Northeastern University

Wireless and Mobile Softwarization Security and Privacy Pandora's Box?

Guevara Noubir

CAE Tech Talk

Northeastern University
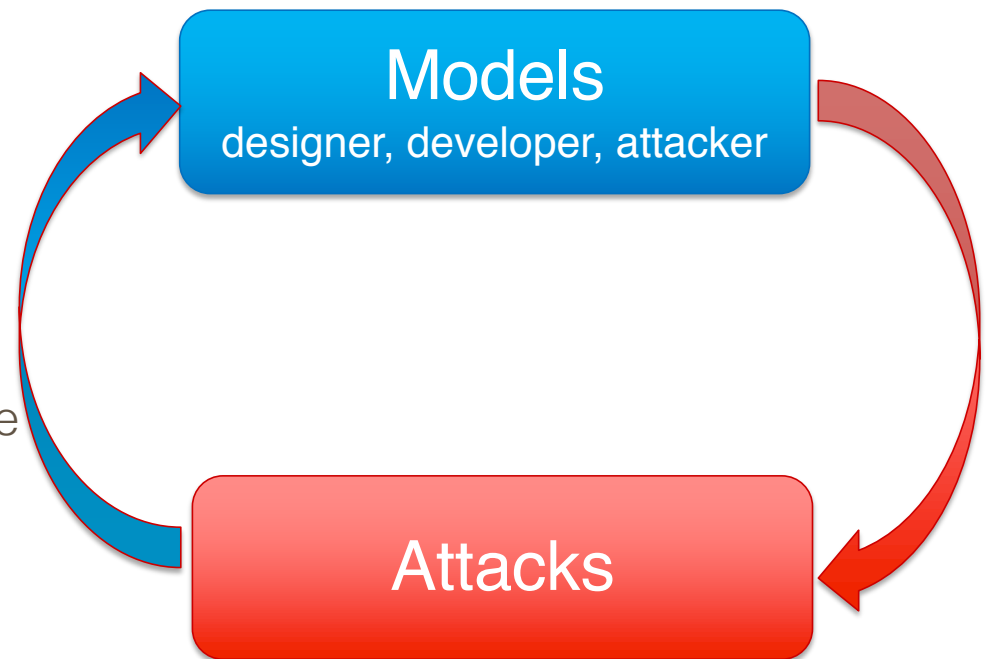*Cybersecurity and Privacy Institute*

E cyberinstitute@ccs.neu.edu ▪ T 617.373.5204 ▪ cyber.ccis.northeastern.edu
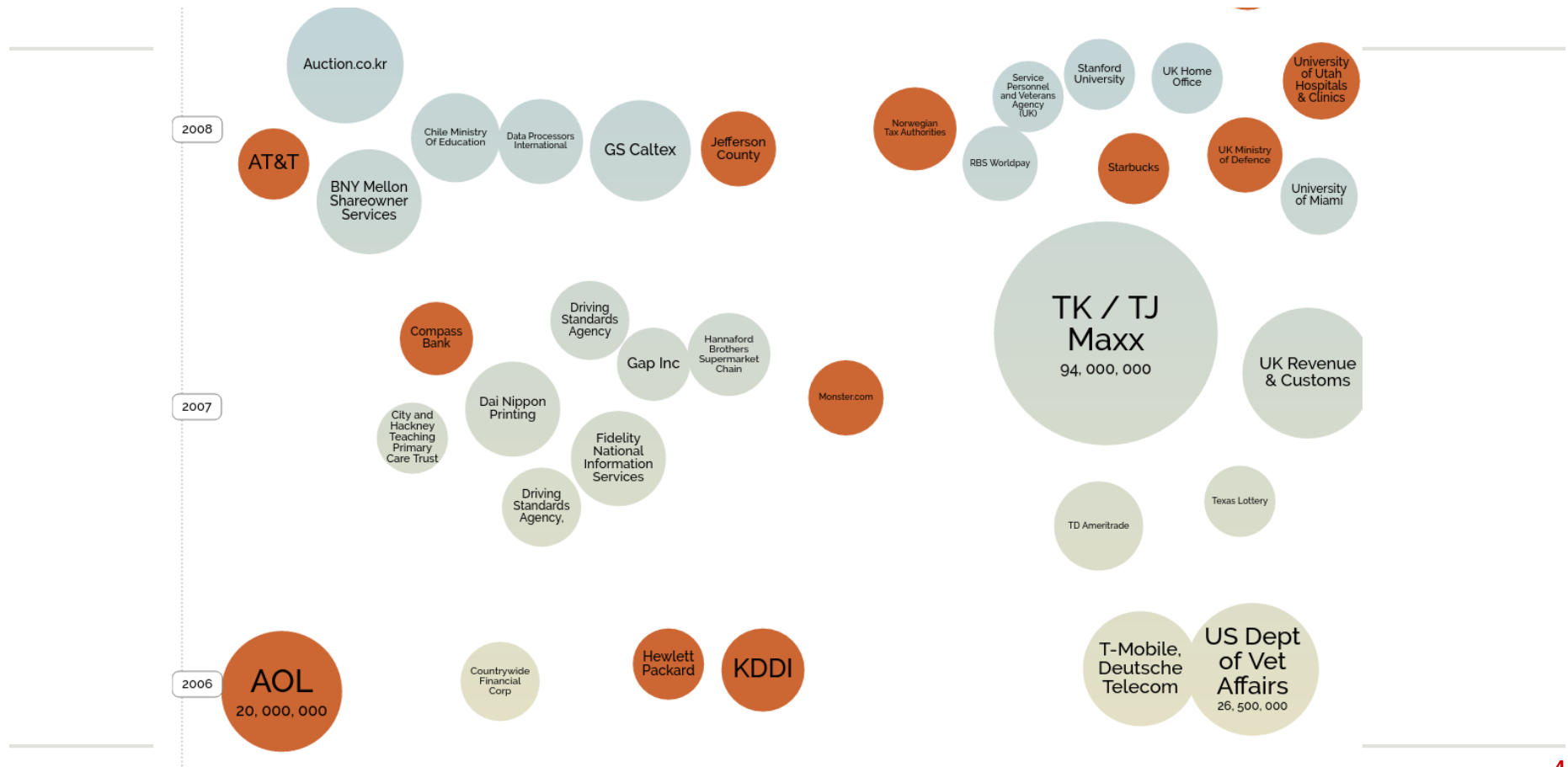
OUTLINE

- Wireless pervasiveness

- A spectrum of attacks in wireless and mobile systems

- Towards security and privacy in wireless and mobile systems
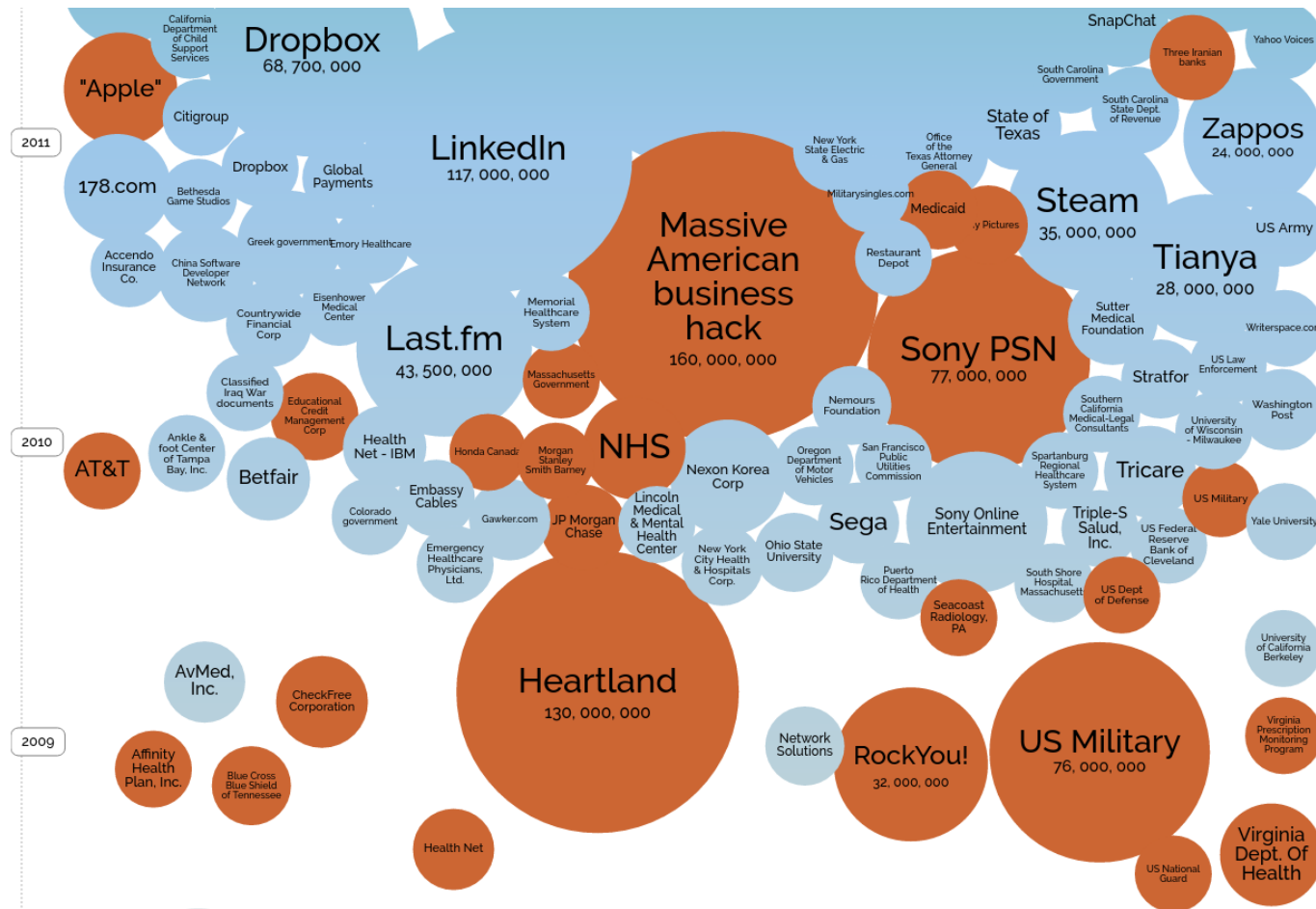
SECURITY CYCLE

- Model with assumptions, proof?

- "Attacker" escapes the model
  - and demonstrates feasibility of attacks

- Ideally a fix that accounts of potential future attacks

- Is this a stable control loop in wireless and mobile systems?
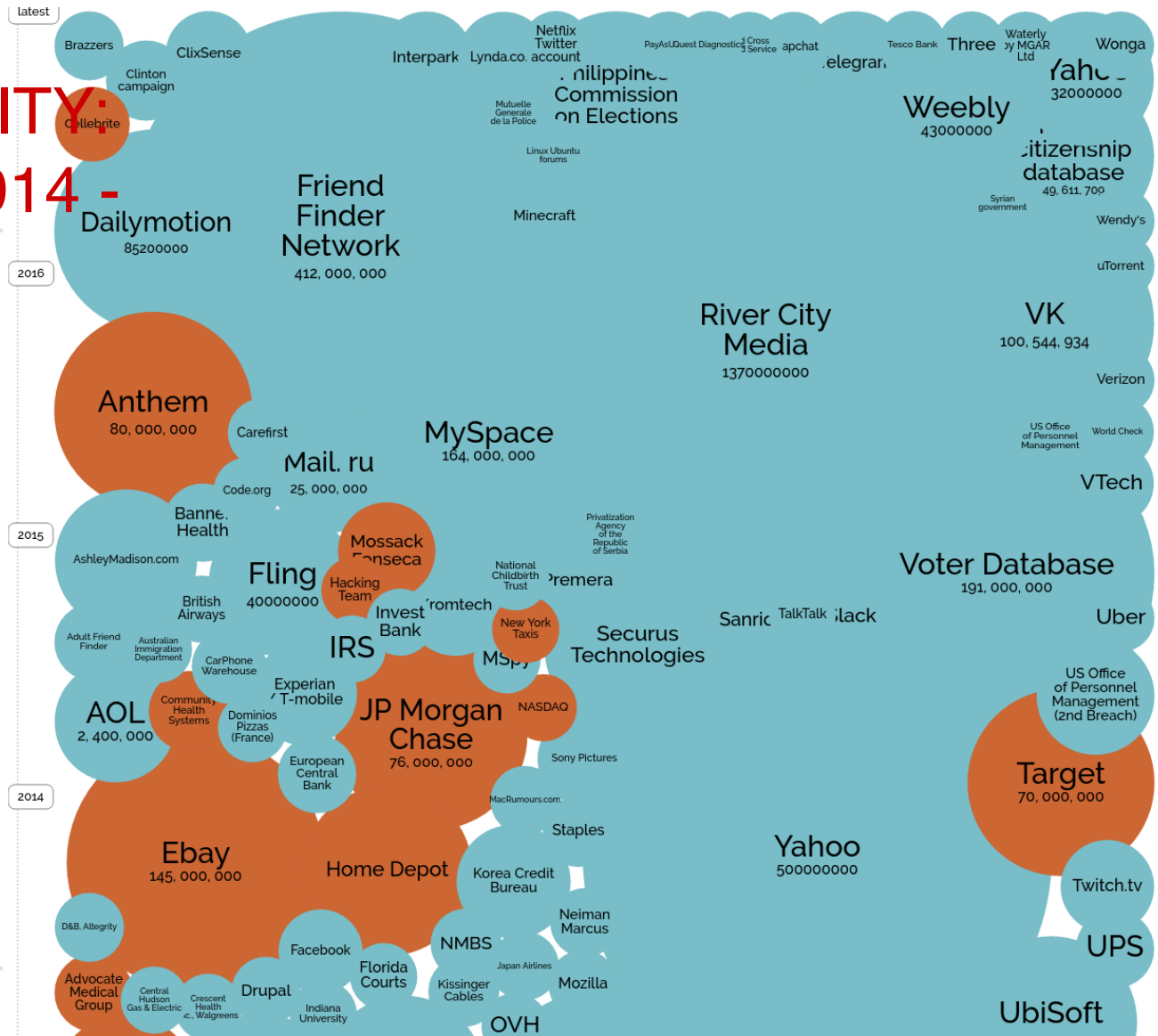

Models
designer, developer, attacker

Attacks

SOFTWARE SECURITY: DATA BREACHES 2006 - 2008

2008

Auction.co.kr

AT&T

BNY Mellon
Shareowner
Services

Chile Ministry
Of Education

Data Processors
International

GS Caltex

Jefferson
County

Norwegian
Tax Authorities

Service
Personnel
and Veterans
Agency
(UK)

Stanford
University

UK Home
Office

University
of Utah
Hospitals
& Clinics

RBS Worldpay

Starbucks

UK Ministry
of Defence

University
of Miami

2007

Compass
Bank

Driving
Standards
Agency

Gap Inc

Hannaford
Brothers
Supermarket
Chain

Monster.com

TK / TJ
Maxx
94, 000, 000

UK Revenue
& Customs

City and
Hackney
Teaching
Primary
Care Trust

Dai Nippon
Printing

Fidelity
National
Information
Services

Driving
Standards
Agency,

TD Ameritrade

Texas Lottery

2006

AOL
20, 000, 000

Countrywide
Financial
Corp

Hewlett
Packard

KDDI

T-Mobile,
Deutsche
Telecom

US Dept
of Vet
Affairs
26, 500, 000

www.informationisbeautiful.net

SOFTWARE SECURITY: DATA BREACHES 2009 - 2011

www.informationisbeautiful.net

SOFTWARE SECURITY: DATA BREACHES 2014 -

latest

2016

2015

2014

Brazzers

ClixSense

Clinton campaign

Cellebrite

Dailymotion
85200000

Friend Finder Network
412, 000, 000

Interpark

Lynda.co.

Netflix Twitter account

Mutuelle Generale de la Police

Philippines Commission on Elections

Linux Ubuntu forums

Minecraft

PayAsUQuest Diagnostics Cross Service apchat

Telegram

Tesco Bank

Three

Waterly by MGAR Ltd

Wonga

Yahoo
32000000

Weebly
43000000

citizenship database
49, 611, 700

Syrian government

Wendy's

uTorrent

River City Media
1370000000

VK
100, 544, 934

Verizon

Anthem
80, 000, 000

Carefirst

Mail. ru
25, 000, 000

MySpace
164, 000, 000

Code.org

US Office of Personnel Management

World Check

VTech

Banner Health

AshleyMadison.com

British Airways

Adult Friend Finder

Australian Immigration Department

Fling
40000000

Mossack Fonseca

Hacking Team

Invest Bank

IRS

CarPhone Warehouse

Promtech

National Childbirth Trust

Premera

Privatization Agency of the Republic of Serbia

New York Taxis

MSpy

Sanric TalkTalk Slack

Securus Technologies

Voter Database
191, 000, 000

Uber

US Office of Personnel Management (2nd Breach)

AOL
2, 400, 000

Community Health Systems

Dominios Pizzas (France)

Experian T-mobile

European Central Bank

JP Morgan Chase
76, 000, 000

NASDAQ

Sony Pictures

MacRumours.com

Staples

Target
70, 000, 000

D&B. Altegrity

Advocate Medical Group

Central Hudson Gas & Electric

Crescent Health c., Walgreens

Drupal

Ebay
145, 000, 000

Facebook

Indiana University

Home Depot

Florida Courts

NMBS

Japan Airlines

Kissinger Cables

Korea Credit Bureau

Neiman Marcus

Mozilla

OVH

Yahoo
500000000

Twitch.tv

UPS

UbiSoft

THE CASE OF PASSWORD LEAKS

	152,445,165	Adobe accounts
	30,811,934	Ashley Madison accounts 🔥
	13,545,468	000webhost accounts
	13,186,088	R2Games accounts
gamigo	8,243,604	Gamigo accounts
HEROES OF NEWERTH	8,089,103	Heroes of Newerth accounts
	5,915,013	Nexus Mods accounts
vtech	4,833,678	VTech accounts
@mail.ru	4,821,262	mail.ru Dump accounts
	4,789,599	Bitcoin Security Forum Gmail Dump accounts
	4,609,615	Snapchat accounts
moneybookers.com	4,483,605	Money Bookers accounts
AdultFriendFinder	3,867,997	Adult Friend Finder accounts 🔥

NETELLER	3,619,948	Neteller accounts
Спрашивай	3,474,763	Спрашивай.ру accounts
MPGH	3,122,898	MPGH accounts
XSplit	2,983,472	XSplit accounts
i-Pmart	2,460,787	iPmart accounts
	2,330,382	Patreon accounts
	1,580,933	Dungeons & Dragons Online accounts
NIVAL	1,535,473	Nival accounts
KM.RU	1,476,783	KM.RU accounts
YOUPORN	1,327,567	YouPorn accounts 🔥
G	1,247,574	Gawker accounts
GAMERZ PLANET	1,217,166	Gamerzplanet accounts
NGU	1,194,597	NextGenUpdate accounts
Yandex	1,186,564	Yandex Dump accounts
Lord of the Rings Online	1,141,278	Lord of the Rings Online accounts

ADOBE BREACH

- Passwords encrypted with 64 bits in ECB (3DES)
  - *Not salted*
  - *Not CBC*
  - *Not AES*

Adobe password data		Password hint	
110edf2294fb8bf4	->	numbers 123456	
110edf2294fb8bf4	->	==123456	❶ 123456
110edf2294fb8bf4	->	c'est "123456"	
8fda7e1f0b56593f e2a311ba09ab4707	->	numbers	
8fda7e1f0b56593f e2a311ba09ab4707	->	1-8	❷ 12345678
8fda7e1f0b56593f e2a311ba09ab4707	->	8digit	
2fca9b003de39778 e2a311ba09ab4707	->	the password is password	
2fca9b003de39778 e2a311ba09ab4707	->	password	❸ password
2fca9b003de39778 e2a311ba09ab4707	->	rhymes with assword	
e5d8efed9088db0b	->	q w e r t y	
e5d8efed9088db0b	->	ytrewq tagurpidi	❹ qwerty
e5d8efed9088db0b	->	6 long qwert	
ecba98cca55eabc2	->	sixxone	
ecba98cca55eabc2	->	1*6	❺ 111111
ecba98cca55eabc2	->	sixones	

Src. Naked Security

ECB VS. CBC ENCRYPTION MODES

Plaintext

ECB Mode Encryption
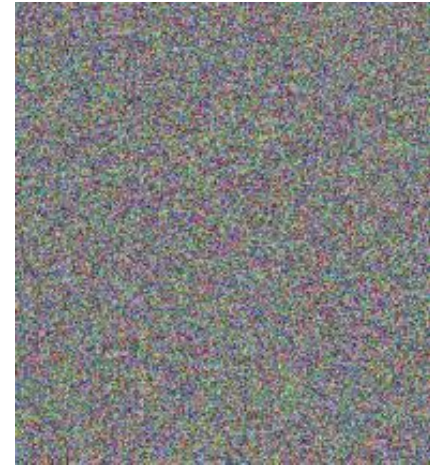
CBC Mode Encryption

$ COST OF CRACKING A PASSWORD (2009)

TABLE 1. Estimated cost of hardware to crack a password in 1 year.

KDF	6 letters	8 letters	8 chars	10 chars	40-char text	80-char text
DES CRYPT	< $1	< $1	< $1	< $1	< $1	< $1
MD5	< $1	< $1	< $1	$1.1k	$1	$1.5T
MD5 CRYPT	< $1	< $1	$130	$1.1M	$1.4k	$1.5 \times 10^{15}
PBKDF2 (100 ms)	< $1	< $1	$18k	$160M	$200k	$2.2 \times 10^{17}
bcrypt (95 ms)	< $1	$4	$130k	$1.2B	$1.5M	$48B
scrypt (64 ms)	< $1	$150	$4.8M	$43B	$52M	$6 \times 10^{19}
PBKDF2 (5.0 s)	< $1	$29	$920k	$8.3B	$10M	$11 \times 10^{18}
bcrypt (3.0 s)	< $1	$130	$4.3M	$39B	$47M	$1.5T
scrypt (3.8 s)	$900	$610k	$19B	$175T	$210B	$2.3 \times 10^{23}

[Percival 2009]

Only includes cryptographic hardware cost
Letters are 26 alphabet letters in lowercase

DISRUPTION EXAMPLES: ENTER CRYPTOCURRENCIES

- Developments
  - scrypt is used as proof-of-work in cryptocurrencies (e.g., Litecoin)
  - ASICs achieve > 10^{10} SHA256 Hash / second

S9j-14.5 TH/s with PSU

Shipping: Sep. 21-30

446 USD

Weight   8 kg

Quantity   [-   1   +]

ARE WE TOO OPTIMISTIC?

- Even the wealthiest computer technology companies are not careful!

KrebsonSecurity
In-depth security news and investigation

21 **Facebook Stored Hundreds of Millions of User**
MAR 19 **Passwords in Plain Text for Years**

WHY? OBSERVATIONS

- Lagging behind
  - Under-estimating attacks
  - Inertia: systems designed and deployed years ago
  - Security mechanisms are not user friendly
  - Increasing rate of attacks
    - *Span both foundations, design, and implementation*
    - *TLS/SSL, WPS, cars, implantable devices, CPS (ADS-B, Water Control System, ILS)*
- Incentives
  - Monetization
  - Cyberwarfare, terrorism, industrial espionage
- New attack-enabling technologies
  - Abuse of privacy infrastructure: Tor, Bitcoins
  - Connectivity
  - Open source software/hardware are exposing the limitations of security through obscurity and fundamental design flaws
    - *Access to cryptography*
  - Policies: BYOD

- Issues exacerbated in wireless and mobile

WIRELESS IS UBIQUITOUS

- Beyond mobile devices (cellular, Wi-Fi, Bluetooth)
  - GPS assist in air traffic
  - Transportation systems
  - Smart grid (power plants sync, smart meters)
  - Implantable devices
- It's security and robustness are critical for a variety of applications
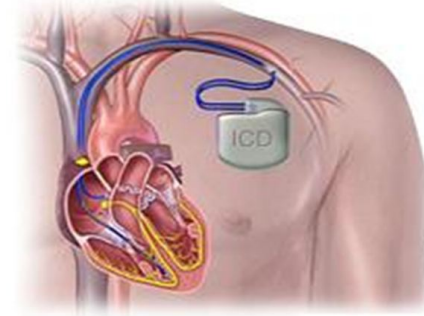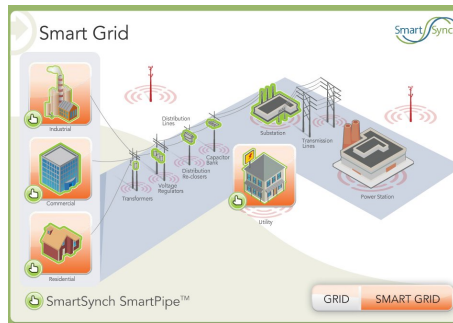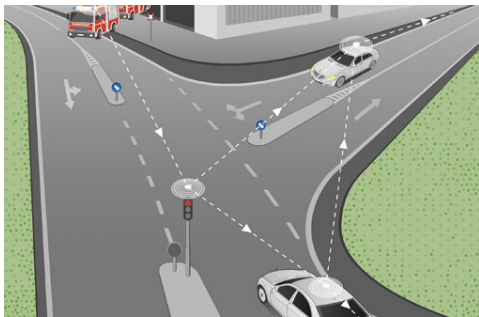
WIRELESS IS UBIQUITOUS

- Beyond mobile devices (cellular, Wi-Fi, Bluetooth)
- It is also used in harmful applications

ISIS Propaganda Video Drops A Bomb From A Drone

ISIS RELEASED THIS PROPAGANDA VIDEO

WIRELESS SYSTEMS CHARACTERISTICS

- Unique characteristics with fundamental constraints:
  - Broadcast medium
  - RF spectrum
  - Energy

- Limited resources led to complex designs and systems
  but also weaknesses

WIRELESS SYSTEMS CHARACTERISTICS

- Unique characteristics with fundamental constraints:
  - Broadcast medium
  - RF spectrum
  - Energy

- Limited resources led to complex designs and systems but also weaknesses

WIRELESS SYSTEMS CHARACTERISTICS

- Unique characteristics with fundamental constraints:
  - Broadcast medium
  - RF spectrum
  - Energy

- **Limited resources** led to **complex designs** and **systems** but also **weaknesses**

ASSUMPTIONS IN WIRELESS & MOBILE SYSTEMS

- Wireless systems are complex

- 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

WIRELESS THREATS TO RESILIENCY

- Past: large easily detectable jammers

- Today: commodity on ebay!
  - Low-cost, small form factor, mobile
  - Repurposed microwave cavity magnetron: $7
  - Youtube DIY videos
  - Proliferation of SDR e.g., HackRF, BladeRF, LimeSDR, XTRX
  - Smart phone as SDRs
    - *Broadcom Wi-Fi SoC w/ TLV vulnerability* [Beniamini 2017]

- Smart energy-efficient cyber-mines
  - Hard to detect, target control mechanisms
  - Combined with malware

- Softwarization of wireless systems including hardware

2016

2015

2014

Brazzers

ClixSense

Clinton campaign

Interpark

Lynda.co.

Netflix
Twitter account

PayAsUQuest Diagnostics Cross Service

apchat

.elegram

Tesco Bank

Three

Waterly
by MGAR
Ltd

Wonga

Yahoo
32000000

Philippines
Commission
on Elections

Weebly
43000000

citizensnip
database
49, 611, 700

Cellebrite

Mutuelle
Generale
de la Police

Linux Ubuntu
forums

Minecraft

Syrian
government

Wendy's

uTorrent

Dailymotion
85200000

Friend
Finder
Network
412, 000, 000

River City
Media
1370000000

VK
100, 544, 934

Verizon

Anthem
80, 000, 000

Carefirst

MySpace
164, 000, 000

US Office
of Personnel
Management

World Check

Mail. ru
25, 000, 000

Code.org

VTech

Banne.
Health

Privatization
Agency
of the
Republic
of Serbia

Voter Database
191, 000, 000

Mossack
Fonseca

AshleyMadison.com

Fling
40000000

Hacking
Team

Invest
Bank

National
Childbirth
Trust

Premera

Uber

British
Airways

romtech

Sanric

TalkTalk

ilack

Adult Friend
Finder

Australian
Immigration
Department

IRS

New York
Taxis

Securus
Technologies

US Office
of Personnel
Management
(2nd Breach)

CarPhone
Warehouse

Experian
T-mobile

MSP

AOL
2, 400, 000

Community
Health
Systems

Dominios
Pizzas
(France)

JP Morgan
Chase
76, 000, 000

NASDAQ

European
Central
Bank

Sony Pictures

Target
70, 000, 000

Ebay
145, 000, 000

Home Depot

MacRumours.com

Yahoo
500000000

Twitch.tv

D&B, Altegrity

Staples

Korea Credit
Bureau

Neiman
Marcus

UPS

Facebook

NMBS

Japan Airlines

Mozilla

Advocate
Medical
Group

Central
Hudson
Gas & Electric

Crescent
Health
c. Walgreens

Drupal

Florida
Courts

Kissinger
Cables

OVH

UbiSoft

Indiana
University

21

BEYOND INTEREST TO MILITARY APPLICATIONS

- Starting point for attacks on privacy: rogue infrastructure
  - Smart-jam & downgrade a cellular network to 2G one-way auth
  - Smart-jam & carry MITM attack against WPA-Enterprise

- Many unencrypted protocols with many possibilities for exploitation
  - Public safety P25 [Clark et al. 2011]
  - Aviation ADS-B broadcast [Strohmeier et al. 2018]
  - Instrument Landing System (ILS) [Sathaye et al. 2019]

CELLULAR WIRELESS COMMUNICATION

- Illustration with GSM system:
  - FDMA:
    - *Carrier channels of 200KHz*
    - *Very few Beacon Frequencies*
  - TDMA:
    - *8 time slots*
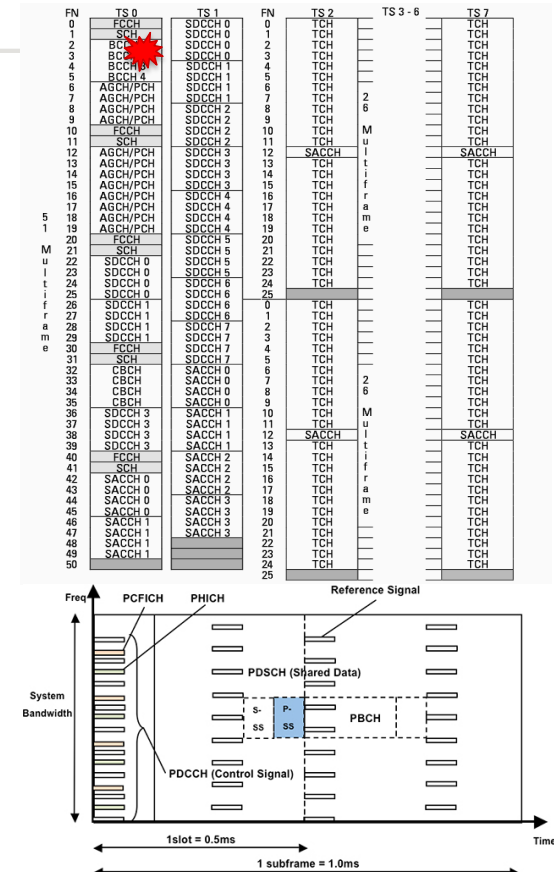   - *TS0: carries most control traffic*
  - Super Frame Structure:
    - *Critical information such as FCCH, SCH, BCCH1 is only scheduled 1/51 frames*
  - ⇒ 1 pulse every 400 timeslots on a 200KHz band (out of many bands) prevents all communication
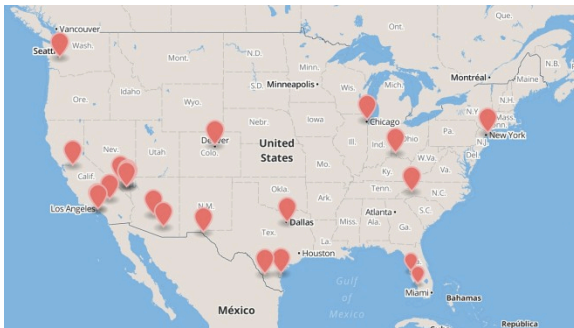
- CDMA, OFDM have similar weaknesses (WiMax, LTE):
  - Pilots, beacons
  - LTE control information is within 1MHz (out of possibly 20MHz)

CELLULAR WIRELESS COMMUNICATION

- Attack steps
  - Stealthy & localized 4G/3G/2G jamming
  - Downgrade to 2G rogue BTS
  - Identify targets: IMSI
  - Insert: SMS, Tweets
- 2014: 19 fake BTS detected; [Li et al. 2017]: many more!
  - Rudimentary techniques

The Register®
Biting the hand that feeds IT

DATA CENTER   SOFTWARE   **SECURITY**   DEVOPS   BUSINESS   PERSONAL TECH   SCIENCE   E

Security

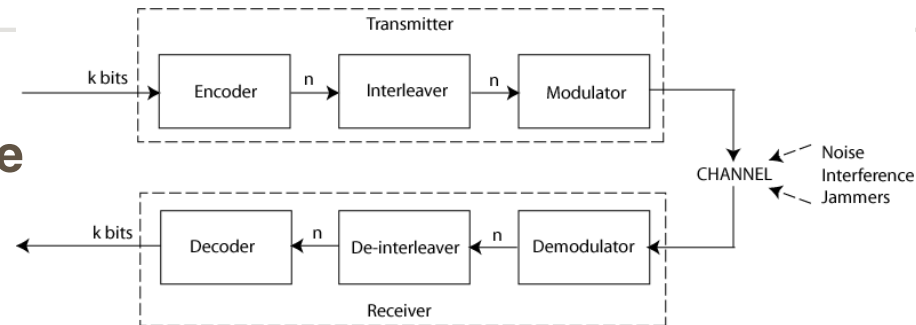**Fake mobile base stations spreading malware in China**

'Swearing Trojan' pushes phishing texts around carriers' controls

By Richard Chirgwin 23 Mar 2017 at 05:02   10 💬   SHARE ▼

JAMMING DATA PACKETS

Link Architecture

Transmitter: k bits → Encoder → n → Interleaver → n → Modulator → CHANNEL ← Noise, Interference, Jammers

Receiver: CHANNEL → Demodulator → n → De-interleaver → n → Decoder → k bits

Jamming Unreliable Communication

UDP

JP

RP

Jamming ECC Protected Communication

UDP
EDP

JP

$> \lfloor d_{min}\text{-}1/2 \rfloor$

Jamming Interleaved ECC Protected Communication

UDP
EDP
IDP

JP

DDP

$> \lfloor d_{min}\text{-}1/2 \rfloor$ errors within a single codeword

UDP: Uncoded Data Packet

JP: Jamming Packet

EDP: Encoded Data Packet in l codewords

RP: Received Packet

IDP: Interleaved Data Packet
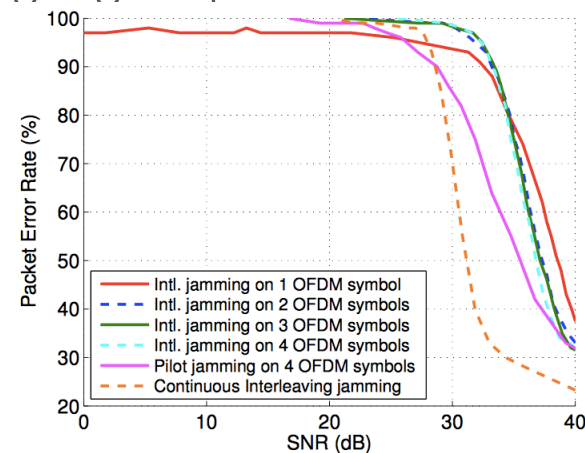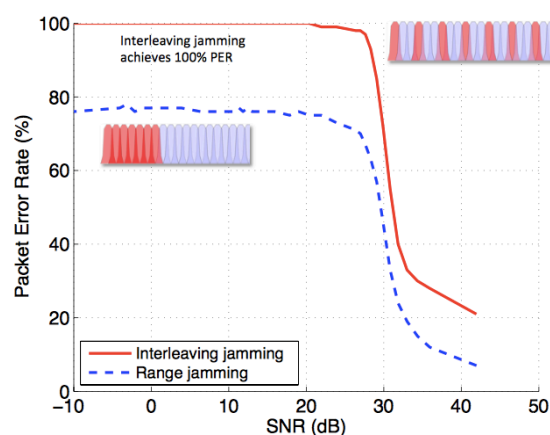
DDP: De-Interleaved Packet

d_{min}: code minimum Hamming distace

Example: IEEE802.11 packet 12,000 bits [Noubir et al. 2003]

APPLICATION TO IEEE802.11AG

- 48 OFDM data sub-carriers with predictable interleaving
  - Jam 7 out of 48; Jam 1-2 OFDM symbols
  - 3 orders of magnitude weaker jamming signal [Vo-Huu et al. 2016]

- Can be combined with smart attacks on RAA
  - Stealthy, up to 5 orders of magnitude lower energy cost

# IEEE802.11 AUTO-RATE ATTACKS

- Observation
  - 2 links with 54Mbps
    - *Each link has a throughput of 17.74 Mbps*
    - *Total throughput: 35.48 Mbps*
  - 1 link with 54M, the other with 1Mbps
    - *54M link: 0.95 Mbps*
   - *1M link: 0.94 Mbps*
    - *Total throughput: 1.89 Mbps*

1 Mbps	54

- Attack [Noubir et al. 2011]
  - Adversary targets weakest link
  - Existing auto-rate protocols easy to keep a node at low-rate,
  - Results in increase of collision probability, some auto-rate protocols exhibit congestion collapse behavior
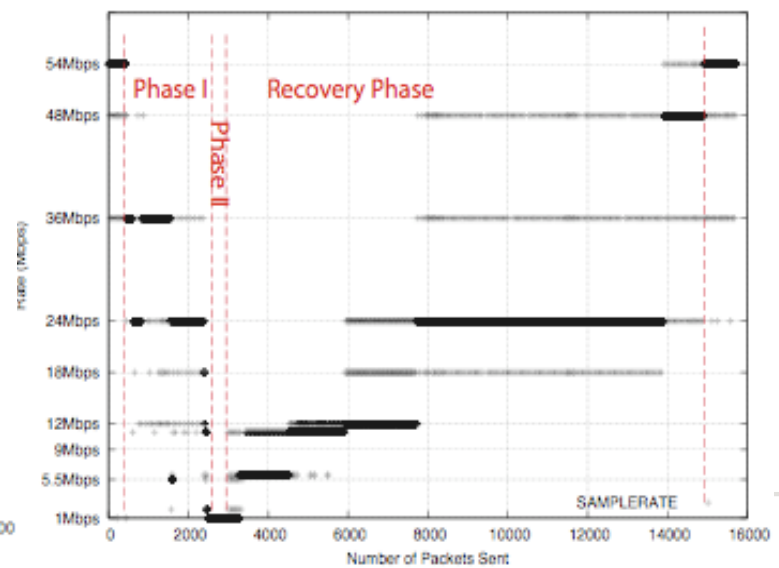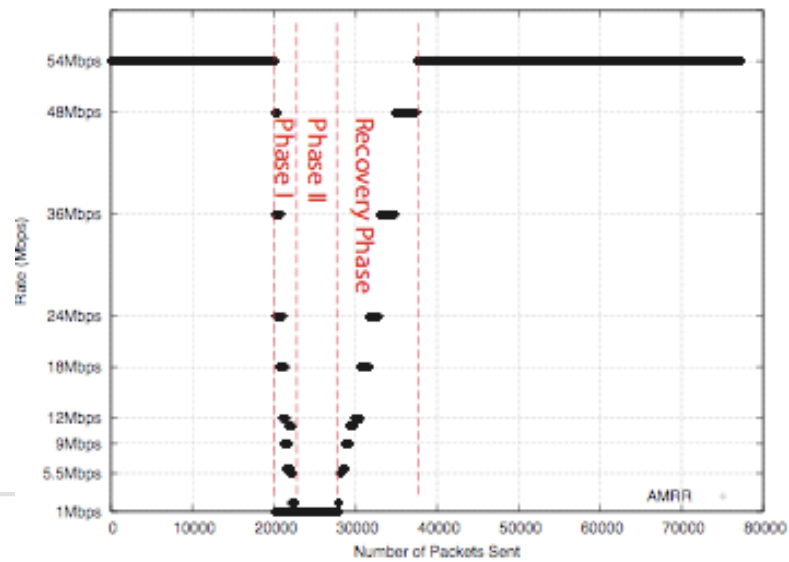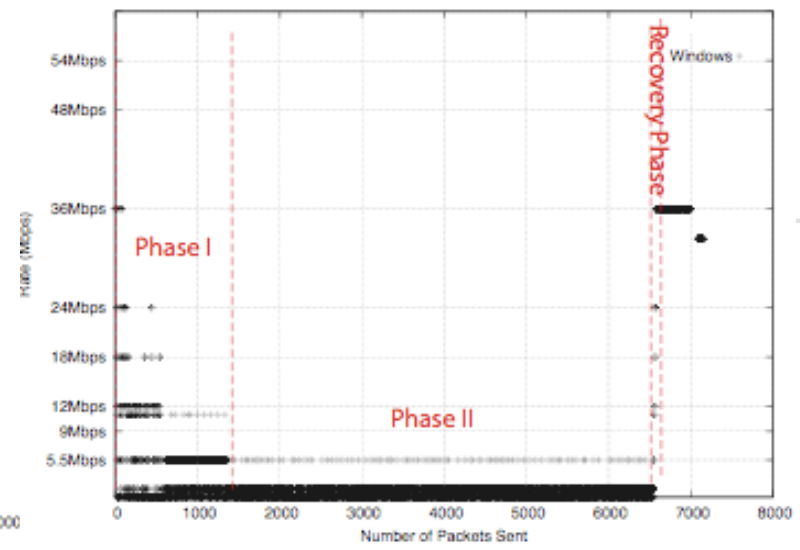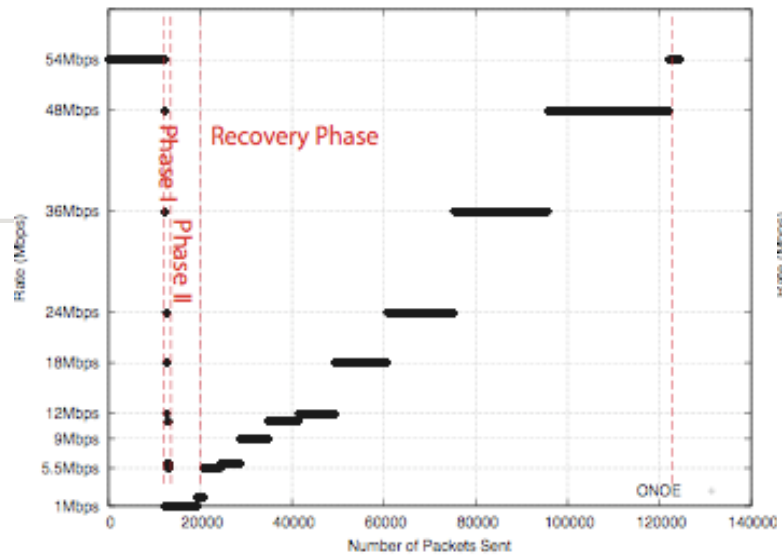
GLOBAL CONGESTION ATTACKS ON WI-FI NETWORKS VIA INTERFERENCE COUPLING

- Congestion that propagates in time and space [Xin et al. 2017]
  - Existence of phase transition behavior
  - Enables remote attacks
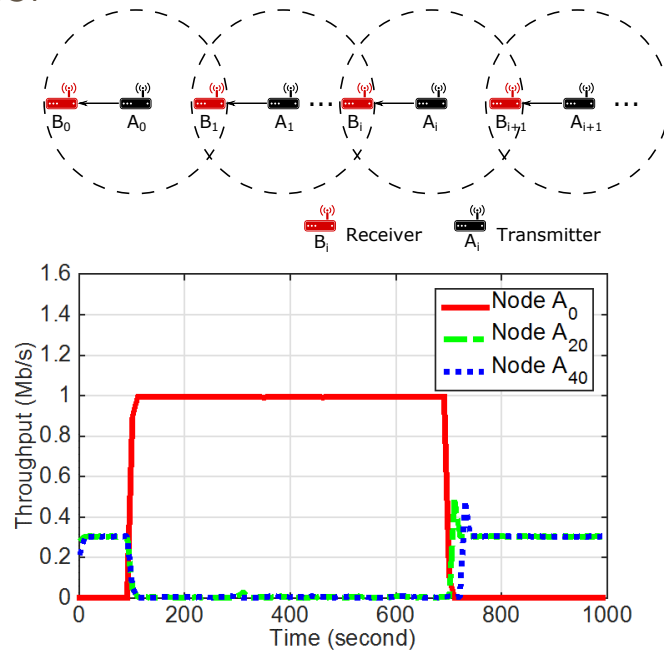
WPA-ENTERPRISE ATTACK

- Targeted & Stealthy credentials capture [Cassola et al. 2013]
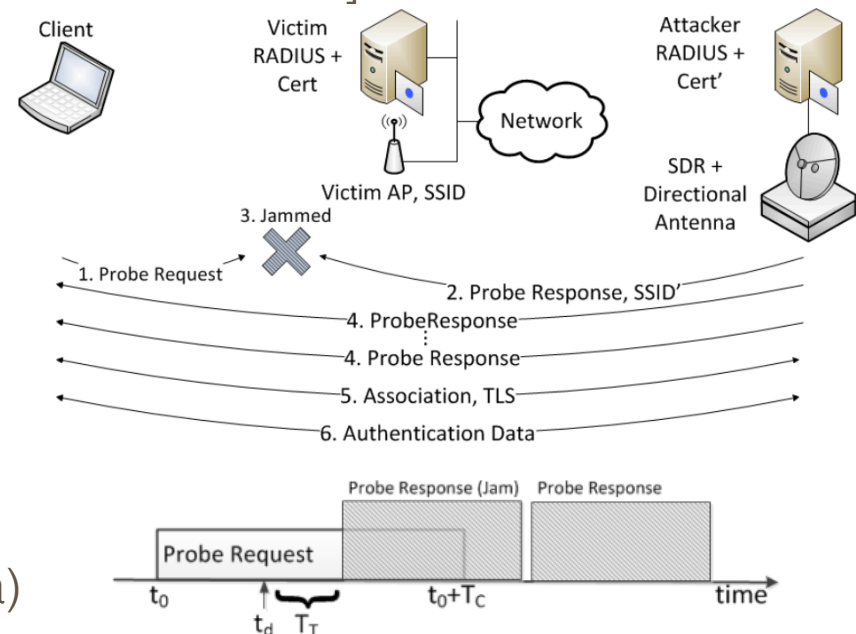 - MAC Address
- Long range 400m

- Several low level details
  - Overcome OS protections

- Rise of Wi-Fi targeted attacks
  - Darkhotel APT through Wi-Fi (mostly Asia)
  - Targets included CEOs, senior vice presidents, sales and marketing directors and top R&D staff

REMOTE SIDE-CHANNEL ATTACKS

- Many powerful side-channel attacks assume physical access to the device

- Screaming channels work shows this assumption to be invalid [Camurati et al. 2018]

- Locally compromised device enables remote side-channel attacks
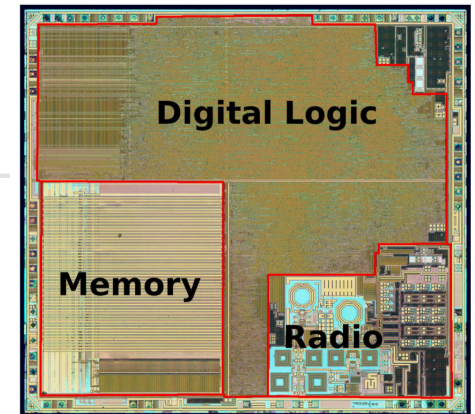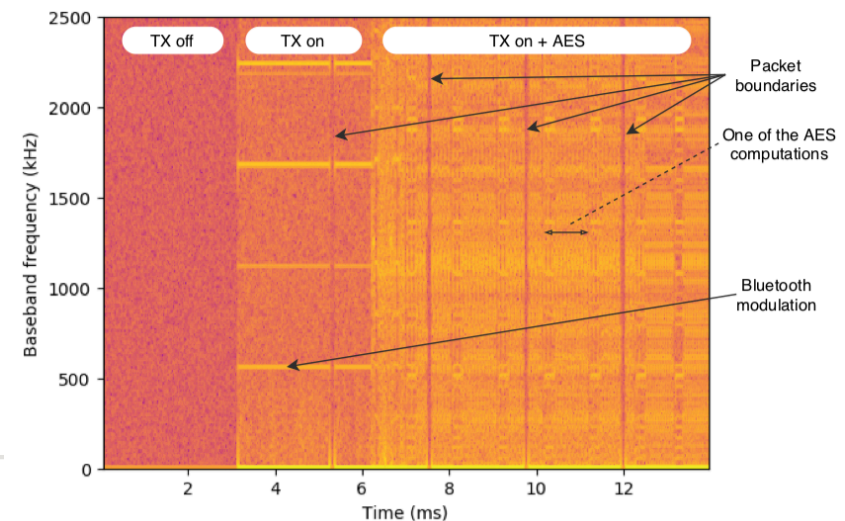 - Tools like nexmon

Figure 1: Labeled die picture from an nRF51822 Bluetooth LE 2.4GHz mixed-signal design chip. Digital and Analog parts of the chip can be easily distinguished (Original picture CC BY 3.0 by zeptobars [56]). This chip is very similar to the chip we use in our experiments.
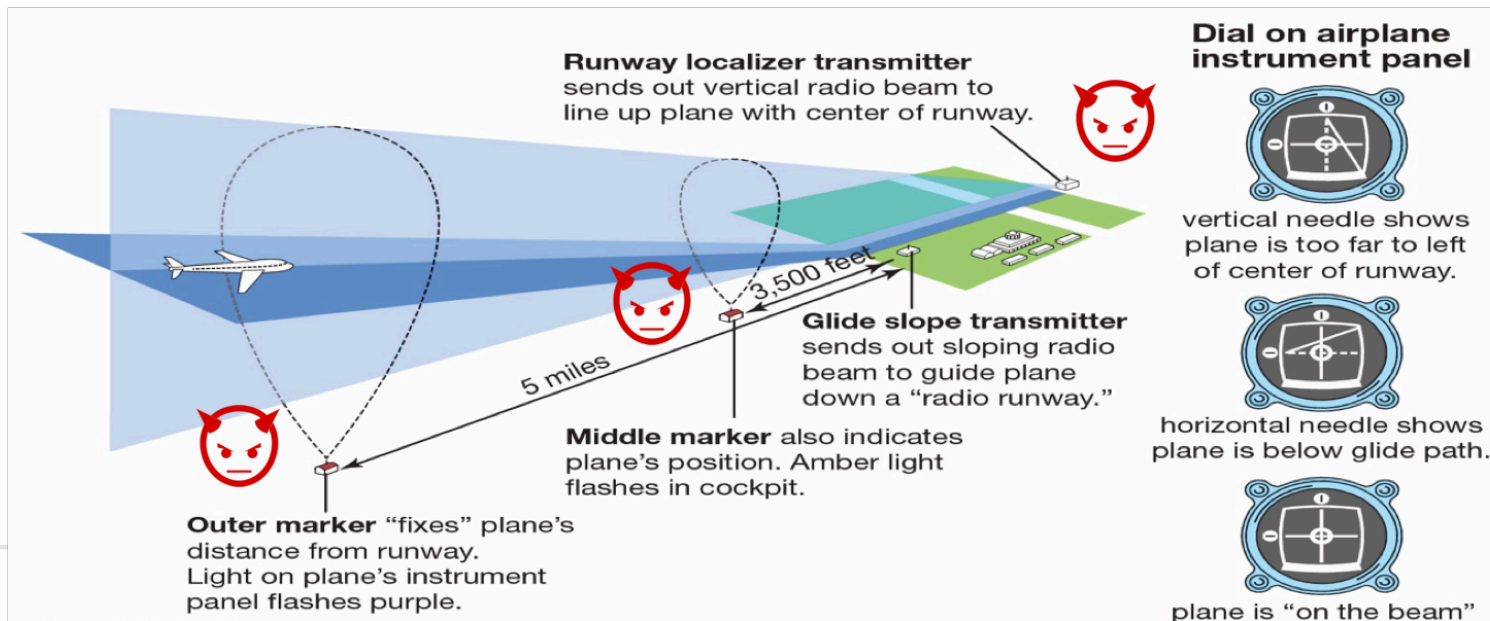
CYBER PHYSICAL SYSTEMS

- Power grid [Shepard et al. 2012]
  - GPS spoofing results in desynchronized PMUs
  - Desynchronized measurements lead to incorrect assessment of electric generators stability
  - E.g., 10 degree difference automatically trips the generators
  - Tripping a single generator can result in a cascade of failures [2003 Blackout]

- Aviation ADS-B (mandated by 2020)
  - Location inference
  - Ghost aircraft disturbance
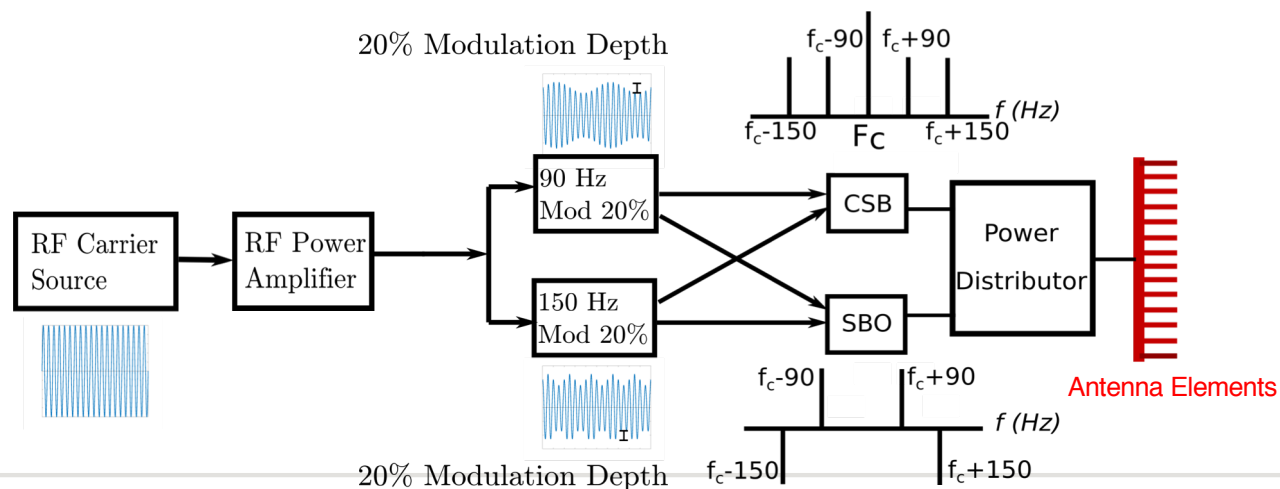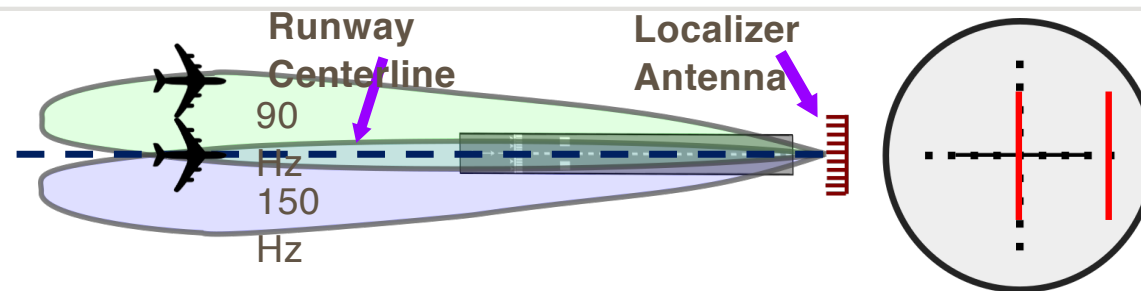 - Privacy breaches: M&A, states relations [Strohmeier et al. 2018]

CPS: AIRCRAFT LANDING SYSTEMS

- **Marker beacon:** allow pilots to accurately guage their distance from runway (on off keying, 75 MHz

- **Localizer:** used to correctly center an aircraft during landing (two yagi antennas, transmitting a code continuously at 108.1 and 111.95 MHz)

ILS TRANSMITTER

Runway
Centerline
90
Hz
150
Hz

Localizer
Antenna

20% Modulation Depth

f_c-90 f_c+90

f_c-150 Fc f_c+150 f (Hz)

RF Carrier Source	RF Power Amplifier	90 Hz Mod 20%	CSB	Power Distributor
		150 Hz Mod 20%	SBO	

Antenna Elements

f_c-90 f_c+90

f_c-150 f_c+150 f (Hz)

20% Modulation Depth

CPS: ILS

- [Sathaye et al. 2019]

HACKING LANDING SYSTEMS —

The radio navigation planes use to land safely is insecure and can be hacked

Radios that sell for $600 can spoof signals planes use to find runways.

DAN GOODIN - 5/15/2019, 6:00 AM

PRIVACY: TRACKING AND BEYOND

Wireless and mobile systems
are riddled with opportunities
for attackers

Softwarization is decreasing the cost

ATTACK ON APPLE WIRELESS DIRECT LINK (AWDL)

$20

- Apple Wireless Direct Link (AWDL) based on Wi-Fi ad hoc mode
  - AWDL is widely used (over billion iOS, macOS, tvOS, watchOS devices)
  - Device-to-device services e.g., Apple AirDrop, and by Apple Watch & TV
  - Services rely on a combination of AWDL and Bluetooth LE

- Design and implementation flaws [Stute et al. 2019]
- Attacks without connecting to the same network
  - Expose users' long-term information
    - *Real MAC address, device owner names, etc.*
    - *Enables efficient tracking*
  - Denial of service attack
    - *Targeted crashing*
    - *Simultaneously crash (blackout)*
  - Man-in-the-middle AirDrop file transfers, intercept and modify
- Disclosed to Apple, released fix to DoS [November 2018]

- Beyond Apple ecosystem: Wi-Fi Neighbor Awareness Networking (NAN), Google Android NAN


```
                              Shell
neo:Desktop demo$ sudo ./mowl -i en0 -a crash -t Janes-iPhone
11:20:21 INFO : WLAN device: en0
11:20:21 INFO : Host device: tap0
```

FINGERPRINTING WIRELESS RADIOS

- Wi-Fi radio fingerprinting [Vo-Huu et al. 2017]
  - RF Techniques: ramp-up/down, CFO/SFO,
  - Wi-Fi specific: scrambling seed
  - Machine learning + heuristics
- Evaluated in the wild on 100 Wi-Fi interfaces
  - 65% to uniquely identify a device
  - 93% to distinguish between 5 interfaces

- Fingerprinting & localization of cellular radio interfaces

(a) Transient at frame start
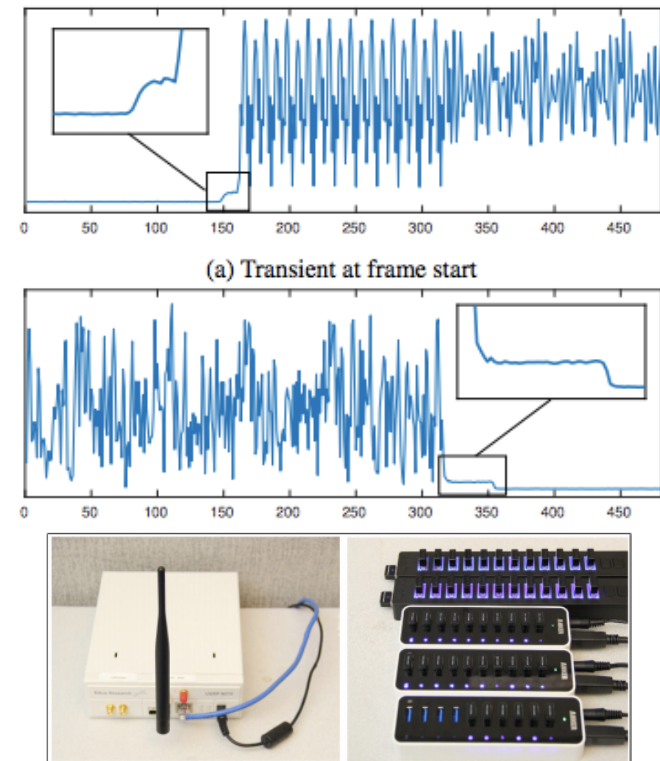
LTE LOCALIZATION/FINGERPRINTING

- Unencrypted control channels
  - Devices unique & temporary identifiers
    - IMSI, TMSI, RNTI
  - Complete access to scheduling information
  - Quantity and location of assigned resources in uplink and downlink

- Can long-term identify & localize a user?
- Tracking and fingerprinting
  - Radio & Identifiers
  - But also the set of apps
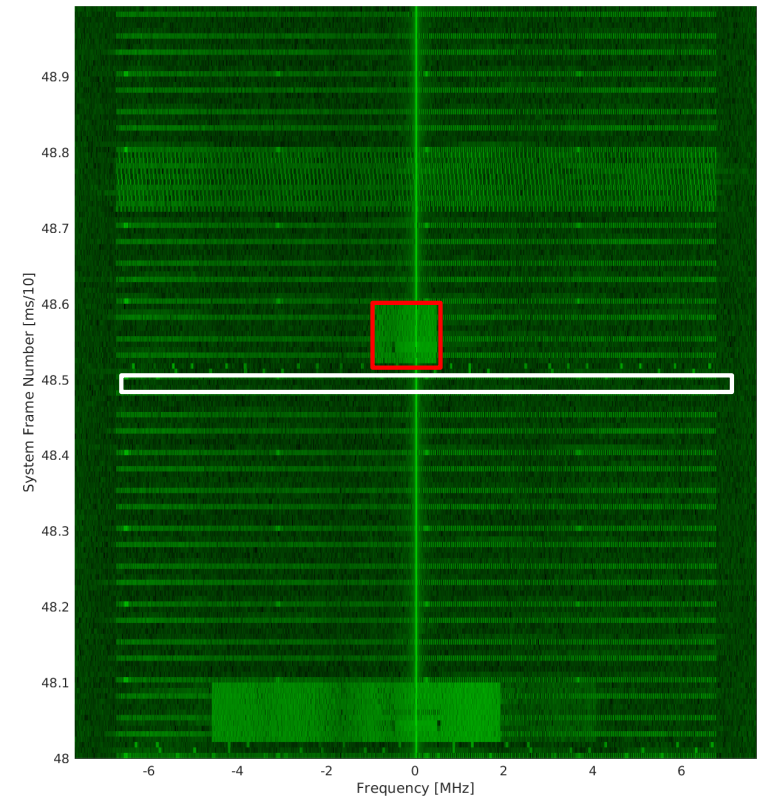
REVISING THE MODELS: ADVERSARY

- Softwarization enables
  - Flexibility in wireless systems e.g., Wi-Fi, Bluetooth, Cellular
  - Standards are available as open source software

- Adversary can
  - Decode, encode, mimick any protocols
  - Operate on a wide spectrum in real time
  - Sense and intercept RF emissions anywhere including being local

- Adversary wants
  - Intercept, block, infer (location, traffic), deceive (drain, jujitsu)

- Adversary will (intentional or unintentional)
  - Jam (GPS case 2013)
  - Fake BTS

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes

REVISING THE MODELS: COMP. & COMMS

- Softwarization enables advanced techniques: flexibility, agility, robustness
  - Information/communications theory, game theory, machine learning

- Software security for wireless systems
 - Trusted Execution Environments for RF

CURRENT STATE OF WIRELESS SYSTEMS

- Today's wireless networks are brittle with complex control mechanisms
    - prone to cross-layer attacks and amplification effects

- Wireless permeates the cyber and physical worlds
    - increasingly connecting legacy and new systems

- Attacks on wireless links have implications on the overall system
    - targeted and stealthy

- Unlike in software, many wireless attacks are not fixed

HOW ABOUT MOBILE SYSTEMS?

HOW MALICIOUS CAN A FLASHLIGHT APP BE?

Reviews

4.7

★★★★★

👤 1,226,372 total

★ 5		1,024,526
★ 4		126,377
★ 3		32,330
★ 2		11,229
★ 1		31,901
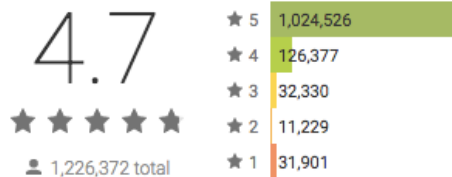
FTC Approves Final Order Settling Charges Against Flashlight App Creator

https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app
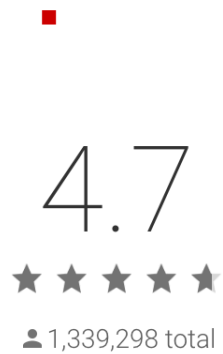
Brightest Flashlight Free ®
GoldenShores Technologies, LLC
Free

Version 2.4.2 can access:

📍 **Location**
- approximate location (network-based)
- precise location (GPS and network-based)

🖼 **Photos/Media/Files**
- modify or delete the contents of your USB storage
- read the contents of your USB storage

📷 **Camera**
- take pictures and videos

ℹ **Device ID & call information**
- read phone status and identity

❓ **Other**
- disable or modify status bar
- read Home settings and shortcuts
- control flashlight
- prevent device from sleeping
- view network connections
- full network access
- install shortcuts
- uninstall shortcuts

IN 2019

4.7

★ ★ ★ ★ ★

👤 1,339,298 total

5	▬▬▬▬▬▬▬▬▬▬
4	▬
3	▪
2	▪
1	▪

Privacy Policy

Below is a summary of the Brightest Flashlight® privacy [policy. The f]ull privacy policy is contained within the [Brightest Fl]ashlight Free® EULA (End-User License [Agreement)], which is reproduced below. In the case where [the polic]y and the EULA disagree, the EULA is the [prevailing d]ocument.
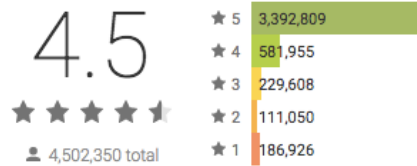
Privacy Policy Summary:

1. COLLECTION & TRANSMISSION OF GEOLOCATION INFORMATION. Goldenshores Technologies and its subsidiaries and agents may collect your geolocation based information and transmit that information to third-party service providers. Geolocation includes data regarding your device's geolocation, including but not limited to GPS-based, WiFi-based, or cell-based location information. The specific category of persons or entities referred to as "third-party service provider" consists of persons or entities that provide

LESS INTRUSIVE FLASHLIGHT APP

-

PURELY MOBILE: ZERO PERMISSIONS MALICIOUS APP

- Variety of sensors
  - Gyroscope, accelerometer, compass, microphone, cameras
  - Many do not require permissions
- Requesting GPS/Location can be viewed as suspicious

- Can we infer?
  - Gender? Age? Health information?
  - Work location, home? Identity? Social circle?

- Since 2014, we demonstrated a variety of attacks
- Illustrated in two attacks Zero Permissions
  - High accuracy keylogging [Narain et al. 2014]
  - Location Tracking [Narain et al. 2016]

Microphones

STMicroelectronics H3G2 Gyroscope

hTC
beats
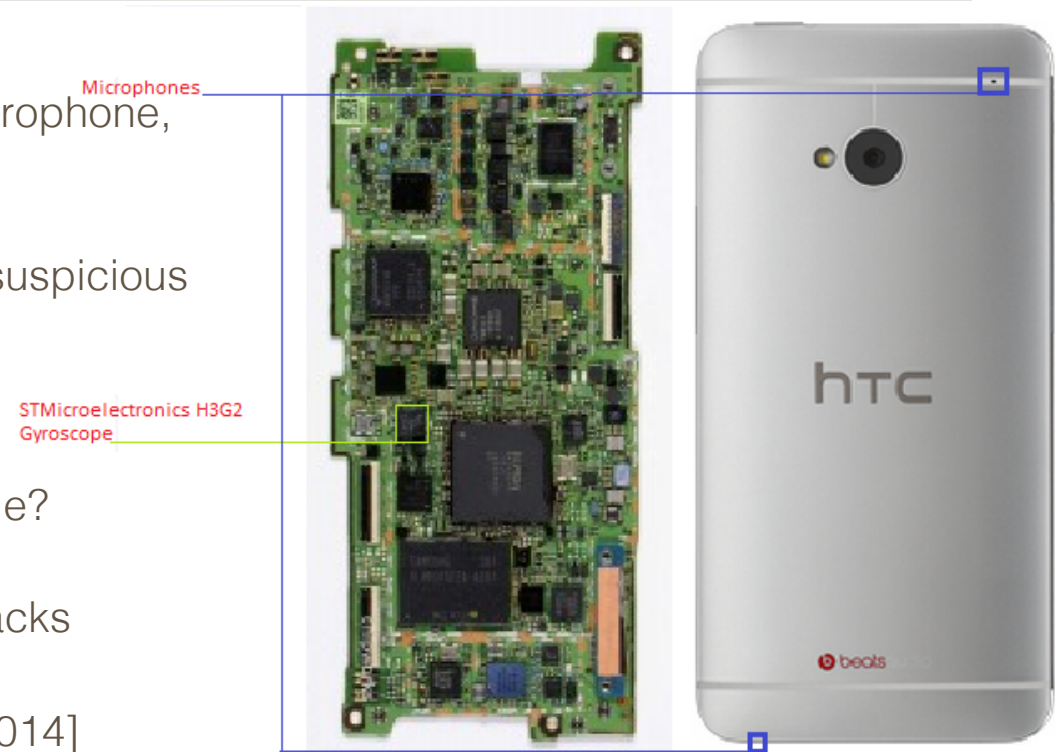
# INFERRING LOCATION INFORMATION WITHOUT PERMISSIONS

- Goal is not to build an Inertial Navigation System
  - Gyroscope is fairly accurate
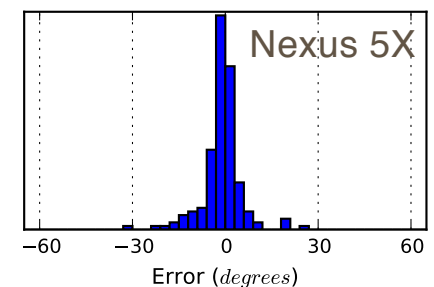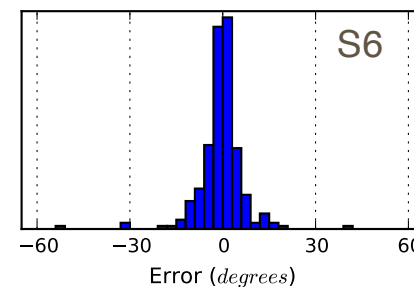 - Accelerometers and compass are noisy
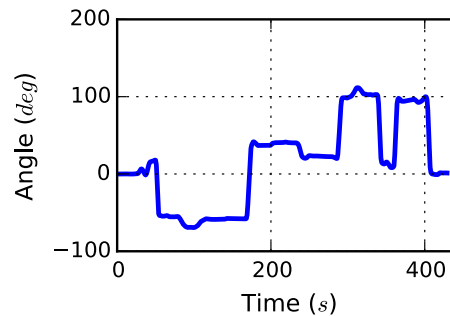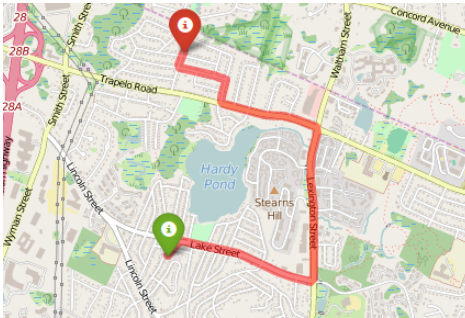
- Collect sequence of turns
- Infer most likely trajectory

INFERRING LOCATION INFORMATION

- Open Street Maps data => build a directed graph
 - Enhance with road signature (curvature, compass headings, speed limit, potholes)
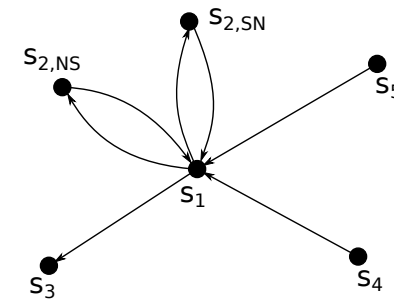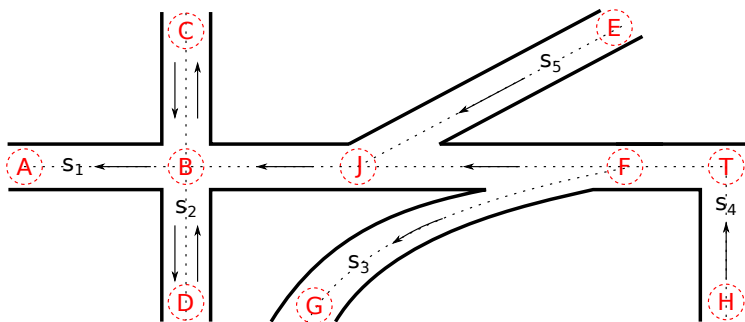
- Problem: finding maximum likelihood path
  - Error approx. by Gaussian

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% path in top 10
  - Real experiments in Boston [140 paths, 1000Km]
    - Boston (30%) and Waltham (60%) single attempt
  - Better results for longer lists, longer paths
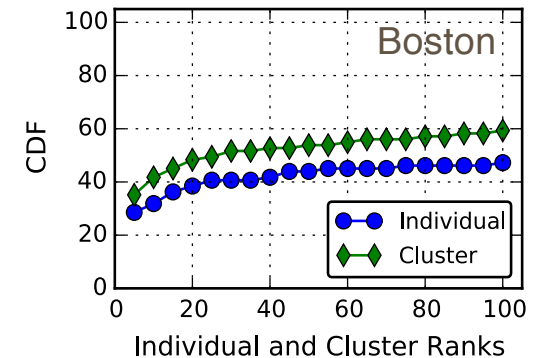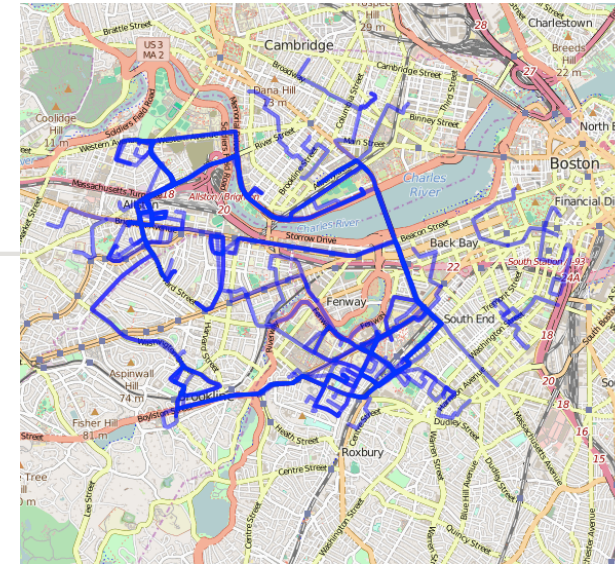
KEYLOGGING

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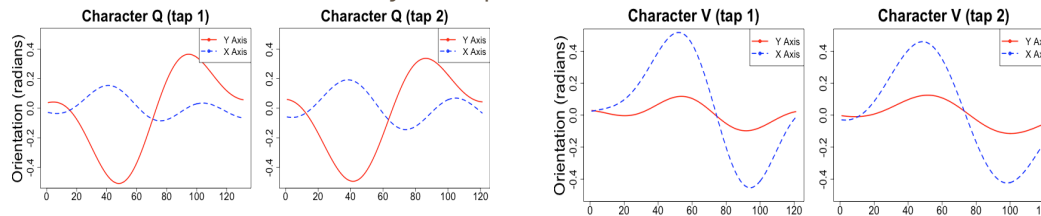
- Stereo-Microphones unique delay & amplitudes e.g., HTC One
  - Distance between microphones: 0.134 m
  - Maximum supported sampling rate: 48 KHz
  - Speed of sound in air: 340 m / s
  - Difference of +*19 samples* to -*19 samples*
- For future devices with higher sampling rate
  - Example sampling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

EVALUATION
(META-ALGORITHM)

- Meta-Algorithm
  - Combines several signal processing & machine learning techniques
  - Decompose keyboard

- Possible to guess keys (qwerty)
  - > 60% using gyroscope
  - > 90% using microphone

- Possible to achieve > 95% for Number keyboard

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 waiting for target app

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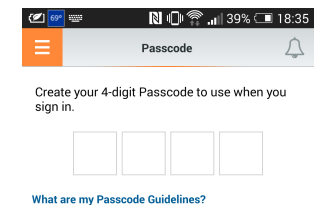
Total	Correct	Correct Digits	Accuracy
PINs			
100	84	376	94%
Credit Cards			
100	52	1467	91.5%

EXPLOITATION

- Access to sensors is either permissionless or easily obtainable

- For using microphone convincing a user to install an App with microphone permission

- Exploiting a vulnerability in a popular App

 # WIRED

LILY HAY NEWMAN SECURITY 05.14.19 12:05 PM

# HOW HACKERS BROKE WHATSAPP WITH JUST A PHONE CALL

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 [Block et al. 2018]
  - 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

Correlation Result,, Grp. Avg. Xamarin Cloud Nexus 622
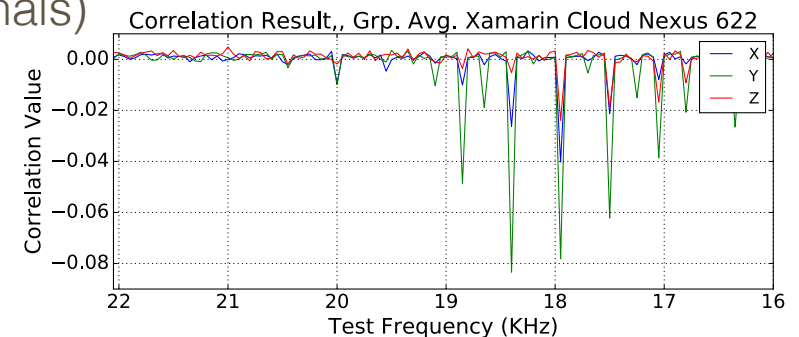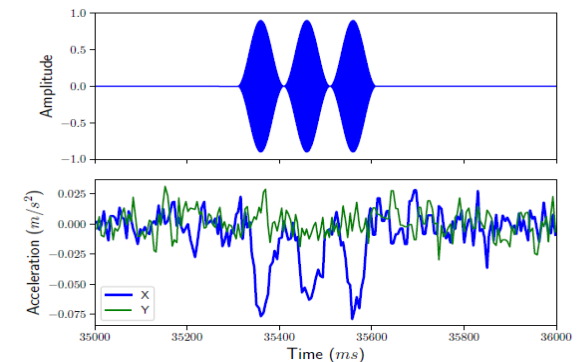
IS THE TRADITIONAL SECURITY CYCLE ADEQUATE?

- We are increasingly reliant on wireless and mobile devices

- Is this control system stable?
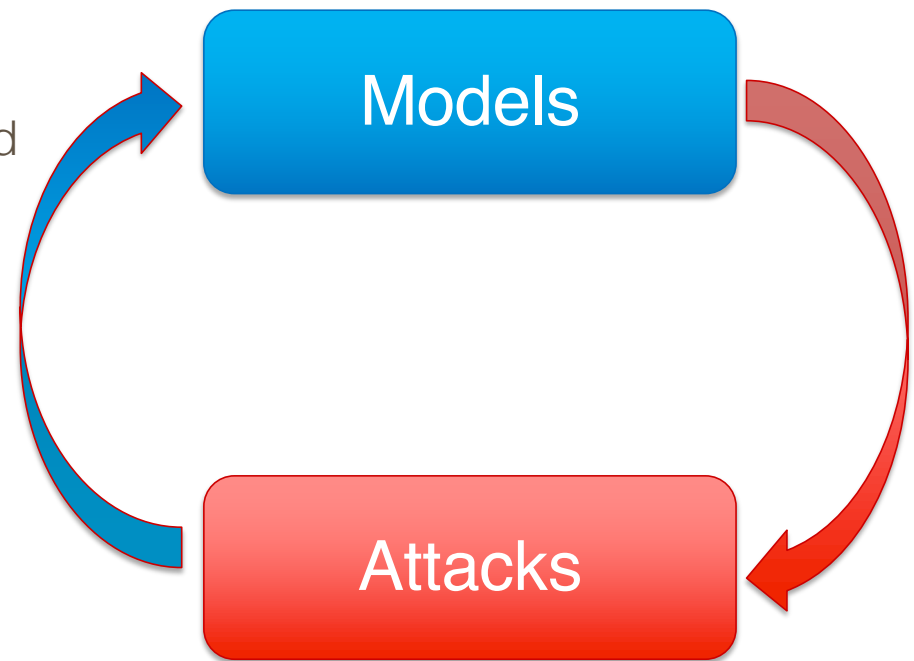
INFORMATION AND COMMUNICATIONS THEORY

- Misconceptions in wireless systems

- Shannon's separation theorem is only for point-to-point communications
  - Not valid for multi-user systems (e.g., massive M2M/IoT)
  - Many open questions in network information theory

- Spread spectrum is not the best technique to counter interference in the wideband regime
  - Impulsive-FSK is!

SECURING WIRELESS AND MOBILE SYSTEMS

- Systematic approach to modeling security threats and defenses
- Security by design considering software-enabled attacks
- Securing timing and localization

- Elastic Networks provide seamless adaptivity
- As the adversary increases effort performance only reduced proportionally to adversaries effort
  - Worst case requires local decision
- No amplification effect across the stack

ELASTIC NETWORKS

- Develop and analyze elastic communication techniques
  - Theoretical foundations (algorithms, analysis, architecture)
  - Experimental evaluation
- Techniques for Elasticity
  - Physical/Link
    - *Multi-carrier/antenna, super-position coding*
    - *Enabling techniques: keyless spread-spectrum, Impulsive-FSK, stealthy rates, game theory*
  - Routing
    - *Back-pressure routing for elastic radios, QoS support, heterogenous links*
  - Transport
    - *Network-coded MultiPath TCP – transparent to applications*
  - Application
    - *Traffic prioritization, adaptive bitrate streaming for multimedia traffic (DASH)*

ILLUSTRATIONS OF ELASTIC NETWORKS

- **FBMC as an illustrative example of elastic PHY/Link**
  - Agility through flexible carriers use
  - Easticity through noise rejection/carriers independence
 - Better than OFDM: spectral efficiency & potential for robustness
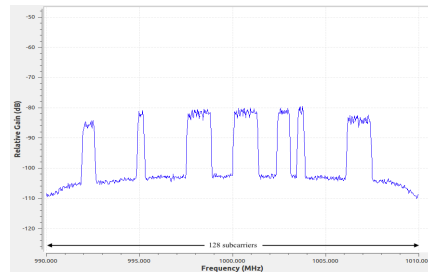
- **Smart antenna systems for anti-jamming, localization**
- **Stealthy rates to prevent smart cross-layer att**
- **Mitigates an attacker with over 5 orders of ma**
  more power
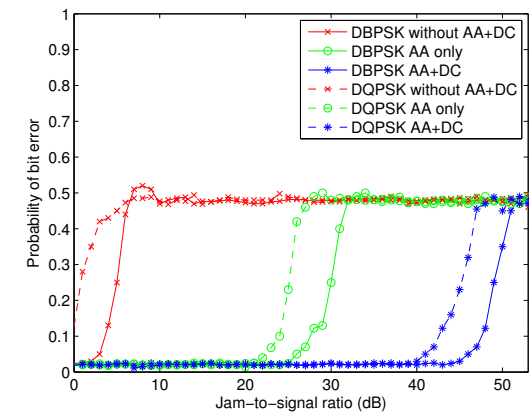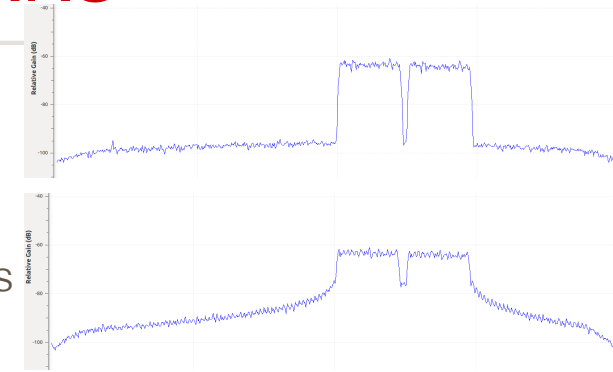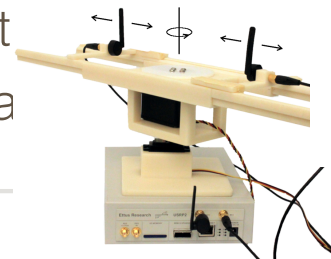
MATRIX: SYSTEMATIC AUDITING & SANDBOXING OF MOBILE APPS

- Auditing: *Privoscope* keeps track and visualizes apps access to services and sensors

- MATRIX: seamless full control on what Apps access [Narain 2019]
  - Sandboxing and Synthetic location/sensors generation
  - Creates a synthetic identity
    - *Home, work, kids schools, favorite restaurants*
  - Generates and feeds synthetic data to apps: location, sensors
  - Trajectories are randomized and indistinguishable from real
    - *Evaluated through ML, and user studies*
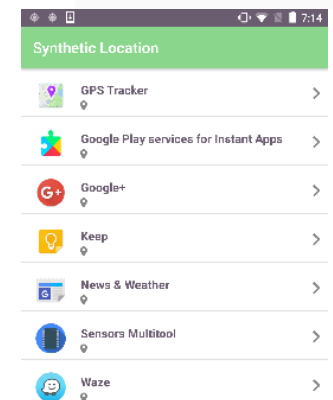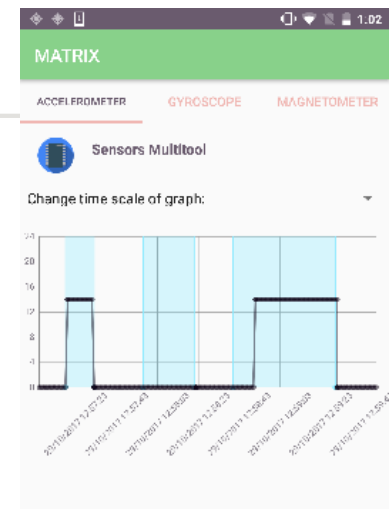
CONCLUSIONS

- Vulnerabilities derive from intrinsic constraints and design choices
  - Softwarization of hardware
  - Pervasiveness
  - Resources constraints
  - Lack of systematic approaches to modeling security in wireless & mobile systems
- We only experienced the tip of the iceberg
  - Sophisticated adversaries can perform significantly more powerful attacks
  - IoT is taking the potential of attacks to a new level
  - Little understanding of what is ahead of us
- Attribution will get even harder
  - Remote exploitation of programmable wireless chips
  - Privacy infrastructure: Tor Onion Services
  - Monetization: cryptocurrencies

QUESTIONS

- Can the security issues related to wireless softwarization be addressed through the attack-and-fix cycle?
  - CPS, DSA (5G), IoT require more vigilance

- Can theory play a bigger role in making wireless communications robust?
  - Softwarization enables more advanced techniques
  - 5G flexibility provides opportunity for increased security, privacy, and robustness

ACKNOWLEDGMENTS

Research in collaboration with colleagues faculty and students

K. Block, A. Cassola, A. Chan, K. Chowdhury, M. Hollick, E. Kirda, S. Narain, H. Nguyen, R. Rajaraman, A. Ranganathan, A. Sanatinia, H. Sathaye, R. Sundaram, T. Vo-Huu, T. Vo-Huu, W. Robertson, M. Salehi, D. Starobinski, M. Stute, L. Xin

Link to papers:

http://www.ccs.neu.edu/home/noubir