Journal of Network and Computer Applications 53 (2015) 74–90

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A review paper on preserving privacy in mobile environments

S. Arunkumar [a,b,*], M. Srivatsa [c], M. Rajarajan [a]

[a] School of Mathematics Computer Science and Engineering, City University, Northampton Square, London EC1V 0HB, UK
[b] IBM, UK
[c] IBM Research, USA

ARTICLE INFO

Article history:
Received 18 August 2014
Received in revised form
10 December 2014
Accepted 13 January 2015
Available online 14 March 2015

Keywords:
Mobile
Privacy
Security

ABSTRACT

Technology is improving day-by-day and so is the usage of mobile devices. Every activity that would involve manual and paper transactions can now be completed in seconds using your fingertips. On one hand, life has become fairly convenient with the help of mobile devices, whereas on the other hand security of the data and the transactions occurring in the process have been under continuous threat. This paper, re-evaluates the different policies and procedures used for preserving the privacy of sensitive data and device location. Policy languages have been very vital in the mobile environments as they can be extended/used significantly for sending/receiving any data. In the mobile environment users always go to service providers to access various services. Hence, communications between the service providers and mobile handsets needs to be secured. Also, the data access control needs to be in place. A section of this paper will review the communication paths and channels and their related access criteria. This paper is a contribution to the mobile domain, showing the possible attacks related to privacy and the various mechanisms used to preserve the end-user privacy. In addition, it also gives a comparison of the different privacy preserving methods in mobile environments to provide guidance to the readers. Finally, the paper summarizes future research challenges in the area of privacy preservation. This paper examines the 'where' problem and in particular, examines tradeoffs between enforcing location security at a device vs. enforcing location security at an edge location server. This paper also sketches an implementation of location security solution at both the device and the edge location server and presents detailed experiments using real mobility and user profile data sets collected from multiple data sources (taxicabs, Smartphones).

Contents

* Correspondence to: 7 Copse View Close, Basingstoker RG248EZ, United Kingdom. Tel.: +44 7738313817.
E-mail addresses: saritha.arun@uk.ibm.com (S. Arunkumar), msrivats@us.ibm.com (M. Srivatsa), R.Muttukrishnan@city.ac.uk (M. Rajarajan).

http://dx.doi.org/10.1016/j.jnca.2015.01.008
1084-8045/

1. Introduction

Mobile devices have become an important tool in modern day communication. Mobile and other handheld devices such as ipads and tablet PCs have overtaken laptops and desktops and hence there has been an increasing research interest in the area of mobile computing in recent years. This includes areas such as quality of communication, usability and the overall end-to-end data security in day-to-day mobile transactions. Today's mobile devices continuously connect to different service providers for day-to-day online activities such as online purchases, online banking, social networking and endless web surfing. In addition to this, devices could be connecting to the service providers to receive or send sensitive information. At the Service Provider end, the data would be stored and Service Provider would only hand-over the data if it confirms that the person requesting it is authorized to receive the information. The exchange of data from one end of the network to the other is a major challenge due to the mishandling of the data by a malicious user. Hence the confidentiality and integrity of the data needs to be protected either by transforming the sensitive information into a non-readable format or by converting it into a cipher text.

Mobile environments are always prone to various security vulnerabilities. A number of papers have been written to highlight the various threats and problems due to the large volume of transactions occurring in the mobile environments (Jamaluddin et al., 2004; Liu et al., 2009). A very popular attack on the mobile environment is the man-in-the-middle attack. Every bit of data that comes into the mobile device and goes out of the mobile device can be assumed to be sniffed by a malicious user. The information can be assumed to be sniffed by the man-in-the-middle and manipulated in order to retrieve the sensitive information. Protecting the information that is being exchanged between the mobile devices is a major challenge and this paper will discuss some of the techniques that can be employed to mitigate the man-in-the-middle attack. The attack discussed above includes a number of attacks such as man-in-the-middle, sniffing and privacy related attacks. Another attack that is described by some of the researches is based on the cross service attack on the mobile devices (Mulliner et al., 2006). Cross service attacks can occur while you are browsing from your mobile handset sitting in a shop with wireless connectivity. The malicious user would be monitoring the new connections to the wireless network and using an exploit published previously he gains access to the phone. Mulliner et al. (2006) describes in detail the proof-of-concept to show the attack and also discusses about the way in which the vulnerability can be exploited.

With the increasing availability of mobile devices, there is a growing demand for location-based applications. In response to such a user demand, various location-based services have been emerging recently (Beresford and Stajano, 2004; ⟨http://www.mobiloco.de⟩).

A very interesting type of attack that has been popular in mobile and smartphones is the video based attack. All 3G smartphones have the bluetooth, camera and video capabilities and hence is prone to video based vulnerabilities. Xu et al.(2009) have come up with stealthy video capturing software that captures the user behavior patterns/data without the owner's knowledge. It then sends the collected information into a remote device. This attack is executed in such a way that the device owner is unaware of the devices activities. Stealthy Video Capturer (SVC) is a spyware that works very well in all 3G smartphones. All it needs is the 3G connectivity and the video recording capability. This works based on the Windows mobile 5.0/6.0 platforms and it uses the relevant API's for it's functioning. The three main components of this spyware are: Video capture, triggering algorithm and file sending. The video capture as the name suggests captures the video without the knowledge of the mobile user. The triggering algorithm identifies the precise time to turn on the video capturing process and passes on the video information. Finally the file sending flow is responsible for sending the recorded video to a remote device. The video is compressed using mobile phone's video compression techniques before it is being sent to the remote location. They also discuss the injection method used in SVC. As most users today download a lot of games from the Internet, the authors in Xu et al. (2009) found a way of injecting the Trojan using a game and to achieve this they used the tic-tac-toe game. In this case the owner of the mobile device downloads the game and is content that he has just received a new game. However, he is totally unaware of the SVC that has also been downloaded together with the game. It can also be noted that the CPU, memory and other details of the phone that needs to be looked at before the triggering algorithm captures a video. The authors also comment that the malware is resistant to all the existing antivirus tools as it is a new type of vulnerability. The key factor contributing to the success of SVC is due to the fact that there is no efficient management policy for system APIs security for Windows Mobile.

In the mobile environment, it is quite common to have a man-in-the-middle trying to sniff at the information being passed between the mobile device and the service providers (Mulliner et al., 2006). Therefore it is crucial to have data access control mechanisms in place.

It would be interesting to highlight the importance of European data protection guidelines that has recently undergone revisions to include the privacy of individual's data and personally identifiable information (PIIs). Some of the notable changes include explicit consent from the user when data is being shared with other third party service providers. More transparency about the way in which the data is handled is another important change to the European Data Privacy Directive. The reform also includes the mandate for complete accountability and responsibility of the service provider when personal data is being processed (⟨http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm⟩).

This review paper mainly covers the various methods used for preserving user privacy. Hence, it presents a detailed review of many methodologies before moving onto the open research problems in the various solutions described. It then moves onto