Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic

Tyler Tucker,* Nathaniel Bennett,* Martin Kotuliak,† Simon Erni,†
Srdjan Capkun,† Kevin Butler,* and Patrick Traynor*

*Florida Institute for Cybersecurity Research (FICS)

†ETH Zurich

Worldwide Cellular Surveillance

Worldwide Cellular Surveillance

Controversial snooping technology 'used by at least seven police forces'

Documents reveal usage of IMSI catchers, which harvest information from phones, is far higher in UK than previously known

The technology presents itself as the strongest mobile signal in the area, prompting all nearby phones to connect to it. Photograph: Manu Fernandez/AP

United Kingdom

2016

Worldwide Cellular Surveillance

Controversial snooping technology 'used by at least seven police forces'

Documents reveal usage of IMSI catchers, which harvest information from phones, is far higher in UK than previously known

The technology presents itself as the strongest mobile signal in the area, prompting all nearby phones to connect to it. Photograph: Manu Fernandez/AP

United Kingdom
2016

Canada
2017

RCMP used unwarranted cellphone surveillance technology six times

Sameer Chhabra @SameerChhabra94

SEP 14, 2017 · 4:42 PM EDT · 4 COMMENTS

Worldwide Cellular Surveillance


Controversial snooping technology 'used by at least seven police forces'

Documents reveal usage of IMSI catchers, which harvest information from phones, is far higher in UK than previously known

The technology presents itself as the strongest mobile signal in the area, prompting all nearby phones to connect to it. Photograph: Manu Fernandez/AP

United Kingdom
2016

Canada
2017

Serbia
2024

RCMP used unwarranted cellphone surveillance technology six times

Sameer Chhabra @SameerChhabra94

SEP 14, 2017 | 4:42 PM EDT | 4 COMMENTS

Worldwide Cellular Surveillance


Controversial snooping technology 'used by at least seven police forces'

Documents reveal usage of IMSI catchers, which harvest information from phones, is far higher in UK than previously known

The technology presents itself as the strongest mobile signal in the area, prompting all nearby phones to connect to it. Photograph: Manu Fernandez/AP

United Kingdom
2016

Canada
2017


RCMP used unwarranted cellphone surveillance technology six times

Sameer Chhabra @SameerChhabra94

SEP 14, 2017 · 4:42 PM EDT · 4 COMMENTS

Serbia
2024

Philippines
2025

How can Adversaries Interact with our Phones?

How can Adversaries Interact with our Phones?

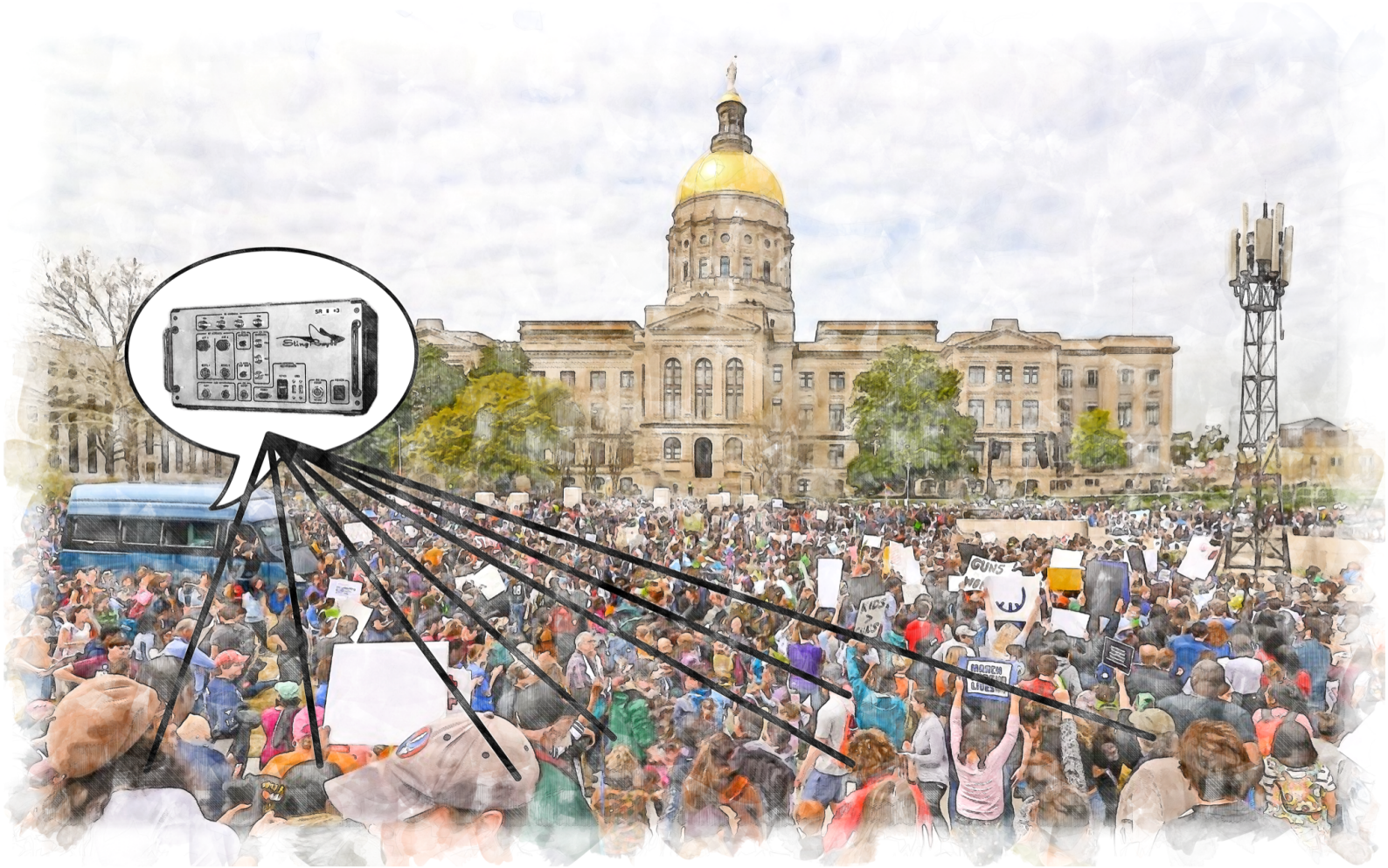
- Telephony is facilitated using central network hardware owned by providers
  - However, anyone can create their own cell tower ("rogue base station"), which our phones will connect to under the correct conditions

How can Adversaries Interact with our Phones?

- Telephony is facilitated using central network hardware owned by providers
  - However, anyone can create their own cell tower ("rogue base station"), which our phones will connect to under the correct conditions
- One RBS implementation is an IMSI-Catcher, which links a network identifier ("IMSI") to an individual to enable location-tracking attacks

Attack Scenario

Attack Scenario



Attack Scenario

A Lingering Threat

A Lingering Threat

2G GSM

1990s

A Lingering Threat

2G GSM

2000s

1990s

3G UMTS

A Lingering Threat

2G GSM

4G LTE

1990s

2000s

2010s

3G UMTS

A Lingering Threat

2G GSM

4G LTE

1990s

2000s

2010s

2020s

3G UMTS

5G NR

Get in Line

Get in Line

False Positives

	IC-SC [10]	TMSB [11]	NB-ICD [21]	ICD-CN [12]	SITCH [13]	Apple Patent [14]	mICC [15]	sICC [15]	App-Based [16]	Crocodile Hunter [17]	GSMK Overwatch [18], [19]	SeaGlass [20]	Our Approach
Noisy Background RF	◐	◐	●	●	◐	◐	●	○	●	◐	●	●	●
Weak Cipher Use	○	○	●	●	●	●	●	●	◐	●	●	◐	●
Freq. Reassociation	◐	◐	●	●	○	●	●	●	○	●	◐	○	●
Freq. Downgrade	○	○	●	●	●	◐	●	●	◐	●	●	●	●
Anomalous Propagation	◐	●	○	○	○	○	○	○	○	○	○	○	●
Temporary Tower	●	◐	○	○	○	○	○	○	○	○	○	○	●
Misconfigured Tower	○	○	○	○	○	○	○	○	○	○	○	○	●

Table I: Efficacy of various detection methods when exposed to suboptimal cellular network conditions. ○ indicates the condition will directly lead to increased false positives in the detection mechanism, ◐ indicates the condition may lead to false positives in the detection mechanism under certain circumstances, and ● indicates the condition has no effect on the detection rate of the mechanism.

Get in Line

False Positives

	IC-SC [10]	TMSB [11]	NB-ICD [21]	ICD-CN [12]	SITCH [13]	Apple Patent [14]	mICC [15]	sICC [15]	App-Based [16]	Crocodile Hunter [17]	GSMK Overwatch [18], [19]	SeaGlass [20]	Our Approach
Noisy Background RF	◐	◐	●	●	◐	◐	●	○	●	◐	●	●	●
Weak Cipher Use	○	○	●	●	●	●	●	●	◐	●	●	◐	●
Freq. Reassociation	◐	◐	●	●	○	●	●	●	○	●	◐	○	●
Freq. Downgrade	○	○	●	●	●	◐	●	●	◐	●	●	●	●
Anomalous Propagation	◐	●	○	○	○	○	○	○	○	○	○	○	●
Temporary Tower	●	◐	○	○	○	○	○	○	○	○	○	○	●
Misconfigured Tower	○	○	○	○	○	○	○	○	○	○	○	○	●

Table I: Efficacy of various detection methods when exposed to suboptimal cellular network conditions. ○ indicates the condition will directly lead to increased false positives in the detection mechanism, ◐ indicates the condition may lead to false positives in the detection mechanism under certain circumstances, and ● indicates the condition has no effect on the detection rate of the mechanism.

False Negatives

	IC-SC [10]	TMSB [11]	NB-ICD [21]	ICD-CN [12]	SITCH [13]	Apple Patent [14]	mICC [15]	sICC [15]	App-Based [16]	Crocodile Hunter [17]	GSMK Overwatch [18], [19]	Seaglass [20]	Our Approach
No Jamming	●	●	●	●	●	●	●	○	●	●	●	●	●
Fixed Location	●	●	●	●	●	○	●	●	●	○	●	●	●
Long-Term Campaign	●	●	●	●	●	●	○	●	●	●	○	○	●
Benign Radio Freq.	●	◐	●	●	○	●	●	○	●	●	●	○	●
No Unusual Paging	●	●	●	●	●	●	○	○	●	●	○	○	●
Benign Ciphers	○	○	●	○	●	●	●	●	●	●	●	◐	●
Parroted Cell-ID	●	●	●	●	○	○	○	○	○	●	●	●	●
Plausible RF Power	●	●	○	●	○	○	●	●	○	○	●	○	●
Benign Broadcast Params	●	●	●	●	●	○	○	○	○	○	○	○	●
Parroted LAC	●	○	○	○	●	●	○	●	○	○	●	○	●
LTE-Only	○	○	○	○	○	◐	○	○	○	●	◐	○	●
New Location	○	○	○	○	○	●	○	○	◐	○	○	○	●
DL Overshadow	○	○	○	○	○	○	○	○	○	○	○	○	●
UL Overshadow	○	○	○	○	○	○	○	○	○	○	○	○	●

Table II: Efficacy of various detection methods against an IMSI-Catcher exhibiting the specified behavior. ○ indicates the behavior will lead to increased false negatives in the detection mechanism, ◐ indicates the behavior may lead to false negatives in the detection mechanism under certain conditions, and ● indicates the behavior has no effect on the detection rate of the mechanism.

Let's Flip This

Let's Flip This

- Existing solutions ask the question, *"How might IMSI-Catchers behave?"*
  - Detectors target variables such as odd configurations, physical layer anomalies, and weak cipher usage
  - As a result, no academic publication has produced plausible evidence of an IMSI-Catcher

This image was created with the assistance of DALL·E

Let's Flip This

- Existing solutions ask the question, *"How might IMSI-Catchers behave?"*
  - Detectors target variables such as odd configurations, physical layer anomalies, and weak cipher usage
  - As a result, no academic publication has produced plausible evidence of an IMSI-Catcher
- Conversely, we ask, *"What must IMSI-Catchers do to achieve their goal?"*
  - They must always force a UE to transmit its IMSI

This image was created with the assistance of DALL·E

Let's Flip This

Let's Flip This

- Let's find out what the cellular standards say can cause a phone to transmit its IMSI?

Let's Flip This

- Let's find out what the cellular standards say can cause a phone to transmit its IMSI?
- It turns out there are 53 different ways to do so throughout 2G through 5G-NSA
  - These messages represent what IMSI-Catchers *must* transmit

Generation	Downlink Message	Reference
2G GSM	Identity Request	GSM TS 04.08 Sec. 4.3.3.1
	Authentication Reject	GSM TS 04.08 Sec. 4.3.2.5
	Abort, Cause #6	GSM TS 04.08 Sec. 4.3.5.2
	Location Updating Reject, #2-3, 6, 11-13	GSM TS 04.08 Sec. 4.4.4.7
	CM Service Reject, Cause #4 or 6	GSM TS 04.08 Sec. 4.5.1.1
3G UMTS	Identity Request	3GPP TS 124.008 Sec. 4.3.3
	Authentication Reject	3GPP TS 124.008 Sec. 4.1.1.2
	Abort, Cause #6	3GPP TS 124.008 Sec. 4.3.5.2
	Location Updating Reject, Cause #2-3, 6, 11-12	3GPP TS 124.008 Sec. 4.4.4.7
	CM Service Reject, Cause #4, 6	3GPP TS 124.008 Sec. 4.5.1.1
	Attach Reject, Cause #3, 6-8, 11-15	3GPP TS 124.008 Sec. 4.7.3.1.3
	Detach Request, Type "re-attach not required", Cause #2-3, 6-8, 11-15	3GPP TS 124.008 Sec. 4.7.4.2.2
	Routing Area Update Reject, Cause #3, 6-7, 9, 11-12, 14	3GPP TS 124.008 Sec. 4.7.5.1.4
	Authentication and Ciphering Reject	3GPP TS 124.008 Sec. 4.7.7.5
	Service Reject, Cause #3, 6-7, 9, 11-12	3GPP TS 124.008 Sec. 4.7.13.4
4G LTE	Identity Request	3GPP TS 124.301 Sec. 4.3.3
	Attach Reject, Cause #3, 6-8, 11-15, 35	3GPP TS 124.301 Sec. 5.5.1.2.5
	Detach Request, Type "re-attach not required", Cause #3, 6-8, 11-15	3GPP TS 124.301 Sec. 5.5.2.3.2
	Tracking Area Update Reject, Cause #3, 6-7, 9, 11-12, 14	3GPP TS 124.301 Sec. 5.5.3.2.5
	Service Reject, Cause #3, 6-7, 9, 11-12	3GPP TS 124.301 Sec. 5.6.1.5
5G NR (NSA)	Same as 4G LTE	3GPP TS 137.340 Sec. 7.1

Testing Our Methodology

Testing Our Methodology

- We hypothesize that legitimate cell towers will tend to minimize those 53 IEMs to protect user privacy

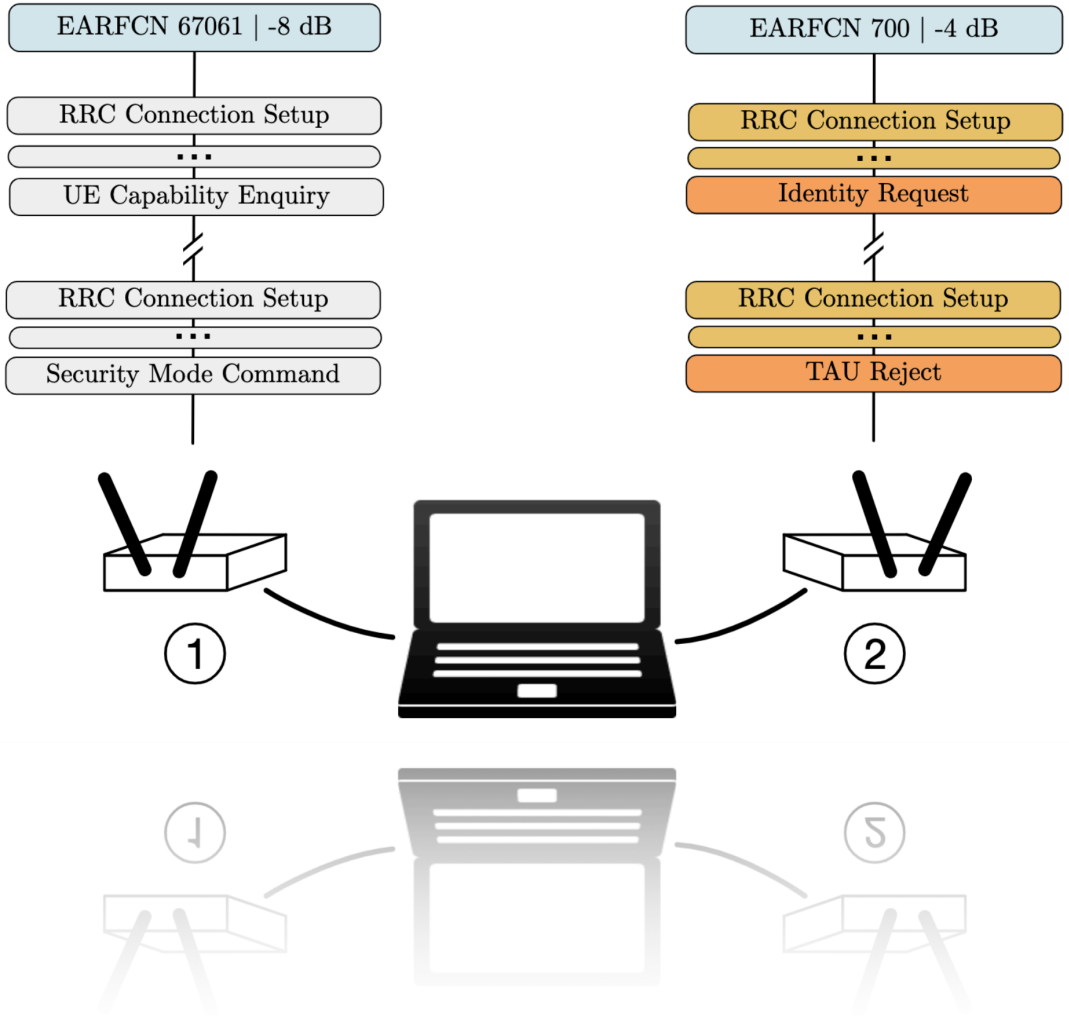
Testing Our Methodology

- We hypothesize that legitimate cell towers will tend to minimize those 53 IEMs to protect user privacy
- To test this hypothesis, we devise a metric called the IMSI Exposure Ratio (IER) that represents the number of connections that contain at least one IEM to the total number of connections

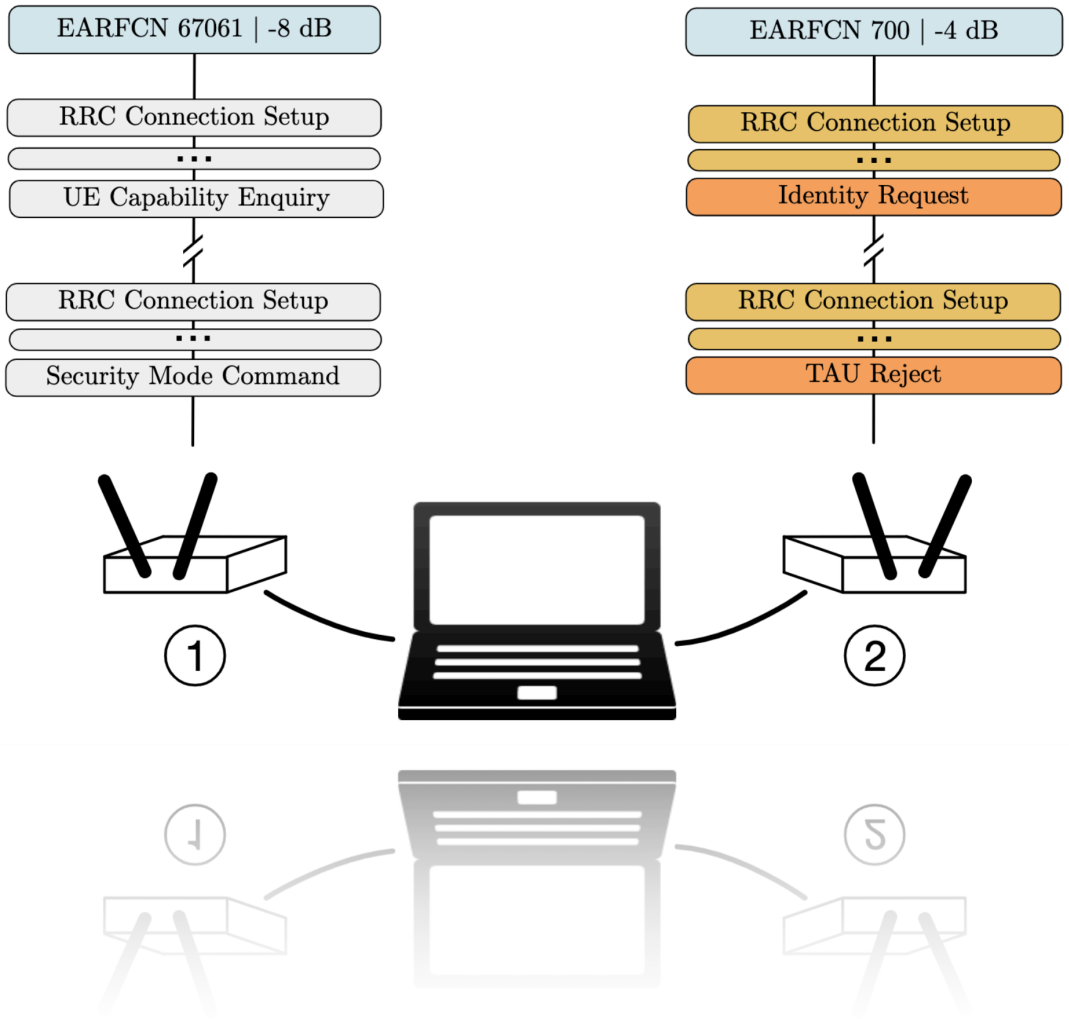
$$\text{IER} = \frac{\text{IMSI Exposing Connections}}{\text{Total Number of Connections}}$$

How to Access Cellular Channels

How to Access Cellular Channels



How to Access Cellular Channels

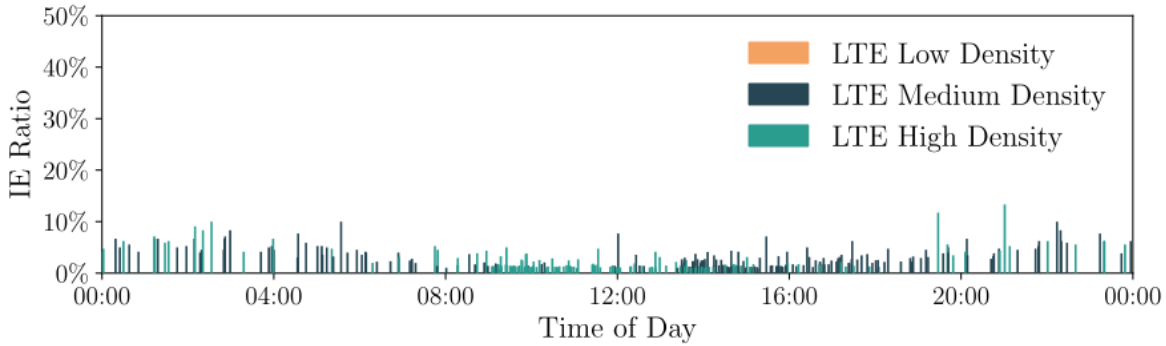


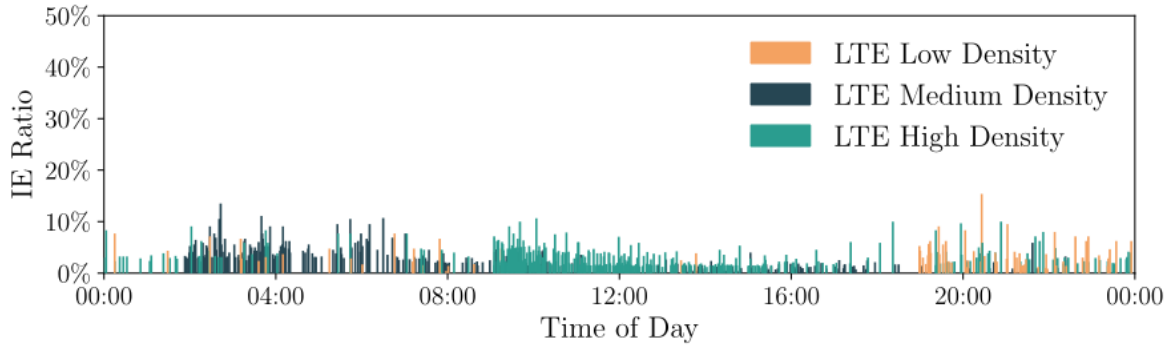
- SDRs can tune to cellular frequencies and see traffic coming from a cell tower
- From this perspective, we can calculate the IER of a base station for a given time window

Commercial Base Stations

Commercial Base Stations

- We calculate IER on 400+ hours of passive network captures from commercial base stations
  - Our captures occur in different countries, cities of varying population density, and events producing temporary periods of high population density (e.g., college football game)
  - Our results show a median IER of 3% for commercial base stations

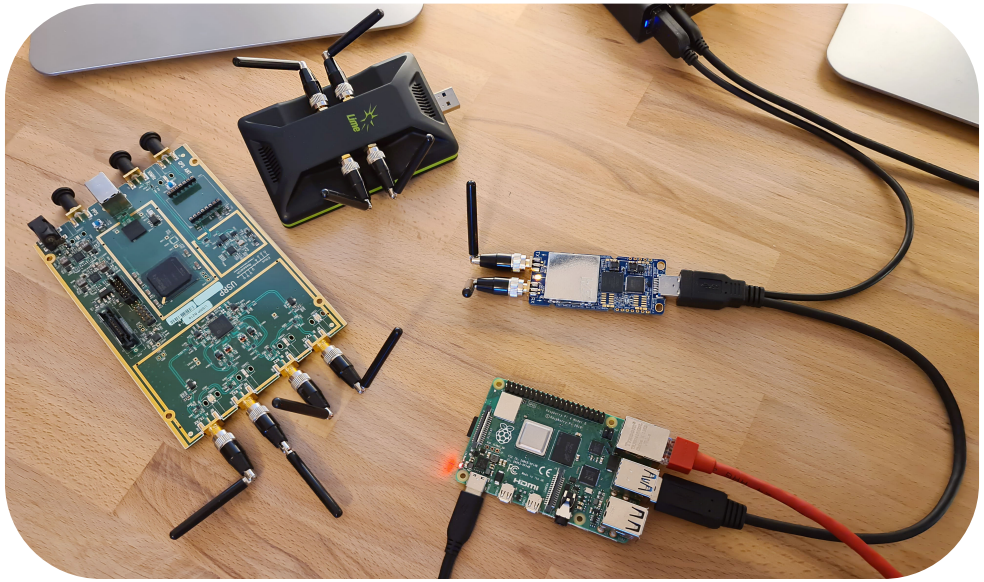




Analyzing IMSI-Catchers

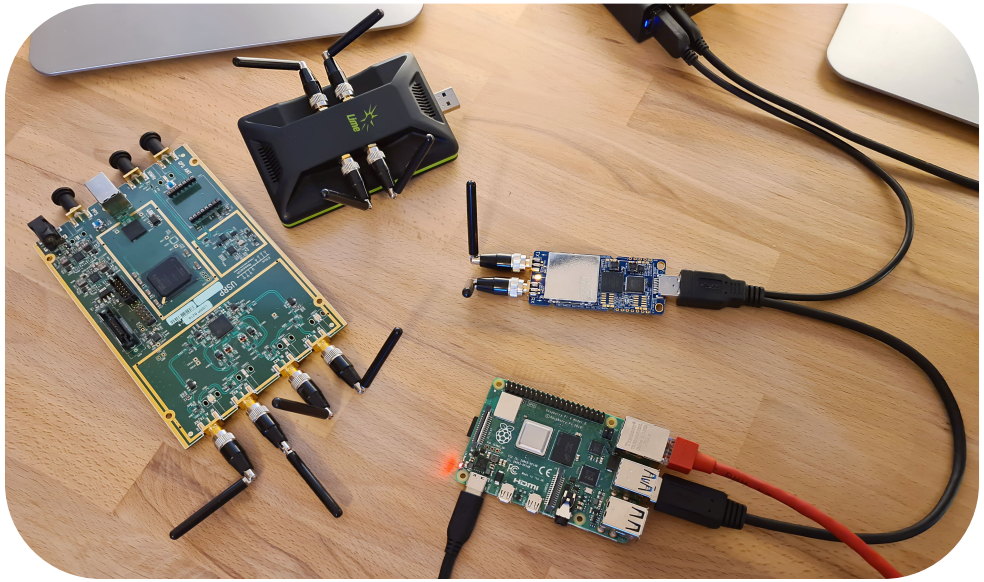
Analyzing IMSI-Catchers

- Obtaining a commercial grade IMSI-Catcher is currently infeasible
  - Therefore, we used public guides and open-source code to create our own 2G GSM, 3G UMTS, and 4G LTE IMSI-Catchers



Analyzing IMSI-Catchers

- Obtaining a commercial grade IMSI-Catcher is currently infeasible
  - Therefore, we used public guides and open-source code to create our own 2G GSM, 3G UMTS, and 4G LTE IMSI-Catchers
- During our tests, we calculated that all connections made to our IMSI-Catchers included an IEM (median IER = 100%)



IMSI-Catcher Hunting

IMSI-Catcher Hunting

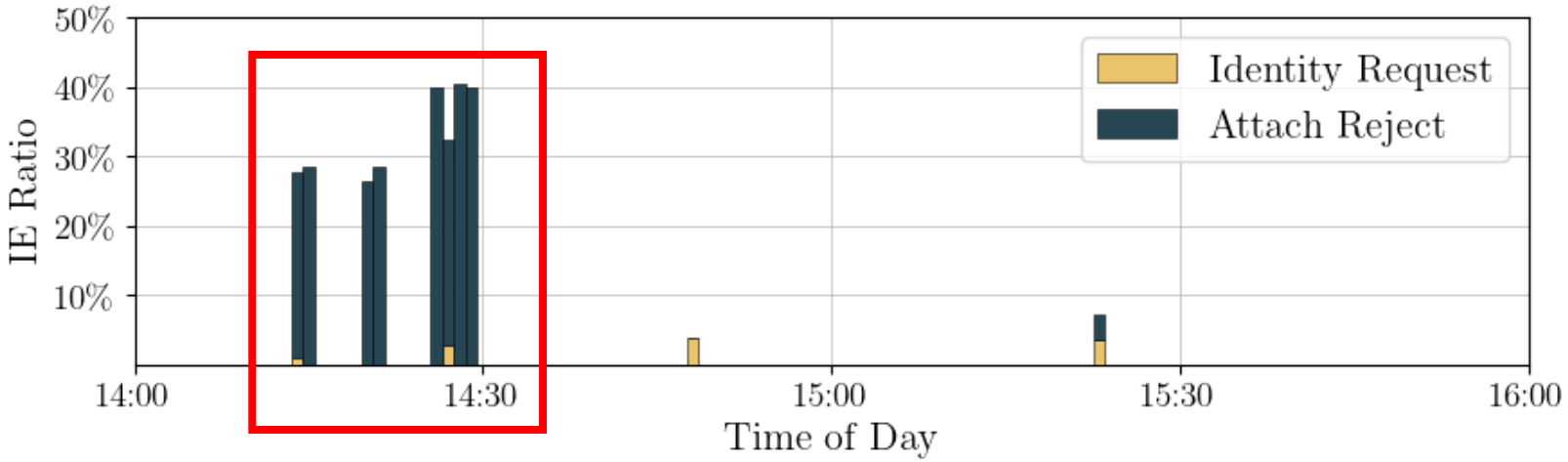
- As a final exercise, we took our detector on the road to several events and locations where we thought an IMSI-Catcher may be in use

IMSI-Catcher Hunting

- As a final exercise, we took our detector on the road to several events and locations where we thought an IMSI-Catcher may be in use
- These locations included public areas surrounding government buildings and two political events with notable law enforcement precautions

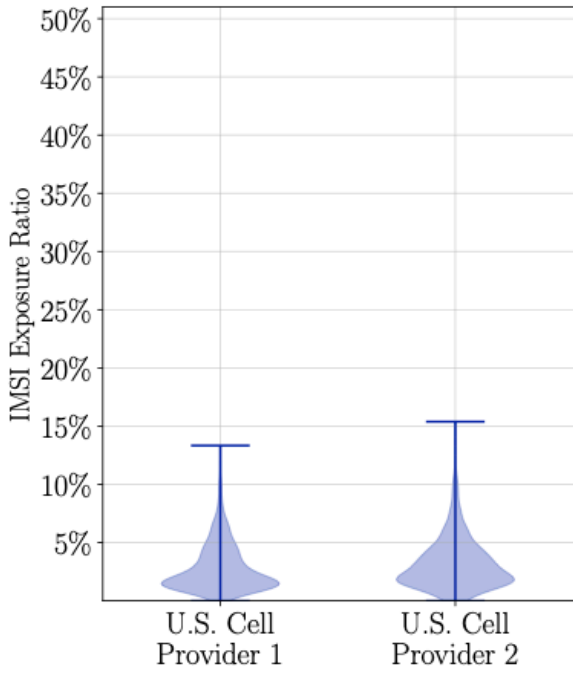
IMSI-Catcher Hunting

- As a final exercise, we took our detector on the road to several events and locations where we thought an IMSI-Catcher may be in use
- These locations included public areas surrounding government buildings and two political events with notable law enforcement precautions
- At one political event, we logged the following results during a fifteen-minute window

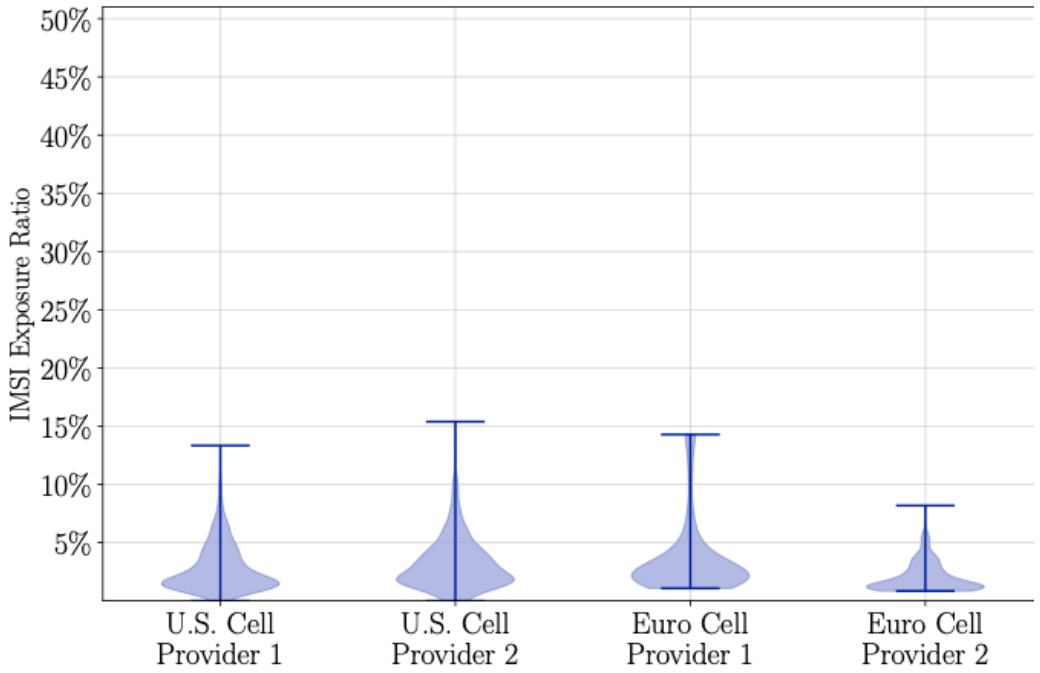


Results

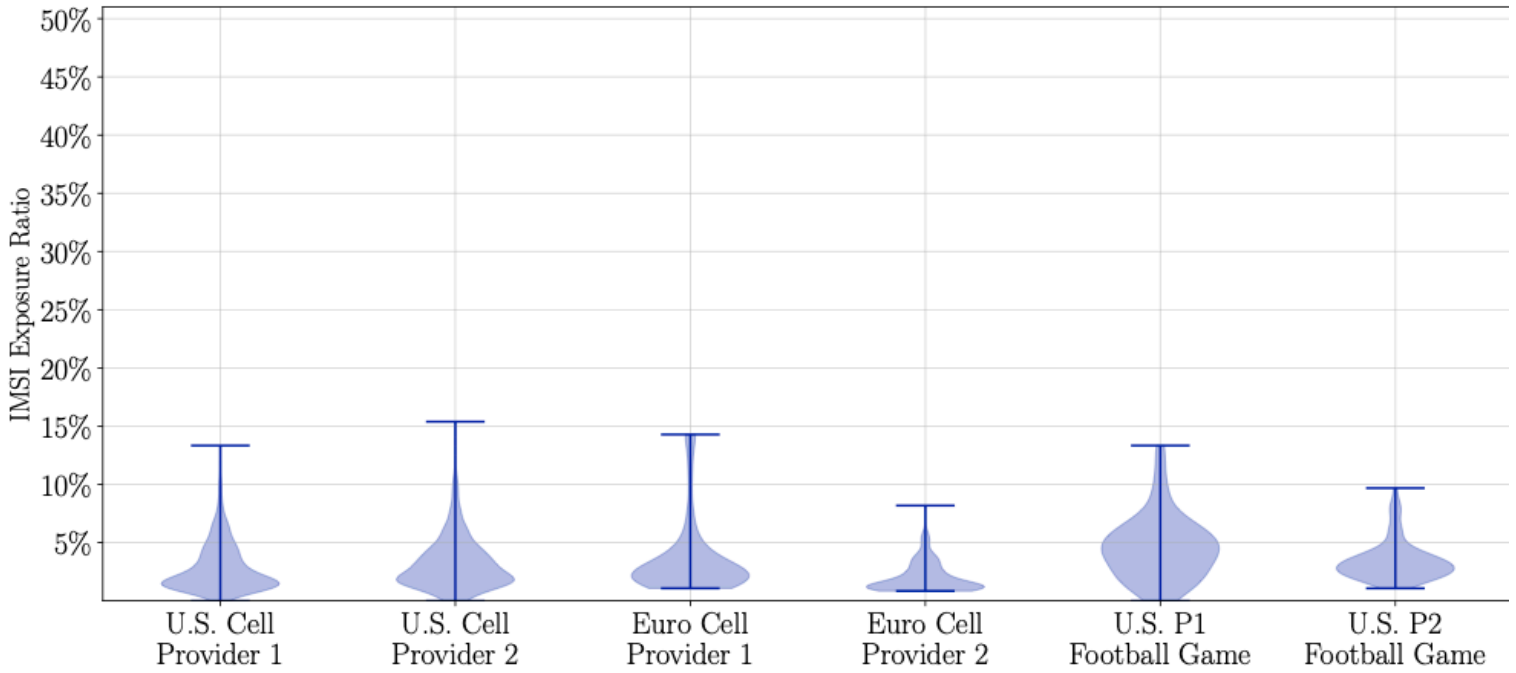
Results


50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
IMSI Exposure Ratio
U.S. Cell Provider 1
U.S. Cell Provider 2

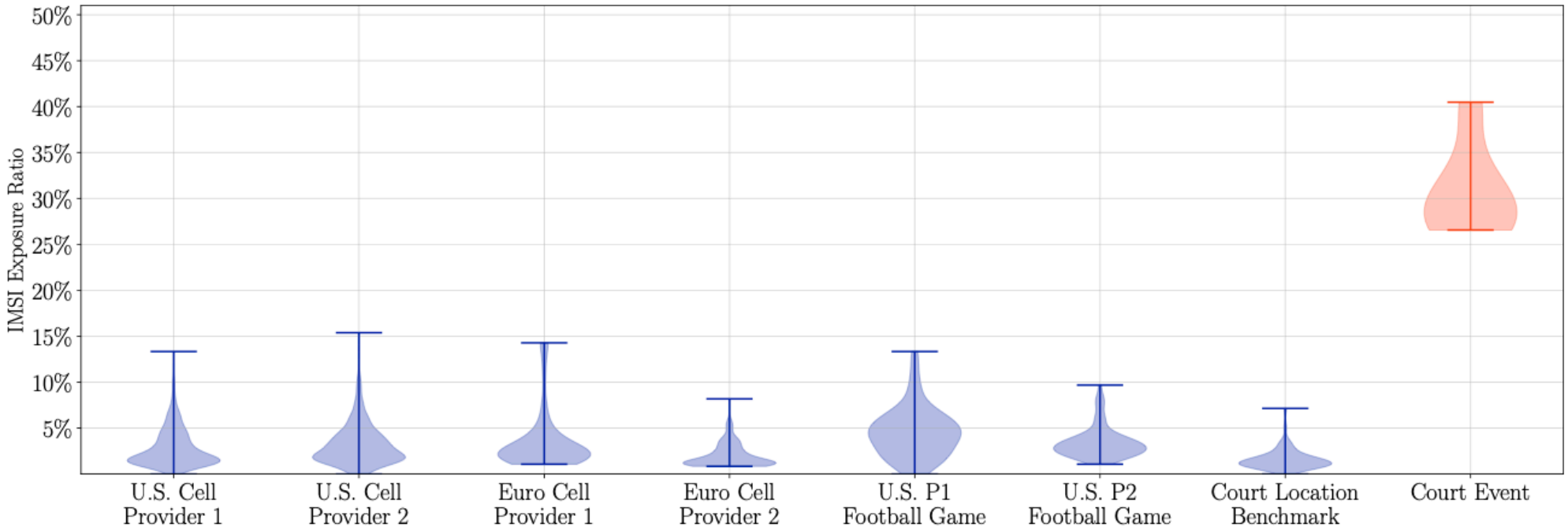
Results


50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
IMSI Exposure Ratio
U.S. Cell Provider 1
U.S. Cell Provider 2
Euro Cell Provider 1
Euro Cell Provider 2

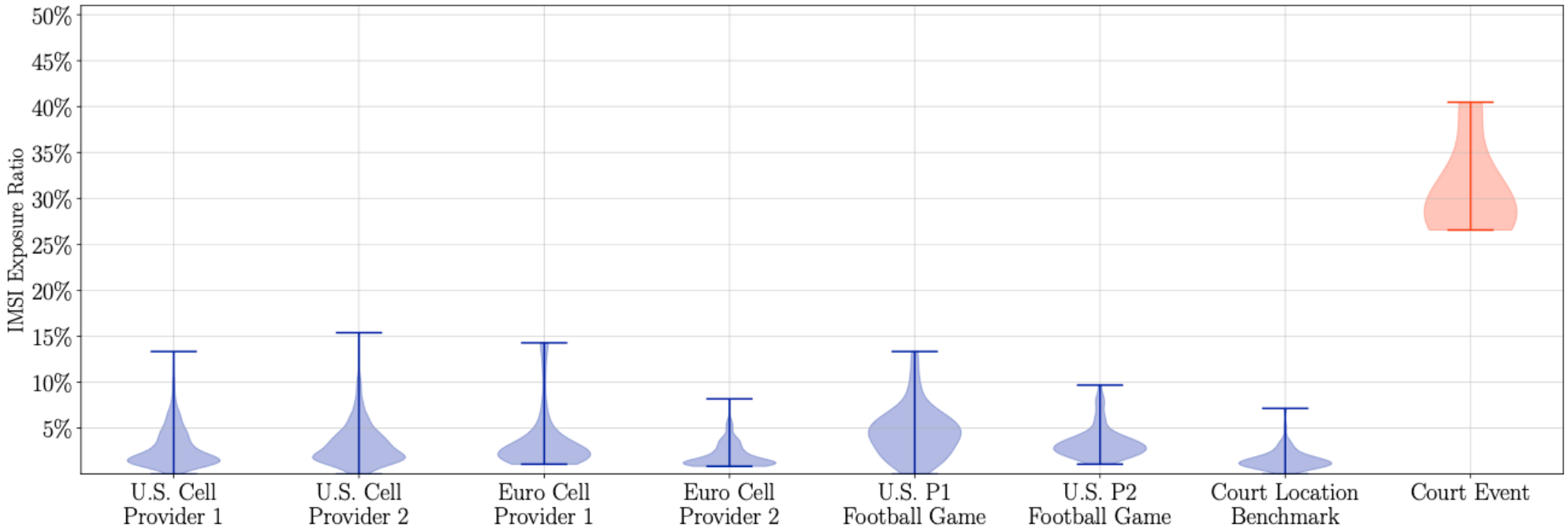
Results


IMSI Exposure Ratio
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
U.S. Cell Provider 1
U.S. Cell Provider 2
Euro Cell Provider 1
Euro Cell Provider 2
U.S. P1 Football Game
U.S. P2 Football Game

Results


IMSI Exposure Ratio
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
U.S. Cell Provider 1
U.S. Cell Provider 2
Euro Cell Provider 1
Euro Cell Provider 2
U.S. P1 Football Game
U.S. P2 Football Game
Court Location Benchmark
Court Event

Results



$p = 2.7e-5$	$p = 2.4e-5$	$p = 3.0e-5$	$p = 3.0e-5$	$p = 7.6e-5$	$p = 5.2e-5$	$p = 6.1e-5$	$-----$

Mann-Whitney Test Result When Compared to Court Event Data

Discussion

Discussion

- We disclosed our findings to the Department of Homeland Security (DHS), who thanked us but did not confirm our findings
  - Recognizing this, we offer statistical analysis to strengthen our findings in this setting

Discussion

- We disclosed our findings to the Department of Homeland Security (DHS), who thanked us but did not confirm our findings
  - Recognizing this, we offer statistical analysis to strengthen our findings in this setting
- Our detector analyzes downlink messages – therefore, we can also detect downlink overshadow attacks
  - Notably, this class of attacks does not rely on a fake base station

Discussion

- We disclosed our findings to the Department of Homeland Security (DHS), who thanked us but did not confirm our findings
  - Recognizing this, we offer statistical analysis to strengthen our findings in this setting
- Our detector analyzes downlink messages – therefore, we can also detect downlink overshadow attacks
  - Notably, this class of attacks does not rely on a fake base station
- Using a 5G sniffer, our approach could be adapted to detect 5G SUCI-Catchers as well

Supporting Future Work

- To support future data collection and community interaction, we provide the source code necessary to run our tool on new data
  - *"Bring your own software-defined radio (SDR)"*
  - If possible, testing this detector (and others) on a commercial-grade IMSI-Catcher would be incredibly insightful

Conclusion

Conclusion

- We implement a new IMSI-Catcher detection methodology based on cellular standards that avoids false classifications
  - In doing so, we reveal over 50 unique messages that IMSI-Catchers can achieve their goal (previous techniques only considered 1 to 2)

Conclusion

- We implement a new IMSI-Catcher detection methodology based on cellular standards that avoids false classifications
  - In doing so, we reveal over 50 unique messages that IMSI-Catchers can achieve their goal (previous techniques only considered 1 to 2)
- We evaluate our approach using 400 hours of cellular traffic captures, tests on lab-controlled IMSI-Catchers, and a public event necessitating IMSI-Catcher presence

Conclusion

- We implement a new IMSI-Catcher detection methodology based on cellular standards that avoids false classifications
  - In doing so, we reveal over 50 unique messages that IMSI-Catchers can achieve their goal (previous techniques only considered 1 to 2)
- We evaluate our approach using 400 hours of cellular traffic captures, tests on lab-controlled IMSI-Catchers, and a public event necessitating IMSI-Catcher presence
- Our publication is the first to substantiate evidence of public IMSI-Catcher use with statistical significance

Thank You

Tyler Tucker

tylertucker1@ufl.edu

www.cise.ufl.edu/~tucker/

Find our project
on Zenodo