Seeing the Forest for the Trees: Understanding Security Hazards in the 3GPP Ecosystem through Intelligent Analysis on Change Requests

Yi Chen, Di Tang, Yepeng Yao, Mingming Zha, XiaoFeng Wang, Xiaozhong Liu, Haixu Tang, Dongfang Zhao

INDIANA UNIVERSITY
BLOOMINGTON

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

WPI

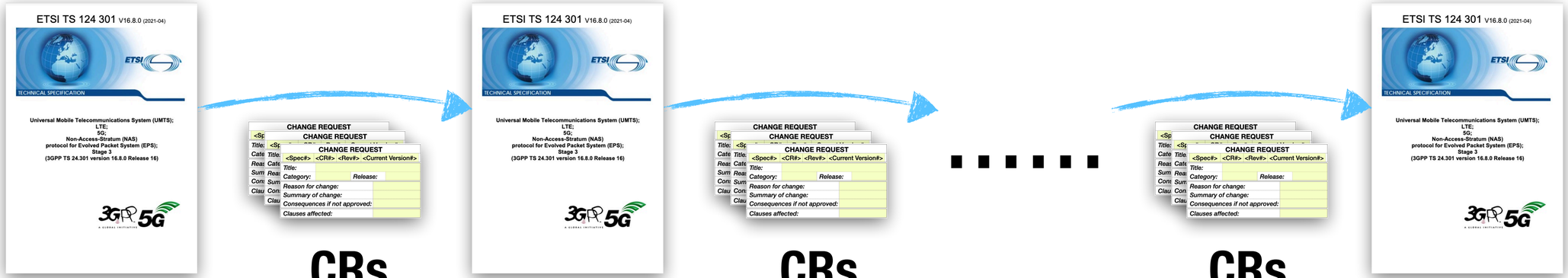

3GPP
A GLOBAL INITIATIVE


ERROR
ETSI TS 124 301 V12.6.0 (2014-10)
ETSI TS 124 301 V16.8.0 (2021-04)
TECHNICAL SPECIFICATION
Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Non-Access-Stratum (NAS)
protocol for Evolved Packet System (EPS);
Stage 3
(3GPP TS 24.301 version 16.8.0 Release 16)

1. Quality of security-related specification content

2. 3GPP specification development procedure

Change Request



Change Request

414,488

16th, Aug, 2021

Security-related Change Request

1,270 SR-CRs

Poor Quality

Inconsistent specification

TS 33.401 v8.6.0

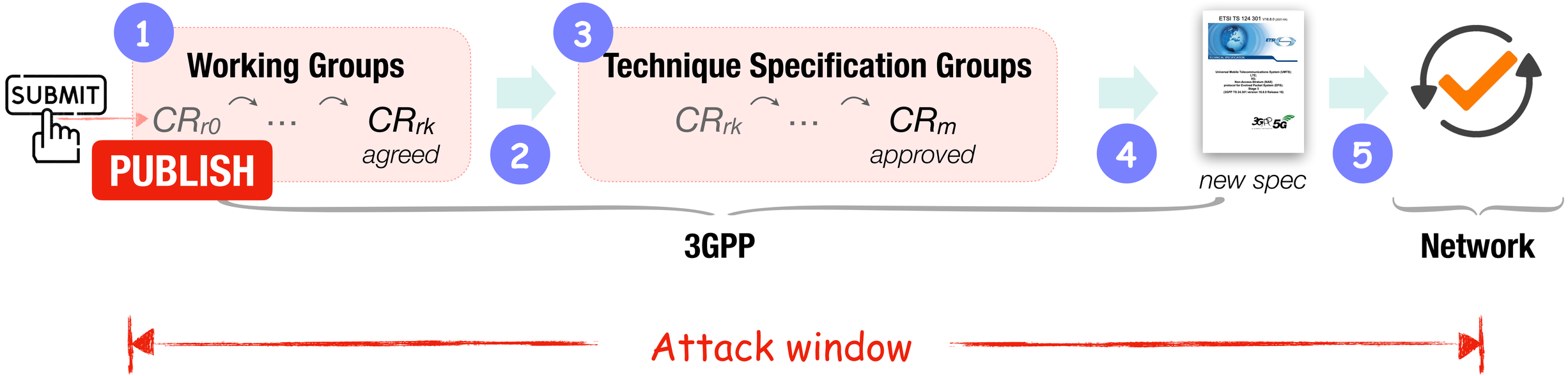
> *… The UE shall discard any message modifying the CSG list if it is not integrity protected.*

TS 24.301 v8.3.0

> *Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the UE or forwarded to the ESM entity, unless the security exchange has been established for the NAS signaling:*
>
> *…*
>
> *ATTACH REJECT (if the EMM cause is not #25)*
>
> *…*

CR: C1-095554

CR processing procedure



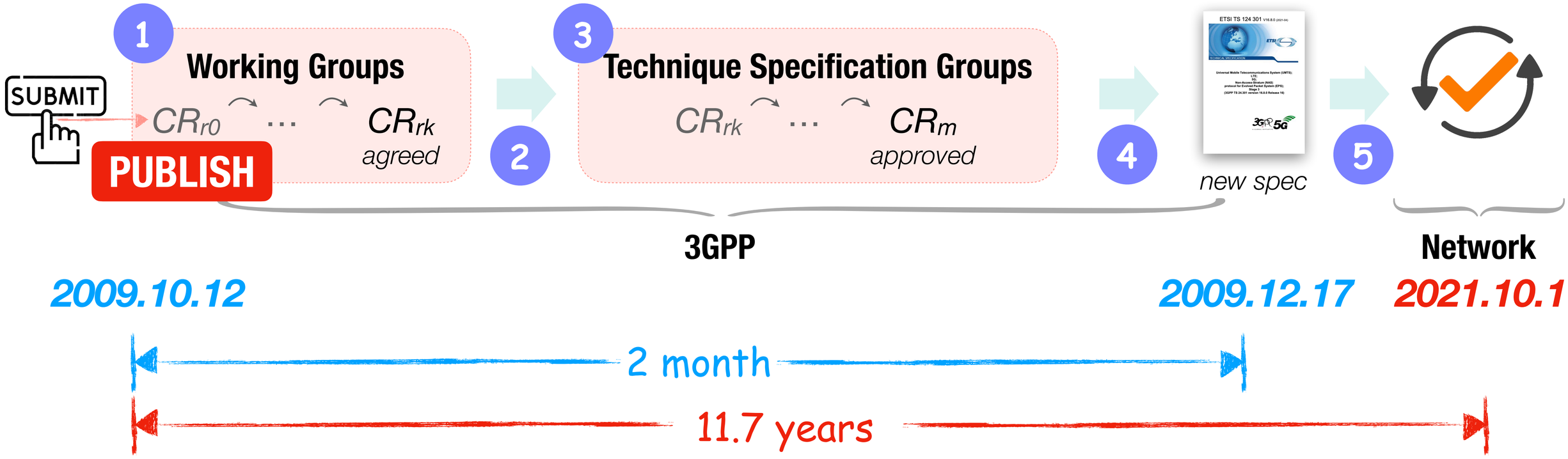
TS 24.301 v8.3.0

C1-094446

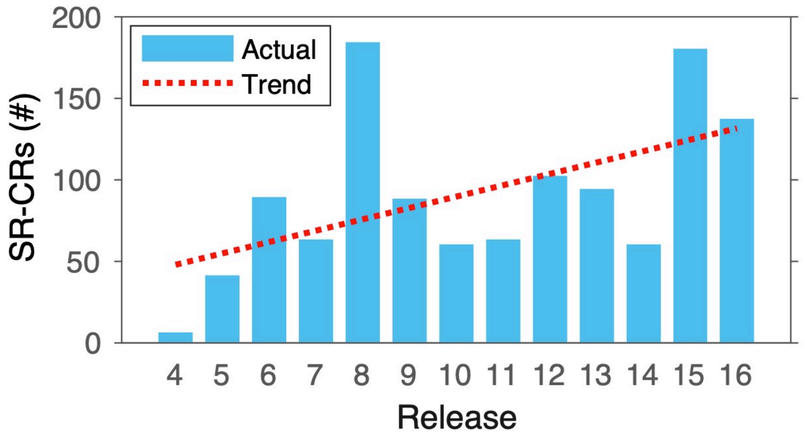
Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the UE or forwarded to the ESM entity, unless the security exchange has been established for the NAS signaling:

…

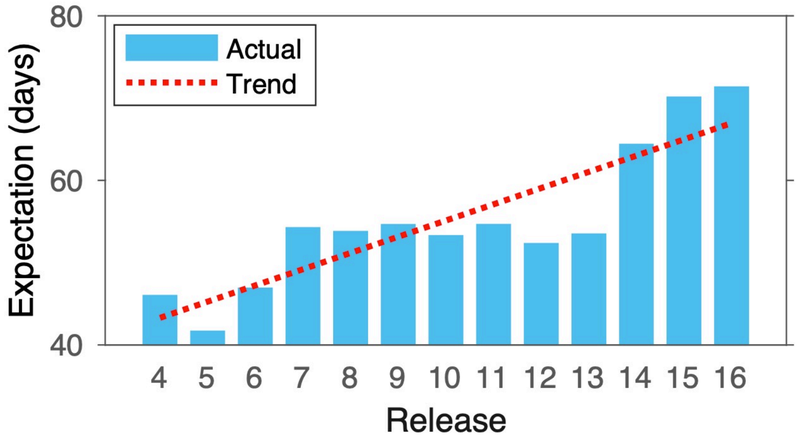
~~*DETACH REQUEST*~~



SR-CRs



Attack window



Inconsistency problem

Attack window