TERENA Networking Conference 2003

Title

The Nomadic Network: providing secure, scaleable and manageable roaming, remote and wireless data services

Authors & Affiliations

Josh Howlett,
Network Specialist,
Information Services,
University of Bristol,
Computer Centre,
Tyndall Avenue,
Bristol BS8 1TJ,
United Kingdom.

email: josh.howlett@bristol.ac.uk
phone: +44 (0)117 928 7850

Nick Skelton,
ResNet Co-ordinator,
Information Services,
University of Bristol,
Computer Centre,
Tyndall Avenue,
Bristol BS8 1TJ,
United Kingdom.

email: nick.skelton@bristol.ac.uk
phone: +44 (0)117

Keywords

Wireless networking; Authentication, Authorisation, and Accounting; Network security; Mobility; Remote Access

Our paper fits into the *Access* and *Security* subject areas of the conference.

Enabling mobile and remote networking

Staff and students can access the University network while 'roaming' on the campus by either attaching their laptop to one of the public network points, or by using the public wireless LAN [2]. Many staff and students also have dial-up and broadband Internet access at home. Using the Nomadic service these Internet connections can be used to access the University network, thereby allowing access to resources that are otherwise inaccessible (for example, due to the gateway firewall or access control based on IP address). Additionally, we have many users at other Academic Institutions in the UK and across the world who use the service daily to keep connected to the University's network.

Secure

There are a great number of security issues relating to the provision of network access services over both conventional and wireless Ethernet, as well as over IP networks in general. The Nomadic network has a single security model for all these styles of access, and so the security of the service is entirely independent of the underlying access

technology in use. Additionally, the security model places no reliance on security mechanisms such as MAC address controls, the Wired Equivalent Privacy (WEP) protocol and IEEE 802.1x that are all of dubious value [3]. The security model provides mechanisms for authentication, authorisation, accounting and encryption.

Furthermore, the security model of the service does not require that wireless access points or Ethernet switches have any security-related functionality. This is because this functionality (including authentication and encryption) are centralised in the systems that provide the service. Consequently, management of the wireless access points and network switches becomes much simpler.

Easily managed

The Nomadic network interfaces with our central authentication service via the RADIUS protocol. Consequently, virtually all aspects of user management (such as registration and de-registration, account suspension, etc), user authentication and authorisation, service monitoring and logging are integrated into our existing processes and infrastructure [4]. Thus, the management overheads of the service are practically nil.

We believe that this combination of features is unique, and provides service unmatched by any other offering that we have found.

The University of Bristol has made the software that provides the service, as well as the documentation, available for download to other UK FE and HE Institutions, in the hope and expectation that other Institutions can benefit from our work, and several have already taken the software with a view to piloting a Nomadic service [5] [6].

Acknowledgements

The authors wish to acknowledge the contributions made by many others in Information Systems & Computing at the University of Bristol that have assisted in the development and realisation of the Nomadic network.

References

2. http://www.resnet.bristol.ac.uk/nomadic/locations.html
3. http://www.uniras.gov.uk/l1/l2/l3/tech_reports/NISCCTechnicalNote04.htm
4. http://www.bris.ac.uk/is/services/register/auth-info/
5. http://www.bris.ac.uk/is/services/computers/nwservices/nomadic/download
6. http://www.ja.net/conferences/network_access/november02/nomadic_network.pdf