

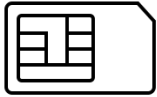
Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

Syed Rafiul Hussain, Mitziu Echeverria[†], Omar Chowdhury[†],
Ninghui Li^{*}, Elisa Bertino^{*}

PURDUE UNIVERSITY, UNIVERSITY OF IOWA

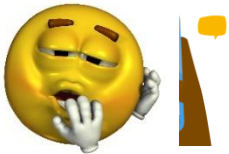


Paging Procedure



IMSI: INTERNATIONAL MOBILE SUBSCRIBER IDENTITY

TMSI: TEMPORARY MOBILE SUBSCRIBER IDENTITY



CONNECTED

Base Station

Core Network

CONNECT (IMSI/TMSI) ← MUTUAL AUTHENTICATION → PAGING REQUEST

<TMSI₁, PS>
<IMSI₁, PS>
<TMSI₂, CS>
<TMSI₃, PS>
⋮

INCOMING SERVICES



Paging Occasion



Monitor



$T = 128$
FRAMES
1 FRAME = 10MS



Can a passive adversary only knowing victim's phone number/Twitter handle

? Identify/track the victim's presence in a target area?
? If present, identify victim's PFI?

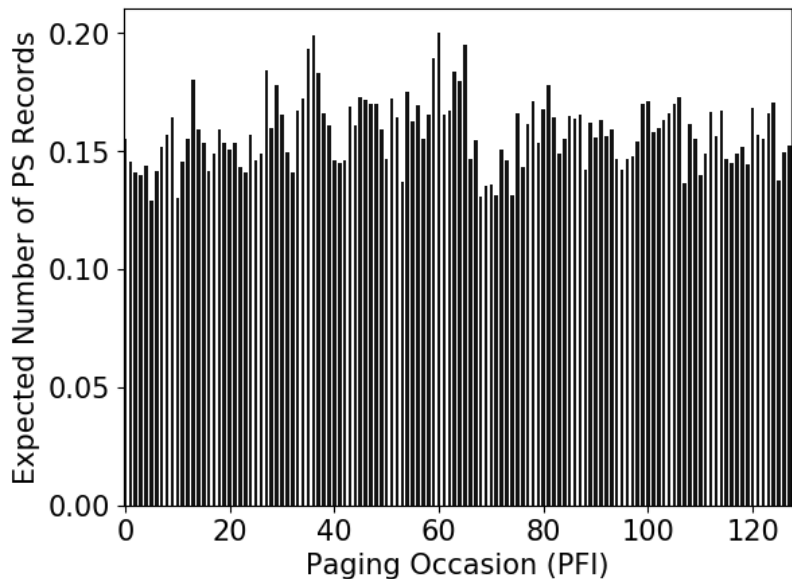
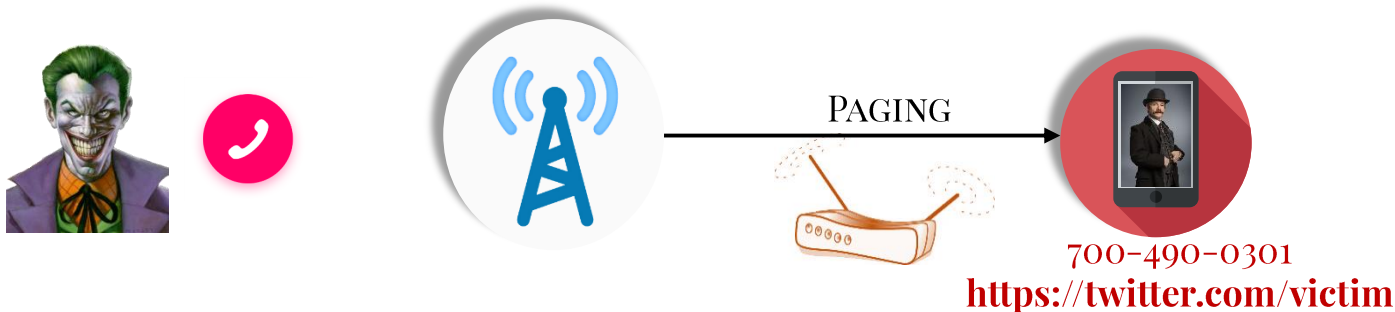
IMSI = 310 260 628687883 = 100011010XXX ... XXX **00001011**

IMSI = 310 260 628687893 = 100011010XXX ... XXX **00010101**

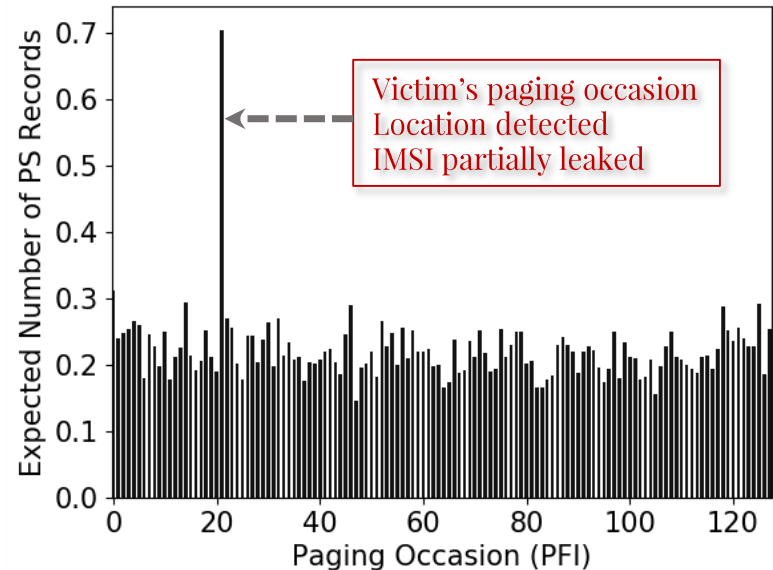
IMSI = 310 260 628687765 = 100011010XXX ... XXX **00010101**

ToRPEDO

TRacking via Paging mEssage DistributiOn



Distribution of paging messages (PS records) when attacker makes no phone call



Distribution of paging messages (PS records) when attacker makes silent phone calls

Filtering - ToRPEDO Attack (1/3)



Assumption: Perfect delivery of paging.




Remove from the set of all PFI values that do not have a paging message



Paging Delivery/Capturing Is Not Reliable

 n: Received PFI = {12, 21, 27, 50, 65, 97} Candidate PFI = {12, 21, 27, 50, 65, 97}

 n+1: Received PFI = {2, 21, 45, 88, 97, 125} Candidate PFI = {21, 97}

 n+2: Received PFI = {7, 21, 39, 65, 91, 117} Candidate PFI = {21}

Counting - ToRPEDO Attack (2/3)



Continue calling until a unique PFI is found satisfying:

k paging out of n calls



Does not filter out the victim's PFI if paging is missed for a call



High number of calls to filter out non-victim's PFI

Likelihood - ToRPEDO Attack (3/3)



16 paging records with PS and CS indication



Timing information



Compute the likelihood L_i of i to be the victim's PFI



Compute the likelihood L_{-1}

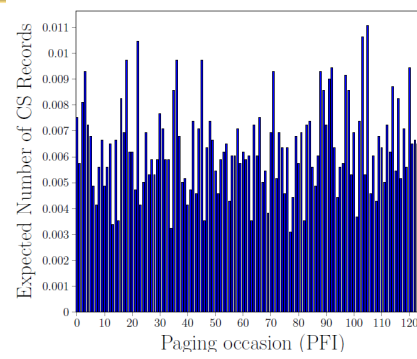
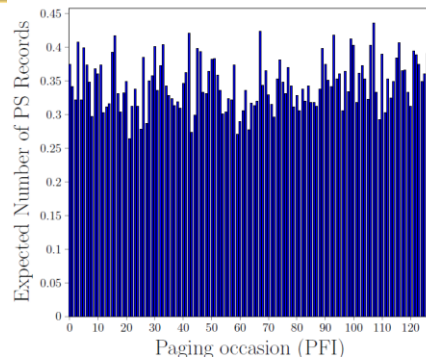


The adversary identifies i as the victim's PFI when

$$\frac{L_i}{L_j} > 10^{\mathcal{T}}$$



Base rate of PS, and CS records



PIERCER (Persistent Information Exposure by the Core network)



MobileInsight

Many network operators use Paging containing IMSI



Link failure during interleaved TMSI reallocation and paging



PAGING

TMSI REALLOCATION

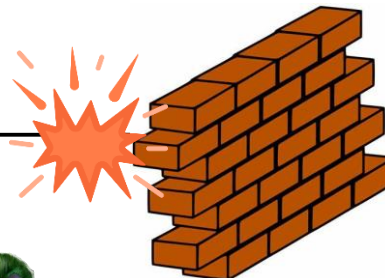


Network failure



Paging with TMSI

Paging with IMSI



Paging channel hijacking?
Need PFI (ToRPEDO)

IMSI-Cracking Attack in 4G



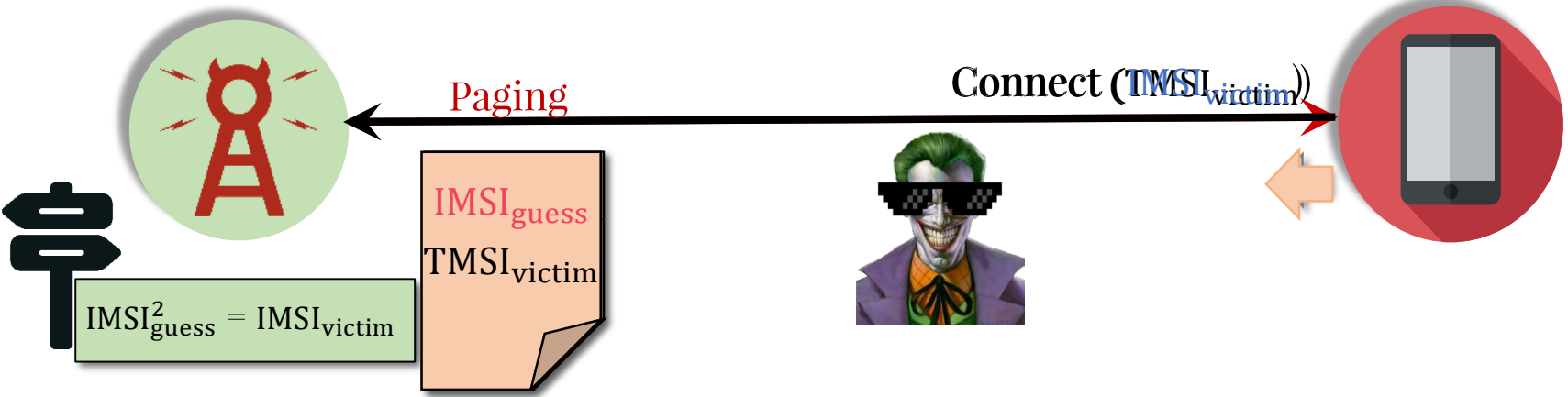
Response to TMSI ≠ Response to IMSI

Respond to TMSI/IMSI whichever comes first

- <TMSI₁, PS>
- <IMSI₁, PS>
- <TMSI₂, CS>
- <TMSI₃, PS>
- ⋮

PFI (ToRPEDO)
TMSI_{victim} (NDSS'12)

Victim



IMSI-Cracking Attack in 5G



No paging with IMSI in 5G

 Exploit Registration Procedure

Check if an IMSI is valid

Check if a valid IMSI belongs to a user




PFI (ToRPEDO)



Registration Request
Auth (IMSI_{guess})
Registration Reject



Authentication Response
Authentication Failure

 $IMSI_{guess}^2 = IMSI_{victim}$

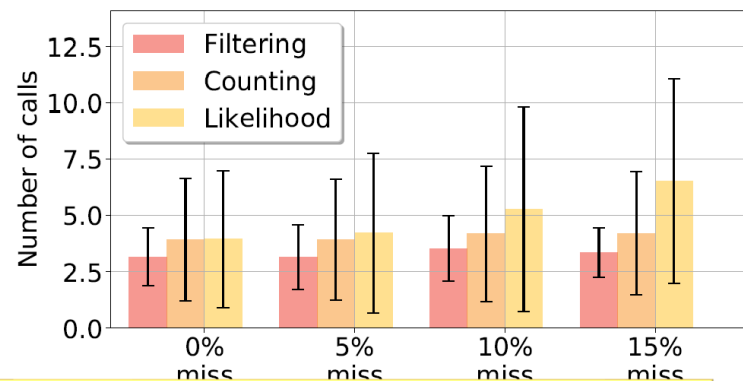
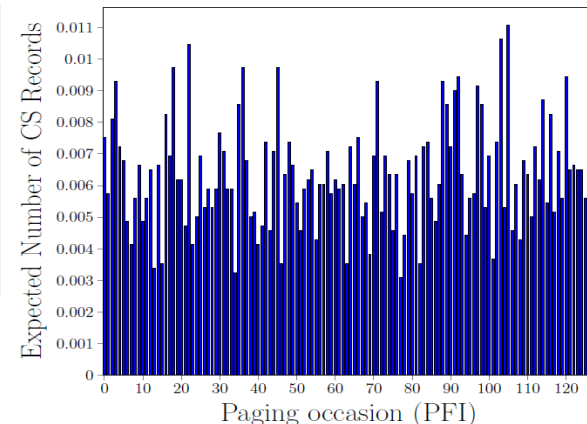
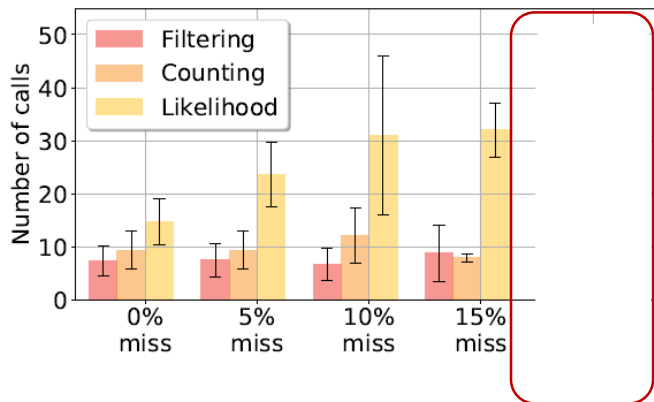
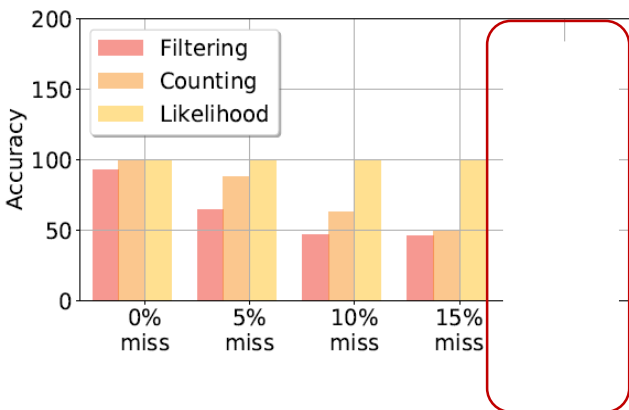


Evaluation

ToRPEDO

VoLTE calls (peak-time)

CSFB calls (peak-time)



PIERCER

1-2 phone call required

1 US
3 GERMANY
3 AUSTRIA
1 ICELAND
3 BANGLADESH

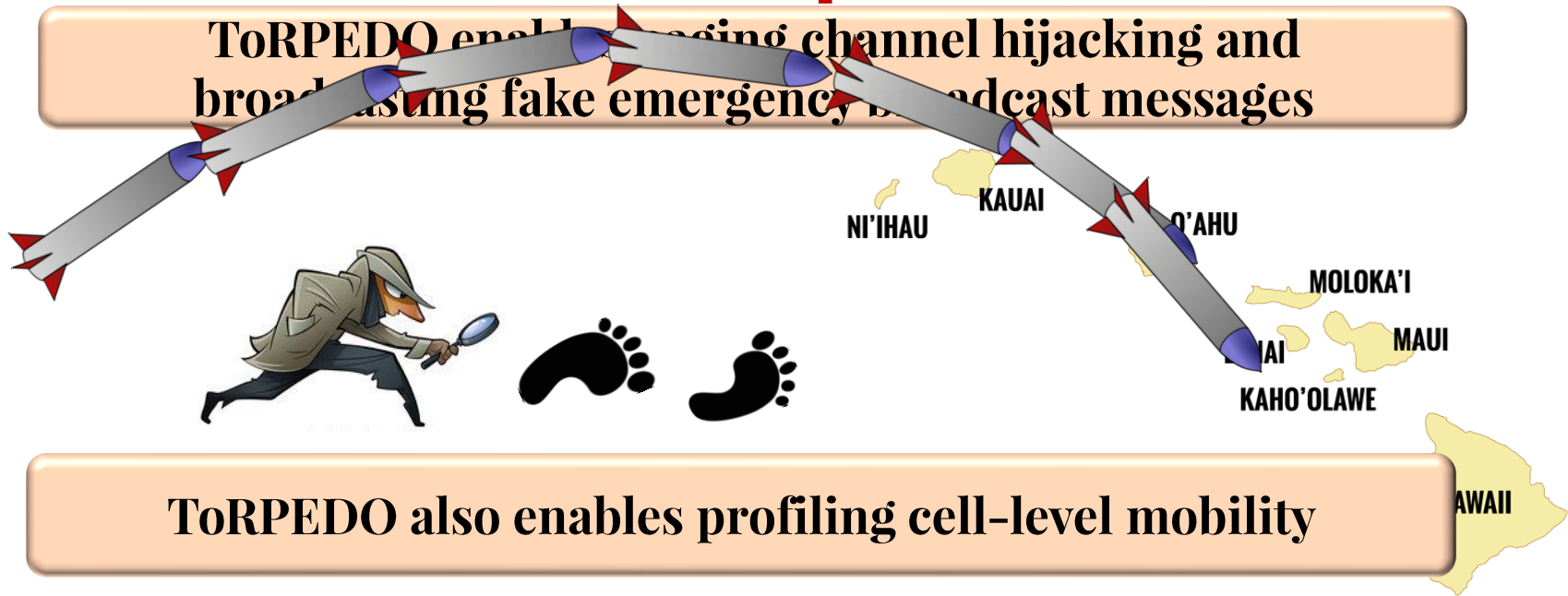
IMSI-Cracking:

207220 paging messages (74 hours)

1 test device does not accept 16 paging records

Attack Impact

ToRPEDO enables hijacking channel and broadcasting fake emergency broadcast messages



ToRPEDO also enables profiling cell-level mobility



IMSI-Cracking is an alternative to Stingrays for both 4G and 5G networks enabling known attacks.

Conclusion



Analyzed and identified inherent design flaws and deployment oversights in 4G and 5G paging protocols



ToRPEDO (Location tracking), PIERCER (IMSI exposure), and IMSI-Cracking



Countermeasures for ToRPEDO

THANK YOU

Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

Syed Rafiul Hussain

PURDUE UNIVERSITY

hussain1@purdue.edu

