Project Area 5: Cyber Security

cnr DIITET
Consiglio Nazionale delle Ricerche
Engineering, ICT and Technologies for Energy and Trasportation Department

Objective: prevention, detection and reaction to cyber-attacks. The needed effort is huge because 1) citizens' everyday life relies on cyber systems, e.g. energy distribution, and healthcare, and their failures can affect millions of people 2) attacks can be caused by people thousands of kilometers far from the affected area 3) one of the main sources of data helping cyber attackers is the people's unaware digital behavior.

Approach: The CNR Project Area Cyber Security fully covers all the above issues by addressing the following topics: (1) Cyber-Physical Systems (CPS) where cyber-attacks may lead to injuries to human beings and loss of lives. (2) Network security i.e. Slow Denial-of-Service (DoS) attacks and monitoring TOR (The Onion Router) WEB network for illegal activities. (3) Intrusion Detection and Protection by means of the measure of (abnormal) power consumption. (4) Privacy risk assessment and privacy-by-design to guarantee high protection of personal data to enable (big) data analytics. (5) Information Sharing and Analytics (ISHA): ma- chine learning, artificial intelligence and data analytics tech- niques to make sense of large amounts of data. (6) Cyber-intelli- gence on Social Media: gathering and analyzing data from Social Media for Intelligence purposes. (7) Secure Software Engineering assures integrated approaches during all the development cycle of software-intensive systems. (8) Access Control and Trust Man- agement are among the most important security tools. (9) Cryp- tography: reliable, efficient implementations of state-of-the-art algorithms and protocols as well as high-performance code breaking platforms. (10) Cloud Security to protect data and re-sources stored and shared on the Cloud, and the business or re- search process that outsourced to the Cloud. (11) Cyber insur- ance is a new domain: damages

Figures:

Scientific Impact/Results: The current research activities and proposed approaches are showing good results from the theoretical and practical point of view, with successful publications and collaborations with national and international industrial partners, and public bodies. On the one side this shows that the right way has been taken, but also that more resources and effort are needed to provide adequate solutions in a world where cybersecurity is perceived as a major challenge by both citizens and institutions, and rightly so.