

Compromising emanations analysis

The invisible threat to information security

Johan Anstrell
Manager Comex International



Definition of compromising emanations

“Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

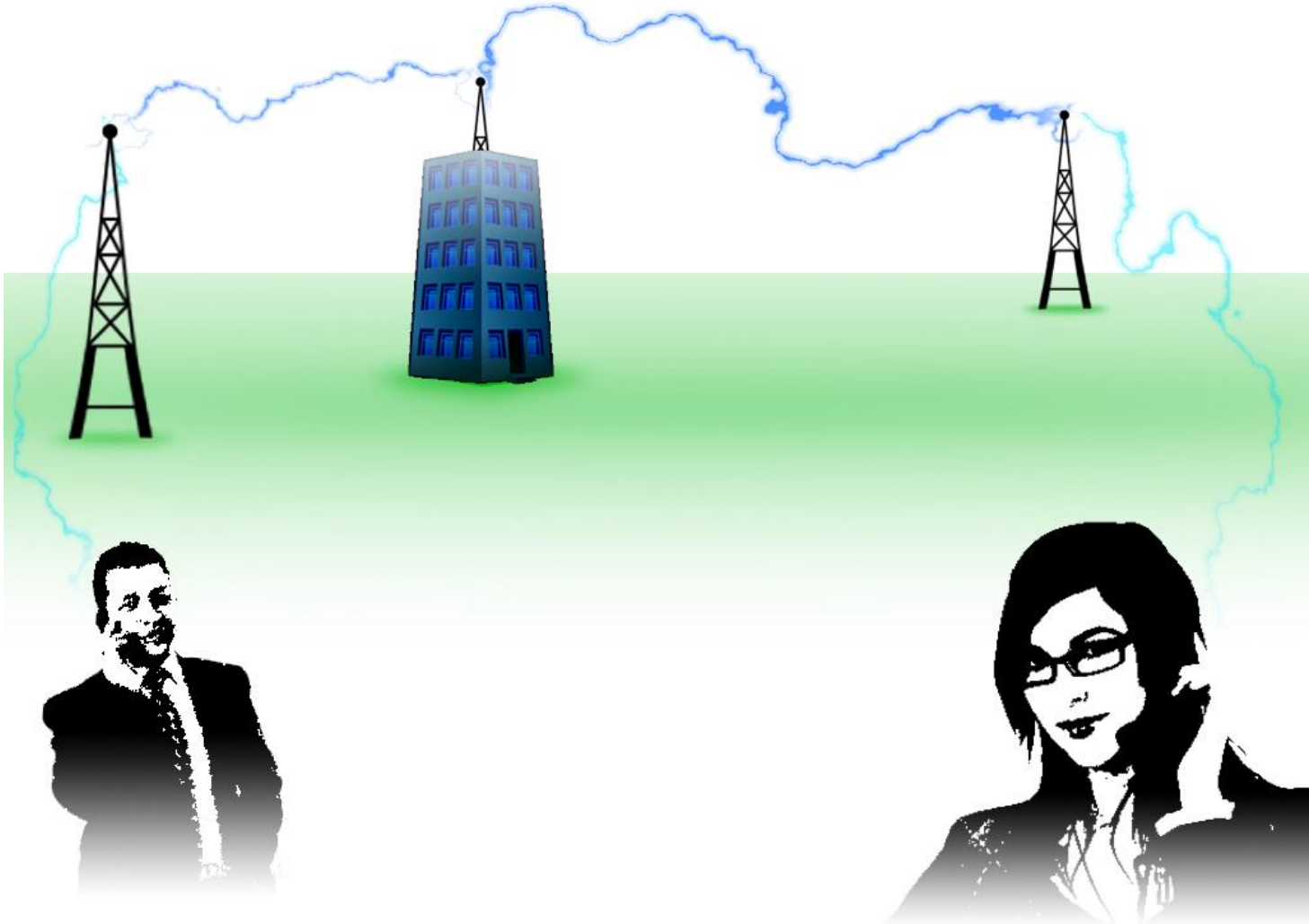
Compromising emanations consist of electrical, mechanical, or acoustical energy intentionally or by mishap unintentionally emitted by any number of sources within equipment/systems which process national security information.”

[From Wikipedia, the free encyclopedia]

Electrical aspect of compromising emanations

- All electric equipment generates unintentional electromagnetic signals that are radiated from the equipment.
- These signals can contain secret information!
- These signals can be transmitted through:
 - The air
 - Water pipes
 - Electrical conduits
 - Ventilation system
 - Etc.
- The defence standard handling this aspect is:
 - TEMPEST (NATO countries)
 - RÖS (Sweden)

Example of electromagnetic signals



Available sources in IT systems

- A computer radiates several information carrying signals, generated by for example:
 - Screen
 - Keyboard
 - Hard drive
 - Etc.
- Peripherals like printers, scanners etc. also radiates information carrying signals.
- An attacker can eavesdrop on these signals and re-create the original information without the knowledge of the user.

Signal recording and analysis

- There are two different approaches:
 - Real-time analysis of detected signals
 - Recording signals for post-collection data analysis
- During the analysis, signals from equipment such as computers can be separated due to the differences in clock frequencies.
- You do not need a laboratory to record and analyze the signals. All you need is:



Raider II from SystemWare-Europé Ltd

Protection against compromising emanations

- What about encryption?
 - Only protects the information during transport or storage – not during modification or displaying situations.
- There are only two options for protecting against compromising emanations:
 - Use of shielded rooms
 - + You can securely use any type of equipment
 - + Easy to update equipment
 - Expensive to build
 - Stationary solution
 - Not user friendly
 - Use of protected equipment
 - + User friendly solution
 - + Flexible solution, easy to change location
 - You must use approved equipment

Examples of protected products



Comex® Notebook



Comex® Tower



Comex® Screen Client



Comex® Scanner



Comex BioSec Reader®



Comex® Colour Printer



Comex® Laser Printer



Comex® Secure Cabinet

Closing remarks

- Everyone uses firewalls
- You can detect if someone hacked your system:
 - How far did they get?
 - What type of information were compromised?

→ You can act accordingly
- Analysis of compromising emanations is an invincible threat that does not leave a trace – you do not know if you are attacked!

For more information visit our website...

www.comex.se/