

Another kind of espionage – unnoticed and noiseless



Even though tensions between East and West are continuing to ease, the threat has not decreased. To the contrary, the media and protectors of the constitution report an increase in worldwide economic espionage. With an adequate budget and suitable measuring equipment, interception specialists cause billions in damage to the world economy every year.

Secret and highly sensitive data such as, for example, information on research and development, human assets or confidential company and customer data, must be kept locked up so that strangers cannot access this information.

To prevent this spurious activity, many official offices, state agencies, protectors of the constitution, federal information services, etc. use Tempest

equipment. Although many IT security officers think encoding data and protecting networks with firewalls is sufficient for data security, they are wrong.

Spying on unsecured IT workplaces and their networks using compromising or revealing emission goes unnoticed by users since this process is silent.

The phenomenon of emission

Electrical and electronic devices emit electromagnetic energy to their surroundings. This also includes the connected data cables and power supply lines. This energy spreads itself over all conductive objects such as, for example, water pipes, radiator pipes, power cables or air-conditioning systems. In addition, this energy also spreads throughout the atmosphere which is then referred to as compromising emission.

In principle, all data flows generate electromagnetic emission

sitemp

SIEMENS

which can be intercepted and analyzed with varying degrees of effort. In expert circles, this type of information/data emission is called compromising emission.

This compromising information (data) is not only contained in the basic wave of the signal. All harmonics, mixed products and superimpositions can also be modulated with the data processed on the device. This means that undesired information can be captured through the air or conductive objects with the aid of reception systems.

Depending on the quality, the sensitivity of selective reception system available to everyone on the market today is between 10^{-10} W and 10^{-15} W - more than 10 decades lower than, for instance, the power emitted by a video output of visual display units.

It is not difficult for a specialist to pick up the contents of a monitor screen with an antenna and then display this information on a conventional television set. Depending on the building itself and the quality of the IT devices, antenna distances vary for interception of data from the compromising emissions. Tests have shown that data can be picked up at distances of up to 500 meters. Even the serial data flow can be received at a distance of 40 to 50 meters.

Tempest equipment qualified by zones

Information espionage can be prevented by so-called Tempest equipment. The Tempest devices are qualified for certain zones based on established standards and are certified and listed by the German federal office of security for information security (BSI). Called NRPL,



this list is prepared by the BSI and revised every six months.

The emission-proof or low-emission Tempest device families are divided into zones 0 to 3. By this we mean a DP area having various zones with different degrees of emission protection due to building construction, and the coordination of the Tempest devices to be installed with the various emission zones.

Natural emission protection varies with the distances to public areas such as streets, parking lots, neighboring apartments or office buildings from which spurious attacks could be launched. Regardless of attenuation, business rooms are assigned to one of the three zones. Similarly, the DP devices are also divided into three emission zones and officially certified by the BSI.

Certification standards

NATO standard SDIP 27 Class A applies to emission-proof PC systems and their I/O and is defined as zone 0. This generation of devices is approved by the BSI for processing confidential information. The BSI

zone model specifies the emission values of zones 1 to 3 for low-emission PC systems and their I/O devices.

Device use

Tempest equipment is currently still mainly used by government authorities and military installations in which emission security is required. Here the BSI offers support and advice. Of course, it would also be a good idea for private industry to install highly sensitive development and research information on espionage-proof DP systems and networks. Information picked up in this way concerning a new development, for instance, could certainly give a distinct market advantage to a competing company who would then be the first to introduce the product or register a patent.

TEMPEST products have been in existence for more than 25 years

As manufacturer of emission-protected computers, Siemens Automation & Drives (A&D) has already been competing successfully in the Tempest marketplace for more than 25

years. Siemens also has its own measuring lab certified by the BSI. As one of two testing stations in Germany, Siemens A&D enjoys the trust of unrestricted performance of certification measurements of the SDIP NATO standard and BSI zone model. Moreover, this measuring laboratory is a recognized testing station for series measurements in accordance with the SDIP NATO standard and BSI zone model.

The Tempest products of Siemens are registered under the brand name SITEMP and are developed, produced and certified by Systems Engineering in Fuerth/Bavaria, a business division of Siemens Automation & Drives (A&D). Manufacturing is subject to rigid security regulations and quality checks and is certified in accordance with ISO 9001. All produced and Tempest-capacity SITEMP devices are put through the function and system test of a 100% emission test (short measurement procedure).

Example: SITEMP PC

SITEMP PC is the combination of ...

- the power of a high-performance computer
- the security functions of a standard device
- and the special characteristics of SITEMP



Certified up to "confidential - top secret" - the HF measurement of every device and an automatic security disabling of a monitor are only two examples of the comprehensive SITEMP package of measures.

The SITEMP palette of products applies to standard products of SDIP 27 class A and BSI zone model - including upgrading and re-measurement of already existing IT systems owned by the customer.

With small quantities, SITEMP PCs are matched to customer requirements by the selection of configurable components.

For larger quantities, PC configurators based on the respective user specification are produced and approved.

Information security terms:

AMSG	Allied Military Security General Publication
BSI	German Federal Office of Information Technology Security
NRPL	NATO Recommended Product List
SDIP	SECAN Doctrine and Information Publications
SITEMP	Registered brand name for Tempest products of Siemens
TEMPEST	Temporary Emanation and Spurious Transmission (synonymous for emission security)

Want more information? We'll be glad to provide it!

Siemens AG – A&D SE EM BD
Automation and Drives
Systems Engineering
Postfach 23 55, D-90713 Fuerth
Tel.: +49 (0) 911-750 9370
Fax: +49 (0) 911-750 9090
E-mail: fritz.fueg@siemens.com
Web: www.siemens.com/sitemp