文章编号:1671-4598(2016)05-0230-04 DOI:10.16526/j.cnki.11—4762/tp.2016.05.065 中图分类号:TP3 文献标识码:A

基于 Android 平台的一种保护隐私的即时通讯工具的设计与实现

陈 望,陈河宏,黄 琼,张视焕,刘雁彬,张琪枫
(华南农业大学 数学与信息学院,广州 510642)

摘要:在移动互联网飞速发展的今天,即时通讯工具已经成为人们生活和工作中不可或缺的工具;但是,国内外主流的即时通讯工具依然面临着两大主要问题;一个是基于不同协议的软件的互联互通问题,另一个是日益严峻的即时通讯的安全性与隐私性问题;为了从根本上解决问题,针对即时通讯工具的特点进行了深入分析,最终设计并实现了一款基于安卓平台上更具安全性、更实用、用户体验更好的即时通讯工具 SecretChat;本工具采用开放的 XMPP 通讯协议,并在 XMPP 上实现 OTR 安全协议;经过系统测试,系统具备稳定性并且具有良好的互联互通性能和隐私保护功能。

关键词:即时通讯;互联互通;安全;XMPP OTR Android

Design and Implementation of Secret Chat on Android Platform

Chen Wang, Chen Hehong, Huang Qiong, Zhang Shihuan, Liu Yanbin, Zhang Qifeng
(College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China)

Abstrct: With the rapid development of mobile Internet, Instant Messaging (IM) has become an integral part of people's life and work. However, domestic and international popular IM software is still facing two main challenges. One is the connectivity between different IM software based on different protocols, and the other is the increasingly serious security problems about IM software. In order to solve the problems, this paper analyses the characteristics of IM software. Ultimately, we design and develop the SecretChat, based on Android, which is a more secure, more practical, better user experience IM software. SecretChat uses open XMPP protocol and implements OTR security protocol on XMPP. The experimental result shows that the system features advantages of high stability with good connectivity as well as encryption communication.

Keywords: instant messaging; connectivity; security; XMPP; OTR Android

0 引言

随着移动互联网的快速发展,即时通讯工具已经成为人们生活和工作不可或缺的工具。而随着 Android 系统的发布与开源,智能手机变得十分的普及。手机具有广泛性、随身性、即时性、便捷性等特点,这些特点恰好与即时通讯功能紧密结合。截止到 2014 年 12 月,手机即时通讯工具使用率已经超过了 PC 端,手机即时通讯网民数为 5.08 亿,手机即时通讯使用率高达 91.2%[1]。

然而,无论是国内还是国外的即时通讯工具依然面临着两大问题:一是通讯协议的差异性,导致不同即时通讯软件不能互联互通,阻碍了用户继续扩展的同时,也给用户带来了诸多不便。另一个是即时通讯的安全性,如果软件的安全性得不到保障,将对用户的利益和隐私带来巨大的威胁。针对软件的互联互通问题,2012 年,微软公司修改其即时通讯软件 MSN messenger 条例,支持 XMPP 协议[2](Extensible Messaging and Presence Protocol,可扩展信息和出席信息协议),使得 MSN 与 G-talk 等其他采用 XMPP 协议的软件直接通信成为可能[3]。2013 年网易提出实现易信与电信手机短信的互联互通,并提出与同类产品互联互通的设想。但是在国内,腾讯等主流 IM 服务商因为商业利益,依然采用封闭的即时通讯协议,拒绝与其他软件互通[4]。近年来,“棱镜门”、iCloud 云端系统被入侵等事件的爆发,即时通讯工具的安全性越来越受关注[5-6]。针对即时通讯软件的安全性问题,以飞信与 QQ 为代表,飞信传输信息过程中并没有使用特别的加密,消息监听者通过简单的网络监听就可以捕获飞信的聊天内容[7]。QQ 等聊天工具加密的是消息在服务器和客户端之间的传输链路,信息将在服务器被还原成明文,存在被监听、篡改、窃取的危险,而且针对 QQ 各个版本的软件,几乎都可以使用特定的工具在不输入密码的前提下,对 QQ 聊天记录进行查看和修改,获取用户的隐私信息,存在较大的安全隐患[8-10]。

针对即时通讯工具面临的互联互通以及安全性这两大问题,本文使用开放的 XMPP 协议实现了即时通讯工具的互联互通性,将 OTR 安全协议作为 XMPP 协议的上层协议,保证了信息传输的保密性和安全性,同时添加第三方登录、“阅后即焚”和其他功能模块,提高了用户登录和聊天操作的便捷性,实现了基于 Android 平台的 SecretChat 工具。

1 系统技术架构

1.1 总体框架

为了解决即时通讯工具的互联互通问题,本文采用 XMPP

收稿日期:2015-11-17; **修回日期**:2016-01-04。

基金项目:广东省大学生创新训练计划项目(201410564292);广东省高等教育教学改革项目(GDJG20141039);华南农业大学教育改革重点项目(JG14009)。

作者简介:陈 望(1993-),男,广东揭阳人,主要从事信息安全方向研究。

黄 琼(1982-),男,江西人,教授,硕士生导师,主要从事密码学与信息安全方向的研究。

协议作为软件的通讯协议。XMPP 协议是一种基于 XML（extensible markup language，可扩展标记语言）的用于即时消息的可扩展的协议族，是目前主流的 IM 协议之一。XMPP 协议具有开放性，可扩展性、安全性等特点，采用 XMPP 协议作为通讯协议，基于或支持 XMPP 协议的即时通讯工具均可以互联互通，有效解决了互联互通问题。同时，软件基于 Oauth2.0[11] 协议开发第三方登陆模块，同时支持腾讯、新浪、百度账号的登陆，通过用户授权可以获得相应账号的基本信息，增强了软件的互联互通功能和便捷性。

本文认为，即时聊天场景下的安全通讯，通讯实体须实现以下 4 点：1）信息保密，即除了接收方，其他人不能读该通讯实体的即时信息；2）验证身份，即该通讯实体可以确信发送方的身份；3）可抵赖性，即用户可以否认其发送信息的行为；以及 4）完美前向保密性，即使泄露了会话密钥，以前的对话内容也不会泄露。OTR[12]（Off-the-Record Messaging，无痕通信）协议是一种可以为即时通讯工具提供加密保护的安全协议。OTR 采用 AES[13] 对称加密算法进行消息加密，采用 Diffie-Hellman 协议[14] 进行密钥协商，并采用消息码验证 HMAC-SHA1 和数字签名结合的方式进行消息认证，满足安全的即时聊天场景的 4 个特性。因此，应用采用 OTR 安全协议对应用进行加密。同时，软件提供阅后即焚功能，有效保护用户的隐私。

SecretChat 工具分为服务端和客户端，采用 C/S 架构。服务器端采用基于 XMPP 协议的 Openfire 开源系统进行二次开发，服务器承担着处理终端用户的各种请求，以及发送响应消息给终端，转发终端的消息给指定终端的功能。服务器在 XMPP 体系结构中，之间是级联、可路由的，保证了不同服务器服务的客户端之间是可以相互联系。客户端是基于 Android 操作系统，综合利用 Activity、Intent 等核心组件进行开发，采用开源的 Smack 库实现基于 XMPP 协议的即时通讯功能，在此基础上，采用开源的 OTR4J 库，在 XMPP 协议上实现 OTR 协议，充分保证应用的安全性。用户可以选择是否进入 OTR 加密模式，随时随地使用 SecretChat 即时通讯工具。系统的架构如图 1 所示。

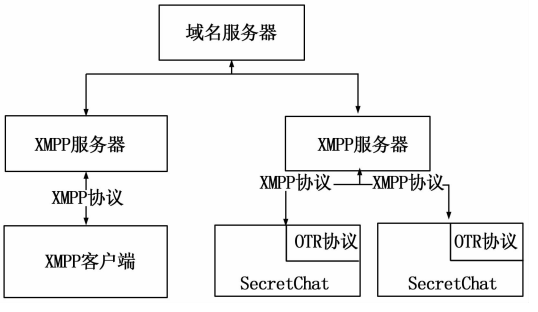

图 1　系统总体设计图

1.2　服务器端设计

系统服务端主要提供以下三点功能：1）实现 XMPP 协议，使得可以和客户端正常通信，对通信数据进行处理和转发；2）提供后台维护管理的功能；3）负责处理和存储系统的通信信息及用户资料等数据。由于 OTR 加密主要是客户端之间的协商加密，所以对于 OTR 加密方面服务端只需要对 OTR 加密的信息进行转发和处理，无需进行 OTR 加密操作。系统的服务端采用开源的 Openfire 框架进行二次开发。

系统主要在 Openfire 服务器已经实现的 XMPP 功能进行应用和根据需求在上面开发出一个第三方登录模块，使得用户可以通过 QQ、微博、百度的账号进行登陆。主要的方法步骤如下：

1）在 Openfire 数据库添加一个存储第三方登陆的数据表，在 XMPP 协议原消息格式的基础上，添加一个传输第三方登录信息的消息格式。

2）以插件开发的方式在 Openfire 上开发一个继承了 IQHandler 类的插件 OAuthPlugin，该插件实现了对第三方登录的信息进行存储和验证的工作。

3）在 Openfire 根目录下面的 build. properties 文件注册该插件，修改 Openfire 对 XMPP 消息进行路由处理的 IQRouter 类，使得接收到客户端第三方登录的信息时，将其移交到 OAuthPlugin 进行相应的处理。服务端的总体框架如图 2 所示。

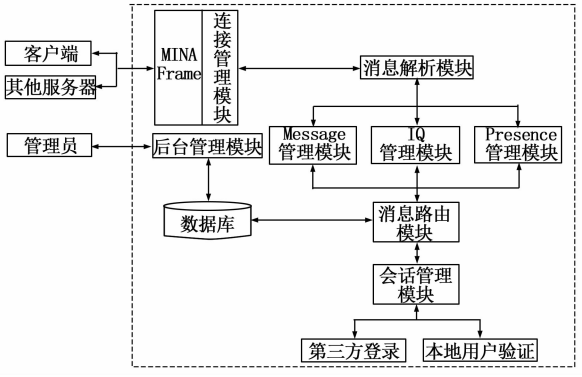

图 2　服务端总体框架图

1.3　客户端设计

客户端是用户与服务端沟通的桥梁，所以客户端既要能够与服务端准确实时地通信，又要提供良好的 UI 交互界面，将获取到服务端的信息展示给用户或者接受用户交互输入。结构上，客户端结构设计采用 MVC 模式。客户端主要包括 XMPP 协议模块、OTR 协议模块以及应用模块几个部分，其总体框架如图 3 所示。

1）XMPP 协议模块是客户端的核心模块，负责整个通讯模块的交互流。该模块主要将客户端与服务器的通信消息转换成 XMPP 协议规定的格式，使得客户端和服务器可以准确高效地进行通信，以及完成和服务器进行身份验证等协商的流程。

2）OTR 协议模块主要负责信息的加解密过程，以确保通讯数据的安全。用户可以选择是否使用 OTR 协议模块所提供的功能。在 OTR 加密模式下，客户端发送的即时通讯信息将会被 OTR 安全协议进行加密，并交给底层的 XMPP 协议，由 XMPP 协议组建相应的 XML 流与服务器进行数据交互，当客户端收到 OTR 加密信息时，会交给 OTR 协议模块进行解密，最终还原出即时通讯信息的明文。

3）应用模块包括用户管理、阅后即焚、图像识别，数据管理，是用户与客户端交流的接口。阅后即焚可以确保发送方发送的内容在接收方查阅之后永久删除；图像识别基于开源 Tesseract-ocr，实现图像信息到文本信息的转换；数据管理负

责存储用户、好友信息、图形信息和语音信息等。

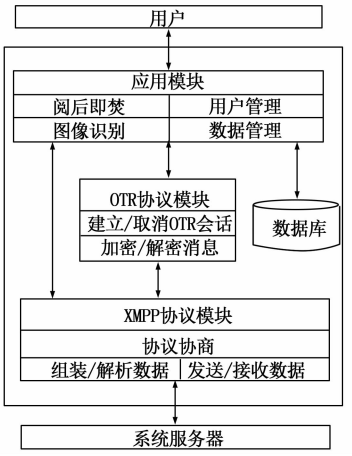

图 3 客户端总体框架图

2 关键技术与特点

2.1 XMPP 在客户端的实现

Android 端可以使用基于 Java 的开源 XMPP 协议包 ASmack 来实现 XMPP 协议。主要步骤如下：

1）利用 ASmack 库的 XMPPConnection 类与服务器建立连接：首先实例化连接的配置类 Connection-Configuration，配置类构造函数的参数为服务器地址和端口号，接着用 SASL-Authentication 类中的 supportS-ASLMachanism 静态方法设置登陆服务器时所选择的验证机制，最后实例化 XMPPConnection 类，其构造函数的参数为前面的 ConnectionConfiguration 对象，至此完成与服务器的连接。

2）利用前面连接服务器成功的 XMPPConnection 对象中的函数，就可以实现基于 XMPP 协议的与服务器的信息传递、服务器对客户端的信息进行处理和转发，从而完成基于 XMPP 协议的即时通讯。其主要操作步骤为：首先，通过 XMPPConnection 对象的 Send-packet 方法向服务器发送 XMPP 协议格式的消息包 P-acket，然后定义一个 Packet 监听器，用于监听从服务器发送过来的消息包，针对不同类型的消息包进行不同的操作。

2.2 OTR 在客户端的实现

OTR 安全协议满足即时聊天安全通讯的 4 个要求，即信息保密、验证身份、可抵赖性和完美前向保密性。因此 Serectchat 采用 OTR 作为安全协议，并在 XMPP 上进行实现。应用采用 OTR4J 库实现 OTR 加密通讯协议。该库包括了加密算法库和 OTR 环境操作库。在实现 OTR 协议过程中，使用 OtrEngine、OtrEngineHost 两个 API 初始化 OTR 库，接着使用 OtrEnginelmpl 接口中的 startSession、transformSending、transformReceiving 来进行 Diffie-Hellman 密钥交换、Reveal 签名交换、签名交换。假设通讯双方为 Alice 与 Bob，Alice 将在第 4 阶段收到 Reveal 签名，发送签名后进入安全状态，而 Bob 在接受到 Alice 发送的签名之后进入安全状态。Alice 与 Bob 的 OTR 会话初始化过程如图 4 所示。

如果会话初始化成功，可以通过 transformSending、transformReceiving 两个方法对即时通讯信息进行加密和解密操作。OTR 信息通过 OTR _ MESSAGE 进行标识。发送 OTR

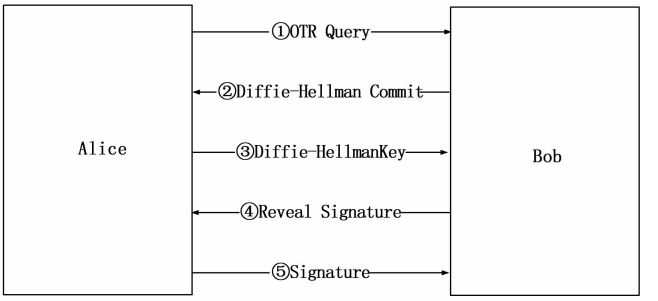

图 4 OTR 会话初始化过程

信息，明文通过 AES 加密算法进行加密，并交给底层 XMPP 协议。接受 OTR 信息后，如果消息标志是 OTR _ MESSAGE，则对信息进行解密操作，最终将密文还原。

当通讯中有一方想终止会话，可以使用 OtrEnginelmpl 接口中的 endSession 方法来结束加密会话。

SecretChat 以 XMPP 作为信息传输协议，在 XMPP 上加载 OTR 安全协议。在保证通讯双方通讯内容的完整性、真实性的同时也实现了完美前向保密性与可抵赖性。由于 OTR 的加密性质，服务器端将无法进行解密出消息“明文”进行存储，有效的防止了信息被监听、篡改、窃取的危险。

3 系统测试与分析

3.1 测试环境

硬件环境：华为荣耀 3C；

软件环境：Android 4.4.2。

3.2 测试分析

由于本文针对的是聊天工具的互联互通性和安全性设计出 SecretChat 工具，所以对系统互联互通性以及加密通讯功能做了全面的测试。

3.2.1 客户端主要界面

如图 5～图 8 所示。

图 5 登陆界面 图 6 信息提示界面

3.2.2 客户端的互联互通性能

本文分别将 SecretChat 客户端与主流的即时通讯工具进行信息交互，并模拟通讯双方轮流发信息给对方，SecretChat 工具的互联互通性见表 1。

表 1 SecretChat 互联互通性测试结果

即时通讯工具	ICQ	Psi	Pidgin	QQ	Secret-Chat	Spark
与 SecretChat 能否互联互通	否	能	能	否	能	能

根据表中数据可以看出，SecretChat 与基于或支持开源

图 7　阅后即焚功能界面

图 8　OTR 加密功能界面

XMPP 协议的即时通讯工具能够互联互通，与采用封闭的即时通讯协议的 ICQ、QQ 不能互联互通。

3.2.3　客户端的加密性能

（1）加密前后发送字节数对比：

本文分别比较未加密和经过 OTR 加密两种情况传输数据的长度，分析加密是否会造成带宽造成负担。每条不同长度的信息均发送 10000 次，得到的平均结果见表 2。

表 2　加密对带宽影响程度测试结果

未加密信息长度	100 字节	200 字节	500 字节
经过 OTR 加密信息的长度	796 字节	932 字节	1332
平均每个字符加密后的长度	7.96	4.66	2.66

根据表中数据可以看出，随着信息长度的增加，平均每个字符加密后的长度将随着减少。而且加密对带宽的影响程度几乎可以忽略不计。

（2）加密前后发送时间对比：

本文在测试过程中，模拟通讯双方轮流发信息给对方，传输每条信息所耗时间包括密钥的生成过程和信息的加解密过程。本文分别比较未加密和经过 OTR 加密两种情况传输数据的长度，分析加密是否对发送效率产生影响。每条不同长度的信息均发送 10000 次，得到的平均结果如图 9 所示。

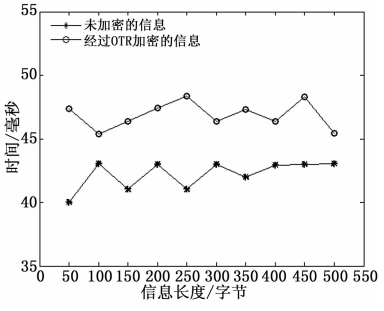

图 9　加密对发送效率影响程度测试结果

根据图 9 中数据，可以看出，未加密的数据的发送时间在 40～45 ms 之间，经过 OTR 加密的数据的发送时间在 45～49 ms 之间。相同信息长度，未加密和经过加密的发送时间相差是毫秒级别的，远小于用户输入的速度。因此，可以认为加密不会对数据传输的实时性造成显著的影响。

（3）加解密不同长度数据所需要的时间对比：

本文在测试过程中，模拟客户端加解密不同长度的数据，测试加解密不同长度信息所需要的时间，分析加解密算法的性能。每条不同长度的信息均模拟加解密 100 万次，得到的平均结果如图 10 所示。

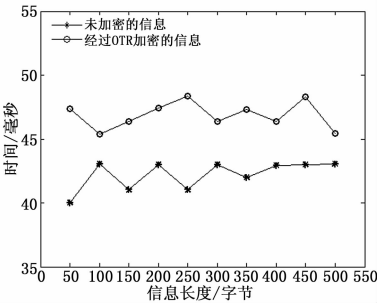

图 10　加解密不同长度数据所需要时间测试结果

根据图 10 中数据，可以看出，加解密时间随着数据的长度的增加而增加。500 字节的数据在 1 ms 内可以完成加解密。

综合（1）至（3），可以认为客户端拥有良好的加密性能。

3.3　测试结果

通过测试，系统实现了与所有基于或支持开源 XMPP 协议的即时通讯工具的互联互通，使用 OTR 协议成功加密了会话内容并具有良好的加密性能，同时实现了用户管理、第三方登录等功能并具备良好的稳定性。系统在保证用户使用的互联互通性和便捷性的同时，也充分保护了用户会话的安全性。

4　结语

本文主要分析了即时通讯工具面临的两大问题，即通讯协议的差异性带来的软件之间的互联互通问题，以及日益严重的即时通讯的安全性问题。XMPP 协议具有的开放性、可扩展性、独立性、安全性等特点解决了不同软件之间的互联互通问题，而 OTR 协议具有可抵赖性、完美前向保密性等特点能有效的解决了软件的安全性问题。本文以 XMPP 作为信息传输协议，在 XMPP 上实现 OTR 安全协议，并为软件提供了第三方登陆、“阅后即焚”等功能，设计和实现了一款更具安全性、更实用、用户体验更好的即时通讯工具 SecretChat。

参考文献：

[1] 中国互联网网络信息中心. 第 35 次中国互联网络发展状况统计报告 [R]. Technical，2015.

[2] Saint-Andre P. Extensible messaging and presence protocol (XMPP)：Core [J]. 2011.

[3] 崔　颖，李　婷. OTT 业务互联互通成趋势或激发网络互联与技术标准化需求 [J]. 世界电信，2012 (12)：59－63.

[4] 李　锐. 浅谈即时通讯工具现状及其发展趋势 [J]. 中国科技信息，2013 (16)：86.

[5] Greenwald G，Macaskill E，Poitras L. Edward Snowden：the whistleblower behind the NSA surveillance revelations [J]. The Guardian. 2013，9：2013.

（下转第 236 页）

的影响具有很好的鲁棒性。

2 实验和数据分析

本文中采用三段经典的运动车辆视频对本文算法进行实验验证。视频（a）中车辆的种类不同，大小不一，路边树木等干扰因素较少。视频（b）中车道是横向的，是从高空俯拍的视频，车辆较小且车辆行驶缓慢，识别难度较大。视频（c）中车辆的个数比较少，视频中也几乎没有什么干扰因素。视频的数据参数如表一所示，视频截图及视频数据如图 5 所示。

（a） （b） （c）

	大小/MB	宽度/像素	视频采样/位	帧速率/帧/秒
视频(a)	8.45	320 * 240	24	15
视频(b)	23.6	320 * 240	24	25
视频(c)	17.6	320 * 240	24	30

图 5 实验视频截图及视频数据

对三段视频进行车辆识别分析，本文比较混合高斯背景建模[13]、改进的帧间差分算法[14]以及本文算法几种算法的检测结果如表 2 所示。

表 2 实验视频车辆检测结果

	实际车辆个数	混合高斯背景建模	改进的帧间差分	本文算法
视频(a)	64	53%	47%	68%
视频(b)	12	47%	43%	60%
视频(c)	26	84%	82%	86%

由上述的实验结果可知，对于视频（c），3 种算法的车辆识别率差不多，但在复杂的背景环境下（视频（a）和视频(b)），本文算法具有更高的车辆识别率。

3 结束语

本文中提到的基于特征点光流聚类的运动车辆检测算法，利用对 Harris 角点做光流提取，并利用 FUNN 聚类算法对特征点光流做聚类分析，有效避免了遮挡和光照变化对车辆检测带来的影响，并且提高了在动态背景下对运动车辆的识别率，非常适用于交通监控中的车辆检测。但是由于算法没有考虑视频图像的尺度变化，使得算法在对较远车辆或在视频图像中较小的车辆目标进行检测时有可能出现漏判或误判。

参考文献：

[1] Y Fan. A real-time algorithm of dynamic background extraction in image sequence [A]. Proc. 4th IEEE Int. Conf. on Machine Learning and Cybernetics [C], Guangzhou: IEEE, 2005, 4997 - 5000.

[2] Takatoo M, Kitamura T, Okuyama Y, et al. Traffic flow measuring system using image processing [A]. Proc. SPIE 1197, Automated Inspection and High-Speed Vision Architectures III [C], Philadelphia: SPIE Digital Library, 1989, 172 - 180.

[3] Hsieh J W, Yu S H, Chen Y S, et al. Automatic traffic surveillance system for vehicle tracking and classification [J]. IEEE Transactions on Intelligent Transportation Systems, 2006, 7 (2): 175 - 187.

[4] 龚 平，刘相滨，周 鹏. 一种改进的 Harris 角点检测算法 [J]. 计算机工程与应用，2010，46 (11)：173 - 175.

[5] 徐 伟，王朔中. 基于视频图像 Harris 角点检测的车辆测速 [J]. 中国图像图形学报，2006，11 (11)：1650 - 1652.

[6] 胡金金. 基于光流法的运动目标快速跟踪算法研究 [D]. 西安：西安电子科技大学，2014.

[7] 李喜来，李艾华，白向峰. 智能交通系统运动车辆的光流法检测 [J]. 光电技术应用，2010，25 (2)：75 - 78.

[8] 胡觉晖，李一民，潘晓露. 改进的光流法用于车辆识别与跟踪 [J]. 科学技术与工程，2010，10 (23)：5814 - 5817.

[9] 陈 聪，朱 煜，肖玉玲，等. 一种有效的车辆跟踪算法与异常车辆检测 [J]. 华东理工大学学报（自然科学版），2015，41 (2)：205 - 209.

[10] 高 磊. 基于光流的动态场景中运动车辆检测与跟踪算法研究 [D]. 合肥：中国科学技术大学，2014.

[11] 裴巧娜. 基于光流法的运动目标检测与跟踪技术 [D]. 北京：北方工业大学，2009.

[12] 孙季丰，王成清. 基于特征点光流和卡尔曼滤波的运动车辆跟踪 [J]. 2005，33 (10)：19 - 23.

[13] 韩 明，刘教民，孟军英，等. 一种自适应调整 K-r 的混合高斯背景建模和目标检测算法 [J]. 电子与信息学报，2014，36 (8)：2023 - 2027.

[14] 王振亚，曾黄麟. 一种基于帧间差分和光流技术结合的运动车辆检测和跟踪新算法 [J]. 计算机应用与软件，2012，29 (5)：117 - 129.

（上接第 233 页）

[6] Greenwald G, Macaskill E. NSA Prism program taps in to user data of Apple, Google and others [J]. The Guardian. 2013, 7 (6): 1 - 43.

[7] 唐 龙，刘中临，刘嘉勇. 关于飞信即时聊天消息监控的研究 [J]. 信息安全与通信保密，2012 (2)：39 - 41.

[8] 陈肇宇，林柏钢. 即时通讯软件的安全性分析 [J]. 信息安全与通信保密. 2005 (09)：70 - 72.

[9] Schrittwieser S, Frühwirt P, Kieseberg P, et al. Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. [C]. In: 2012.

[10] 程 瑶，应凌云，焦四辈，等. 移动社交应用的用户隐私泄漏问题研究 [J]. 计算机学报，2014 (1)：87 - 100.

[11] Hardt D. The OAuth 2. 0 authorization framework [J]. 2012.

[12] Borisov N, Goldberg I, Brewer E. Off-the-record communication, or, why not to use PGP [C]. In: ACM, 2004. 77 - 84.

[13] 何明星，范平志. 新一代私钥加密标准 AES 进展与评述 [J]. 计算机应用研究，2001 (10)：4 - 6.

[14] Diffie W, Hellman M E. New directions in cryptography [J]. Information Theory, IEEE Transactions on. 1976, 22 (6): 644 - 654.