ETSI

The Standards People

Coordinated Vulnerability Disclosure (CVD): ETSI, GSMA and 3GPP programs

S. Compans & A. Zugenmaier

05/10/2022

ETSI Security Week:

Improving 5G Security through Coordinated Vulnerability Disclosure - GSMA CVD Programme

Alf Zugenmaier
CVD Panellist
Munich University of Applied Sciences / NTT Docomo

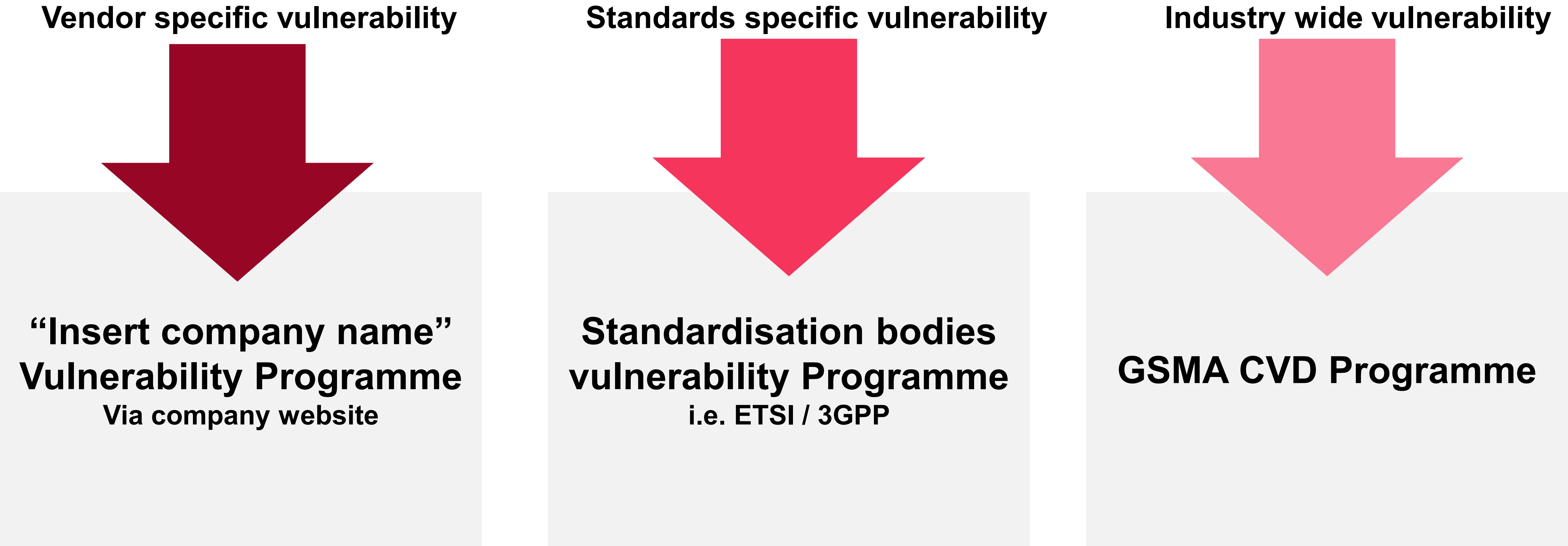
Roger Brown
Security Services Manager
GSMA

October 2022

GSMA™

GSMA CVD Scope

Which CVD scheme should I take my research to?



Vendor specific vulnerability

“Insert company name” Vulnerability Programme

Via company website

Standards specific vulnerability

Standardisation bodies vulnerability Programme

i.e. ETSI / 3GPP

Industry wide vulnerability

GSMA CVD Programme

Benefits for Industry and consumers

- Enables early notification of vulnerabilities
- Provides time to respond and remediate vulnerabilities before they become public
- Enable trustworthy communication between researchers and organisations
- Improves security awareness and readiness

GSMA Coordinated Vulnerability Disclosure Programme scope

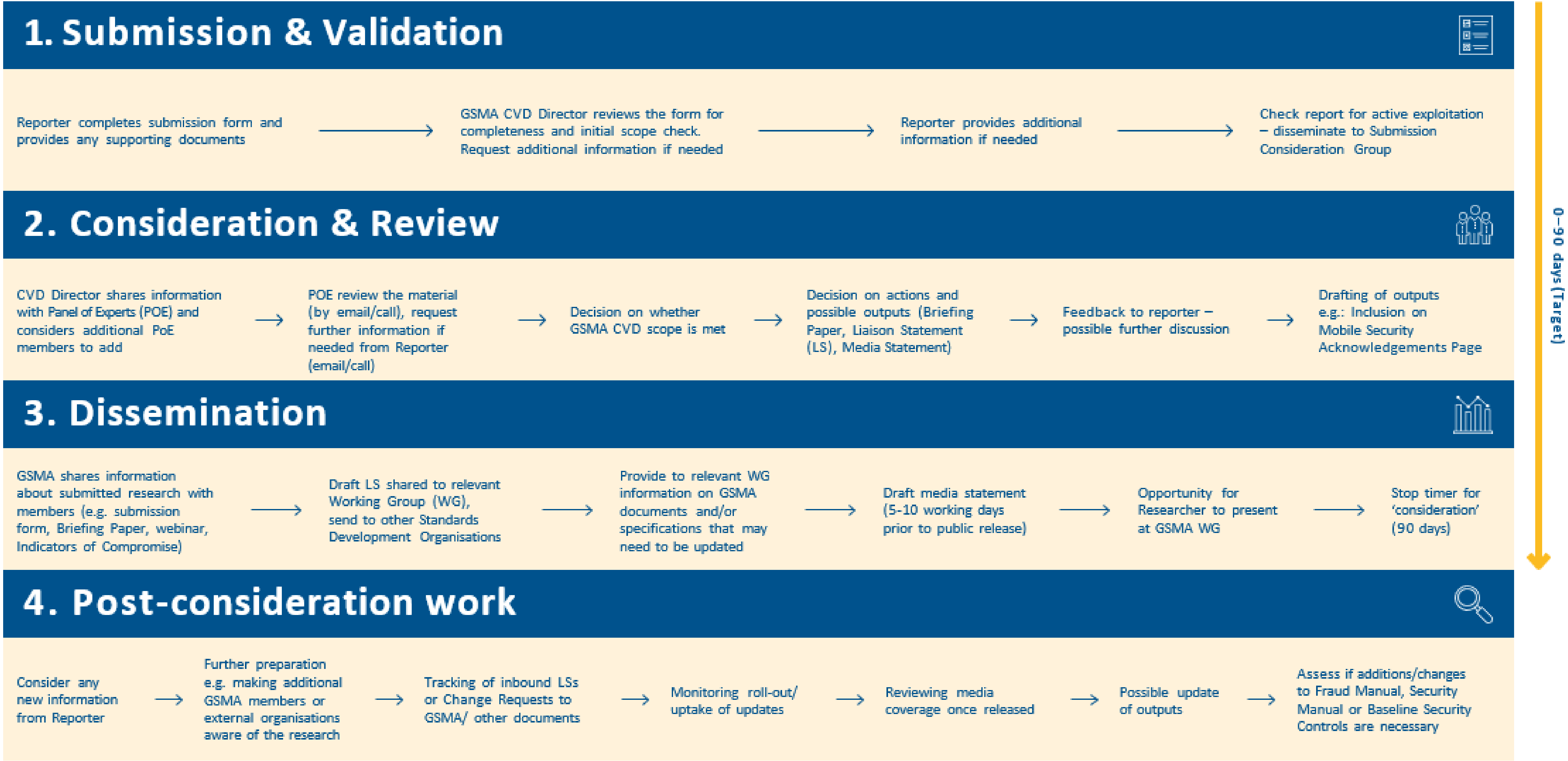
Examples: 4G, 5G, SS7, eSIM, AKA protocols, OAuth2.0

Not previously in the public domain

Must not only apply to vendor specific technologies or services

Focus on open standards based technologies

Researcher process slide and CVD panel activities. Process



1. Submission & Validation

- Reporter completes submission form and provides any supporting documents
- GSMA CVD Director reviews the form for completeness and initial scope check. Request additional information if needed
- Reporter provides additional information if needed
- Check report for active exploitation – disseminate to Submission Consideration Group

2. Consideration & Review

- CVD Director shares information with Panel of Experts (POE) and considers additional PoE members to add
- POE review the material (by email/call), request further information if needed from Reporter (email/call)
- Decision on whether GSMA CVD scope is met
- Decision on actions and possible outputs (Briefing Paper, Liaison Statement (LS), Media Statement)
- Feedback to reporter – possible further discussion
- Drafting of outputs e.g.: Inclusion on Mobile Security Acknowledgements Page

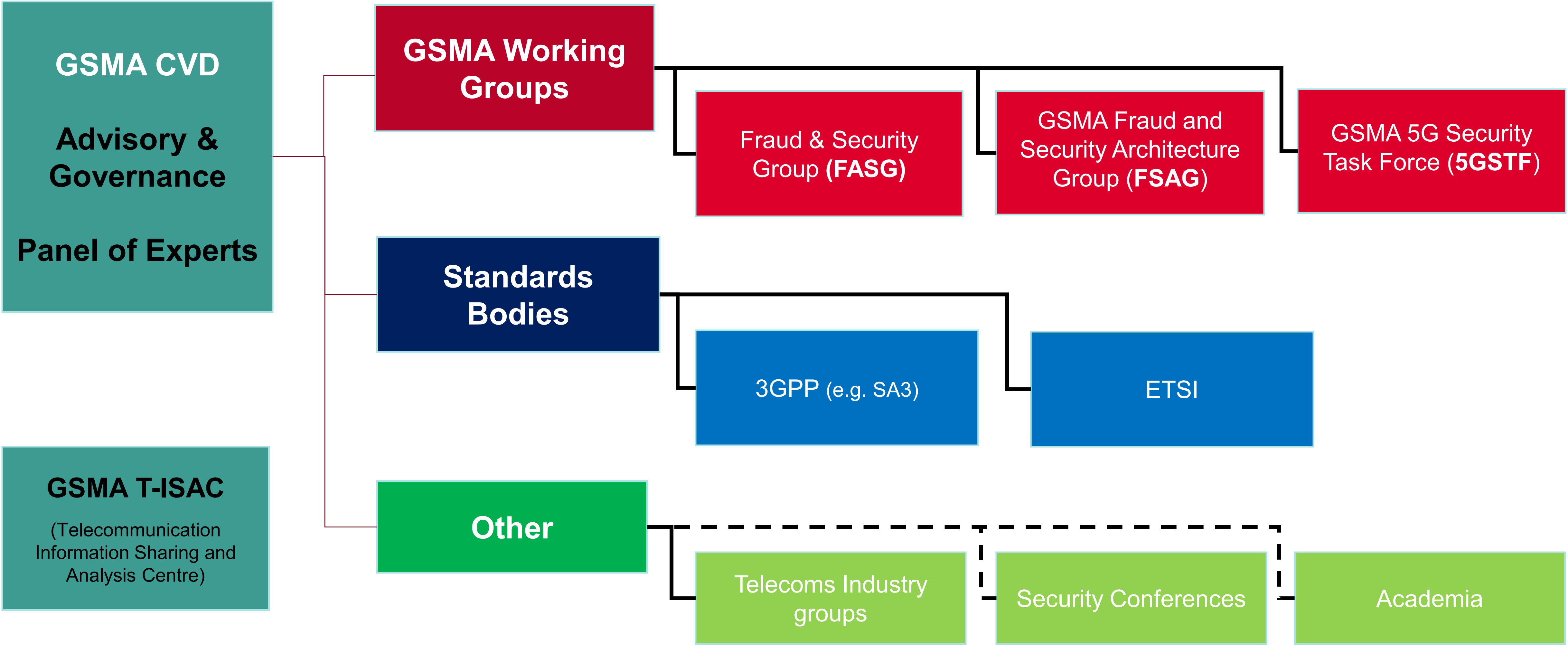
3. Dissemination

- GSMA shares information about submitted research with members (e.g. submission form, Briefing Paper, webinar, Indicators of Compromise)
- Draft LS shared to relevant Working Group (WG), send to other Standards Development Organisations
- Provide to relevant WG information on GSMA documents and/or specifications that may need to be updated
- Draft media statement (5-10 working days prior to public release)
- Opportunity for Researcher to present at GSMA WG
- Stop timer for 'consideration' (90 days)

4. Post-consideration work

- Consider any new information from Reporter
- Further preparation e.g. making additional GSMA members or external organisations aware of the research
- Tracking of inbound LSs or Change Requests to GSMA/ other documents
- Monitoring roll-out/ uptake of updates
- Reviewing media coverage once released
- Possible update of outputs
- Assess if additions/changes to Fraud Manual, Security Manual or Baseline Security Controls are necessary

GSMA CVD Environment



GSMA CVD

Advisory & Governance

Panel of Experts

GSMA Working Groups

Fraud & Security Group **(FASG)**

GSMA Fraud and Security Architecture Group (**FSAG**)

GSMA 5G Security Task Force (**5GSTF**)

Standards Bodies

3GPP (e.g. SA3)

ETSI

Other

Telecoms Industry groups

Security Conferences

Academia

GSMA T-ISAC

(Telecommunication Information Sharing and Analysis Centre)

How to join the Panel of Experts (POE)

GSMA POE Recruitment Phase

1. Applicant fills out and returns CVD application form

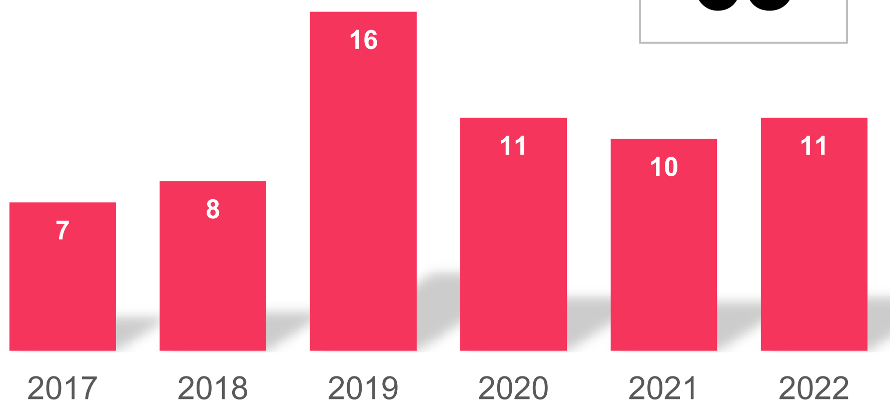
2. GSMA assesses each application using a scoring method

3. New recruits are added to the panel for 2 year term

CVD Dashboard - All CVD submissions

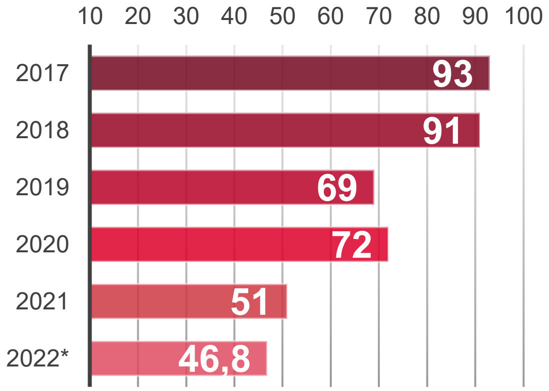
Information correct at 5 Sep 2022

Submissions received per year

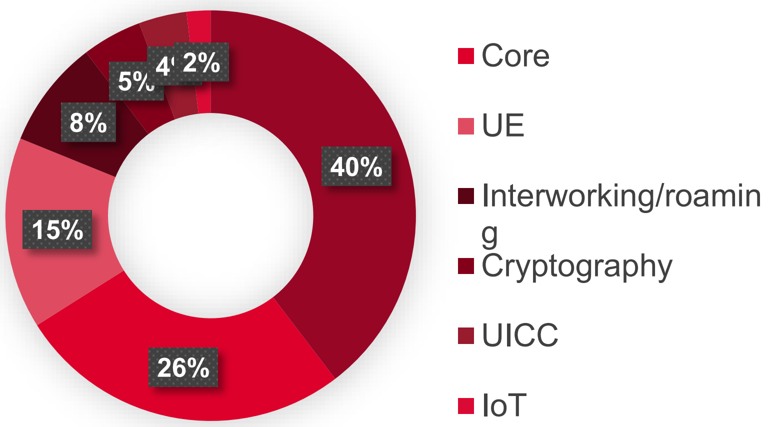


Total
63

Average resolution time - receipt to closed (days)



Technology types
(may be multipe per submission)



Outputs to GSMA members

Briefing Papers and other advisories

29

Mobile Security Acknowledgements

2017	5
2018	5
2019	5
2020	3
2021	6
2022	5

29

Notable Submissions

- Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 - Ruhr University Bochum, Univ Rennes, Inria, Simula UiB, Universite Paris-Saclay, UVSQ (2020)
- VoLTE Eavesdropping – Ruhr Bochum University & NYU Abu Dhabi (2020)
- LTE User plane integrity – Ruhr Bochum University & NYU Abu Dhabi (2018-2020)
- Simjacker – Adaptive Mobile (2019)

Standards bodies engagement

Includes liaison statements, agenda items and contact with working group chairs

24

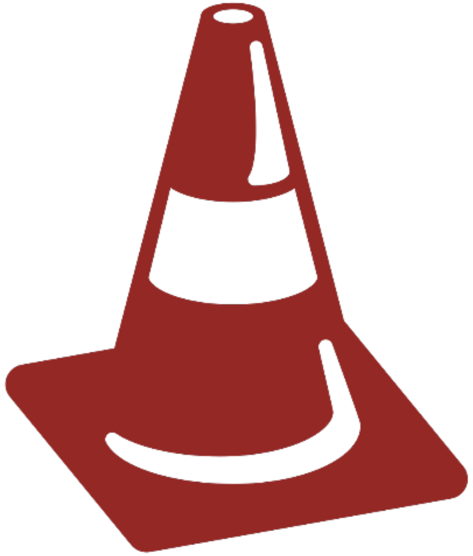
3GPP CVD

Suresh Nair, SA3 Chair, Nokia
Mirko Cano Soveri, SA3 Secretary, MCC
Alf Zugenmaier, Munich University of Applied Sciences and NTT DOCOMO

3GPP CVD Process

- Under Construction

- Previously: ad hoc
- Then: introduction of standing agenda item in meeting agenda
- New process being defined now



3GPP CVD Intake Proces

- Submit over 3GPP Web portal
- Inform a panel of experts for 1st round of discussions
  - Contact authors for a formal presentation of the submission.
  - Invite a panel of experts for the presentation based on the topic/vulnerability
- Assign tracking ownership of CVD to one of the 3GPP experts
- Tracking and log of CVD within 3GPP/SA3

Processing of CVD

Based on initial assessment of the novelty, severity of the vulnerability:

- Invite the authors for a presentation to a 3GPP panel of experts
  - Potentially within 2/3 weeks of the submission.
- Request experts familiar with the paper
- Output: Recognize the authors
  - Follow up in 3GPP: Is CR, SID/WID required?
  - CVD owner to follow up in 3GPP SA3 or other WGs
  - Follow up in regular 3GPP meetings
    - Public discussion
    - Risk assessment
    - Trade-offs
    - Consensus decision

Statistics

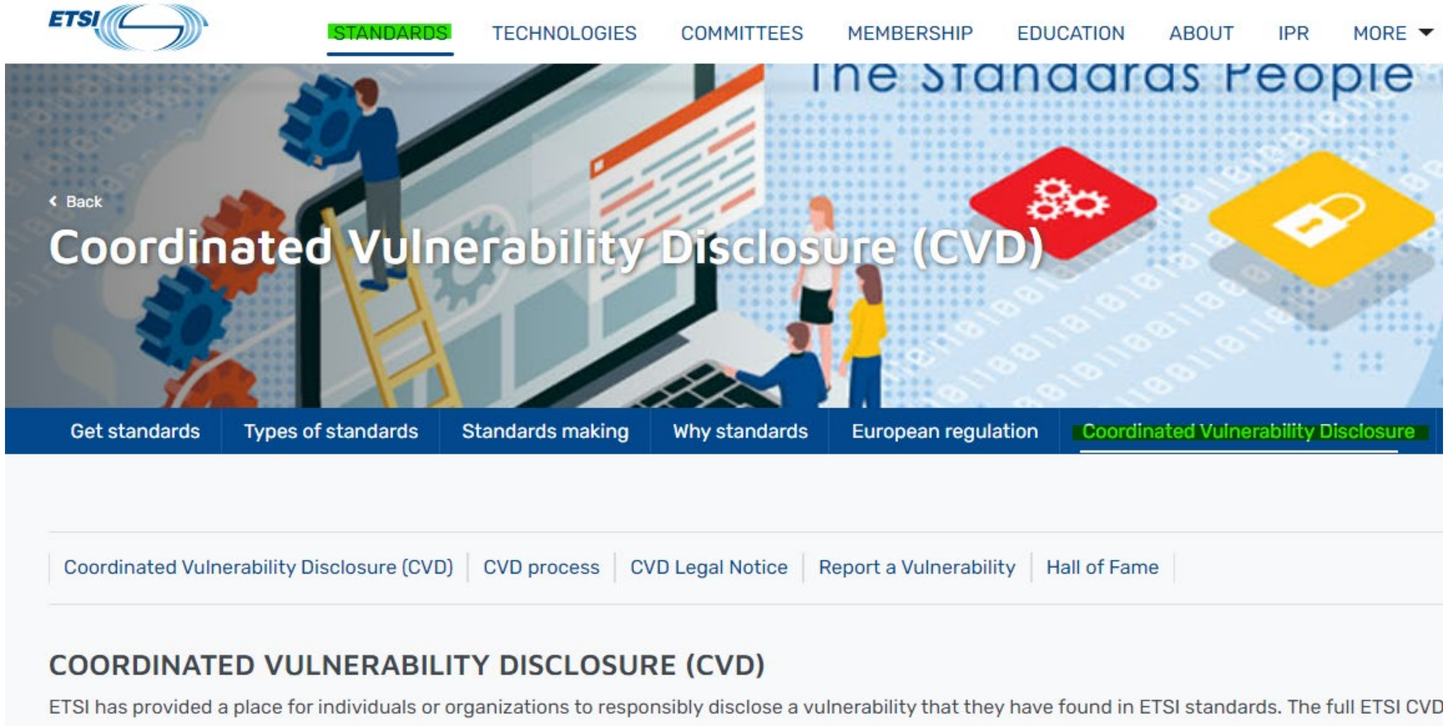
- Total received since the creation of 3GPP CVD (2019): 23
- Total received during this year: 6 (1 related to 3GPP FORGE)
- Related to the 3GPP website, FTP or FORGE: 8
- Related to 3GPP specifications: 15

ETSI CVD

Sonia Compans, ETSI Technical Officer & ETSI CVD point of contact

ETSI CVD

https://www.etsi.org/standards/coordinated-vulnerability-disclosure



Coordinated Vulnerability Disclosure (CVD)

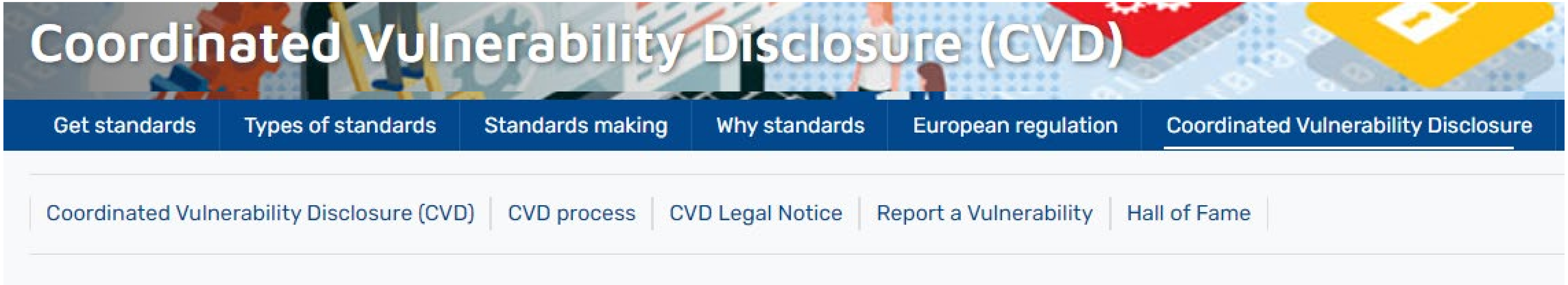
COORDINATED VULNERABILITY DISCLOSURE (CVD)

ETSI has provided a place for individuals or organizations to responsibly disclose a vulnerability that they have found in ETSI standards. The full ETSI CVD

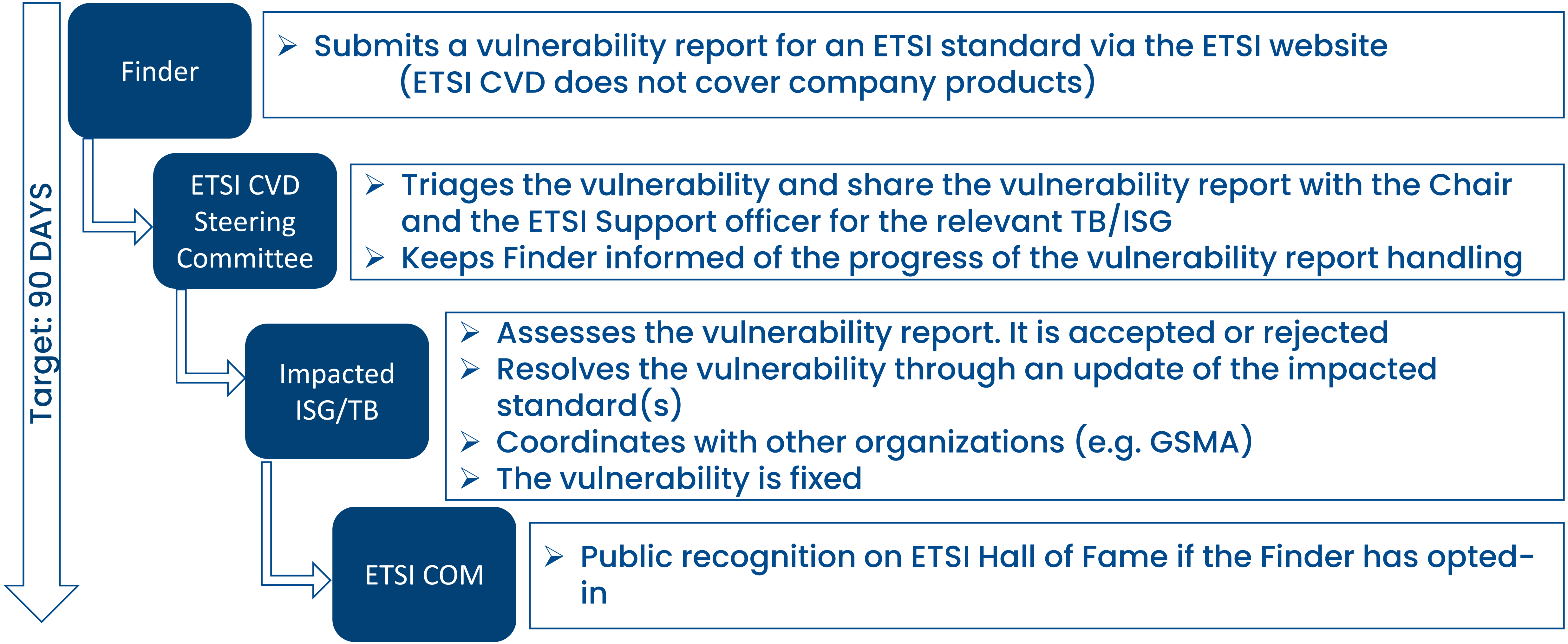
Can also be found through https://www.etsi.org/.well-known/security.txt

ETSI CVD web page

- Introduction
- ETSI CVD Process description (for transparency and to set expectations)
- ETSI CVD Legal Notice
- Form to report a vulnerability
- ETSI Hall of Fame



When a vulnerability is found



Target: 90 DAYS

Finder

- Submits a vulnerability report for an ETSI standard via the ETSI website (ETSI CVD does not cover company products)

ETSI CVD Steering Committee

- Triages the vulnerability and share the vulnerability report with the Chair and the ETSI Support officer for the relevant TB/ISG
- Keeps Finder informed of the progress of the vulnerability report handling

Impacted ISG/TB

- Assesses the vulnerability report. It is accepted or rejected
- Resolves the vulnerability through an update of the impacted standard(s)
- Coordinates with other organizations (e.g. GSMA)
- The vulnerability is fixed

ETSI COM

- Public recognition on ETSI Hall of Fame if the Finder has opted-in

ETSI CVD Statistics

Total received since the creation of ETSI CVD (2020): 63

Related to ETSI IT (website, portal, FTP, Forge): 58

Related to ETSI specifications: 2

Related to 3GPP specifications: 3

HELPING ORGANIZATIONS FIX SECURITY VULNERABILITIES

ETSI released in January 2022 a Guide to Coordinated Vulnerability Disclosure.

ETSI TR 103 838 helps companies and organizations of all sizes to implement a vulnerability disclosure process and fix vulnerability issues before they're publicly disclosed.

- How to receive a vulnerability report
- Responding to a vulnerability disclosure
- Vulnerability management
- Example of vulnerability policy

Conclusion: Use our CVD programs to make products and standards more secure

Alf Zugenmaier alf.zugenmaier@hm.edu

Sonia Compans sonia.compans@etsi.org

Appendix and References

CVD-2018-0012

A Formal Analysis of 5G Authentication

Lucca Hirschi, David Basin, Jannik Dreier, Saša Radomirović, Ralf Sasse, Vincent Stettler

- **Described flaws in the 5G standard which could lead to network deployments not fulfilling critical security goals of 5G AKA (Authentication and Key Agreement)**
- **This claimed to allow an attacker to bill a different subscriber, impersonate a serving network towards a subscriber, or how an active attacker can trace a subscriber if the attacker stays in physical vicinity of the subscriber**
- **Suggested changes within the paper to authentication process cause possible issues with backwards compatibility (including NSA 5G deployments)**
- **Limited media pickup**
- **Resolution: partly fixed already (TS 33.501), further standards work triggered to update 3GPP 5G standards (S3-183653)**
- **GSMA Hall of Fame (HoF) – included for academic merit**

CVD-2018-0014

Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information ("ToRPEDO")

Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li and Elisa Bertino

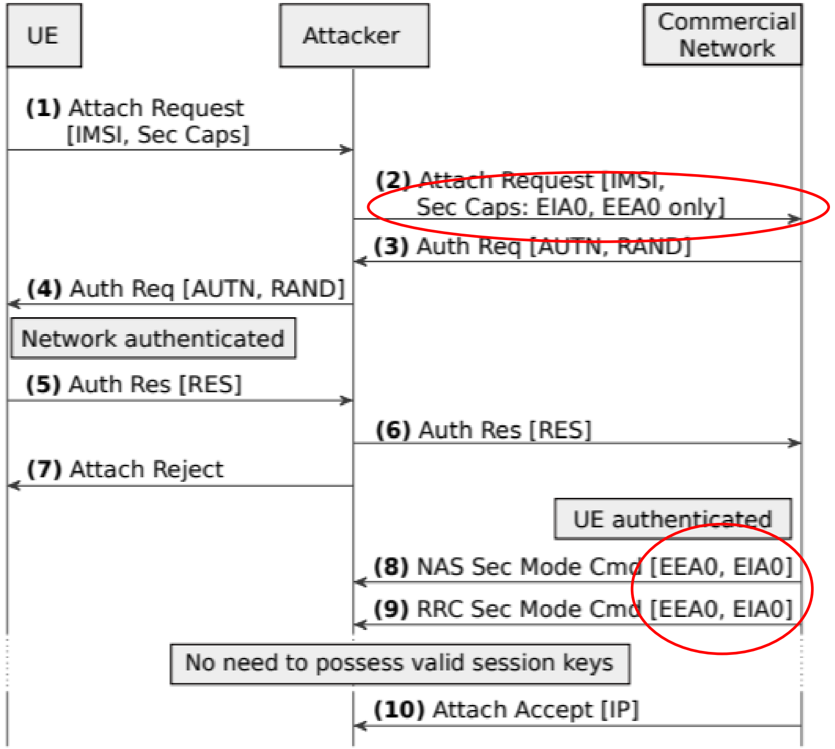
- **Describes a design weakness of the 4G cellular paging protocol which can be exploited using a false base station**
- **Used to target a subscriber's IMSI/SUPI by sending multiple messages in quick succession and then monitoring the network to identify increased traffic against a specific subscriber**
- **This approach would have to be performed in specific timeslots and be based on trial and error which would be an exhaustive and time consuming process (hours)**
- **Significant media pickup – however limits of exploit not noted in coverage**
- **Resolution: 5G procedures were changed in 3GPP TS 38.304 v15.1.0 – investigations within 3GPP about fixing for 4G**
- **GSMA HoF – based on academic research approach**

CVD-2018-0013

LTE Security Disabled - Misconfiguration in Commercial Networks

Merlin Chlosta, David Rupprecht, Thorsten Holz, Christina Pöpper

- **Discussed how some 4G networks were configured insecurely and failed to enforce standards-compliant behaviour. 5G also affected**
  - Standards-compliant behaviour: mandatory rejection of UEs without integrity protection on NAS and RRC (except emergency calls in some jurisdictions)
- **Researchers demonstrate how an attacker can exploit this misconfiguration and request insecure operation – possible billing fraud (with false base station)**
- **No media pickup**
- **Resolution: 3GPP TS 24.301/24.501 updated for EPS and 5GS to clarify the expected behaviour (reject UE)**
- **GSMA HoF – for standards and real-world impact**



UE

Attacker

Commercial Network

(1) Attach Request [IMSI, Sec Caps]

(2) Attach Request [IMSI, Sec Caps: EIA0, EEA0 only]

(3) Auth Req [AUTN, RAND]

(4) Auth Req [AUTN, RAND]

Network authenticated

(5) Auth Res [RES]

(6) Auth Res [RES]

(7) Attach Reject

UE authenticated

(8) NAS Sec Mode Cmd [EEA0, EIA0]

(9) RRC Sec Mode Cmd [EEA0, EIA0]

No need to possess valid session keys

(10) Attach Accept [IP]

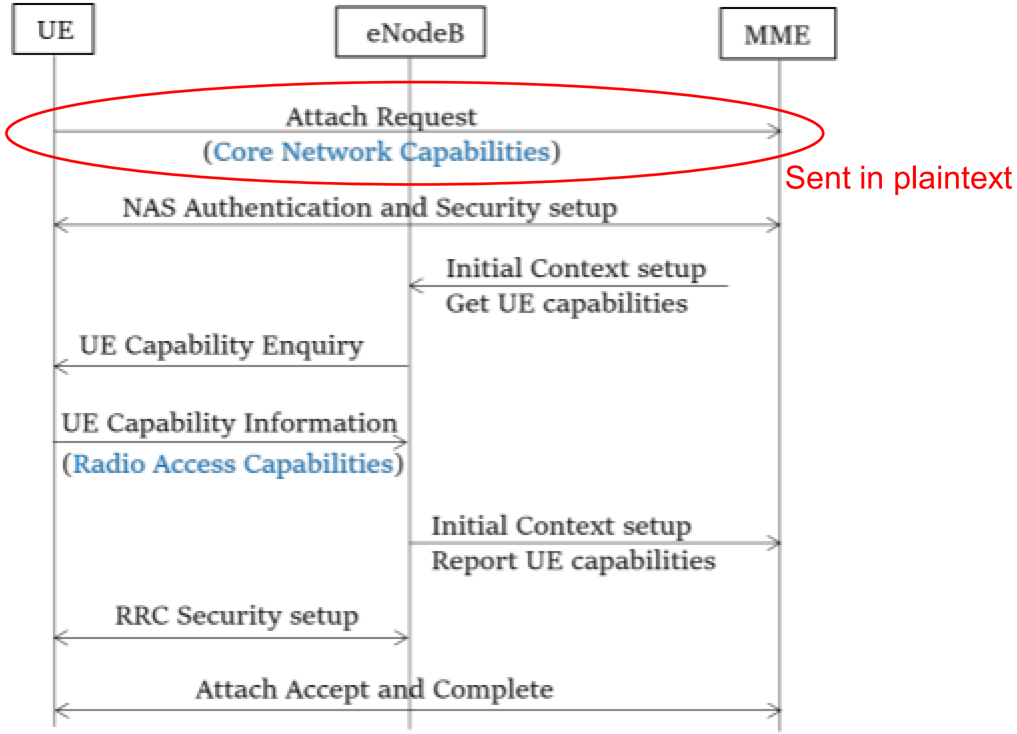
LTE Security Disabled—Misconfiguration in Commercial Networks, Chlosta et al.

CVD-2019-0018

New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities

Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, Jean Pierre Seifert

- **Discussed a standards flaw allowing unprotected exchange of device capability information between the device and the network - now resolved**
- **This was claimed to allow an attacker to profile a device/network to target further attacks**
- **Media pickup as part of Blackhat presentation**
- **Resolution: 3GPP TS 36.331 change – to set up security before exchange of UE capability information**
- **GSMA HoF – for detection of flaw in standards**



New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities, Shaik et al.

CVD-2019-0029

5GReasoner - Vulnerabilities in the NAS and RRC layers of 5G control plane protocol stack

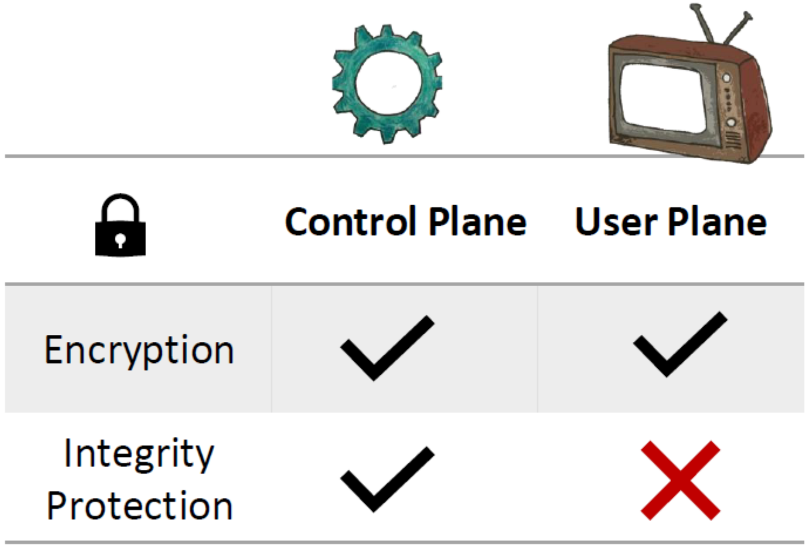
Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino

- **Several scenarios related to the 5G phase 1 standards**
- **Scenarios judged as nil or low impact in practice – some claims not within the stated security goals for the 5G design – emergency calls, poor network configuration, increase power usage, find temporary identifier (GUTI/I-RNTI). Appreciate the authors' work to identify where the standard is written ambiguously**
- **On 24-bit NAS COUNT in 5G, it seems clear the intention of the 3GPP specifications is that the same value of NAS COUNT should never be used twice**
- **Some media pickup**
- **Resolution: standards work ongoing in 3GPP relating to NAS COUNT issue – make unambiguous what should happen when receiving same NAS count repeatedly (3GPP TS 24.501)**
- **GSMA HoF – included for identifying ambiguously written standard**

CVD-2019-0024 and CVD-2018-0008

IMP4GT: IMPersonation Attacks in 4G NeTworks
David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper

- **Exploits false base station, lack of user plane integrity protection and packet reflection behaviour to create cryptographic oracle - but only within limited area (MITM)**
- **Allow an attacker to encrypt packets - impersonation of user to-network or network-to-user for limited purposes**
  - Billing fraud
  - Network-asserted identity impersonation
  - Bypass network filtering
- **CVD-2018-0008 – limited to DNS manipulation: send user to false website**
- **Resolution: work ongoing within 3GPP on 5GSA (TS 38.300/24.501)**
- **GSMA HoF – real world impact**



🔒	Control Plane	User Plane
Encryption	✓	✓
Integrity Protection	✓	✗

IMP4GT: IMPersonation Attacks in 4G NeTworks presentation, NDSS Symposium, Rupprecht et al.