Chapter XIII
A Tool Supported Methodology for Developing Secure Mobile P2P Systems

James Walkerdine
Lancaster University, UK

Peter Phillips
Lancaster University, UK

Simon Lock
Lancaster University, UK

ABSTRACT

The growth of mobile devices with near PC equivalent capabilities has brought with it the possibility of mobile Peer-to-Peer (P2P) systems. However, the unique nature of mobile devices introduces new challenges that need to be considered during the development process, especially when considering critical aspects such as system security. This chapter presents the PEPERS Development Methodology (PDM), a tool-supported methodology that aims to assist designers in developing secure mobile P2P systems, and encourages them to consider specific mobile P2P design issues from an early stage. The PDM is demonstrated within the context of a real-world case study of a system developed for a security company.

INTRODUCTION

The rapid growth in availability of mobile devices with ever increasing functionality has brought with it the possibility of mobile Peer-to-Peer (P2P) systems. More recently, advances in wireless networking and mobile computing technologies, such as wireless LANs, wireless mesh networks and 3G cellular networks have further facilitated the migration of the P2P paradigm into wireless...
mobile computing. The combination of mobile and P2P technologies could be ideal for organisations that possess characteristics such as, decentralised management styles, geographically dispersed or highly mobile workforces, a wide range of computing and communications devices, etc.

However in developing real-world mobile P2P systems, designers can face a new set of development challenges - particularly when it comes to providing security and privacy. Ensuring such characteristics exist within a system is of particular importance in an environment that, by its very nature, is ad-hoc and heterogeneous.

The issue is complicated, however, by the fact that the P2P approaches used and the underlying mobile technologies will also have an impact on a system’s characteristics (Walkerdine, 2001). For example, the choice of P2P topology can significantly impact on how well a system can provide security. Decentralised P2P systems are likely to be better suited for handling denial of service attacks; the central authority provided by semi-centralised P2P systems would be better suited for handling authentication. Likewise the resource constraints (e.g. memory, battery life) of mobile devices can limit the amount of computation that can be performed or the level of communication between devices.

Such issues are important, and necessary to consider when developing a secure mobile P2P system. Having a development method to accommodate them is vital but, unfortunately, is something which is currently lacking within the domain. This chapter presents the PEPERS Development Methodology (PDM), a tool-supported methodology that provides such development assistance. The PDM encourages designers to consider the issues that are central to mobile P2P system development (for example, identifying security concerns, considering mobility and technical constraints, and making architectural design decisions) from an early stage. It supports the designer throughout the development cycle, from initial requirements elicitation through to the final implementation - ensuring that security and mobile concerns are properly addressed throughout. In particular, it assists developers in determining the most suitable P2P topologies and application reference architectures for their design, based on the system, security and mobility requirements that they have identified. The PDM comes with tool support and this is also illustrated within this chapter.

The PDM was developed as part of the EU funded PEPERS (PEPERS, 2006) project that has developed an infrastructure to support the design, development and operational deployment of secure mobile P2P applications. The outcomes of the project have been utilised and evaluated by industrial user partners within their own business domains, as well as a number of mobile software development companies. In order to help illustrate the use of the PDM and support tool, a real-life case study is provided that involves one of these industrial systems.

This chapter begins by discussing some of the key issues that need to be considered when developing a secure mobile P2P system. An overview of the PDM is then provided, along with a description of the case study and developed tool support. The PDM is then described in detail, referring to the case study to demonstrate each stage in use.

BACKGROUND

Although in general developers can draw upon existing software engineering techniques for developing secure mobile P2P systems, the distributed and unpredictable nature of P2P coupled with the technical challenges of mobile technology and security constraints, means that there are a number of specific issues that designers must consider.
Related Content

Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance
www.irma-international.org/article/tails-linux-operating-system/179897/

An Exploration of the Cybersecurity Workforce Shortage
www.irma-international.org/article/an-exploration-of-the-cybersecurity-workforce-shortage/210626/

Bandwidth Management Algorithms by Using Game Models
(2014). Game Theory Applications in Network Design (pp. 311-351).
www.irma-international.org/chapter/bandwidth-management-algorithms-by-using-game-models/109815/

Service Offerings for Fixed-Mobile Convergence Scenario: An Integrated Operator Case
www.irma-international.org/chapter/service-offerings-fixed-mobile-convergence/49815/

An Exploration of the Critical Need for Formal Training in Leadership for Cybersecurity and Technology Management Professionals
www.irma-international.org/article/an-exploration-of-the-critical-need-for-formal-training-in-leadership-for-cybersecurity-and-technology-management-professionals/210628/