HANDLING INSTRUCTIONS

GENERAL

Unless otherwise indicated, CSIS agrees that this report may be distributed through appropriate intelligence channels to government personnel possessing the appropriate security clearance and having a need to know the information contained therein.

SECURITY INSTRUCTIONS

Classified material must be handled, shared, and communicated in accordance with Government Security Policy requirements.

USE OF SINGLE SOURCE INTELLIGENCE REPORTS AND BRIEFS: Unless otherwise indicated, single source intelligence reports may be used in compiling intelligence summaries or reviews provided:

(a) the material is incorporated in paraphrased and preferably disguised with collateral information and attributed, i.e., "According to a CSIS report;"

(b) the summaries or reviews receive at least the same security classification and are subject to the same handling and security instructions as the original single source reports.

L I M E S O N R E P O R T S: This indicates that the information has been received from a foreign intelligence or security service through established liaison channels. No independent verification of the accuracy, adequacy of the information or the reliability or evaluation of the validity of the information is normally available beyond that provided by the originating service. Where indicated, the gist of such reports may be incorporated into intelligence summaries or reviews, but verbatim photographs, reports, or translations and the paraphrases that must not be released, even by implication, which contain details identified to CSIS on the understanding that they are not passed on to nationals of any third country. Canadian officials are also to be advised of the contents of Limex reports to any but other Canadian officials as set out in the Handling Instructes above.

EXTRACTING AND COPYING: Where it has been agreed that a replacement copy or copy of single source material be retained on file, such material must be accorded the same handling and security classification as the original single source report from which they are drawn and should be attributed to CSIS.

PHOTOGRAPHS, PLANS, AND SKETCHES: Photographs, plans and sketches attached to single source reports may not be copied or otherwise reproduced without the consent of CSIS.

SOURCE DESCRIPTIONS: Source descriptions are classified in such a way as to assist clients to appreciate and utilize the information in single source reports. Clients will, of course, recognize the need to protect the identity of sources.

Any queries regarding the material or these instructions should be addressed to CSIS.
Introduction

1. Many entities within the retail, healthcare, financial services, education and the public sector have adopted the use of wireless computer networks because of their easy of installation, low cost and of the mobility they offer. A number of these networks are not configured in a secure manner, and many hackers know how to exploit this vulnerability. As a result, wireless hackers (commonly called "wariders") can break into these computer networks in homes, businesses and government offices using a laptop or portable PC, an antenna, a wireless access card and wireless-scanning software. The use of these tools to locate and exploit such networks is called "war-riding" or "war-walking" depending on the form of transportation used. Hackers worldwide, including some in Canada, are participating in the First International War-Driving Day, scheduled for 31 August 2002. (U)

The First Alberta International War-Driving Day

2. A number of computer enthusiasts and media relating Internet Web sites provide the details of war-driving sessions that have occurred in the US, the UK, Europe, Australia, and within Canada in BC, Ontario, Nova Scotia, Saskatchewan and Alberta.

3. A computer enthusiast from Edmonton posted a press release on 21 August 2002, stating that he was arranging a war-driving session in Southern Alberta, on 31 August 2002 as a component of the internationally scheduled event. He said he would scan networks in Calgary, Edmonton and other communities in Alberta had been selected because of the absence of a significant scan of Red Deer. (U)

4. Wireless technology makes it easier for system hackers to search for data and invade the privacy of network users, since computer networks have no physical barriers.

*The term "war-riding" is derived from the term "war-dialing," which is the process of using a computer, modem, telephone and a computer program to dial phone numbers that can successfully make a connection with a computer modem. The program automatically dials a random range of phone numbers and logs and saves all the numbers that successfully connect to the modems. Some programs can also identify the particular operating system running in the computer and may also conduct automated password guessing. In both cases, the computer program uses a predetermined list of common user names and passwords in an attempt to gain access to the system. As a result, the terms "war-driving" and "war-walking" describe the mobile process of scanning for wireless computer networks using laptops or portable PCs and wireless access cards and antennas. (U)
Vulnerabilities of Wireless Computer Networks

5. Given the right tools, it is easy to detect the existence of a wireless network and determine if the network is open, closed or protected. While most wireless networks and LANs can encrypt network traffic using the security protocol Wired Equivalent Privacy (WEP), a capability of the wireless network software, many administrators do not enable this capability.

There are numerous reports in the media of hackers breaking into wireless LANs with off-the-shelf software tools such as AirSnort or WEPcrack. Any wireless computer network that provides a potential route to valuable resources requires more security than that offered by WEP. (C)

9. Wireless computer network vulnerabilities can be reduced