Secure zero configuration in a ubiquitous computing environment

Shenglan Hu and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London

Abstract

In this paper, we discuss the need for secure zero configuration in a ubiquitous environment. Security issues in ubiquitous environment are identified, and future research directions are outlined.

1 Introduction

We are living in a world where computing capabilities are being woven into the fabric of everyday life. However, in general, we know less and less about their existence. This is part of an evolution of existing computing systems towards *Ubiquitous computing*, a method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user [3].

Zero configuration networking is required for environments where administration is impractical or impossible. In a ubiquitous computing environment, typically no skilled administrator is present and most of the users are non-experts. Moreover, the number of interconnected devices could be hundreds or even thousands. The lack of centralised administrator and server, the potential need for manual management, and the growing number of devices in a ubiquitous environment means that zero configuration is a highly desirable goal.

2 Zero configuration in ubiquitous computing

Our goal is that, in a ubiquitous environment, a device can dynamically join a network, automatically obtain an IP address and other configuration parameters, advertise its capabilities, and learn about the presence and capabilities of other devices. Moreover, we wish it to interact with other devices and discover the services available in the network without any user administration or centralised service discovery servers.

Assigning a unique address to each device in a network is a prerequisite for participation in the network, and is the first essential parameter that must be configured to enable participation by a host in a network. IPv6 Stateless Address Autoconfiguration (IPv6 SAA) [2] allows a host to connect to a network, configure an address and start communicating with other nodes without ever registering or authenticating itself. Based on IPv6 SAA, many protocols have been proposed for IP address autoconfiguration in ad hoc networks [1, 4]. Other protocols may be proposed in the future for different scenarios in a ubiquitous environment. However, the goal of all these protocols remains the same: devices must be configured automatically and be connected to the network without any centralised servers or user intervention.

After connecting to a network, a device should be able to automatically discover the services provided by other devices in the network and utilise them. The devices in the network should also be able to automatically detect when services become unavailable. To be effective in a ubiquitous environment, service discovery protocols should not require service discovery servers, user administration, or prior configuration. The ubiquitous environment is characterised by a heterogeneous mix of services and technologies, and rapid growth of the number

of devices; in particular, future applications may need to utilise services across multiple service locations simultaneously. Hence service discovery protocols must also address issues of scalability and interoperability of heterogeneous devices.

3 Security issues

If we want to employ zero configuration in a ubiquitous computing environment a number of serious security issues must be addressed. We briefly review some of the key such issues.

Wireless networking is widely used in the ubiquitous environment. Wireless links are vulnerable to both passive and active attacks, such as eavesdropping and denial-of-service attacks. Potential damage includes compromise of transmitted secret information, interfering with messages, and impersonating nodes. Limited bandwidth of wireless connections also gives a target for denial-of-service attacks.

Devices used for ubiquitous computing are varied and numerous; some are likely to have limited physical protection, and are therefore more likely to be captured, compromised, and/or hijacked. Attacks from such compromised nodes are a serious threat and are also difficult to detect.

The lack of central servers and user administration in a zero configuration setting also raises serious issues about security. Where there is no centralised management or user intervention, key generation, distribution and maintenance become very difficult. As a result, providing security services such as access control, data integrity and authentication of nodes, which require cryptographic keys, is difficult.

Ubiquitous computing environments can continuously change over time because of the movement of devices. Any security solution involving static configuration of a node is therefore inappropriate because of the dynamic topology of the network. In order to achieve high availability, a distributed architecture without reliance on central management entities is needed.

4 Future work

Ongoing research focussing on secure zero configuration solutions for ad hoc networks is currently directed at the following areas:

1. *Secure IP address autoconfiguration solutions in ad hoc networks*: IP address autoconfiguration is a fundamentally important task for zero configuration of devices in an ad hoc network. However, providing security for IP address autoconfiguration in ad hoc networks is still an unsolved problem. The main concern is how to obtain an IP address for a node in an ad hoc network in an automatic and secure way.
2. *Secure service discovery solutions*: A device should be able to recognise which of the available services in a network can be trusted. Services are also a target for denial-of-service attacks. We should provide countermeasures to these attacks, and also ensure that only authenticated devices can access certain services.

References

[1] Z. Fan. IPv6 stateless address autoconfiguration in ad hoc networks. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Proceedings of IFIP-TC6 8th International Conference, PWC 2003, Venice, Italy*, volume 2775 of *Lecture Notes in Computer Science*, pages 665–678. Springer-Verlag Berlin, September 2003.

[2] S.Thomson and T.Narten. Ipv6 Stateless Address Autoconfiguration. December 1998. IETF RFC 2642.

[3] Mark Weiser. Ubiquitous computing. *Nikkei Electronics*, pages 137–143, December 1993.

[4] K. Weniger and M. Zitterbart. IPv6 autoconfiguration in large scale mobile ad hoc networks for hierarchical mobile ad hoc networks. In *Proceedings of European Wireless 2002, Florence, Italy*, February 2002.