Security Roadmap Towards 6G Systems

Mohammed Ramadan
Cyber Security Unit
RISE - Research Institute of Sweden
Stockholm, Sweden
mohammed.ramadan@ri.se

Abstract:

6G system is in an active race to be fully deployed by 2030. 6G system is expected to provide (100-1000) more advanced key performance indicators (KPIs) than 5G systems, such as ultra-low latency, low power consumption, ultra-high capacity, seamless coverage, high localization precision, massive MIMO (small cell), millimeter-wave (mmWave), terahertz (THz) bands. Consequently, these high-performance specifications will enable new technologies within 6G systems such as the internet of everything (IoE), multi-sensory extended reality (XR), autonomous systems, Artificial intelligence (AI), machine learning (ML), heterogeneous wireless networks (HWN), intelligent and distributed environments, cell-free and visible light communications, wireless brain-computer interactions (BCI), etc. These new technologies will open the door widely to new security issues; and will significantly impact the security and privacy of the upcoming 6G system. Therefore, novel security techniques (encryption, authentication, privacy-preserving, key agreement, access control) or fundamental changes must be considered. For instance, distributed mutual authentication protocols are highly required for some 6G-based emerging technologies (e.g., HWN, IoE), whereas end-to-end security and encryption protocols are needed for other emerging technologies. Hence, extensive research works are supposed to be carried out to meet all these security requirements and ensure the reliability and functionality of the upcoming 6G system.

***Keywords*:** Cyber security, 6G security, 6G security prospects.