LCN 2016, Dubai, United Arab Emirates, November 7-10, 2016

Probr – A Generic and Passive WiFi Tracking System

Joel Scheuner, Genc Mazlami, Dominik Schöni, Sebastian Stephan, Alessandro De Carli, Thomas Bocek, and Burkhard Stiller

Communication Systems Group CSG, Department of Informatics Ifl University of Zürich UZH stiller@ifi.uzh.ch



Motivation Probr-Architecture Case Study Conclusions



Motivation (1)





Ubiquity of WiFi-enabled devices – WiFi traces can reveal interesting patterns

Motivation (2)







Motivation (3)

Hurdle for distributed analysis

- Infrastructure setup is time-consuming
 - Set up devices
 - Manage devices (e.g., start, pause, resume, stop experiment)
 - Debug strangely behaving devices
 - Collect results

Design Goals

	Snoopy [35]	Mo-Fi [31]	CreepyDOL [28]	Probr
On-line Use Cases	×	✓	v	✓
Support Commodity Capturing Devices	~	~	~	~
Support Ad-hoc Experimentation	×	×	×	~
Extensible Architecture for Analysis	~	×	×	~
Entirely Open Source and Free	×	×	×	~

The Probr System



Probr – A Generic and Passive WiFi Tracking System



Probr Architecture (1)

Probr-Core

- Manage devices (register, start monitoring)
- Execute commands



Probr-Analysis

• Explore WiFi captures





Probr Architecture (2)



ItI

Use Cases

U1) Room utilization

- How many people are in a room at any given time?
- U2) Device localization
 - Where are devices located in a room?
- □ U3) Person tracking

– Is it possible to reproduce the daily routine of a person?

- □ U4) Device statistics
 - Can the data expose device vendor preferences for different communities?



Terminology

Probr Packet

- Represents a single WiFi probe request
 - Category 802.11 management frames
- Contains
 - Timestamp
 - Source Media Access Control (MAC) address
 - Destination MAC address
 - Service Set Identifier (SSID)
 - Received Signal Strength Indicator (RSSI)
 - Tags (Probr-defined)
 - Location of capturing device (Probr-defined)

U1) Room Utilization – Web Interface



U1) Room Utilization – Session Model

- Session covers multiple Probr packets from the same source MAC address
- Conditions
 - Maximum inter-packet time (e.g., 5 min)
 - Minimum session length (e.g., 1 min)



U2) Device Localization – Web Interface



U2) Device Localization

Proportional growth multilateration algorithm

- RSSI as indicator of physical distance
- Based on experimentally derived formula from [36]



Case Study

- \square 2 days experiment in a ~35 m² meeting room
- □ 20-25 people attending a scientific project meeting
- □ > 200,000 probe requests
- Capturing devices
 - 6x ODROID-C1 single-board computers



Case Study – U1) Room Utilization



ifi

Case Study – U2) Device Localization



ifi

Summary – Probr

On-line use cases

- Perform incremental analysis
- Support commodity capturing devices
 - Portable shell client
- Support ad-hoc experimentation
 - Integrated device administration
- Extensible analysis use cases
 - Modularization (Core + Analysis), plugin architecture
- Entirely open source (MIT License)
 - github.com/probr

Conclusions

□ U1) Room utilization

- How many people are in a room at any given time?
 - Utilization graph shows room utilization over time tolerating slight overestimation
- □ U2) Device localization
 - Where are devices located in a room?
 - Heatmap indicates where the majority of devices are located

prøbr

	S STARTED - DOCUMENTATIO	N▼ USAGE▼ FAQ	D USECASE O GITHUB
Dre	br		
Velcome! Probr is a generic and distributed wifi-tracking system, designed and develo s to make it easier to conduct research projects in the domain of wireless s analyses. The project is split into two independent parts.	ped over the course of a mass sniffing (i.e., wireless tracking)	ter's project at the Un by leveraging an exis	liversity of Zurich. It's aim sting platform for custom
Welcome! Probr is a generic and distributed wifi-tracking system, designed and develo is to make it easier to conduct research projects in the domain of wireless s analyses. The project is split into two independent parts. Core	ped over the course of a mas sniffing (i.e., wireless tracking) Analysis	ter's project at the Un by leveraging an exis	niversity of Zurich. It's aim sting platform for custom
Welcome! Probr is a generic and distributed wifi-tracking system, designed and develo s to make it easier to conduct research projects in the domain of wireless s malyses. The project is split into two independent parts. Core probr-core is a python-django based system for remote device administration. It allows to setup basic *NIX devices to use for various asks, including but not limited to sniffing. It processes *,pcap files and stores their content in numerous databases. You can write your own randlers to adjust probr-core to your use case.	ped over the course of a mass niffing (i.e., wireless tracking) Analysis probr-analysis is a NodeJS I our analysis of collected devices using their MAC-Ad an custom-made algorithm.	ter's project at the Un by leveraging an exis based frontend that vi probe requests. It a dress, as well as moni	iversity of Zurich. It's aim sting platform for custom isualizes core concepts of llows to track individual itor room utilization using



docs & setup: probr.ch fork & us: github.com/probr



ifi

Appendix



Probr in Numbers

- □ Operated >4 months
- □ Captured almost 30 000 000 probe requests
- □ 30 GB of WiFi traces

Future Work

□ Probr

- Currently only considers probe requests
- Countermeasures against MAC-Randomization
 - Device fingerprinting (e.g., based on sequence numbers, SSIDs)
- Case study
 - Larger room and more participants
 - Quantitive analysis of localization accuracy

MAC Randomization





Countermeasures

	Chainfire Tools		• • • • • 5 252 •
	channie 10013		A A A A A 0.202 A
	3 PEGI 3		
	Bietet In-App-Käufe an () Diese App ist mit einigen d	einer Geräte kompatibel.	
•		Tur Wunschliste hinzufüge	n Installieren
ा हि । Pry-Fi	19:36 🔮 👐 🕏 🔊	ON 19:38	
Pry-Fi v0.60	Pry-Fi v0.60		
Copyright © 2014 - Chainfire Twitter: @ChainfireXDA G+: http://google.com/+Chainfire	Copyright © 2014 - Chainfire Twitter: @ChainfireXDA G+: http://google.com/+Chainfire Too to visit XDA thread		
Tap to visit XDA thread	Tap to Yian Aury Uniteda		
Upgrade to Pro	Upgrade to Pro		
Tap to visit XDA thread Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features are already available	Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features already available	s are	
Tap to visit XUA thread Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features are already available OPTIONS	Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features already available OPTIONS	s are	
Tap to virit, XIAN Immeda Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features are aiready available OPTIONS MAC status	Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features already available OPTIONS MAC status	s are	>
Tap to vail XXX meed Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features are viewed y available OPTIONS MAC status Originat D022 BE66 F4.09 Warnet WA	Vigo transaction lineace Vigo transaction lineace Vigo transaction lineace Support the development of my apps. Completely optional - (for now) all features already available OPTIONS OPTIONS OPTIONS Originat (2022) EE-56 F4 09 Warrent (6) OP EF-97 65 0	s are	>
Tap to varia XIAA meeas Upgrade to Pro Support the development of my apps. Support the development of my apps. Support the development of my apps. Variation of the model of the normalization MAC status Original: 00:222 BE66 F4.09 Named: NZA Devent: 00:222 BE66 F4.09	Upgrade to Pro Support the development of my apps. Completely optional - (for now) all features already available OPTIONS MAC status Original. D0:22:8E:66:F4:09 Wardet: 66:DE:8F:977:65:D Current: 66:DE:8F:977:65:D	s are	>
Tap to verify TAXA minese Jpgrade to Pro Upgrade to Pro Completely optional - (for now) all features are investy available PPTIONS WARGET VA Supreme: D0:228.E66.F4.09 Wandet: VA Wandet: VA Wandet: VA Wandet: NA WAN WANDEt: NA WANDE	Pup transformer Upgraduate to Pro Support the development of my apps. Completely optimal - (for now) all features already available OPTIONS MAC status Original: D022:BE6.6F 4.09 Wardet 66:DE8.977.76:50 Ourmet 66:DE8.977.76:50 Ourmet 66:DE8.977.76:50	s are	>
Tap to varia XAA thread Upgrade to Pro Suppart the development of my apps. Suppart to the development of my apps. WAC status Originat. D0228.E66.F4.09 Wandet: NA Current: D0228.E66.F4.09 Manage networks Remove entremista and configure MACs to use pre networks	Upgrade to Pro Support the development of my apps. Completely optimal - (for now) all features already available OPTIONS MAC status Original: D022:BE6.66.F4.09 Wardet 66.0E.BF.97.76.50 Ourmet 66.0E.BF.97.76.50 Manage networks Remove networks and configure MACs to par network	sare	>
Tap to virial XAA thread Upgrade to Pro Suppart the development of my apps. Completely optional - (for now) all features are aready available OPTIONS MAC Status Organic 10.22.8E:66.F4.09 Wened: IVA Durrent: D0.22.8E:66.F4.09 Manage networks Remove networks and configure MACs to use per network Go to warf	Vigo transaction mease Vigorande to Pro Support the development of my apps. Completely cognal - (for now) all features aready weakable OPTIONS MAC status Original 10.22.8E6.6F8.40.9 Wardet 660.EBF.97.75.50 Current 660.EBF.97.75.50 Manage networks Remove networks and configure MACs to per intervente	use	>
Uggrade to Pro Support the development of my apps. Completely optical: (for now) all features are already available OPTIONS MAC status Original: 00:22:8E:66:F4:09 Manage netWorks Remove networks and configure MACs to use per rotentic D0:22:8E:66:F4:09 Manage netWorks Benove networks and configure MACs to use per rotentic Bo to var1 Emulate dozens of people police/ong the tracked area for best results. This significantly necesses battery draid	Vaporade to Pro Support the development of my apps. Completely optional - for now all features already available OPTIONS MAC status Originat: D0220E66674.09 Warket 6602E8/977.650 Current: 6	use her	>



Beschreibung mit Google Übersetzer in Deutsch übersetzen? Übersetzen

You are being watched...

Retailers, crooks, the government, and others shady individuals are tracking your movements. Even when your Wi-Fi is turned off, your phone may be broadcasting information to whomever is in range which can be used both to track repeated visits to as well as your exact movements in an area under surveillance.

Probing Behavior



Freudiger, J. (2015, June). How talkative is your mobile device?: an experimental study of Wi-Fi probe requests.



Challenges

□ Probr

- Big data (up to 30 million packets)
- Generic device support
- Case study
 - Legal situation
 - Informed the meeting attendees
 - Anonymous analysis (no mapping of MAC addresses to participants)
 - Attendees could request exclusion of their devices

U3) Person Tracking – Web Interface



Case Study – U3) Person Tracking





U4) Device Statistics – Web Interface

LOG UTILIZATION	LOCATION	STATS TRAC	CKING acelab -	10/21/2015 7:20 AM -	10/22/2015 7:20 PM		
Stats							
Vendor pie chart:				Top 15	vendors:		
				Rank	Vendor	Count	Percentage
				1	Apple, Inc.	177	31.3 %
				2	Motorola	115	20.4 %
				3	Samsung	72	12.7 %
				4	Intel	38	6.7 %
				5	Siemens	28	5 %
		//		6	Murata Manufacturing Co., Ltd.	20	3.5 %
				7	Hon Hai Precision Ind. Co.,Ltd.	18	3.2 %
				8	Sony	15	2.7 %
				9	Microsoft	13	2.3 %
				10	НТС	8	1.4 %
				11	Liteon Technology Corporation	7	1.2 %
				12	Nokia	6	1.1 %
				13	WISOL	5	0.9 %
				14	Shenzhen Ogemray Technology Co., Lt	d. 4	0.7 %
				15	LG	3	0.5 %
Total Devices:		Non-Ra	andomized Devices:	Rando	nized Devices:	Randomized Ratio:	
TOTAL DEVICES.		NOIFRO	andonnized Devices.	Kalluul	IIIZeu Devices.	Ranuonnizeu Ratio.	

Case Study – U4) Device Statistics



(a) Distribution during Case Study

(b) Distribution over 4 Months

Device Vendor Distributions

