

5-1-2007

A Study of the Geographic Spread and Security of Wireless Access Points

Stuart Cunningham

Glyndwr University, s.cunningham@glyndwr.ac.uk

Vic Grout

Glyndwr University, v.grout@glyndwr.ac.uk

Follow this and additional works at: <http://epubs.glyndwr.ac.uk/cair>

 Part of the [Computer and Systems Architecture Commons](#), [Digital Communications and Networking Commons](#), [Hardware Systems Commons](#), and the [Systems and Communications Commons](#)

Recommended Citation

Cunningham, S. and Grout, V. (2007) 'A Study of the Geographic Spread and Security of Wireless Access Points.' [Paper presented to the Seventh Trans-European Research and Education Networking Association (TERENA) Networking Conference (TNC 2007) held at the Technical University of Denmark 21st-24th May 2007]. Copenhagen, Denmark.

This Conference Paper is brought to you for free and open access by the Computer Science at Glyndŵr University Research Online. It has been accepted for inclusion in Computing by an authorized administrator of Glyndŵr University Research Online. For more information, please contact d.jepson@glyndwr.ac.uk.

A Study of the Geographic Spread and Security of Wireless Access Points

Abstract

The facility of having wireless access to networks and the Internet has grown significantly in recent years. The advent of Wi-Fi and Wireless Access Points (WAP s) allows huge degrees of flexibility and easy access to information and resources. To this effect, it is now common to find multiple access points in public areas, in the home, and in the working environment. The security of WAPs is now an issue of paramount importance. However, as the technology has spread throughout such a diverse market of users, the security aspects have not been so quickly adopted. This has lead to numbers of unsecured private and corporate access points being left open to abuse and given scope for 'war driving'. In this work we investigate and establish the uptake of wireless networking facilities in a common urban area, investigate the correlations with the known societal and economic backgrounds of these areas, and establish exactly to what extent security vulnerabilities are indicated within these varied constituent environments.

Keywords

Security, wireless networks, WAP distribution.

Disciplines

Computer and Systems Architecture | Digital Communications and Networking | Hardware Systems | Systems and Communications

Comments

This paper was presented to the Seventh Trans-European Research and Education Networking Association (TERENA) Networking Conference (TNC 2007) held at the Technical University of Denmark in Copenhagen, Denmark on 21st-24th May 2007. Copyright © 2007 Authors. It appears here by permission of the author and conference organisers. Details of the conference are located at <http://tnc2007.terena.org/>

A STUDY OF THE GEOGRAPHIC SPREAD AND SECURITY OF WIRELESS ACCESS POINTS

Stuart Cunningham & Vic Grout

Centre for Applied Internet Research (CAIR), University of Wales, NEWI
Plas Coch Campus, Mold Road, Wrexham, LL11 2AW, North Wales, UK
s.cunningham@newi.ac.uk | v.grout@newi.ac.uk

Keywords

Security, wireless networks, WAP distribution.

Abstract

The facility of having wireless access to networks and the Internet has grown significantly in recent years. The advent of Wi-Fi and Wireless Access Points (WAPs) allows huge degrees of flexibility and easy access to information and resources. To this effect, it is now common to find multiple access points in public areas, in the home, and in the working environment. The security of WAPs is now an issue of paramount importance. However, as the technology has spread throughout such a diverse market of users, the security aspects have not been so quickly adopted. This has led to numbers of unsecured private and corporate access points being left open to abuse and given scope for 'war driving'. In this work we investigate and establish the uptake of wireless networking facilities in a common urban area, investigate the correlations with the known societal and economic backgrounds of these areas, and establish exactly to what extent security vulnerabilities are indicated within these varied constituent environments.

As part of this work, we conducted a live survey of WAPs in a limited geographic location (approximately 16 km²) which constituted a built-up town, industrial, and residential areas. In the first instance we examine the density and distribution of access points and map this against different area classifications to show proliferation and uptake of these resources and how they correspond to the areas within which they are situated. We also consider the socio-economic significance relating to the concentration of access points in particular exemplar areas. Further to this, we determine which of the active WAPs are secure and non-secure and this additional parameter further informs the analysis and study of the received data and the connections with geographic placement.

The results from our study show that there is significant uptake of wireless networking facilities in both the residential and business areas surveyed. Unsurprisingly, there is much more structure and consideration given to both the placement and security aspects of employing access points in the industrial and business locations. The number of access points present in some residential areas is large, and given the relatively small distances between access points there is undoubtedly traffic which is crossing private boundaries. We show that a large proportion of access points, particularly in residential and suburban areas, have little or no security, and are at high risk of being exploited. There is variation across perceived economical backgrounds as to the density of WAPs and also the employment of

basic security measures to protect access points and networks from intrusion, and we propose a further area of study would be to examine why there is heightened awareness of security issues in these particular residential locations; we present some initial thoughts on this subject. As an additional advice, we briefly outline simple security measures which are easily employed to attempt to address this critical issue.

Vitae

Stuart Cunningham

Stuart Cunningham was awarded his BSc degree in Computer Networks in 2001, and in 2003 was awarded the MSc Multimedia Communications degree with Distinction, both from the University of Paisley (UK). He is a Member of the British Computer Society and the Institute of Engineering & Technology. Stuart is also a member of the MPEG Music Notation Standards working group.

Stuart is a PhD student at the University of Wales, studying under the supervision of Dr. Vic Grout.

Vic Grout

Vic Grout was awarded the BSc(Hons) degree in Mathematics and Computing from the University of Exeter (UK) in 1984 and the PhD degree in Communication Engineering from Plymouth Polytechnic (UK) in 1988.

He has worked in senior positions in both academia and industry for twenty years and has published and presented over 100 research papers. He is currently a Reader in Computer Science at the University of Wales NEWI, Wrexham in the UK, where he leads the Centre for Applied Internet Research (CAIR). His research interests and those of his research students span several areas of computational mathematics, particularly the application of heuristic principles to large-scale problems in network design and management.

Dr. Grout is a Chartered Engineer, Chartered Scientist and Chartered Mathematician, a member of the IMA, IEE, ACM and IEEE and a Fellow of the British Computer Society (BCS). He chairs the biennial international conference series on Internet Technologies and Applications (ITA).

Full Paper

To follow ...