Communications security

Dr. Talal Alkharobi

Communications security (COMSEC)

- Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

Communications security (COMSEC)

3

- Communications security includes
  - cryptosecurity,
  - transmission security,
  - emission security,
  - traffic-flow security
  - physical security of COMSEC equipment.

cryptosecurity

4

- The component of communications security that results from the provision of technically sound cryptosystems and their proper use.
- This includes insuring message confidentiality and authenticity.

5

Traffic-flow security

- The use of measures that conceal the presence and properties of valid messages on a network to prevent traffic analysis.
- This can be done by operational procedures or by the protection resulting from features inherent in some cryptographic equipment.

6

Traffic-flow security Techniques

- changing radio callsigns frequently
- encryption of a message's sending and receiving addresses (codress messages)
- causing the circuit to appear busy at all times or much of the time by sending dummy traffic
- sending a continuous encrypted signal, whether or not traffic is being transmitted.

Transmission security (TRANSEC)

7

- Protect transmissions from interception and exploitation by means other than cryptanalysis.
- Examples are frequency hopping and spread spectrum

Transmission security (TRANSEC)

8

- security include:
  - Low probability of interception
  - Low probability of detection
  - Antijam — resistance to jamming

9

Emission security (EMSEC)

- Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems (computers), and telecommunications systems.

10

Compromising emanations

- Unintentionial signals which, if intercepted and analyzed, disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
- Laboratory and field tests have established that such CE can be propagated through space and along nearby conductors.

11

Compromising emanations

- Compromising emanations consist of electrical or acoustical energy unintentionally emitted by any of a great number of sources within equipment/systems which process information.
- This energy may relate to the original message, or information being processed, in such a way that it can lead to recovery of the plaintext.

12

Compromising emanations

- The interception/propagation ranges and analysis of such emanations are affected by a variety of factors,
  - the functional design of the information processing equipment;
  - system/equipment installation;
  - environmental conditions related to physical security and ambient noise.

13

Compromising emanations

- The term "compromising emanations" rather than "radiation" is used because the compromising signals can, and do, exist in several forms such as magnetic and/or electric field radiation, line conduction, or acoustic emissions.

14

TEMPEST

- Codename referring to investigations and studies of compromising emanations (CE).
- It is often used broadly for the entire field of Emission Security (EMSEC).
- Has been variously reported as standing for
  - "Transient ElectroMagnetic Pulse Emanation STandard“
  - "Telecommunications Electronics Material Protected from Emanating Spurious Transmissions."

15

TEMPEST certification

- The NSA-USA publishes lists of labs approved for TEMPEST testing and equipment that has been certified.
- The United States Army has a TEMPEST testing facility, as part of the U.S. Army Information Systems Engineering Command
- Similar lists and facilities exist in other NATO countries.

16

TEMPEST certification

- Certificates must apply to entire systems, not just to individual components, since connecting a single unshielded component (such as a cable) to an otherwise secure system could easily make it radiate dramatically more RF signal.
- Users who must specify TEMPEST certification could pay much higher prices, for obsolete hardware, and be severely limited in the flexibility of configuration choices available to them.
- A less-costly approach is to place the equipment in a fully shielded room.