

Translation Shoppe

E-Mail: info@translationshoppe.com ∞ Skype: Translation_Shoppe

<http://www.translationshoppe.com>

Sample Text

Rogue wireless hardware is easy to introduce. Wireless access points are relatively inexpensive and easily deployed. A well-intentioned team of consultants working in a conference room might install a wireless access point in order to share a single wire port in the room. A malicious hacker can sit in a cafeteria with a wireless-enabled laptop scanning for unencrypted or WEP-encrypted traffic. In both cases, unacceptable risks are introduced. Regardless of whether there is malicious intent, the introduction of rogue hardware can compromise the confidentiality and integrity of network traffic. Rogue wireless devices can be detected by physically examining installations (known as “war driving”), using radio frequency (RF) scanners to determine the location of wireless devices, or by using systems designed to analyze network traffic for unauthorized devices.

Japanese

不正な無線ハードウェアの持ち込みは簡単です。無線アクセスポイントは、比較的安価であり、設置も簡単です。例えば、善意のコンサルタントチームが、会議室にある唯一の有線ポートを共有するために、無線アクセスポイントを設置したと仮定します。この時、悪意に満ちたハッカーが、カフェテリアの中で、ワイヤレス機能を持ったノートパソコンを使い、暗号化されていない、あるいはWEPで暗号化されたトラフィックを調べているかもしれません。善意とか悪意といった意図とは関係なく、不正なハードウェアは、ネットワークトラフィックの機密性と完全性対して有害です。こうした不正機器は、無線周波数スキャナを使って無線装置の場所を特定する物理的なインストール検査（別名「ウォードライビング」）によって検知できます。あるいは、不正機器向けのネットワークトラフィック分析用に開発された様々なシステムを使っても検知できます。

Rates for our services are determined by the languages involved for each translation, the length, and complexity of material as well as the timeframe of the project. Please contact the Translation Shoppe via e-mail at: info@translationshoppe.com, Skype at Translation_Shoppe or by telephone at 561.352.0065 in the US or 020-8123-6328 in the UK to discuss the details of your project and obtain an estimate.

<http://www.translationshoppe.com>