1. Problem Scenario

Analyzing encrypted WLAN traffic

Passively Capture WLAN traffic

1. User’s online activities
2. Type of Apps Usage
3. Launching event of an app

2. Challenges & Motivation

- Mobile app typically has a more focused objective – something with a single functionality.
- User runs many sensitive apps in their mobile devices.
- Each app has unique frame size interaction sequence – application DNA.

STUDY ON HEALTH SECTOR:
1. Clinicians use 6.4 mobile devices per day on average.
2. 66% doctor use tablets for medical purpose.
3. 70% physician use smartphone to research medication at least once a week.

Mobile devices can be easily compromise.

3. Design Principle

- TRANSPARENT to the client and the server side of the apps.
- FLEXIBLE and CONFIGURABLE to the user or the network administrator.
- COMPATIBLE with the existing Off-the-shelf mobile devices.
- EFFICIENTLY hide the wireless traffic at the edge of the network.

4. System Components

Scheduler can create artificial delay of the traffic flow by controlling the start/stop dequeueing of the packet.

We develop the scheduler with two linux multiq qdisc, one for normal apps and other for sensitive apps.

Flow Manager is a software OpenFlow switch that direct traffic flow of sensitive apps to the proper qdisc.

We extend the Flow Manager to provide traffic shaping actions: padding, aggregating, and splitting, in addition with IPsec, GRE tunnel.

5. Methodology

- Initially, the hand-shaking happens between the agents in the mobile device and the AP/controller.
  - Define per-flow/per-app traffic actions.
- The agent in the mobile device uses OpenFlow protocol to add actions in OVS for securing sensitive app's traffic flows.
  - Apply IPsec, GRE, traffic shaping.
- The agent in the AP/Controller apply reverse actions in OVS to retract the original packet.

6. Evaluation

We can identify the app with at least 90% accuracy by looking at the initial frame interaction sequence.

IMPLEMENTATION
→ We extend the OVS kernel Datapath for new action of padding random bytes at the end of the packet.
→ We use IP option header to encode the padding information in the IP packet.
→ We randomly select the packet of a flow for applying the padding action.

Randomly padding to 80% of the packets reduces the app identification accuracy to 70%.

7. Future Work

- Analyzing the network and computation overhead.
- Impact on user's QoE or app performance.
- Evaluation of securing the sensitive app's traffic flow and its content.
- Maintain the QoS of the traffic flow.