Prévenir les menaces potentielles

Menace : dysfonctionnement du microprocesseur ou du logiciel provoquant un flux de données entre les ports.

Solution : la transmission unidirectionnelle des données est assurée en « dur » par des « diodes » sur les données de sorte que la séparation des données ne dépend pas de l'intégrité des logiciels, mais uniquement du matériel.

Menace : modification malveillante du logiciel du microprocesseur permettant la fuite des données entre les ports.

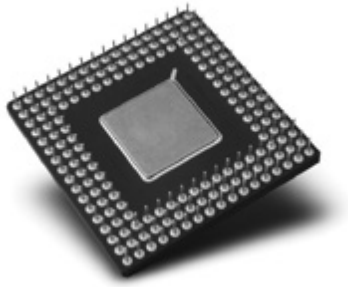
Solution : les microprocesseurs ne sont programmables qu'une fois et soudés sur le circuit imprimé. L'isolation des données ne dépend pas de l'intégrité du logiciel.

Menace : espionnage par détection des rayonnements électromagnétiques émis par l'appareil.

Solution : le boîtier métallique possède un double blindage aux endroits critiques.

Menace : détection de signaux d'un ordinateur par surveillance des signaux reçus par diaphonie (fuite) sur un autre ordinateur.

Solution : il n'existe pas de connexion vers les entrées analogiques sensibles, tels que les ports pour microphone. Un écart diaphonique minimal est assuré entre les signaux d'entrée ou d'entrée/sortie d'un ordinateur à l'autre (80 dB pour les modèles VGA et 60 dB pour les modèles DVI).



Menace : attaques par chrono-analyse (observation de l'activité sur un port pour déterminer les séquences de données sur un autre).

Solution : un seul ordinateur est connecté en même temps sur un circuit partagé. Les liens sont à sens unique, empêchant ainsi la chrono-analyse.

Menace : transmission de signaux par court-circuit ou surcharge de l'alimentation.

Solution : chaque port est alimenté de manière indépendante par son port USB. Court-circuiter l'alimentation d'un port ne coupera pas l'alimentation des autres ports

Menace : transfert des données par stockage commun ou RAM commune.

Solution : à chaque changement de canal, l'alimentation des circuits partagés, du clavier et de la souris est coupée afin de supprimer de la mémoire volatile toute trace de la connexion précédente..

Menace : forçage physique du commutateur.

Solution : le commutateur possède des scellés holographiques jouant le rôle de preuve pour protéger contre le forçage du boîtier.

À propos de Black Box

Black Box est la plus grande entreprise mondiale de services techniques spécialisée dans la conception, l'installation et la maintenance de systèmes complexes d'infrastructures informatique et téléphonique.
Black Box, c'est 175 000 clients, une implantation dans 141 pays et 195 bureaux dans le monde.
Black Box propose plus de 118 000 références produits. Pour en savoir plus, consultez le site web www.blackbox.fr.

Copyright 2011. Black Box® et le logo au double losange sont des marques déposées de BB technologies, Inc, et ServSwitch™ est l'une de ses marques commerciales. Toutes les autres marques mentionnées dans cette publication appartiennent à leurs propriétaires respectifs.

BLACK BOX NETWORK SERVICES

TEMPEST

Common Criteria

Commutateur KVM ServSwitch Secure VGA et USB, qualifié EAL4+/TEMPEST niveau 1

Combattez les menaces de fuites de données avec ces switchs KVM ultra-sûrs.

- » Empêchez les fuites de données d'un port sur l'autre.
- » Empêchez le stockage des données sensibles dans l'appareil.
- » Empêchez l'espionnage électronique.

Hautement sécurisé à chaque étape : conception,

Switch KVM avec vidéo VGA de niveau 1 (niveau A) à faible émissivité électromagnétique.

Tous les modèles de commutateurs KVM ServSwitch™ Secure USB sont qualifiés TEMPEST USA NSTISSAM niveau 1 et OTAN SDIP-27 niveau A.

Cela signifie que le faible rayonnement émis par ces switchs répond aux exigences sur les émissions électromagnétiques par rayonnement ou conduction.

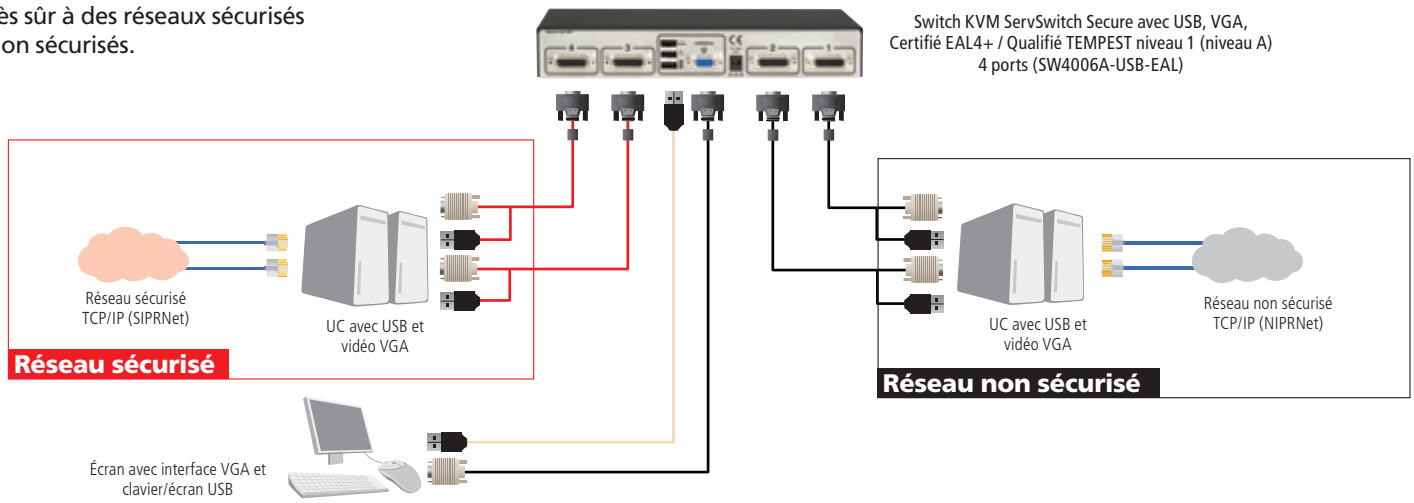
La certification TEMPEST est souvent exigée par les organismes militaires. Cette norme de sécurité fait partie des contre-mesures, des normes et de l'instrumentation qui empêchent ou réduisent l'exploitation des équipements de transmission de données vulnérables par des procédés de surveillance technique ou d'écoute.

Encore mieux, deux des modèles VGA disposent d'un lecteur de carte CAC *(Common Access card)* qui améliore ses fonctions et apporte une sécurité sans faille. Les boîtiers se désactivent automatiquement si leur intégrité physique est altérée. De plus, ces modèles avec lecteur de carte prennent également en charge les lecteurs de cartes USB (CAC) indépendants.

Caractéristiques

- Haut niveau d'isolation électrique entre les ports, facilitant la séparation « rouge/noir » des données.
- Connexions purement matérielles empêchant tout accès d'une UC à l'autre ou d'un réseau à l'autre.
- Scellés externes permettant d'identifier toute tentative de forçage.
- Isolation diaphonique entre canaux de 80 dB empêchant de capter les signaux et rendant impossible l'utilisation d'un logiciel sur un ordinateur pour accéder à un autre.
- Commutation sûre entre un maximum de quatre ordinateurs opérant à des niveaux de sécurité différents.
- Absence de mémoire ROM flashable pour éviter tout risque de reprogrammation hostile.
- Véritable prise en charge de DDC (vidéo) qui peut être inhibée pour les applications nécessitant la plus haute sécurité.
- Solide coffret métallique avec double blindage aux endroits critiques.
- Robuste isolation assurée entre les réseaux : ce commutateur est idéal dans des applications gouvernementales qui accèdent à des réseaux hautement sécurisés en plus des réseaux publics comme l'internet.
- L'isolation matérielle avec des « diodes » sur les données garantit la circulation à sens unique des données et offre une forte protection contre les fuites d'un port sur l'autre.

Accès sûr à des réseaux sécurisés et non sécurisés.



fabrication et jusqu'à la livraison chez vous !

Accédez à la fois à des réseaux sécurisés et non sécurisés depuis un poste écran, clavier et souris.

Ces commutateurs permettent de prendre le contrôle de manière complètement séparée de quatre UC ou serveurs, qu'ils soient reliés à des réseaux sécurisés ou non sécurisés, à partir d'un seul poste écran, clavier, souris. Outre les fonctionnalités de sécurité présentées en **page précédente**, ces commutateurs se distinguent par les caractéristiques suivantes.

Flux unidirectionnel des données clavier et souris

Il est ainsi impossible à un ordinateur de transmettre des données sur les circuits des signaux clavier et souris. La conception avancée du procédé d'isolation physique des données évite que les interfaces clavier/souris ne deviennent des canaux clandestins de transmission entre ordinateurs en cas de failles ou de bugs imprévus du logiciel.

Énumération clavier/souris seulement depuis leurs ports respectifs

Le clavier et la souris ne peuvent être énumérés qu'à partir de leurs ports dédiés. Tout autre périphérique USB se verra incapable de fonctionner ce qui interdit tout téléchargement ou chargement de données à partir d'une clef de mémoire USB, par exemple.

Contrôleur d'hôtes USB effaçant la RAM à chaque commutation

À chaque changement de canal, le contrôleur d'hôtes USB qui gère les périphériques partagés efface toute sa RAM. Cela empêche la présence de toute donnée résiduelle dans le canal et son transfert sur un autre ordinateur.

Protections supplémentaires contre les données résiduelles

À chaque changement de canal, les périphériques USB partagés sont mis hors tension puis redémarrés et énumérés à nouveau. Ceci limite aussi la possibilité de transférer des données résiduelles. De plus, à chaque changement de canal, l'alimentation du contrôleur d'hôtes USB est coupée puis rétablie, garantie supplémentaire de non transfert de données résiduelles.

Bus DDC dédié et émulation EDID en mémoire sur chaque port

Ceci empêche que le canal utilisé par l'écran partagé ne serve pour des attaques clandestines. Les données EDID sont récupérées de l'écran une seule fois, à l'allumage du commutateur, et transférées une seule fois, dans un seul sens, à chacun des ports. Comme chaque port dispose de sa propre copie EDID, il est impossible à un ordinateur de transférer des informations à un autre via le bus DDC et l'échange d'informations l'EDID.

Sélection claire et sans malentendu des canaux

La présence d'un unique bouton par canal évite toute possibilité de confusion dans le choix des ordinateurs. Un témoin visuel coloré confirme la sélection du canal.

Aucune alimentation commune

Les ports sont alimentés via les ports USB des ordinateurs, alors que le clavier, la souris et l'écran partagés sont alimentés par l'alimentation du commutateur. L'absence d'alimentation commune réduit au minimum les risques d'émission électroniques.

Absence de connexion pour microphone

Les circuits électroniques pour microphone à l'intérieur d'un ordinateur permettent d'enregistrer de faibles signaux analogiques. Même un très faible niveau de diaphonie pourrait être « enregistré » et permettre à un ordinateur de lire les données transmises vers un autre ordinateur.

EAL4+ : des critères de sécurité de la conception à la distribution.

Tous les commutateurs KVM de la gamme ServrvSwitch Secure USB présentés dans ce document ont été certifiés comme répondant aux Critères Communs d'évaluation jusqu'au niveau 4+ (EAL4+), en plus de ALC_FLR.2 et ATE_DPT.2.

Qui représentent ces Critères Communs ? C'est le procédé normalisé au niveau international d'évaluation, de validation et de certification dans le domaine de la sécurité informatique. Aux USA, ce programme est placé sous l'égide de la NSA *(National Security Agency)* à travers le programme national pour la sécurité de l'information (NIAP).

EAL4+ définit un ensemble de tests pour évaluer la sécurité d'un matériel informatique compte tenu de sa chaîne d'approvisionnement, depuis sa conception jusqu'à sa fabrication et sa distribution. En conséquence, les clients peuvent avoir un bon niveau de confiance sur la façon dont le matériel a été conçu, testé, fabriqué et livré.

Aucune commutation possible à distance

L'utilisation de raccourcis clavier/souris pour commuter est exclue, ce qui empêche tout contrôle de la commutation à distance.

Disponibilité du certificat d'authentification

Vous pouvez demander un certificat d'authentification qui vous sera adressé séparément du switch. Les utilisateurs pourront vérifier le statut du firmware et s'assurer qu'il n'a pas été compromis.

De plus, les modèles avec lecteur de cartes incluent une vérification active de l'authentification qui permet à l'utilisateur de contrôler le statut des circuits internes de détection de falsification du switch. Une détection permanente empêche le fonctionnement normale du commutateur. Si une falsification est détectée, toute tentative ultérieure d'authentification échouera.

Désignation	Code
KVM ServSwitch Secure USB + VGA, certifié EAL4+/qualifié TEMPEST niveau 1 (niveau A)	
2 ports	SW2006A-USB-EAL
4 ports	SW4006A-USB-EAL
2 ports avec lecteur de carte	SW2009A-USB-EAL
4 ports avec lecteur de carte	SW4009A-USB-EAL
Cordons pour commutateur KVM ServSwitch VGA	
VGA et PS/2® vers HD26, 1,8 m	EHNSECURE1-0006
VGA et USB vers HD26, 1,8 m	EHNSECURE2-0006
VGA, USB et CAC USB vers HD26, 1,8 m	EHNSECURE3-0006
Écran VGA, 1,8 m	EHNSECURE4-0006
REMARQUE : les cordons VGA existent aussi en longueur de 3,7 m.	
Ou bien choisissez les modèles avec vidéo DVI, certifiés EAL4+…	
KVM ServSwitch Secure USB + DVI, certifié EAL4+	
2 ports	SW2008A-USB-EAL
4 ports	SW4008A-USB-EAL
Cordons pour KVM ServSwitch Secure DVI	
DVI + USB vers DVI + USB,	
1,8 m	EHN900024U-0006
3,0 m	EHN900024U-0010