BEWARE OF THE MICROCHIP: TEMPEST STANDARDS AND COMMON CRITERIA

It should come as no surprise that the federal government is concerned about signal leakage. In fact, its interest goes back to the days of World War II when the Army was trying to exploit weaknesses of enemy combat phones and radio transmitters. Since then, the scope of the government's interest has broadened beyond the battlefield. In the last 40 years, the National Security Agency (NSA) has taken several industry measurement standards for signal protection and greatly enhanced them. These enhanced criteria are commonly referred to as the TEMPEST standards (although the NSA also calls them EMSEC standards, short for "emissions security"). TEMPEST pertains to technical security countermeasures, standards, and instrumentation that prevent or minimize the exploitation of vulnerable data communications equipment by technical surveillance (A.K.A. eavesdropping!). It involves designing circuits to minimize emanations.

Another set of testing standards is called Common Criteria (EAL4+). Both standards are important, but they test for different things.

TEMPEST

Many things put your data communications at risk. Any device with a microchip generates an electromagnetic field, often called a "compromising emanation" by security experts. With the proper surveillance equipment, these emanations can be intercepted and the signal reconstructed and analyzed. Unprotected equipment can, in fact, emit a signal into the air like a radio station—and nobody wants to risk his or her job and a whole lot more by broadcasting national security or trade secrets to the wrong people.

Some of the most vulnerable equipment includes speakerphones, printers, fax machines, scanners, external disc drives, and other high-speed, high-bandwidth peripherals. And if the snoop is using a high-quality interception devices, your equipment's signals can be acquired up to several hundred feet away.

TEMPEST testing, while classified, is regarded as a process that assesses the threat of data linking by various covert electromagnetic

eavesdropping mechanisms. TEMPEST testing and certification is often required by military organizations, and ensures that equipment is designed to minimize emanation.

The TEMPEST standards require red/black separation. In military and government IT setups, that is the most common segregation between secure and non-secure networks. “Red” circuits are normal, unsecured circuits and equipment. Separation is ensured by maintaining physical distance or installing shielding between “red” and “black” circuits and equipment.

TEMPEST is vital for areas where physical security is either not possible or limited. When equipment is on a vehicle or deployed in an active zone, use of TEMPEST-rated equipment is a must when sensitive data is involved. It can be a user’s only line of protection.

Common Criteria (EAL4+)

Common Criteria is an international standardized process for information technology security evaluation, validation, and certification. The Common Criteria scheme is supported by the National Security Agency through the National Information Assurance Program (NIAP).

Common Criteria defines a common set of tests regarding the process of design, testing, verification, and shipping of new security products. Common Criteria enables customers to assess a level of trust in how a product has been designed, tested, built, and shipped.

Source: https://bboxblog.wordpress.com/2011/04/11/beware-of-the-microchip-tempest-standards-and-common-criteria/