INTRODUCTION

Compromising emanations are defined as unintentional intelligence bearing signals data related or revealing information which, if intercepted and analyzed, disclose the classified and security information transmitted, received, handled or otherwise processed by any information-processing equipment. Therefore, the main objectives of hardware security evaluation laboratory include following:

- Determining the security requirements applicable to a given system.
- Measuring the extent to which the system satisfies its applicable security requirement and introduces residual risk.

SERVICES

- Hardware Evaluation
  - Detecting spyware by the analysis of system on Board and chip level.
  - Hardware system security assessment in the level of revision of System, Board and Chip based on methodologies developed.
  - Hardware systems safety assessment in terms of malfunction of other devices.
  - Safety assessment in terms of robustness against interference in operational areas.
  - Validating the performance of equipment based on determining the originality of parts.
- Propagation Evaluation
  - Security assessment of the propagation of equipment and providing a safe zone for equipment.
  - Security assessment of the propagation of side channel in encryption systems.
  - Security assessment of systems in terms of propagation power.
  - Monitoring system within a specified time in terms of propagation.
- Protocol Evaluation
  - Designing the attack scenario and protocol penetration testing.
  - Protocol security evaluation according to the studying of protocol and conceptual analysis of system security.
  - The initial assessment of protocol security according to threat reported.
  - Documentation and classification of protocol security level based on provided documents.

CAPABILITIES

- Handling hardware security training courses, such as EMC and TEMPEST Learning.
- Designing, mobilizing and setting up Hardware Security Evaluation Laboratory.
- Designing and building security room for critical data processing center.
- Defining security requirements for specific system from design to production.