Northeastern University
Khoury College of
Computer Sciences

On the Security and Privacy of Wireless Systems: Threats and Some Defenses

Guevara Noubir

Northeastern University

Boston Cloud Connect Summit

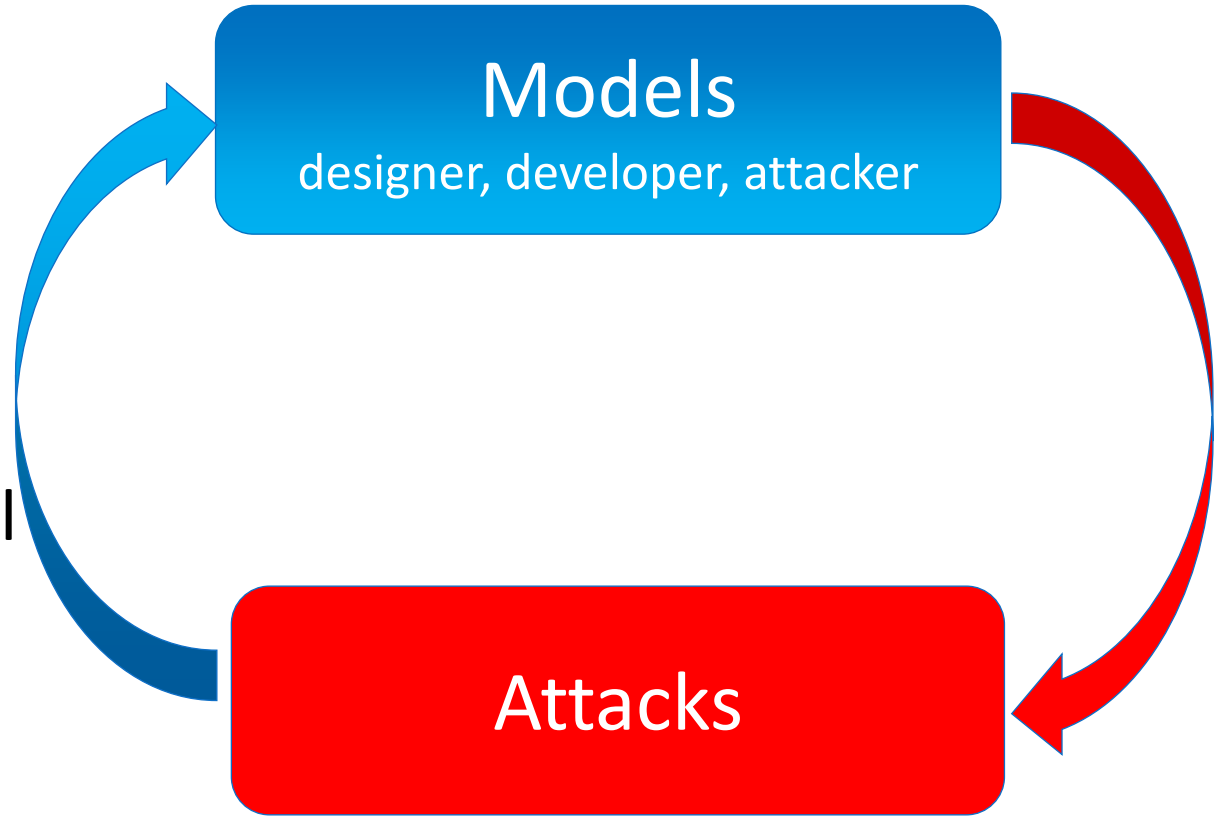
November 7, 2024

Outline

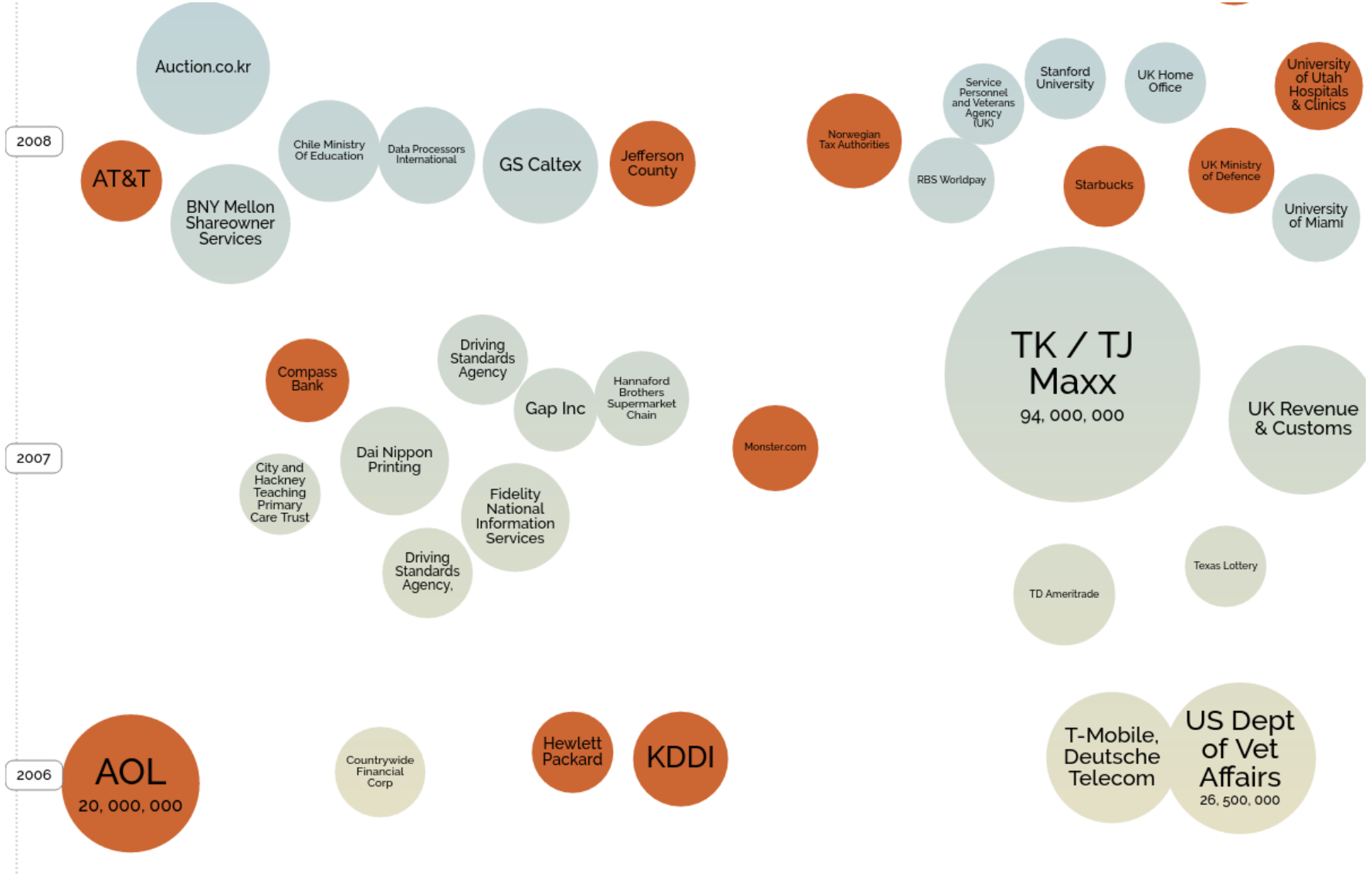
- Security Cycle: Academia vs. the Real-World
- Three examples of attack types
  - IoT devices
  - Mobile devices/apps: side-channels and zero permission attacks
  - Wireless systems: tracking, traffic analysis, MITM, and denial of service
- Discussion of threats and defenses

Security Cycle: Largely Reactive

- Model with assumptions, proof?
- "Attacker" escapes the model
  - and demonstrates feasibility of attacks
- Ideally a fix that accounts of potential future attacks
- Academia vs. industry
  - This cycle might project differently on the real world

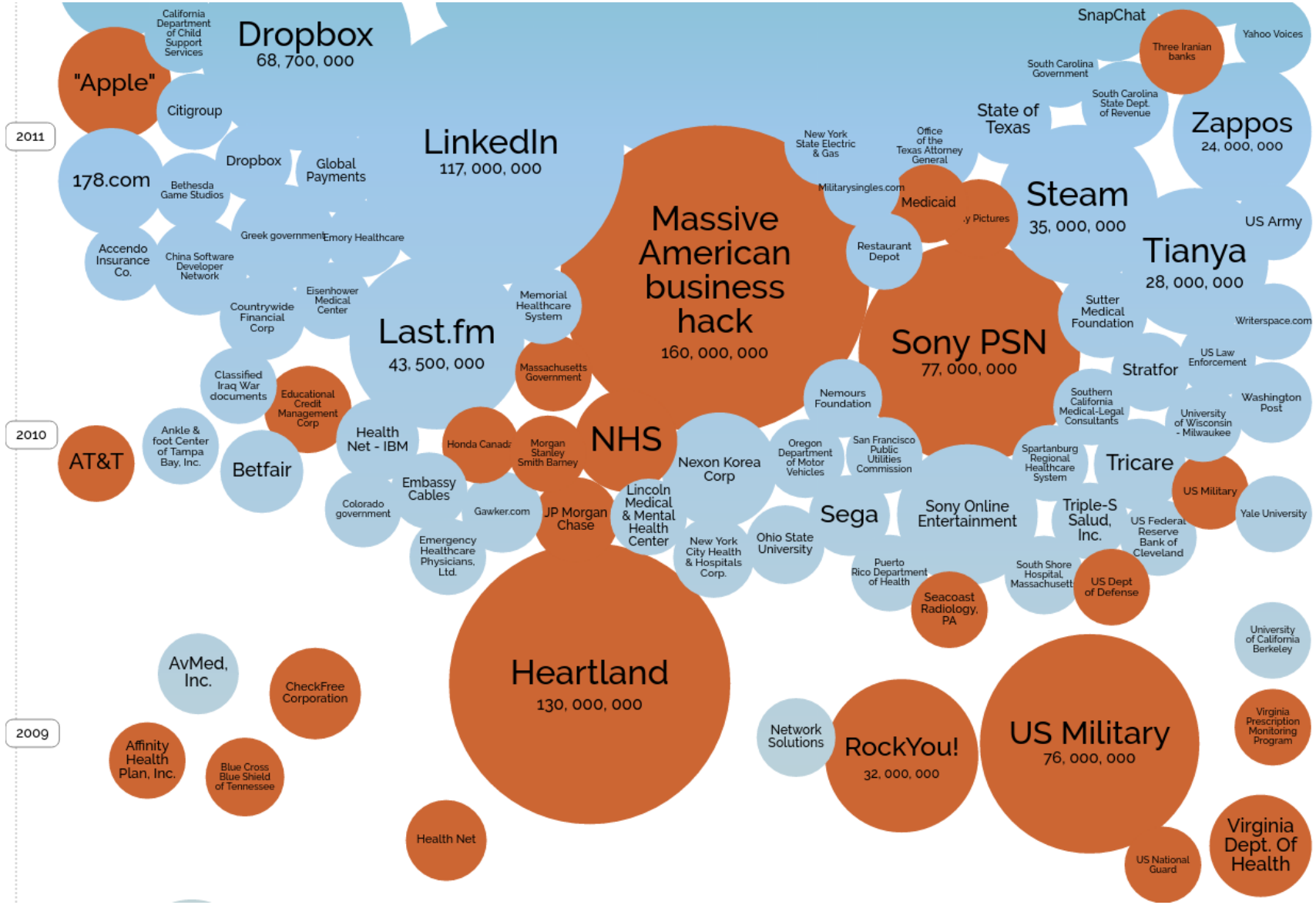


Software Security: Data Breaches 2006 - 2008



www.informationisbeautiful.net

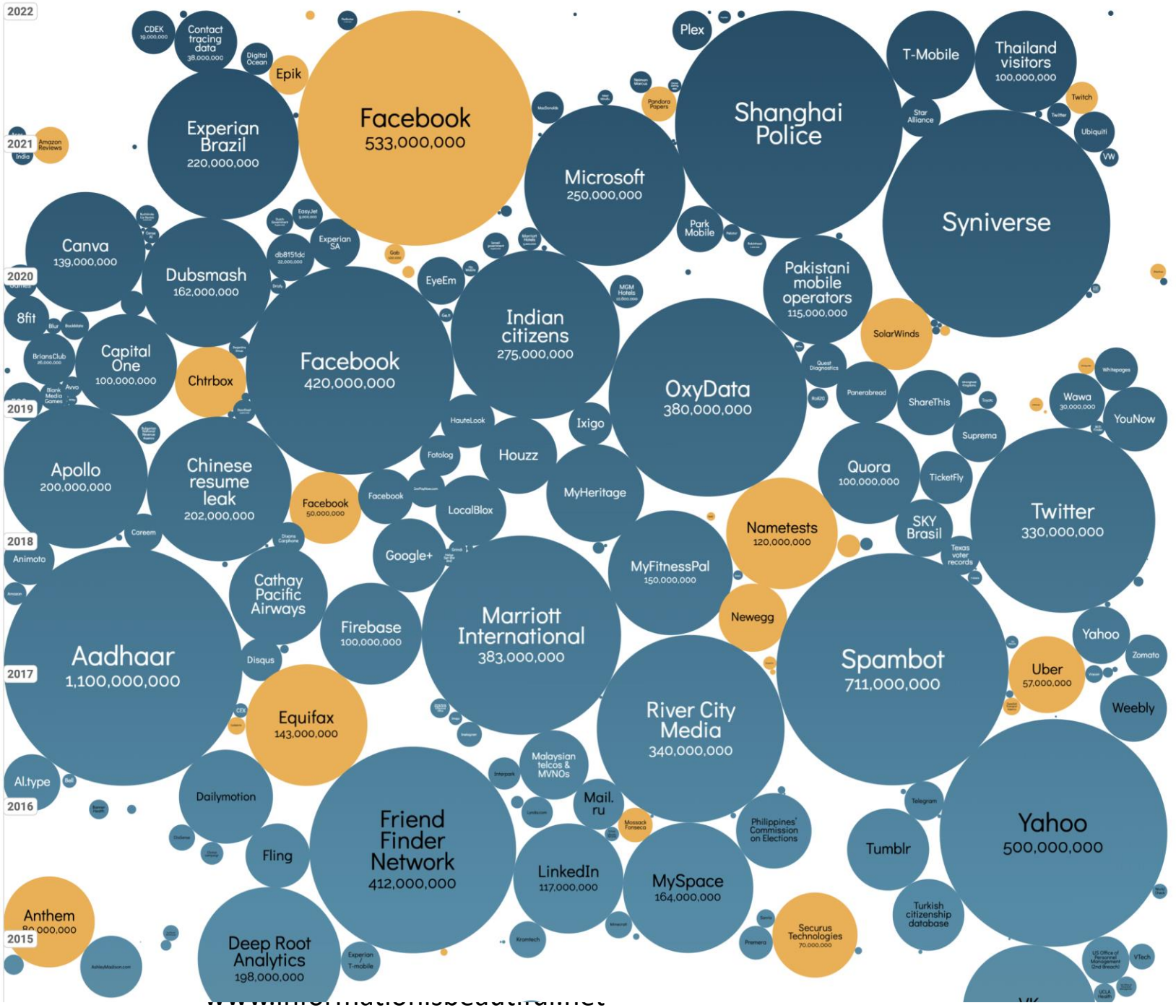
Software Security: Data Breaches 2009 - 2011



www.informationisbeautiful.net

Routine Breaches

- Not all threats materialize
- Prevention is better than remediation



IoT, Mobile, and Wireless Systems?

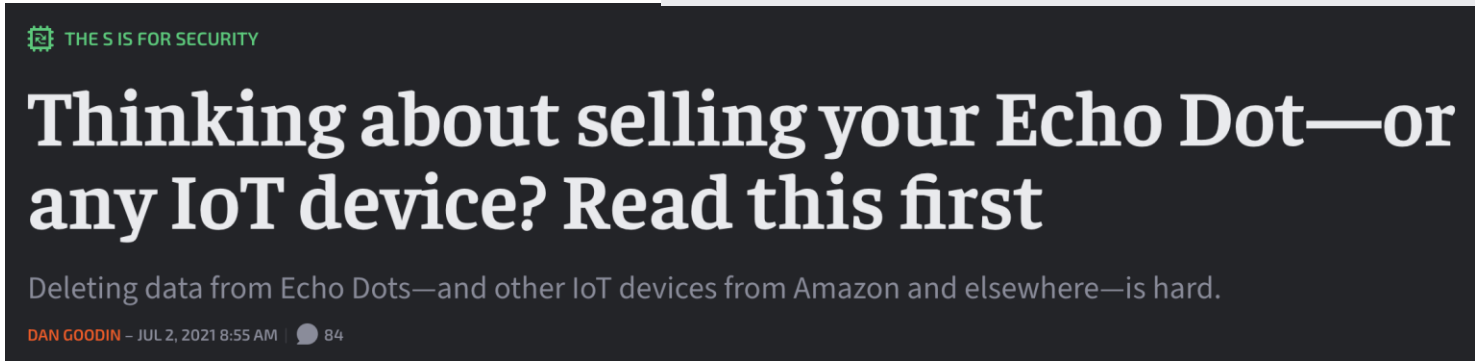
- Ubiquitous and provide increasing opportunities for exploitations

- Uniquely exposed to side-channels attacks

Threats of IoT Devices

- Proliferation of IoT devices
  - Home/enterprise appliances (IP phones/cameras, STB, smart speakers, locks, eReaders, digital signage, sockets), wearables, BYOD
- Connected, with sensing and actuation capabilities
  - Including Operational Technology assets
  - More and more self-driving cars, robots, toys, water systems
- Limited visibility on what they really do
  - Most IoT devices run on limited resources microcontrollers
  - Can be compromised and leveraged
- Limited visibility on how many there are
- What happens to them over time

Examples of Attacks/Findings



- Reverse engineering/analysis of smart speakers
  - Amazon Echo Dot, Google Home
  - Storage is not encrypted
  - Factory reset does not delete data (flash wear leveling)
- Study: bought/analyzed 86 devices (eBay)
  - Desoldered the flash (minutes)
  - 61% not reset
  - Even broken devices still contained personal data
  - Wi-Fi (SSID/Password); user's information, location;
- Ethical disclosure and privacy-preserving analysis
- "Amazon Echo Dot or the Reverberating Secrets of IoT Devices", ACM WiSec 2021

- Other issues
  - Wake-up words, local vs. remote processing
  - IoT devices upload various private information to the cloud
  - Two ultra-sound sources can generate voice commands and manipulate smart-speakers stealthily (inaudible to humans)
  - IoT Wi-Fi MIMO/CSI allows to see inside homes from a distance
  - A camera can listen by analyzing small motion (e.g., bag of chips demo)

Lot of Potential Attacks (An Old Slide from 2017)

A university was attacked by its lightbulbs, vending machines and lamp posts

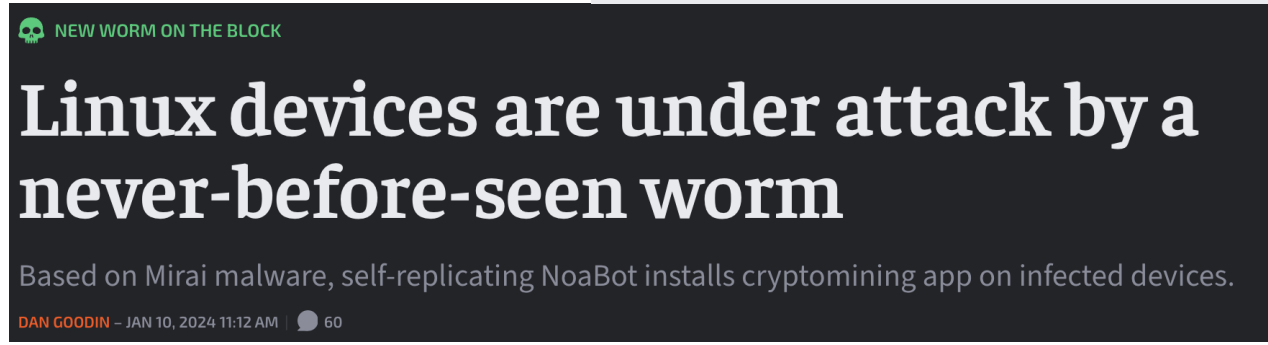
- Privacy Infrastructure
  - Tor Hidden Services
  - Bitcoin

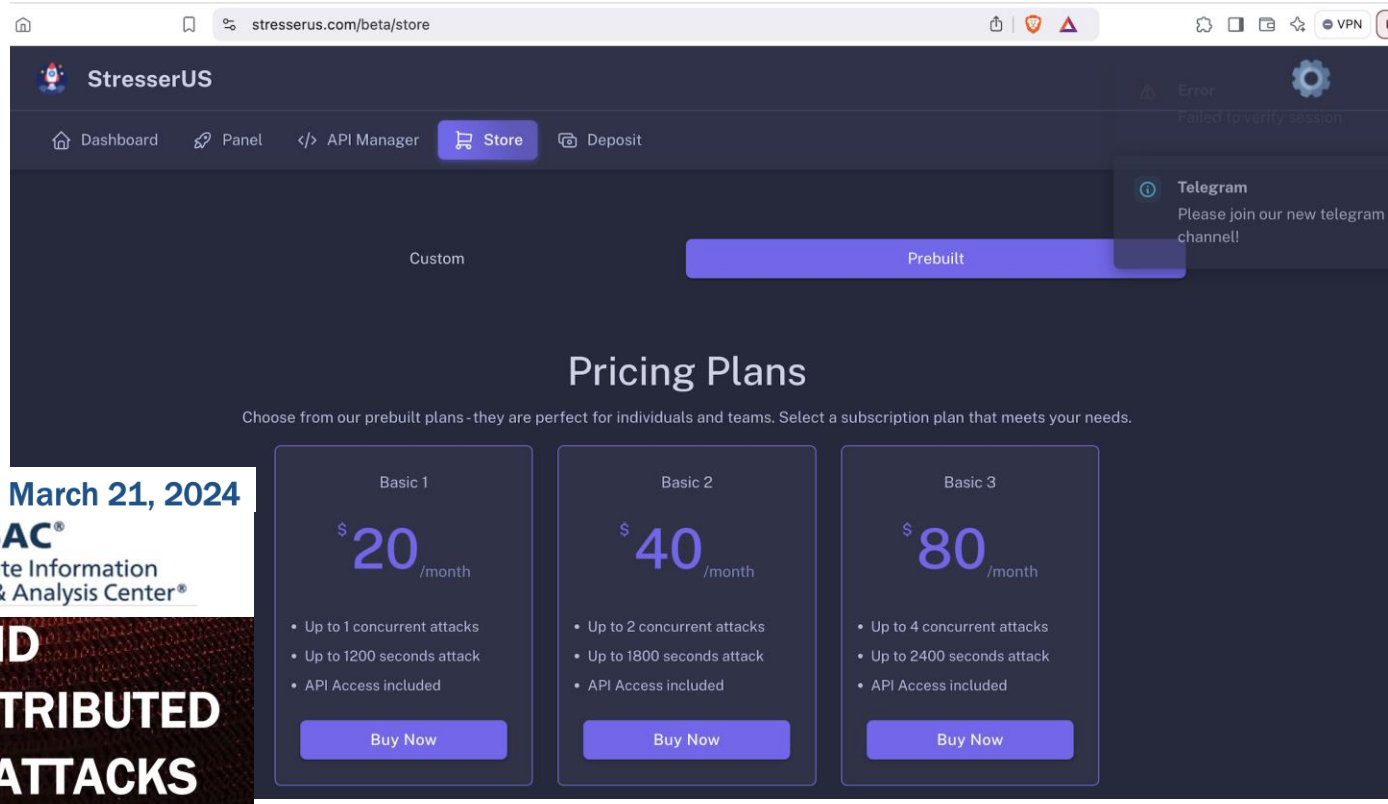
The Romantik Seehotel Jäegerwirt 4-Star Superior Luxury Hotel was hit by a ransomware attack that locked guests in and out of the rooms.

Stuffed toys leak millions of voice recordings from kids and parents

IoT/OT Malware

- Increasing threat
  - Zscaler reported a 400% growth in IoT malware attacks (2023 Threat Report)
- Mirai is still around, with new variants
  - NoaBot, Gafgyt, etc.
- Currently mostly exploit low hanging fruits
  - Default credentials, web interface, unpatched firmware
  - Used to create bots for DDoS (Booter/Stresser))
  - Some monetization related to bot-as-a-service



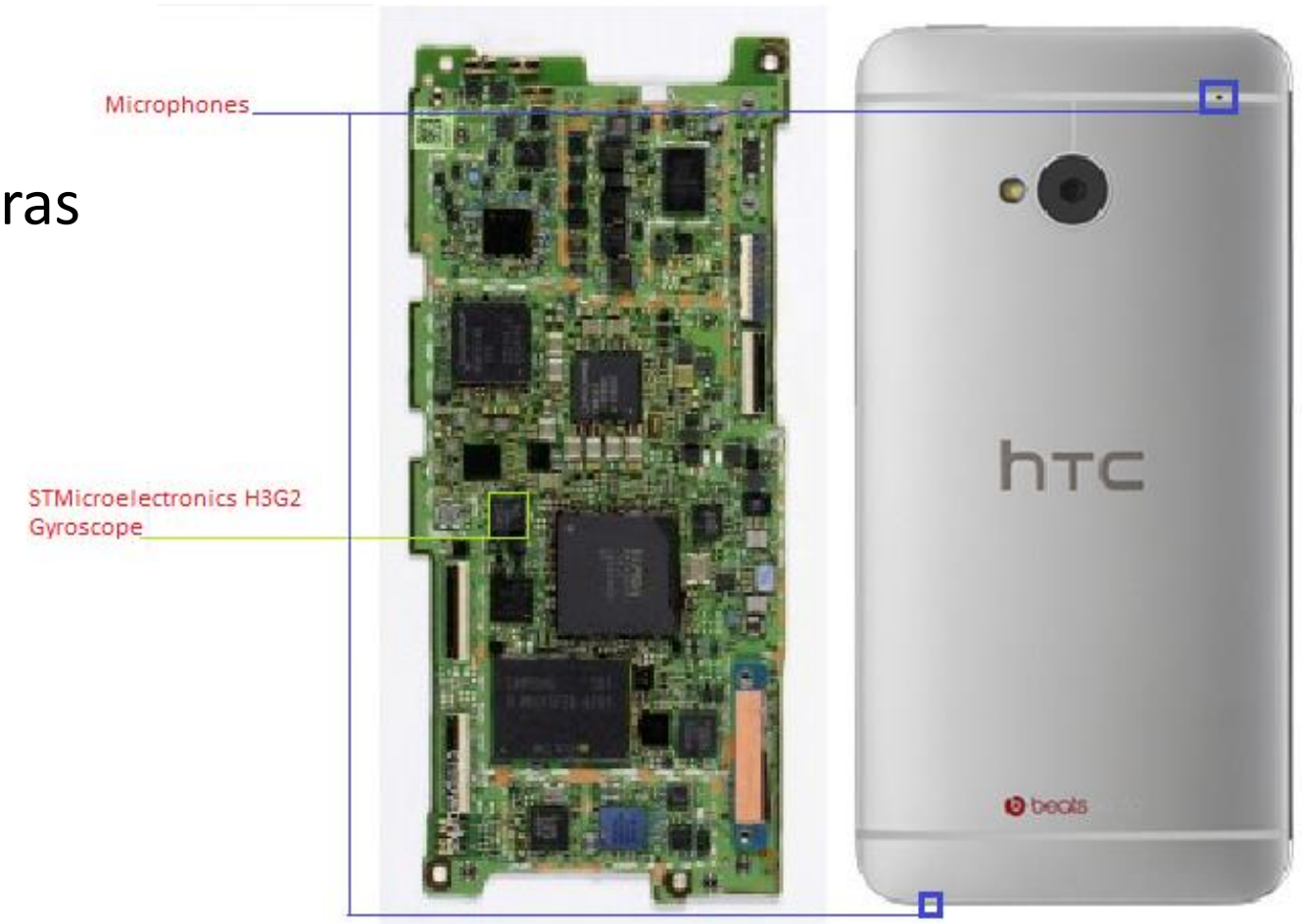


Mobile Devices & Apps

Mobile Sensors for Side Channel Attacks

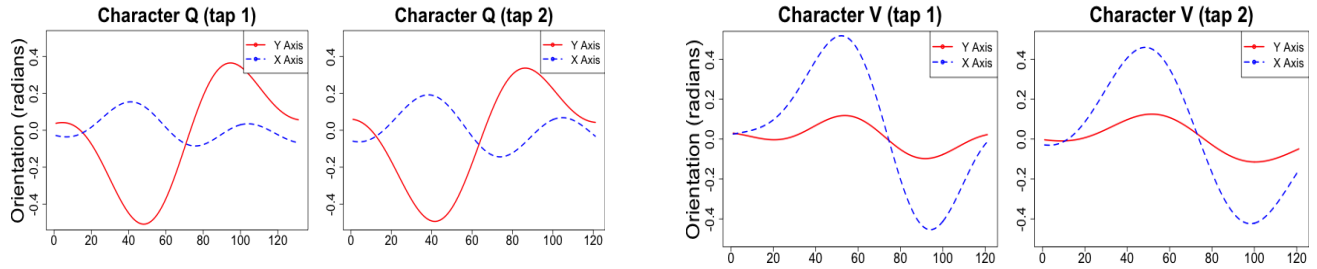
- Variety of sensors
  - Gyroscope, accelerometer, compass, microphone, cameras
- Malicious app can monitor other apps

- Some attacks
  - High accuracy keylogging
  - Location Tracking
  - Exfiltration



Mobile Sensors

- Gyroscopes
  - Sensitive to motion but not very noisy
  - Similar pattern for same keys and different for other keys on x/y axes
  - Does not work well for all keys, experiences drift, etc.



- Stereo-Microphones unique delay & amplitudes e.g., HTC One
  - Distance between microphones: 0.134 m
  - Maximum supported sampling rate: 48 KHz
  - Speed of sound in air: 340 m / s
  - Difference of +***19 samples*** to -***19 samples***
- For future devices with higher sampling rate
  - Example sampling rate: 192 KHz
  - Difference of 2****75 samples*** for tap close to one microphone

Evaluation 2014
(Meta-Algorithm)

- Meta-Algorithm
  - Combines several signal processing & machine learning algorithms
  - Decompose keyboard
- Possible to achieve > 90% for QWERTY keyboard
- Possible to achieve > 95% for Number keyboard
- Some sample sets between 44-56%
  - Noise
  - Gyroscope Drift

User	Keyboard	Count	Gyro	Mics	Comb
HTC One					
User1	Number	306	68%	93%	93%
User2	Number	200	44%	94.5%	93%
User3	Number	300	72%	91%	91%
User4	Number	300	75%	94%	95.5%
User5	Number	323	45%	83%	83%
User3	QWERTY	782	80.5%	89.5%	94%
User4	QWERTY	860	56%	83%	83%
User5	QWERTY	877	66%	73.5%	84%
Samsung S2					
User1	Number	137	75.5%	-	-
User2	Number	542	84%	-	-
User3	Number	202	83%	-	-
User4	Number	200	81.5%	-	-
User5	Number	512	81%	-	-
User1	QWERTY	366	63.5%	-	-
User2	QWERTY	620	77%	-	-
User5	QWERTY	312	74%	-	-

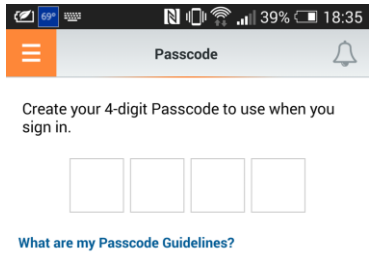
Attack Scenario

- Adversary lures victim to install Trojan app
  - e.g., ‘To-do’ app that supports speech recognition
- App records sensor data when user types in Trojan app
  - Builds training models from collected data
    - On the phone / On a central server
- App invokes service that waits for sensitive activity to start
  - e.g., targeted bank login page
- App records sensor data when sensitive activity
  - Generates predictions from sensitive data using training models

Evaluation of Keylogging

(End-to-End Attack)

- Collected on banking app with fake numbers
  - Every UI page is known as an activity
  - Trojan queries for the foreground activity every 5s
- 100 four digit PIN numbers
  - 376 out of 400 digits predicted correct (94%)
  - 84 predicted completely correct
- 100 sixteen digits Credit Card numbers
  - 1467 out of 1600 digit predicted correct (91.5%)
  - 52 predicted completely correct

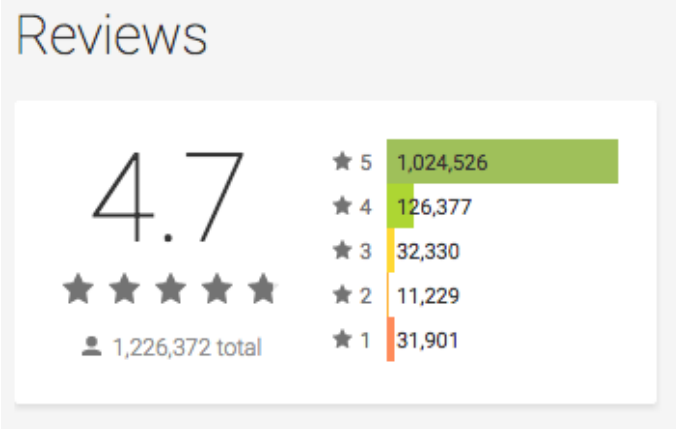


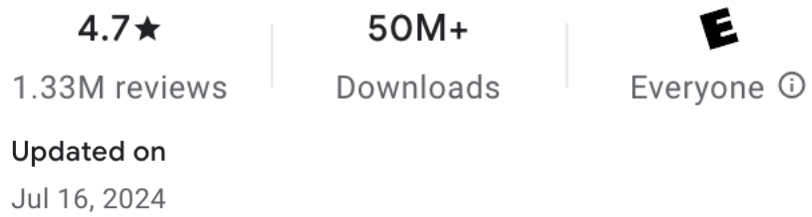
Total	Correct	Correct Digits	Accuracy
PINs			
100	84	376	94%
Credit Cards			
100	52	1467	91.5%

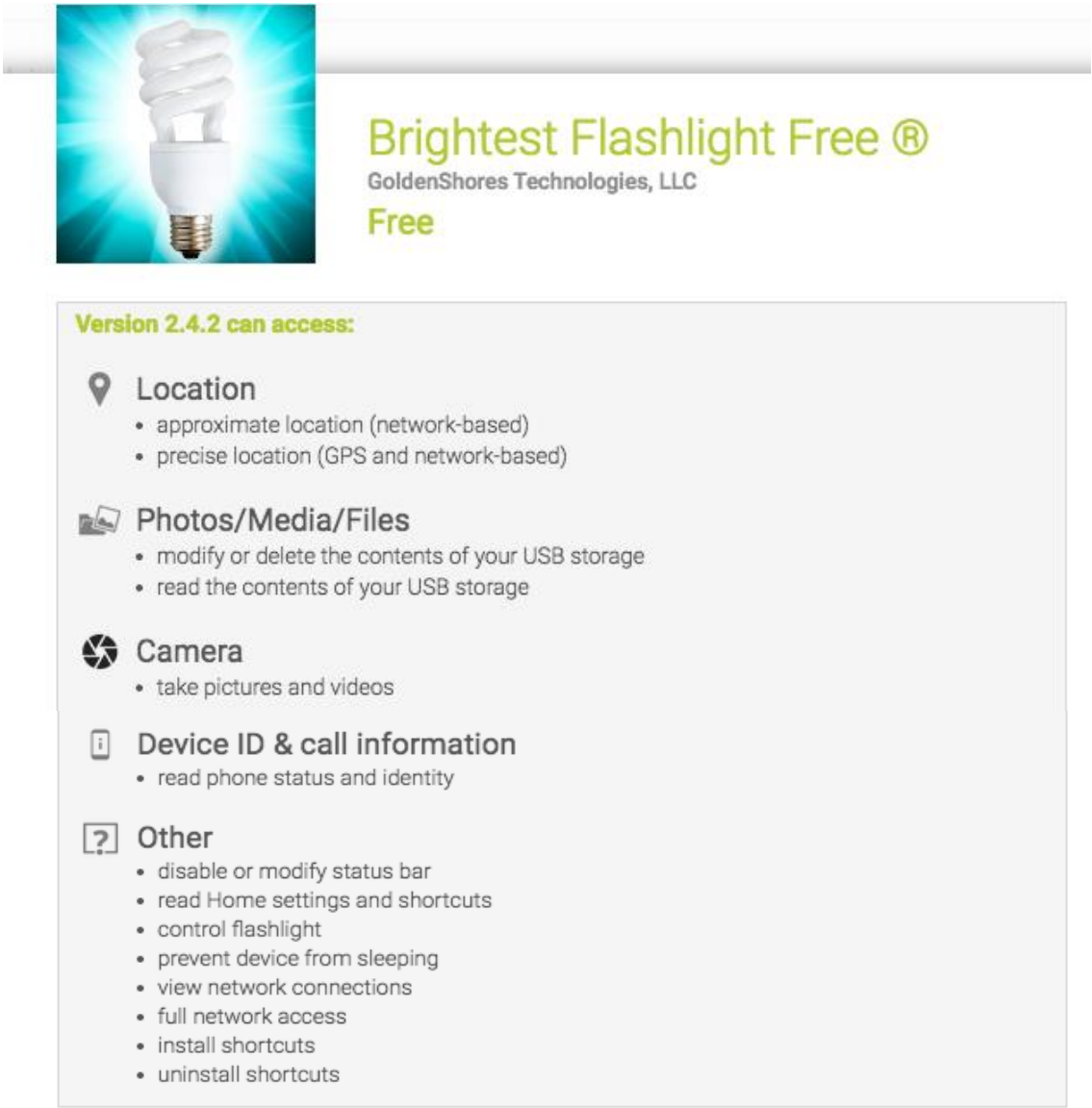
How malicious can a Flashlight App be?

FTC Approves Final Order Settling Charges Against Flashlight App Creator

https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app





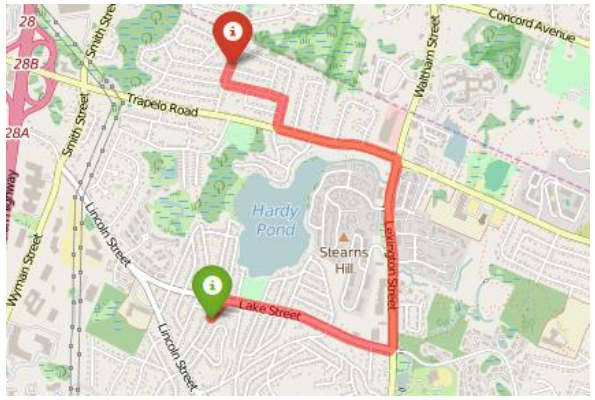


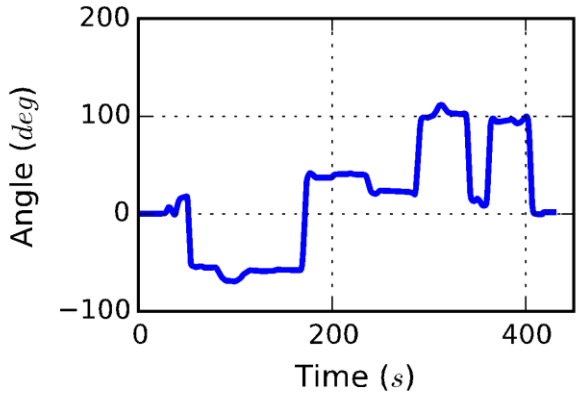
Zero Permissions Malicious Apps [S&P'2016]

- Observation
  - No need to request permission for accelerometer, gyroscope, compass, barometer
  - Most Apps obtain Internet access
  - GPS/Location can be viewed as suspicious
- Can we infer?
  - Gender? Age? Health information?
  - Work location, home? Identity? Social circle?

Inferring Location Information

- Goal is not to build an Inertial Navigation System
  - Gyroscope is fairly accurate
  - Accelerometers and compass are noisy

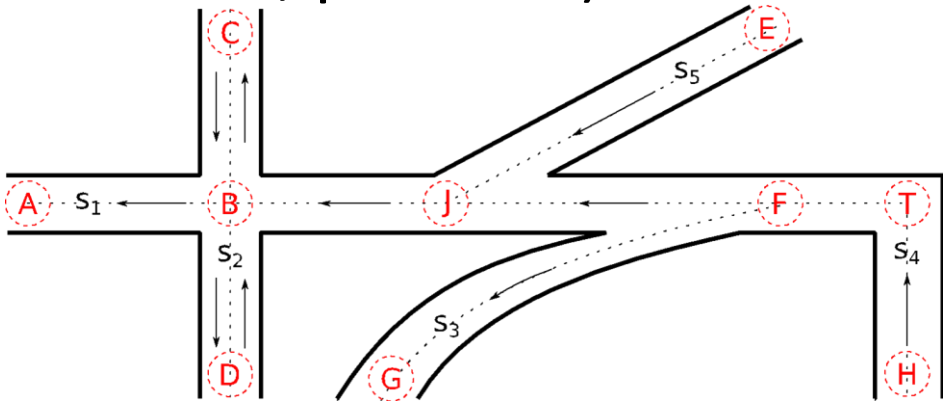


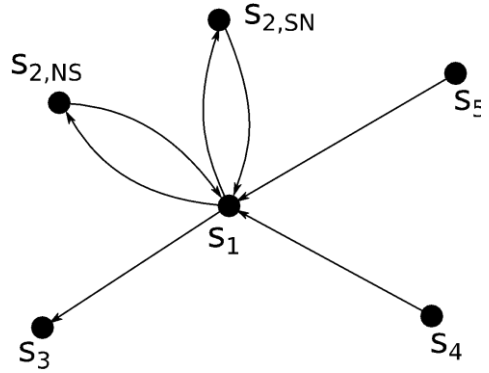


- Collect sequence of turns
- Infer most likely trajectory

Inferring Location Information

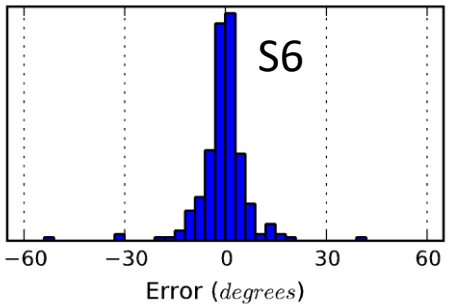
- Open Street Maps data => build a directed graph
  - enhance with road signature (curvature, compass headings, speed limit, potholes)

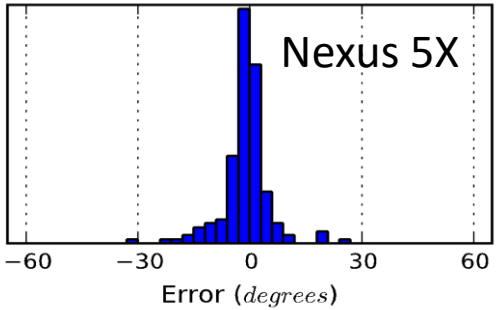




- Problem: finding maximum likelihood path
  - Error approx. by Gaussian

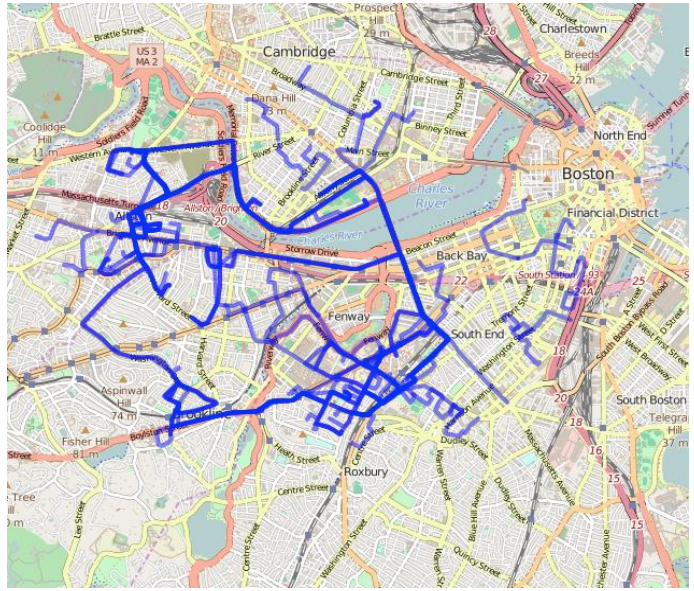
    but deletions





Techniques and Evaluation

- Developed several techniques
  - Processing data (compensating gyroscope bias, eliminating idle time)
  - Maximum likelihood path incorporating gyroscope & compass, curvature, speed limit with simple assumption on turns distribution

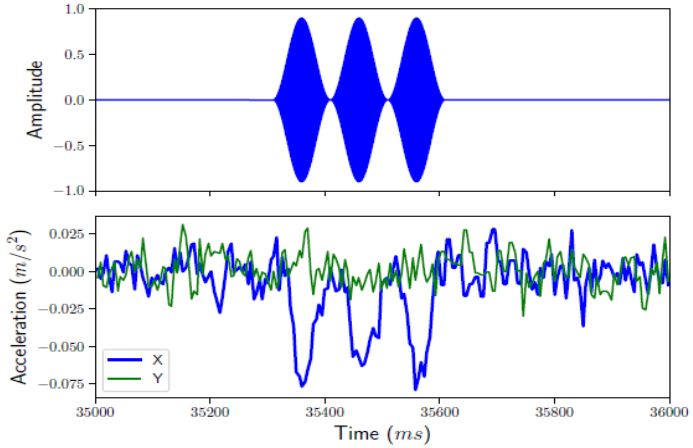


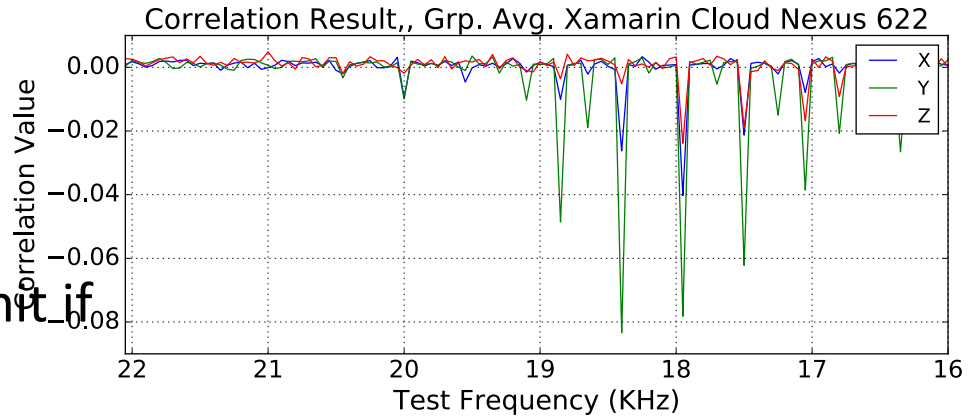
- Evaluation
  - Simulation on 11 cities: prob > 50% to output path in top 10
  - Real experiments in Boston (30%) and Waltham (60%)
  - Better results for longer lists, longer paths

- Next steps: work-place, colleagues, sensitive locations, family
- Disclosed to Apple/Google
  - Now, Apps needs a permission to access sensors in the background

Covert Channels for Data Exfiltration

- Consider two mobile apps
  - App 1: Trusted with sensitive information but no communication, e.g., password manager, journal
  - App 2: Not given access to sensitive information but has access to the network, e.g., game
- Existence of stealthy cover channels
  - Source: permissionless speaker (ultrasonic signals)
  - Receiver: permissionless accelerometer
- Channel characteristics
  - Multiple bands unique to device
  - Axis are independent enabling MIMO
  - Source gets the received data and can code/retransmit if necessary





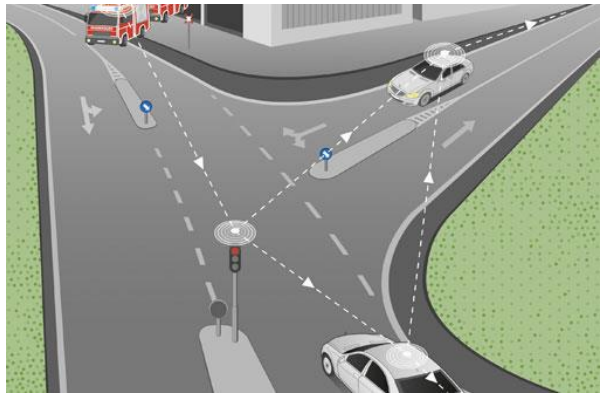
Wireless Systems

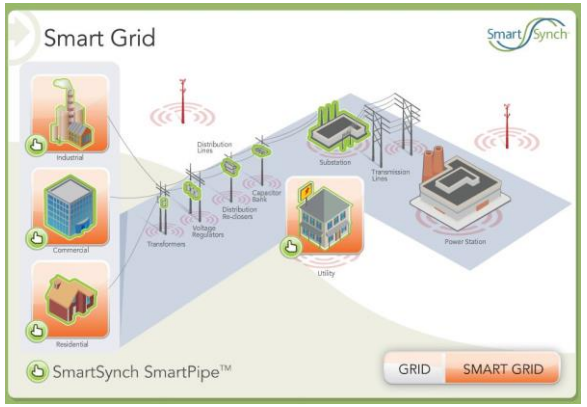
Bluetooth, 5G

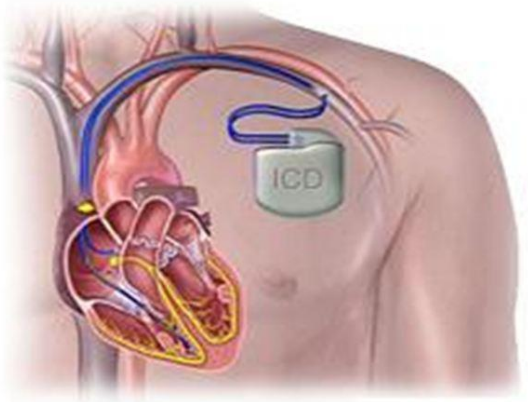
Avionics, (privacy-preserving) BLE, Wi-Fi

Wireless is Ubiquitous

- Beyond mobile devices (cellular, Wi-Fi, Bluetooth)
  - Transportation systems
  - Smart grid (power plants sync, smart meters)
  - Implantable devices
  - Avionics: ADS-B, GPS, ILS, ACARS, TCAS,
- Its security and robustness are critical for a variety of applications







Wireless is Ubiquitous

- It is also used in harmful applications
  - Jamming, IEDs, drones, etc.

Wireless systems Characteristics

- Unique characteristics with fundamental constraints
  - Broadcast medium
  - RF spectrum
  - Energy
- Limited resources led to complex designs and optimizations

  but also weaknesses & leakage

- Softwarization of wireless systems: SDR, libraries, protocols stacks, etc.
- Over the years we demonstrated several attacks (and defenses) against wireless systems
  - 3GPP, AWDL, Bluetooth, Wi-Fi, ILS, ACARS

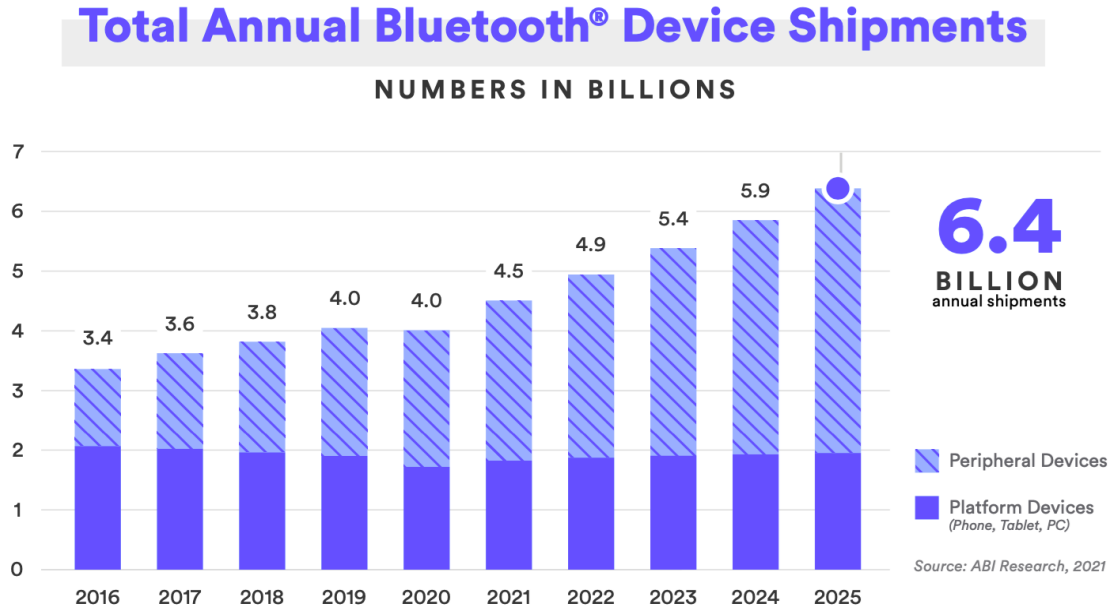
Changing Landscape in Wireless Systems

- Security assumptions are increasingly disproved:
  - Wireless systems are too complex for common adversaries
  - Attacks are impractical e.g., adversary has to be local
  - Adversary needs to operate over a wide spectrum
  - Adversary needs to operate in real time
  - Why would someone do this?
  - Adversary will not dare and will be caught

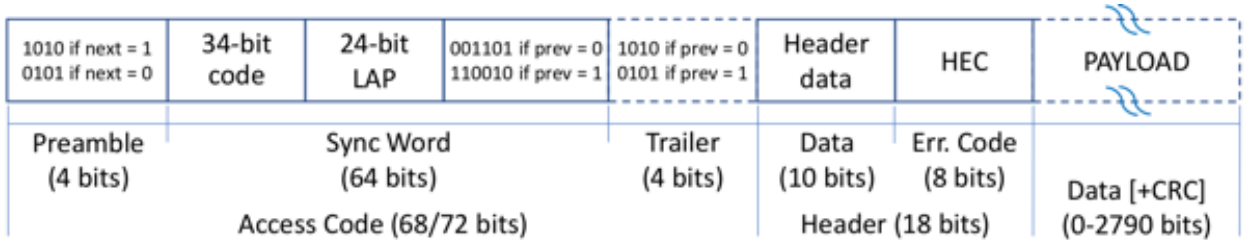
Bluetooth Tracking

Bluetooth Privacy

- Tracking in wireless systems
  - Tracking has always been a concern
  - 3GPP 2G-5G gradually improved privacy
  - Wi-Fi (Apple & Google) introduced MAC address randomization in 2014
  - Bluetooth was believed to be secure against tracking
- Bluetooth is increasingly ubiquitous
  - Phones, wearables, cars, headsets, IoT
- Bluetooth 5 covers multiple physical layers
  - Fairly clear distinction between Bluetooth Classic and Bluetooth Low Energy (BLE)
- BLE is the basis for most privacy-preserving contact tracing apps

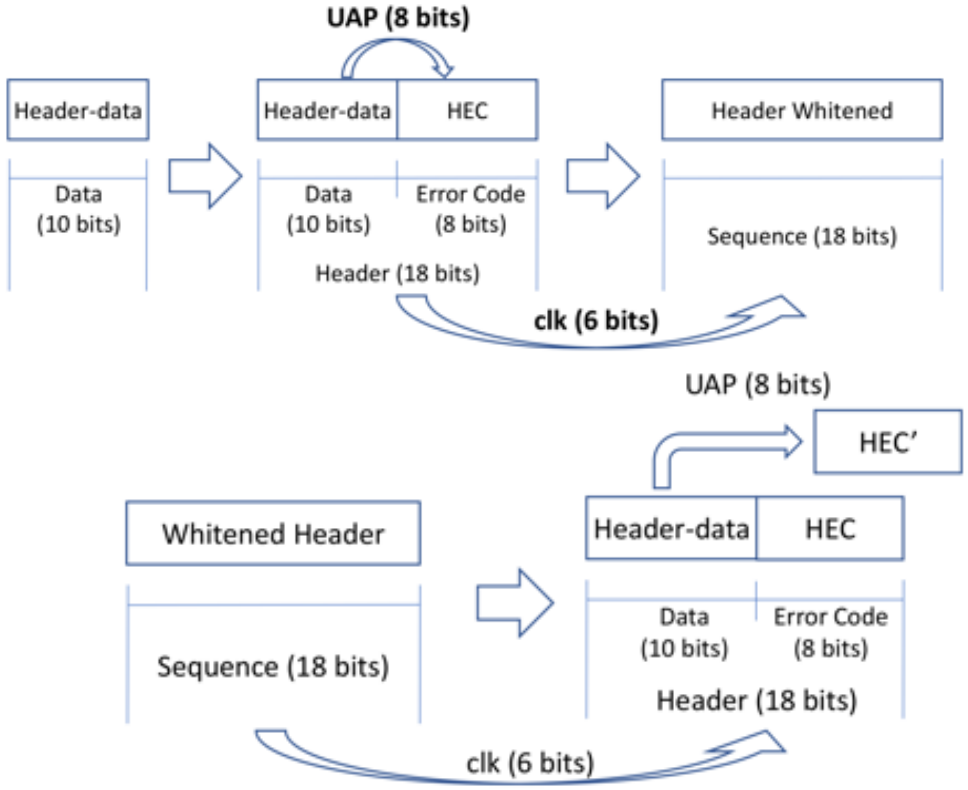


Bluetooth Classic



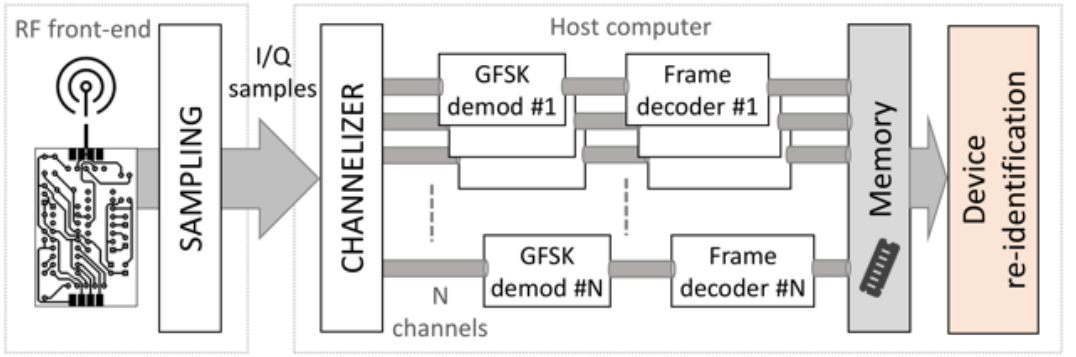
- For many years believed to be immune to tracking

- Why?
  - 48 bits MAC address (BDADDR) never fully transmitted in clear (unlike Wi-Fi)
  - MAC address is whitened with clock info
  - Hops 1600/second 79 channels (79 MHz)
  - 3000 pages standard

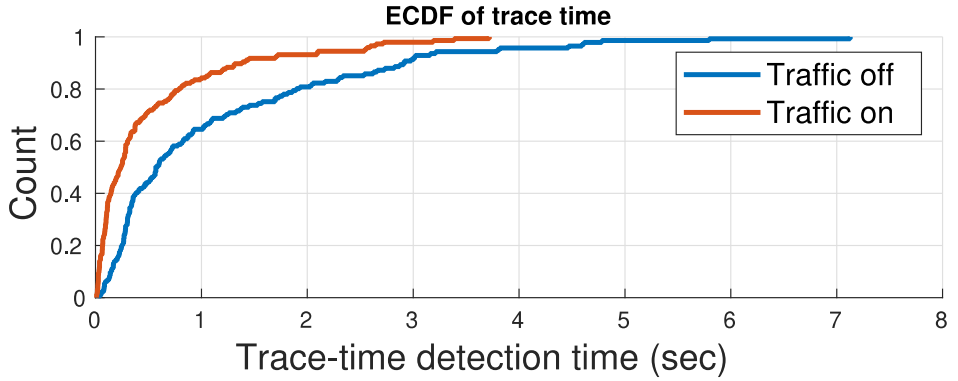


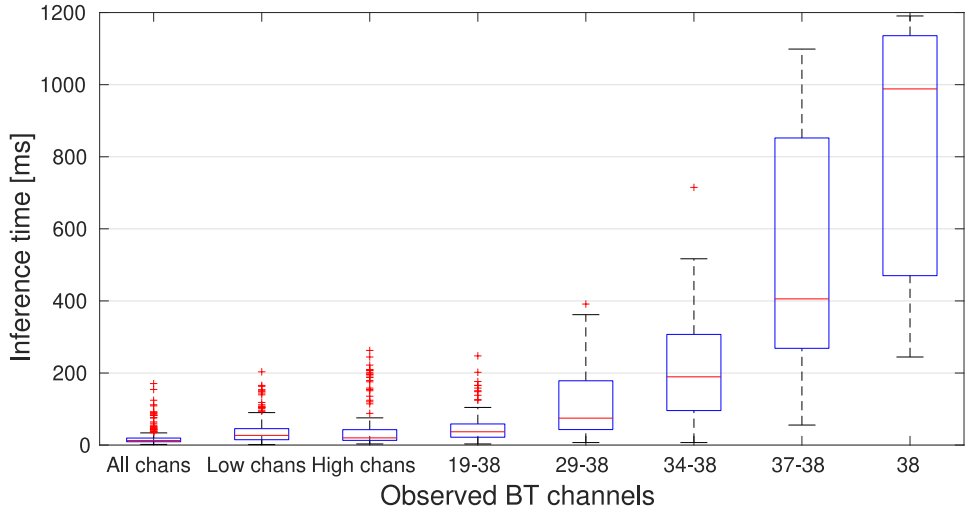
$$wh = [hd_i \mid \mathbf{HEC}(hd_i, u_i)] \oplus \mathbf{w}(clk_i),$$

Bluetooth Classic Tracking [S&P 2020]



- Algorithms & SDR system
- Reveals the BDADDR in almost any setup
- Experimental evaluation
  - 80% in < 1 second; 100% in < 4 seconds
  - Up to 85 meters away
  - With streaming or idle
  - Cars, headsets, etc.
- Attack can be implemented on some phones
  - Nexmon framework leveraging the Wi-Fi chipset as SDR …
- It is possible to track virtually every person/vehicle
  - and discover interesting other patterns
- Follow-up work: BLE linkage to BTC
  - BLE privacy-preserving apps are not secure



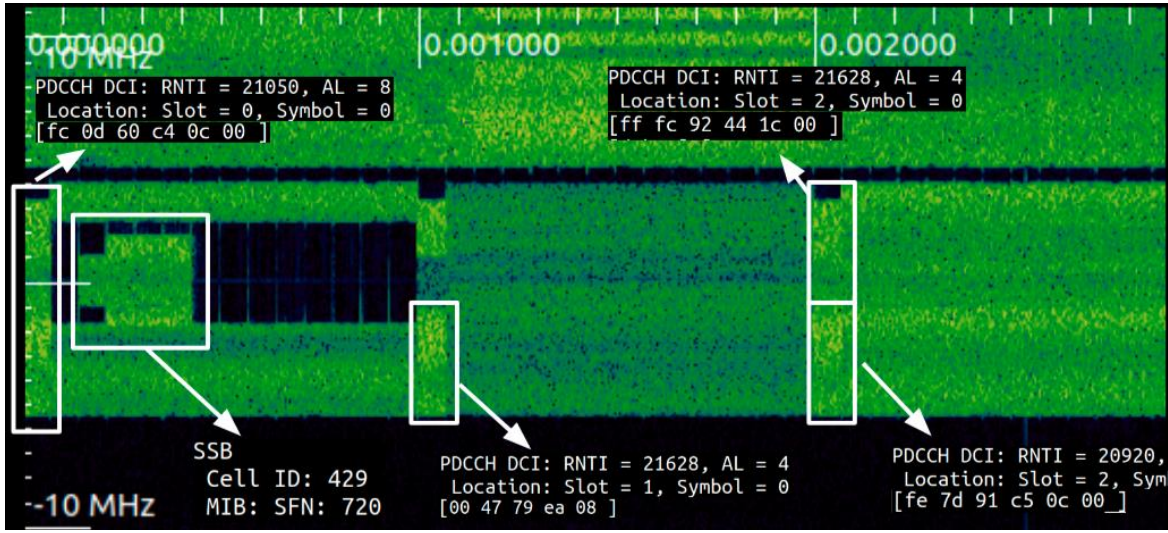


3GPP 5G Security

Security Analysis of 3GPP 5G [2020-2024]

- 2G – 4G have various vulnerabilities
  - DoS, tracking
- 5G introduced new privacy mechanisms and considered for use by DoD
  - Analysis of security and privacy (US ONR funded project)
  - Leakage from signaling e.g., PSS, SSS, PBCH (MIB)
    - Broadcast constant values, predictable values, predictably repeating values
  - Several attacks identified, evaluated and demonstrated
    - Significantly more efficient than naïve attacks
    - Exposure: 10s of dB gains to a smart adversary (miles away)
    - MIB: no encryption/integrity ability to over-shadow at power < legitimate signal (~5dB)
      - DoS: smart-jamming, but also cross-layer e.g., set cellBarred bit
  - Traffic analysis
  - Key-point of entry for other attacks
    - Rogue infrastructure; multiple denial of service attacks (disappearance of networks, cell barring, redirection to other parts of the spectrum spoofing other signaling e.g., SIB), tracking

From 5G Sniffing to Harvesting Information Leakage [S&P 2023]



- 5G introduced a SUCI to limit tracking
- 5G control channels leak info
  - Existence of UEs, location,
  - Characteristics of traffic

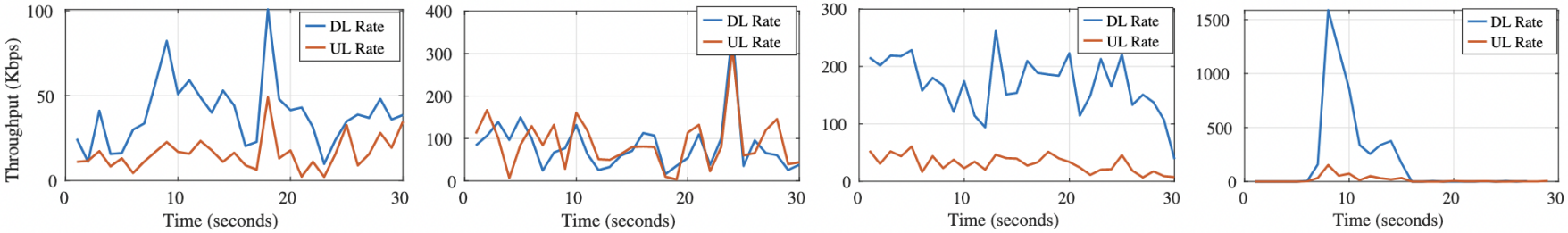
- 5G Sniffing is in principle more challenging than LTE
  - Sniffing is different from decoding traffic
  - Naïve sniffer brute force 44 bits and has a very high false positives rate
    - Multiple DCIs each sub-frame (1ms)

- Vulnerabilities in 5G and optimization techniques enabled us to develop a real time sniffer *5GSniffer*
  - SSB info (PSS, SSS, MIB), SIB1, but most importantly the PDCCH (DCI/RNTI)

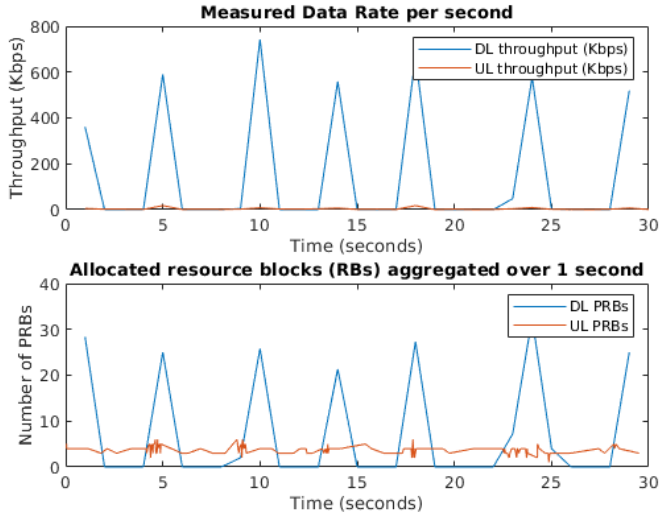
- 5GSniffer + vulnerabilities in privacy-focused messengers (Signal and Telegram) $\Longrightarrow$ presence of phone (#), traffic analysis

5G Sniffer Enables Traffic Analysis

- Enables retrieval of
  - RNTI in real-time
  - DCI, MCS ⟹ number of bits for each RNTI traffic analysis



(a) Voicecall (b) Videocall (c) Video streaming (d) File transfer, 10MB

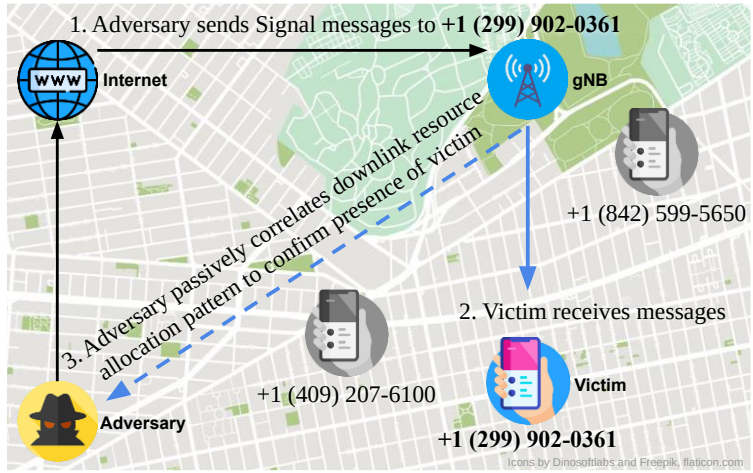


- But 5G introduced the SUCI, prevents reuse TMSI, releases RNTI if inactive for 10-30s

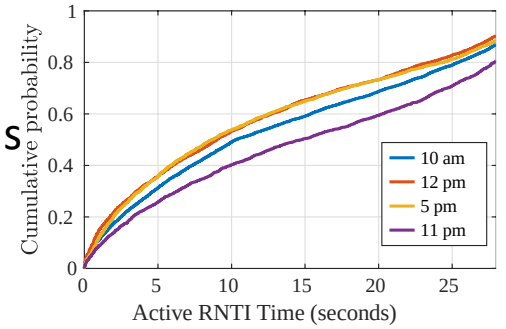
  ⟹ prevents exposure of long-term user identifiers

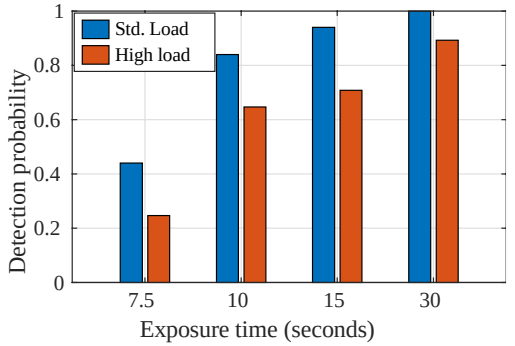
5G Sniffing: Exposing Presence of Users of Signal/Telegram Users

- Adversary sends *stealthy messages* to target phone number
- Stealthy messages exploit Apps vulnerabilities
  - Corrupted cryptographic MAC, padding up to 196KB (Signal) or 65K (Telegram)
  - Telegram also has disable_notification flags and remote deletion of messages

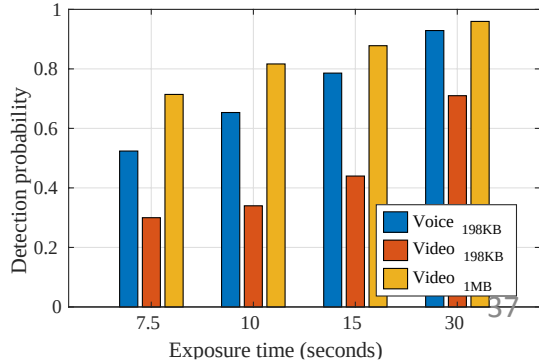


- Most RNTIs do not last for long
  - Maintaining an RRC connection filters most RNTIs





- It is possible to achieve nearly 100% exposure of target within 30 seconds
  - Over the air experiments (targeted our own devices)
  - Attack is highly accurate even with high network load, and when target had a video call
- Proposed mitigations
  - And disclosed to Signal & Telegram



Finals Remarks (I): Does It Matter?

- IoT/Mobile/Wireless Systems provide unique opportunities for attacks
  - Ubiquity, sensing, actuation capabilities
  - Inertia, limited resources and difficulty to update
  - Security mechanisms not always user friendly
- Academia can be creative, but does it matter in the real-world?
  - Incentives: monetization vs. cyberwarfare, industrial espionage
  - Privacy-preserving infrastructure (e.g., Tor, Bitcoin) make it easy to get away with it
  - Serious threat from nation-state actors
- Why does it matter for industry/companies?
  - Can be used to collect information and enable targeted attacks
  - Can be used to launch attacks inside/outside

Final Remarks (II): Defenses

- Awareness
  - Assume that motivated attackers know everything about you so any message you receive could be malicious, yet look authentic
- Best practices: prevention, tolerance, detection, mitigation
  - Inventory, only use devices that can be adequately managed/updated
  - Segregate devices/networks (e.g., separate SSID/VLANs for IoT)
  - Scan network/RF spectrum: all devices/comms should be accounted for
    - Remove any device/app not necessary
    - Only allow encrypted traffic, between authorized endpoints
  - Remove incentives: backups, fast recovery mechanisms, controlled diversity of devices (lot of Arm, Xtensa cores)
  - Legal mechanisms
- Defense-in-depth