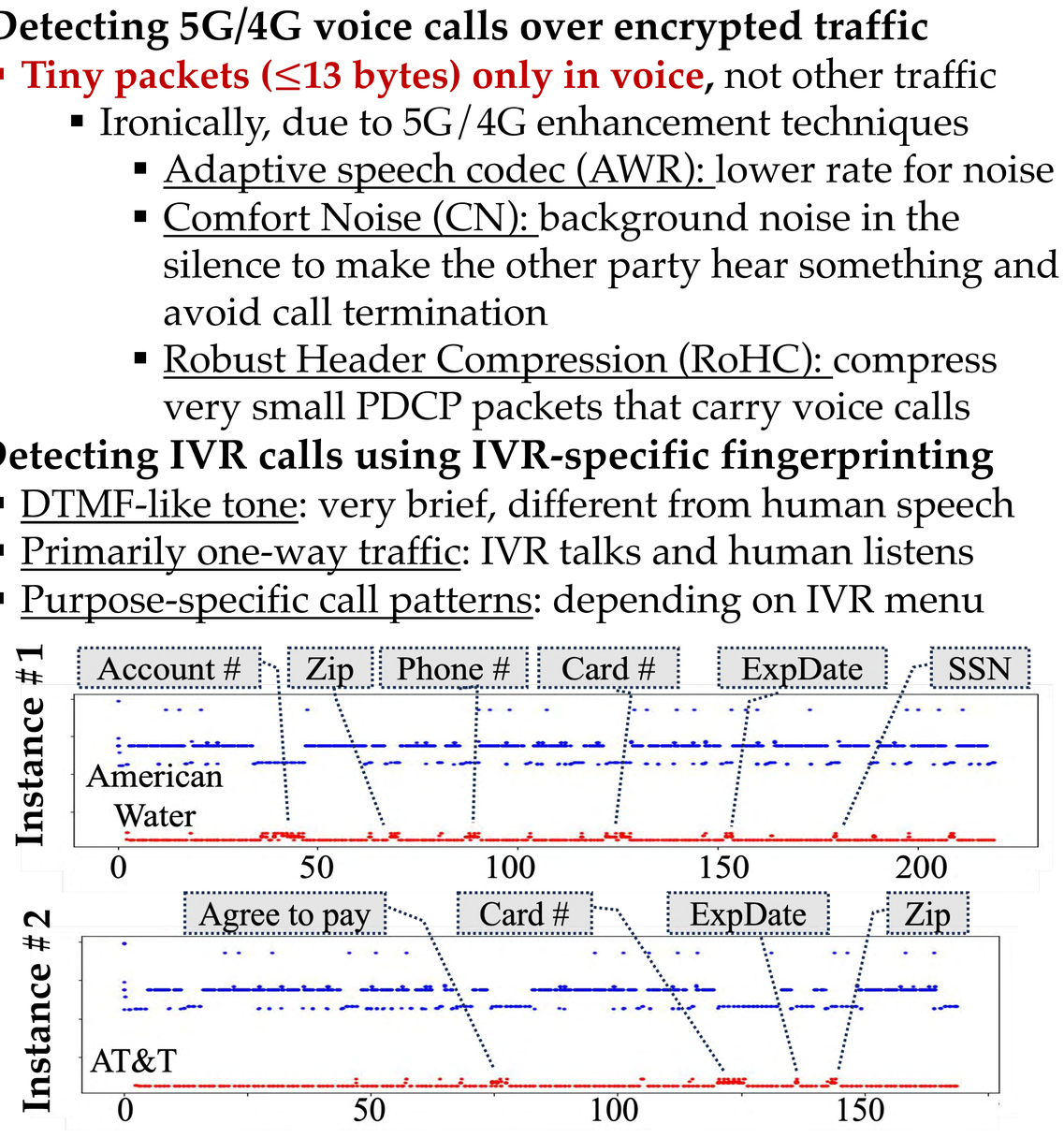
- **100% contactless, ready to launch now**
  - No access, comprise or malwares on UE, 5G/4G NET, IVR
  - Many attack scenarios:
    - Snooping students, staffs and professors @LWSN
    - Snooping neighbors @home
    - Snooping customers @mall/Starbucks …
    - …
- **Unexpected, despite encryption protection in 5G/4G**
  - Authentication and key agreement (AKA)
  - Layer 2: ciphered by PDCP
  - Layer 3: encrypted by IPSEC …



Attack Solution

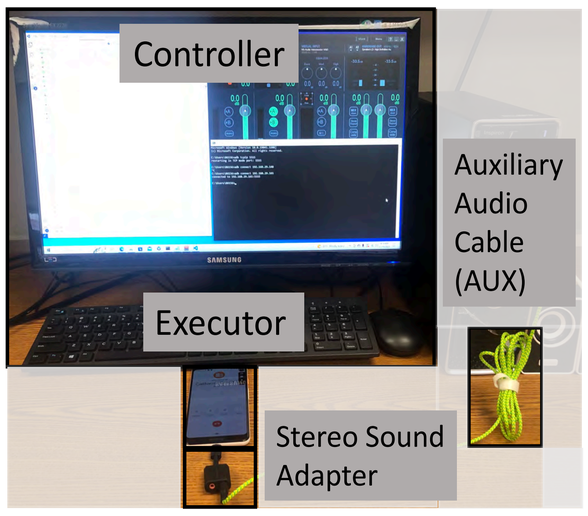


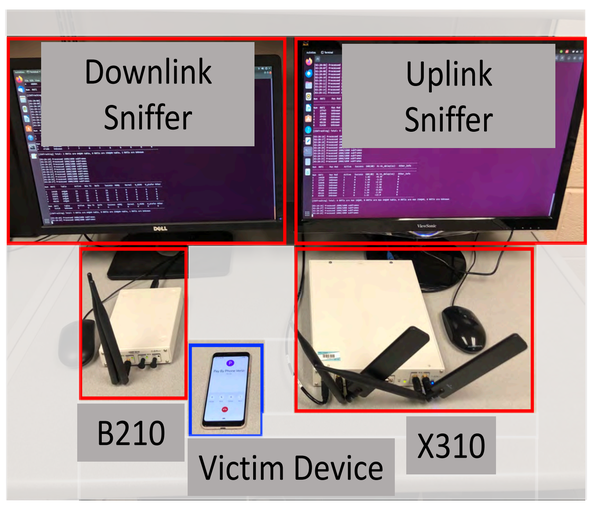
- **Detecting 5G/4G voice calls over encrypted traffic**
  - **Tiny packets (≤13 bytes) only in voice**, not other traffic
    - Ironically, due to 5G/4G enhancement techniques
      - Adaptive speech codec (AWR): lower rate for noise
      - Comfort Noise (CN): background noise in the silence to make 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)

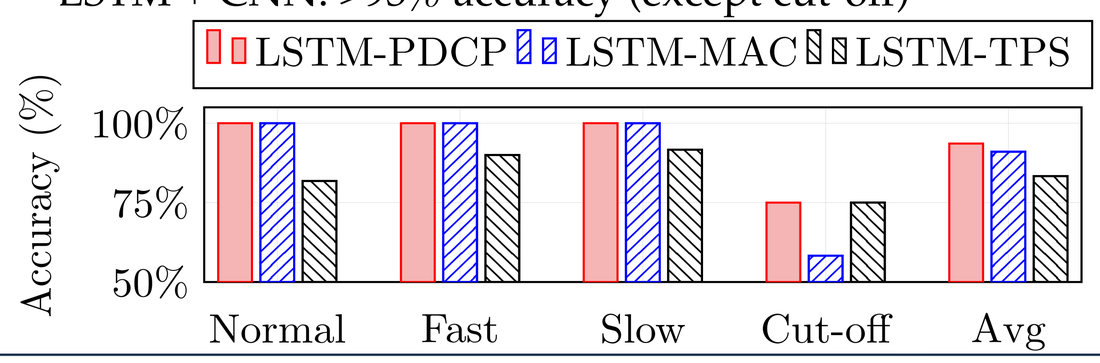




(a) Training (data collection) (b) Launching the attack

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)



PURDUE UNIVERSITY

Contact Faculty
Chunyi Peng (CS)
chunyi@purdue.edu

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

CERIAS