BLACK BOX NETWORK SERVICES

Secure Switching Technology Brief: Standards & Clarification

Read immediately:

Understand the difference between TEMPEST and Common Criteria (EAL4+).

Compromising Emanations.

What puts your data communications equipment at risk? Many things. But first and foremost, its microchip. 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 analysed. Unprotected equipment can, in fact, emit a signal into the air like a radio station and, with the right technology, can be compromised.

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

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

TEMPEST.

TEMPEST testing, while classified, is regarded as a process that assesses the threat of data linking by various covert electromagnetic eavesdropping mechanisms. Unprotected equipment can emit a signal into the air, much like a signal from a radio station; electronic snooping can intercept those signals. TEMPEST testing and certification ensure that equipment is designed to minimise emanation. The TEMPEST designation is often required by military organisations.

TEMPEST pertains to technical security countermeasures, standards, and instrumentation that prevent or minimise the exploitation of vulnerable data communications equipment by technical surveillance or eavesdropping. It involves designing circuits to minimise emanations.

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 handle plain text classified or sensitive information, including some carrying encrypted signals. "Black" 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 standardised process for information technology security evaluation, validation, and certification.

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.

The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself — it simply states at what level the system was tested.

The Black Box® ServSwitch™ Secure KVM switches featured on the other side of this flyer have been certified for Common Criteria Evaluation Assurance to Level 4+ (EAL4+) augmented by ALC-FLR.2 and ATE-DPT.2, which refer to a method of remediating flaws in a timely fashion. VGA models are both EAL4+ and TEMPEST Level 1 certified.

	Competitor "A" *				Competitor "B" *		Black Box Secure Switches		
	DVI-I	VGA VGA/CAC	UAD	DVI	VGA	DVI	SW2008A-4008A-USB-EAL	SW2006A-4006A-USB-EAL	SW2098A-4009A-USB-EAL
Number of computers	2, 4	2, 4, 8	4	4, 8	2, 4, 8	2, 4	2, 4	2, 4	2, 4
Type	Dual link	VGA	DVI-I	DVI-I	VGA	Dual link	DVI-dual link	VGA	VGA
Dual head	—	No	No	8-port only	—	—	No	No	No
Max. resolution	2560 x 1600	2048 x 1536	1920 x 1200	Up to 1920 x 1200	1920 x 1440	2560 x 1600	2560 x 1600	2048 x 1536	2048 x 1536
Audio	Yes	No	Yes	No	No	Yes	Yes	No	No
Microphone (Yes=Bad)	Yes	No	Yes	No	No	Yes	No	No	No
Connectivity (User)	USB 4 ports	USB/PS2 2 ea.	USB 2 ports	PS2	USB 2 ports	USB 2 ports	USB 2 ports	USB 2 ports	USB 3 ports
Connectivity (PC)	USB only	USB/PS2	USB only	PS2	USB only	USB only	USB	USB/PS2	USB/PS2
Card reader support	Yes	200 only	No	No	No	No	No	No	Yes
Combined keyboard/ card reader support	Yes	200 only	No	No	No	No	No	No	Yes
TEMPEST Level 1 qualified	No	No	No	No	No	No	No	Yes	Yes
EAL4+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protection profile supported	v1.0	v1.0	v1.0	v1.0	v1.2	v1.2	v1.2	v1.2	v1.2
TAA compliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security Features									
Product authentication	No	No	No	No	No	No	No	No	Yes
Tamper-evident/ holographic seals	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Advanced tamper	Yes	Yes	No	No	—	—	No	No	Yes
OTP firmware/locked	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	Yes
Actively clears memory once used	Yes	Yes	—	—	—	—	Yes	Yes	Yes
Clears data buffers	—	—	Yes	Yes	—	—	Yes	Yes	Yes
Additional devices prohibited	Yes	—	—	—	—	—	Yes	Yes	Yes
Microphone connections banned	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes
Unidirectional keyboard/mouse data flow	No	No	No	No	No	No	Yes	Yes	Yes
Keyboard / mouse data isolation	No	No	No	No	No	No	Yes	Yes	Yes
Single key switch per port	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hotkey and mouse switching	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Colour-coded port LEDs	—	—	—	—	—	—	Yes	Yes	Yes
True EDID collected from display	—	—	—	—	—	—	Yes	Yes	Yes
EDID disable feature	—	—	—	—	—	—	Yes	Yes	Yes
Port-to-port crosstalk isolation	60 db	—	60 db	60 db	—	—	60 db	>80 db	>80 db
Dual shielding techology	—	—	—	—	—	—	Yes	Yes	Yes
Separate power domains per port	—	—	—	—	—	—	Yes	Yes	Yes
Powers down at switchover	—	—	—	—	—	—	Yes	Yes	Yes
Resets peripherals at switchover	—	—	—	—	—	—	Yes	Yes	Yes
Active power line filtering	—	—	—	—	—	—	Yes	Yes	Yes
Emissions minimised cables	Yes	No	No	Yes	No	No	Yes	Yes	Yes
Rackmountable	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

* Based on most recent public data published on manufacturer's Web site