

Translation Shoppe

243 Spoonbill Lane South ∞ Jupiter, FL 33458 USA ∞ 561-352-0065

KnowledgeDock Business Centre ∞ 4-6 University Way ∞ London E16 2RD UK ∞ 020-8123-6328

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.

Traditional Chinese

非授權硬體的設置非常容易。無線存取點的架設既便宜又簡單。一群善意的顧問就會為了分享會議室中唯一的線埠而架設一個無線點。更不用說一個駭客就可以在咖啡店裡利用無線手提電腦偷看未加密或只以 WEP 加密的通訊。不管是哪一種情況，或是否有惡意的有心人士，非授權硬體危及了通訊的機密性與完整性，呈現了不被樂見的風險。非授權硬體可以藉由實際檢查設施，即所謂的駕駛攻擊(war driving)，以無線射頻探測器來找尋其位置，或利用系統來分析網路通訊中是否存在不被授權的裝置。

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>