International)(Wardriving Day 2002

PRESS ALERT!

WIRELESS HACKERS INVADE RED DEER !

NEWS RELEASE **PAGE 1 of 3**

FOR IMMEDIATE RELEASE
August 21, 2002

For more information contact:
"Render", Jason Kaczor

Edmonton Contact	"Render"
	(780) 619-0924 render@renderlab.net

Calgary Contact	Jason Kaczor
	(403) 870-6373 jkaczor@acoupleanerds.com

Hackers and geeks worldwide will be inaugurating the first international wardriving day, Saturday August 31st, 2002.

"Wardriving" is a cousin of "war dialing," a term popularized in the 1983 movie "War Games.". War dialing used software to dial many phone numbers automatically, looking for tones which indicated a modem. Wardriving, also known as "net stumbling," is a new variant, focused on discovering wireless computer networks.

This is a "high-tech" hobby, where participants armed with laptops, wireless networking gear, global positioning units and vehicles compete to find as many "wireless" networks in their regions as possible. There are literally tens of thousands of wireless networks operating throughout the world.

Hundreds have already been mapped in Calgary and Edmonton, let alone other communities throughout Alberta.

While there are no prizes, no rules and definitely no glamour, this activity is constructive in that it raises awareness with regards to: privacy, security (or alternatively a complete lack of security), and the growing number of wireless networks sending information over, around and through an area.

On Saturday, August 31st, participants will depart from Edmonton and Calgary converging on Red Deer, Alberta. At which point, we will plan a wardriving route, which we will then use to map Red Deer upon departure.

Meeting time & location:
10 AM
White Spot
6701 - 50th Avenue, Red Deer, AB

We would be pleased to include media representatives for participation as passengers, or competitors. We can provide transportation or setup instructions as appropriate. Space is obviously limited, so contact us ASAP.

MORE...

International)(Wardriving Day 2002

PRESS ALERT!

WIRELESS HACKERS INVADE RED DEER !

NEWS RELEASE

FOR IMMEDIATE RELEASE
August 21, 2002

For more information contact:
"Render", Jason Kaczor

More information:

- Alberta International Wardriving Day 2002 Website

  http://www.renderlab.net/projects/wardrive/group.html

- Alberta samples of wardriving, maps/networks

  http://www.renderlab.net/projects/wardrive/

- Wardriving background, overview & explanation

  http://www.bitshift.org/wardriving.shtml

  http://www.netstumbler.com/index.php

  http://www.wardriving.com/

  http://home.attbi.com/~digitalmatrix/wardriving/

  http://www.warchalking.org/

- Tools, Software & How-to guides

  http://www.netstumbler.com/

- News/media articles & reports related to war-driving

  http://www.dis.org/projects.html
  http://80211b.weblogger.com/

MORE...

INTERNATIONAL)(WARDRIVING DAY 2002

PRESS ALERT!

WIRELESS HACKERS INVADE RED DEER !

NEWS RELEASE

FOR IMMEDIATE RELEASE
August 21, 2002

For more information contact:
"Render", Jason Kaczor

Terminology:

- "Hacker"

1. A person who enjoys exploring the details of technological systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
3. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
4. *[deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term is "cracker".*

- "Wireless" (also known as: WiFi, 802.11, 802.11b)

High-frequency wireless local area network (WLAN). This technology is rapidly gaining acceptance in many companies and homes as an alternative to a wired LAN. Designed to be extremely compatible with existing Ethernet/networking standards, in addition to allowing users to roam in and out of various coverage areas.

These wireless networks send and receive information, notify potential users of their availability, and allow users to access their resources, either internal information and networks, or potentially allowing access to the global internet.

Unless adequately protected, a wireless LAN can be susceptible to access from the outside by unauthorized users, some of whom have used the access as a free Internet connection! Companies using wireless LAN technologies are urged to add security safeguards such as the Wired Equivalent Privacy (WEP) encryption standard, the setup and use of a virtual private network (VPN) or IPsec, and a firewall or DMZ.

In practice, over 70% of the networks found via wardriving activities use NO security safeguards whatsoever.

- "Warchalking"

Closely related to wardriving, this activity takes place in primarily urban metropolitan centers, where there are a significant number of wireless access points, and a large amount of pedestrian traffic.

Participants use chalk to mark "open" or freely accessible wireless networks, thereby allowing others "in-the-know" to access them at a later time. Coined by founder Matt Jones this activity is a direct descendant of "hobo-languages" from Depression-era America. How "depressed" a participant has to be to actually use these networks is another story, taking into consideration equipment costs... Hobos' used symbols to let each other know where a free meal, or a safe environment could be found.

###