Towards Resilient Community Wireless Mesh Networks

Sara Bury and Nicholas J. P. Race

Computing Department, Lancaster University, Lancaster LA1 4WA, UK
{sara.bury,race}@comp.lancs.ac.uk

Abstract. Wireless Mesh Networks are an increasingly common technology providing connectivity in many communities, particularly where Internet access is unavailable or restricted via more conventional means. Their comparative ease of installation and relatively low cost makes this especially true for communities which might previously have lacked the technical knowledge or skill to attempt such an endeavour. In such a situation it is important that the operation of the network should be easily manageable; to this end the overall resiliency of the network is a key factor, enabling the network to resolve and remediate problems as they arise without requiring external technical understanding or input. This research aims to improve the resilience of community mesh networks by improving their security, initially examining the use of risk analysis techniques in this environment to identify potential attack vectors. This understanding will then be used to investigate intrusion detection techniques for operation specifically in a community environment.

1 Introduction

Wireless mesh networks (WMNs) are becoming increasingly common, particularly to provide network connectivity to communities where wired deployment strategies are either not possible or are prohibitively expensive. The proliferation of 'off the shelf' mesh hardware and software [1, 2] has resulted in communities creating wireless mesh networking installations themselves where previously they might not have possessed the understanding or technical skill. These factors combined with the many potential issues which might occur throughout the operation of a wireless mesh have led to a requirement for increased resiliency, enabling the network to resolve and remediate against problems as and when they arise without the need for external technical understanding or input.

Resilience in this context can be thought of as the aim to provide an acceptable level of service when challenges to network operation occur, whatever the adverse event or condition might be [3]. A resilience strategy to address potential problems has been developed as part of the EU FP6 ANA Project – D^2R^2+DR. This consists of two ongoing phases, firstly (D^2R^2) Defence against potential challenges and Detection of their presence as and when they occur, Remediation of the effects and eventual Recovery of the system back to normal operation.

Secondly, (DR) consists of Diagnosis and Refinement of the system based on the results of previous first phase iterations.

WMNs are intended to be resilient by design. Their infrastructure is created using a combination of wireless networking technology and ad-hoc routing protocols to create a self-managing network in which all nodes act as routers [5], able to route traffic either directly or via a multi-hop path. Unfortunately, whilst WMNs are considered to be functional the technology and protocols behind these mechanisms are still relatively new and research is ongoing to improve their dependability and efficiency [4]. Security is a necessary facet of resiliency in wireless mesh networking; resilient routing protocols and autonomous configuration can only go so far if these processes can be abused by attackers. Due to this security has been chosen as the main focus of this research.

2 The Research Problem

The specific scenario being investigated is that of community wireless mesh networking – situations where mesh networking technology has been introduced into a community environment, rather than through any commercial application, and where it is operated by the users themselves. An example of this is the situation at Wray, a small rural village in the North West of England. In 2003, members of the community approached academics at Lancaster University searching for a solution to their lack of broadband Internet access. The result was the deployment of a WMN throughout the village with nodes owned and hosted by individual members of the community, making available an Internet connection fed into the local school via a 5.8Ghz radio link [6]. In this situation, though the University has access to use the network for research purposes, the villagers themselves oversee and operate the network on a daily basis and users with a range of expertise and computer literacy have responsibility and control over how the network runs. The resilience of the network is incredibly important. In many cases the users rely on the network as their sole method of access to the Internet, but they lack the technical experience and knowledge of computer networking to manually fix problems if they arise.

For generic network security there are goals which applications aim to achieve: confidentiality, integrity, availability, authentication, authorisation and accountability - in a WMN there are specific challenges to these goals over and above those found in more conventional wired networks. The shared wireless medium exists such that any one with suitable wireless hardware has the ability to listen to traffic on the network, launch jamming attacks to deny network functionality, or even to send out malicious control traffic to other routing nodes [7]. Also, a lack of physical protection for the mesh nodes themselves could result in legitimate mesh infrastructure becoming compromised; this is emphasised by the nature of ubiquitous access within a community mesh, all members of the community are offered network access, but with no specific assurance that attackers won't come from within the community group, potentially hosting the infrastructure they have compromised. In a community WMN scenario, attack vectors can occur externally and internally to the network infrastructure and this results in an extremely wide scope of potential attacks to combat. Another factor alongside this is the diversity of needs, requirements and backgrounds within the community. A single community group may contain home users, small businesses, people making use of the network for educational purposes and so on, all with different understandings of what the network provides and what functionality is most important to them. Also each of these users may have particular security requirements, for stored data or important communications.

Without a clear idea of these requirements, the security needs for the network are both vague and wide in scope. This makes the development of a security strategy for use in this scenario incredibly difficult. An understanding of the uses, priorities, and necessary services would substantially aid the creation of security systems, procedures, and policies by narrowing the problem space involved.

3 Chosen Approach

In order to gain an insight into the utilisation of the network and the requirements of individual users, we need to understand from the perspective of the users themselves what they consider to be their most important assets and what they feel are most vulnerable to attack. The concept of risk analysis within computer networking is not new; there are many tried and tested frameworks for the assessment of such factors, particularly within enterprise scale networks used for businesses or academia. Examples include the OCTAVE risk based strategic assessment process [8], or STRIDE, a practice for computer security threat modelling [9]. Unfortunately due to the distinct operational nature and requirements of community mesh networks, such proven formalised methods are not directly applicable. Other work in the area of mesh network resilience has often focussed on specific perceived threats, from low level protocol improvements to hardware solutions for increased link availability; little work has been carried out which takes the opinions and concerns of the mesh users into account when identifying threats to resilience. This research intends to apply risk analysis techniques in a community wireless mesh network setting, with the aim identifying the most important risks for the users from their own perspective, what assets exist and are most appealing to an attacker, and the weighted probability of the occurrence of types of attack aimed at specific assets.

This approach has been chosen firstly because of the benefits of being able to narrow down the attack vectors present in a WMN, but secondly to investigate whether risk analysis techniques can be formalised for use in similar situations. Such a formalised process would enable community users of mesh networks to perform risk analysis themselves, looking for ways to improve their security without involving external consultants. The process of consulting members of the community about their own security concerns also fits well with the way that community WMNs operate – everyone having a hand in their continued functionality and contributing to the project as a whole.

Before involving network users in the project, certain decisions must be made regarding the suitability of particular risk analysis techniques and assumptions within this community scenario. For example, the concept of an 'asset' is likely to be different when compared with an enterprise setting – users may consider the safety of their children on the Internet of the utmost importance, whereas within a company employees would be expected to in many respects look after themselves. The community risk analysis will be carried out through small focus groups and discussion sessions with real world users, using carefully selected scenarios and lines of questioning to help explain the project. The research is in its preliminary stages and over the course of the next year sessions are planned with members of the community at Wray.

4 Conclusion

Resiliency in WMNs is a complex area and security is a critical factor. This research aims to improve the resilience of WMNs by examining improvements in the area of security. Firstly by reducing the problem space involved, then leading to the development of a security strategy with relevant and appropriate security systems for use in community WMNs. In order to reduce the problem space, a breakdown of assets and risks from the perspective of community WMN users will be produced; the process of creating which should indicate the feasibility of formalising this risk analysis procedure for users themselves to carry out as a community project. This information will be used to narrow down the number of attack vectors necessary to anticipate, prevent and detect in the target development of an IDS to demonstrate the functionality in a community WMN environment.

Acknowledgements

The authors are grateful to the resilient networking group for their work in developing the D^2R^2+DR resilience strategy, which will guide this work. More information available from: http://www.comp.lancs.ac.uk/resilinets

References

1. LocustWorld, http://www.locustworld.com/
2. Kiyon Autonomic Networks, http://www.kiyon.com/
3. Sterbenz, J. P. G., Schller, M., Jabbar, A. & Hutchison, D.: Resiliency and Security Framework, First Draft. ANA - Autonomic Network Architecture, Deliverable FP6-IST-27489/WP3/D3.2 (2007)
4. Lee, M. J., Zheng, J., Ko, Y.-B. & Shrestha, D. M.: Emerging Standards for Wireless Mesh Technology. In: IEEE Wireless Communications, vol. 13, pp 56-63 (2006).
5. Akyildiz, I. F., Wang, X. & Wang, W.: Wireless Mesh Networks: A Survey. In: Computer Networks, vol. 47, pp 445-487 (2005)

6. Ishmael, J. & Race, N. J. P.: Building a Rural Community Mesh Network. In: IST Broadband Europe Conference, Geneva, Switzerland. (2006).
7. Zhang, W., Wang, Z., Das, S. K. & Hassan, M.: Security Issues in Wireless Mesh Networks. In: Wireless Mesh Networks: Architecture and Protocols, Houssain, E. & Leung, K. (eds), pp 309-330, Springer, Heidelberg (2008).
8. Alberts, C., Dorofee, A., Stevens, J. & Woody, C.: Introduction to the OCTAVE Approach. Available from: http://www.cert.org/octave/approach_intro.pdf (2003).
9. Hernam, S., Lambert, S., Ostwald, T. & Shostack, A.: Uncover Security Design Flaws Using The STRIDE Approach. In: MSDN Magazine, http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx (2006).