

## Drive-by hacking

Wireless networks are the future for computer users, freeing them from their offices - but with the new technology comes a new breed of hackers - is your company system safe from a drive-by invasion? Jon McGhie has this special report.

=====

### **CHANNEL 4 NEWS**

SPECIAL REPORTS

Drive-by hacking

**Broadcast: November 20, 2001**

### **Reporter: Jon McGhie**

It's called drive by hacking. Invisible wireless networks use the latest in computer wizardry - radio fields which allow people to stay logged into their network throughout an office.

But for hackers, it's like an open invitation. Channel 4 News has discovered that from outside the networked building any hacker with a few pieces of easily available equipment can break straight into the most confidential information.

Most companies are not taking even the most basic security precautions, leaving highly sensitive data unprotected. John McGhie reports:

A man riding his bicycle around the City of London has the capacity to break into hundreds of different computer networks. Law firms, banks, accountants and a host of big high street names are all vulnerable. If he wanted to, he could easily pluck their secrets out of thin air. They call it drive-by hacking.

Vortex:

"We generally ride in fairly dense urban areas we will focus on areas that seem to have a focus or interest in high technology. We map the locations of where computer networks are and where they are emanating radio signals. Later on we collect the data onto audio streams and we share it and publish it."

The biker won't be identified but calls himself Vortex. Together with his group "War Peddlaz" he cycles round picking up radio waves from wireless computer systems. Each time he enters one of their fields his lap top registers the network's identity and location. Back at base, Vortex maps the networks as part of his campaign for public access to the airwaves. Vortex never breaks into any of the systems. But for the less scrupulous, Wireless Computing is an open invitation to hack.

Vortex:

"I think it is very easy to overlook the fact that radio leaks out wires you can control, wires you lay you lock in a building, they're hidden away, but radio signals transmit outwards beyond your control..."

Essentially wireless systems get rid of phone lines and connect to each other and the Internet by radio signals sent out by a small transmitter. Free from wires, people can now roam around offices within range of the radio waves with their laptops still connected to the Internet.

One estimate predicts that by 2005 there will be 137 million wireless users world-wide.

But, as we've learned, with this new technology has come a huge problem.

Richard Hollis, Orthus:

"You come in completely behind the firewall and behind any defences whatsoever. You come in and you're identified as an authorised user and given user privileges - so what more do you want? That is the objective of the hacker to get in and not be confronted by any security measures. This is the perfect crime."

Computer security company Orthus wanted to find out how seriously firms were protecting data within their wireless networks. The concern is that highly confidential legal, financial and even sensitive

government data might be leaching out into the airwaves. So they conducted their own survey in the City of London to discover which systems had any security at all.

Channel 4 News:

“When you were driving around what sort of addresses were you seeing?”

Richard Hollis, Orthus:

“Prominent businesses, prominent financial Institutions, high street retailers - just about everyone who uses the web for convenience. We used a lap top and a wireless card and some special software. We got in a taxi and drove through London and, as we came within the range of the frequency, the wireless card would light up...”

The results of Orthus’s survey were dramatic. In just a few hours driving round the City, they found 124 wireless computer systems giving access to 207 different information networks. Most worrying was the fact that more than two thirds were not protecting their systems with the basic security tool of encryption.

Tim Pickard RSA Security:

“There is a problem with wireless technology at the moment and that is to do with encryption and the privacy of the information that’s being passed across the wireless network. We are passing messages in plain text and that message goes out into the ether and can be picked up very very cheaply and easily. So people can listen to your conversations and they can interrupt them they can send their own messages. They can hijack your network and send messages as you. It’s very, very important for people to understand the security implications of wireless networks.”

Using encryption clearly makes sense because it scrambles data to make it impenetrable to hackers. But we’ve learned that even the minority who bother to use it all are at risk. Hackers we’ve talked to claim that standard wireless encryption can be broken in under ten minutes.

All the evidence has shown how easily these systems could be penetrated. But we wanted to see if we could go the next step and actually break into a network.

To stay the right side of data laws, we asked if we could hack into someone’s wireless system with their permission.

We positioned a colleague in a café with a wireless connection and asked him to send an email to his office via the airwaves. My task was to get inside his transmission zone and intercept it.

My only tools were a laptop and some standard kit costing less than a hundred pounds.

Jon McGhie in van:

“Now, lets see if we can get the information they say we can. If I just push this button here and wait...and yes, there’s an email. It says “Dear Colleague, I am sending this email as a test to see if John McGhie can read my email...” Well, I can and if I can do it that easily then anyone can.”

Elizabeth France, Information Commissioner:

“Information is so valuable to companies it always surprises me how little attention they pay to security. Now, from my point of view, I’m concerned with the risk to privacy but they should also be concerned about their commercial risk, the two together make it a very real issue.”

The industry is now racing to fix the gaping gaps in wireless security. But until they develop better encryption it seems vast amounts of our personal data is being pumped into the air, just waiting for the wrong person to pick it up.