Example references for re-use. IEEE style: <https://ieee-dataport.org/sites/default/files/analysis/27/IEEE%20Citation%20Guidelines.pdf>

MITRE follows IEEE’s reference style for citing sources. See <https://comm.mitre.org/strategiccommunications/mpg/writing-style/references/> and it points to https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

Note that ATT&CK has the date right after the author (example: 3GPP. (2000, January). A Guide to 3rd Generation Security. Retrieved December 19, 2016.) , while this IEEE source indicate to put the date last.

|  |  |
| --- | --- |
| Name | URL |
| The name that will appear on the website | The fully functional URL that will be the hyperlink for the text in the left hand column. |
| 3rd Generation Partnership Project (3GPP) TR 33.926: “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes”, Technical Report, v17.3.0, December. 2021, clauses <…> | <https://www.3gpp.org/DynaReport/33926.htm> |
| 3rd Generation Partnership Project (3GPP) TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, Technical Specification, v17.4.0, March 2022. | <https://www.3gpp.org/DynaReport/23502.htm> |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks> |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, November 2019. | <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks> |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | <https://arxiv.org/abs/2005.05110v1> |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | <https://arxiv.org/abs/2108.11206> |
| European Union Agency for Cybersecurity (ENISA), “Signaling security in telecom SS7/Diameter/5G”, March 2018 | <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g> |
| 3rd Generation Partnership Project (3GPP) TS 33.501: “Security architecture and procedures for 5G system”, Technical Specification, v17.5.0, March 2022, clauses <…> | <https://www.3gpp.org/DynaReport/33501.htm> |

|  |  |
| --- | --- |
| Name | URL |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | <https://arxiv.org/abs/2005.05110v1> |