



文章编号:1001-9081(2017)02-0402-06

DOI:10.11772/j.issn.1001-9081.2017.02.0402

移动智能终端安全即时通信方法

张帆¹, 张聪¹, 赵泽茂², 徐明迪^{3*}

(1. 武汉轻工大学 数学与计算机学院, 武汉 430023; 2. 丽水学院 工程与设计学院, 浙江 丽水 323000;

3. 武汉数字工程研究所, 武汉 430205)

(* 通信作者电子邮箱 siemendy@whu.edu.cn)

摘要:针对移动智能终端即时通信安全问题,提出了一种不可信互联网条件下移动智能终端安全通信方法。该方法设计并实现了一种在服务器和通信信道均不可信情况下的可信密钥协商协议。理论分析表明,所提出的密钥协商协议可以确保通信双方所协商会话密钥的真实性、新鲜性和机密性等诸多安全特性。密钥协商完成之后,基于透明加解密技术即可以确保即时通信双方语音/视频通信信息的机密性和完整性。真实移动互联网环境下的测试也表明该方法是高效和安全的,密钥协商可以在1~2 s完成,攻击者无法获取即时通信的明文信息。

关键词:移动智能终端安全;即时通信;可信密钥协商;协议安全

中图分类号: TP309 文献标志码:A

Secure instant-messaging method for mobile intelligent terminal

ZHANG Fan¹, ZHANG Cong¹, ZHAO Zemao², XU Mingdi^{3*}

(1. School of Mathematics & Computer Science, Wuhan Polytechnic University, Wuhan Hubei 430023, China;

2. School of Engineering and Design, Lishui University, Lishui Zhejiang 323000, China;

3. Wuhan Digital and Engineering Institute, Wuhan Hubei 430205, China)

Abstract: Instant messaging is fundamental to various mobile Internet applications; however, it is still an open problem to implement secure instant messaging in untrusted Internet environment. An approach for secure instant messaging of mobile intelligent terminal was presented, and a protocol for Trusted Session Key Agreement (TSKA) was designed and implemented. Theoretical analysis shows that the proposed TSKA can ensure the authenticity, freshness and confidentiality of the negotiated session key, even in the condition that both of the instant messaging server and the communication channel are not trusted. After TSKA, instant audio/video messages can be sent to the other side in a confidential and complete way. Experimental results in real Internet environment show that the proposed approach is efficient and secure, the session key can be negotiated within 1~2 seconds, and attackers cannot obtain any plaintext of instant messages.

Key words: mobile intelligent terminal security; instant messaging; trusted key agreement; protocol security

0 引言

目前,移动智能终端已经远超台式设备占据了市场的主导地位,我们正快速进入崭新的移动互联网时代。即时语音/视频通信(以下简称即时通信)作为移动互联网的重要基础,获得了广泛的应用,如:社交APP、警用监控、军事侦查、娱乐购物等各种领域。产业界对即时通信表现出高度的兴趣,并将其视为当前移动互联网产业竞争的核心领域之一^[1-2]。但是,如何保证即时通信的安全性却仍然是一个开放课题。目前主流的即时通信软件存在着不合理的安全假设。以占据国内市场主导地位的微信为例,其将即时通信的安全性建立在服务器绝对可信的假设之上^[3]。显然,这个假设是不合理的,斯诺登所揭露的美国监听欧盟事件表明,通过技术手段入侵并控制服务器,是完全可行的。因此,必须寻求一种在服务器不可信的情况下,即时通信双方仍能进行安全通信的方法。

本文默认即时通信服务器(以下简称服务器)已被黑客

完全控制,服务器和网络攻击者具有Dolev-Yao模型攻击能力。在此基础上,遵从现有主流即时通信软件所采用的即时通信模型(参见图1),基于普通商用移动智能终端,设计并实现了一种不可信互联网环境下的安全即时通信方法。即本方法可以在服务器不可信以及网络不可信的敌手环境下,可信地协商会话密钥以进行“端-端”可信通信。理论分析表明,只要密钥能够协商成功,则所协商的会话密钥一定是真实、新鲜和保密的;而真实互联网环境下的原型系统测试也表明该方法是高效和安全的。

当前主流即时通信软件均采用如图1所示的即时通信模型:整个架构采用“客户端—服务器—客户端”的C/S模式。服务器负责两类工作:客户端之间的会话密钥协商;对不同客户端进行注册、监控和管理等。

以国内占据市场绝对份额的即时通信软件微信为例,不同微信客户端之间的即时通信信息采用高级加密标准(Advanced Encryption Standard, AES)加密,但AES会话密钥

收稿日期:2016-08-22;修回日期:2016-09-28。 基金项目:国家自然科学基金资助项目(61502438, 61502362); 湖北省自然科学基金重点项目(2015CFA061); 浙江省自然科学基金资助项目(LY15F020015); 2015年湖北省建设厅科技计划项目。

作者简介:张帆(1977—),男,湖北当阳人,副教授,博士,CCF会员,主要研究方向:信息系统安全、软件安全; 张聪(1968—),男,上海人,教授,博士,主要研究方向:多媒体通信和安全; 赵泽茂(1965—),男,四川蓬溪人,教授,博士,主要研究方向:隐私保护、软件安全; 徐明迪(1980—),男,湖北武汉人,副研究员,博士,主要研究方向:信息系统安全、可信计算。



是由即时通信服务器生成并用 RSA 加密之后发布给终端使用的^[3]。显然,如果服务器是不可信的,那么服务器所生成的 AES 会话密钥、以及 RSA 加解密涉及的私钥均可能泄露,从而导致即时通信过程敏感信息泄露。

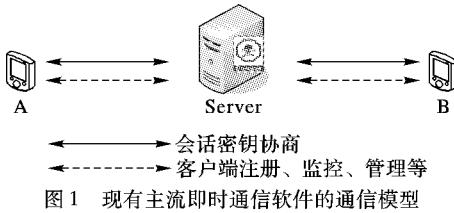


图 1 现有主流即时通信软件的通信模型

Fig. 1 Communication model of mainstream instant messaging software

为此,设计并实现了一种安全即时通信方法,其具有如下特点:1)基于图 1 所示的主流即时通信模型进行实现。除了将会话密钥协商协议替换为本文所设计的密钥协商协议之外,无需对即时通信模型作其他任何硬件层或者软件层修改,保证了系统的兼容性和易用性。2)默认服务器是不可信的,黑客可以完全控制服务器。这从根本上去除了当前主流即时通信软件“将即时通信的安全性建立在服务器绝对可信之上”的不合理安全假设。3)设计并实现了可信会话密钥协商协议。理论分析表明,只要会话密钥能够协商成功,则通信双方所协商的会话密钥一定是真实的(Authenticated)、新鲜的(Fresh)和保密的(Confidential),从而保证即时通信是安全的。4)基于普通商用移动智能终端进行设计实现。除了要求通信双方所使用的移动智能终端是可信的(即不存在恶意硬件和恶意软件)之外,对移动智能终端无需任何其他安全假设和安全增强。5)实现了原型系统。真实互联网环境下的实验表明,方法是安全和有效的。

1 相关研究

1.1 即时通信安全

文献[3-4]分别对具有代表性的主流即时通信软件微信、以及 Skype 和 QQ 的通信安全性进行了研究。上述软件的问题在于,它们均将即时通信的安全性建立在服务器绝对可信的不正确安全假设之上。而在实际应用中,服务器作为高价值对象,其不仅被攻击概率高,而且对其攻击是完全可行的。文献[5-6]分别提出了基于椭圆曲线公钥体制和基于身份的即时通信安全协议。但两者的问题在于它们仍然是基于服务器是绝对可信的。文献[7]基于 PGP(Pretty Good Privacy)实现安全即时通信,但文献[7]仍然要把 PGP 的密钥对存放在可信的服务器之中。文献[8-9]分别从隐私保护和即时通信恶意软件(IM Malware)的角度研究了即时通信的安全问题。但两者并没有回答在服务器和网络不可信的情况下,应该如何保证即时通信的安全。

在国内产业界,微信、QQ、钉钉、来往(钉钉前身)、陌陌等知名即时通信软件均不支持端-端加密。软件安司密信提供了端-端加密,但其必须采用特定的硬件才能实现,这不仅额外增加了成本,而且使用不便。本文的方法完全基于软件协议实现了端-端加密,避免了上述问题。国外 Whatsapp、Line、Viber 等于 2016 年 4 月到 7 月刚刚推出端-端加密功能。Facebook Messenger 于 2016 年 7 月刚刚进行端-端加密功能测试。但是,这些工作的端-端加密的细节不仅没有公开(从而无法确认是否存在后门),而且它们仅能实现“端-端”通信的机密性,无法保证完整性。“端-端”通信完整性在需要进

行远程控制的场景是很有意义的。Telegram 在 2013 年推出了端-端加密功能,但其协议可能遭受 MIMT(Man-In-the-Middle Attack)中间人攻击,而理论分析表明,本文的工作完全避免了 MIMT 攻击。

1.2 密钥协商

文献[10]介绍了几种典型的密钥协商方法。首先是经典的 Diffie-Hellman 方案,它的问题在于无法防御中间人攻击。为了解决中间人攻击问题,通过在经典形式上增加认证,形成了端-端密钥协商 STS 和 MTI/AO 密钥协商方案。这两种方案均需要有可信权威机构 TA(对应于 PKI 中的证书认证中心 CA)来提供证书或者签名。这又带来如下问题:一方面,在图 1 所示的即时通信模型中,服务器本身是不可信的;另一方面,移动智能终端由于数量巨大,为每一个移动智能终端都提供相应的证书在工程上难以实现。因此,上述两种方案无法在本文中应用。进一步地,文献[10]还介绍了无证书的 Girault 密钥协商方案,然而其仍然需要可信权威机构 TA 来生成秘密和辅助协商生成密钥。最后,文献[10]介绍了加密密钥交换 EKE 协议,EKE 使用共享口令来协商会话密钥,但是如何在数量巨大的移动智能终端中间为每两个终端建立共享秘密口令也是难以克服的问题。

无证书密钥协商是目前密钥协商的一个热点^[11-15],但无证书密钥协商方法的主要问题在于,它们仍然需要一个可信的第三方私钥生成中心(Private Key Generator, PKG),且有些中间计算步骤需要通过安全的方式从 PKG 返回给密钥协商双方。这也是难以实现的。

2 可信会话密钥协商协议

本质上,整个系统的关键在于通信双方如何在服务器和通信网络不可信的敌手网络环境下可信地协商会话密钥,从而实现“端-端”可信通信。

2.1 协议目的和背景

2.1.1 协议目的

协议的目的在于确保通信双方在敌手网络环境下可信地协商会话密钥,保证所协商会话密钥的真实性、新鲜性和机密性。因此,协议需要防止常见的伪造和篡改攻击(真实性),以及回放攻击(新鲜性);同时,协议还需要确保除了通信双方之外,其他任何第三方(包括服务器)都无法获知所协商的会话密钥(机密性)。

2.1.2 协议设计背景

说明 1 攻击者既包括网络攻击者,也包括服务器。

本文默认网络攻击者和服务器具有 Dolev-Yao 模型攻击能力。协议设计时,必须综合考虑上述攻击双方。

说明 2 服务器和即时通信客户端(以下简称客户端)公私钥对的安全性。

首先,对服务器而言:①服务器的公钥真实、新鲜地公开给所有客户端。这可以通过证书实现,极端情况下,也可以硬编码到客户端中。②服务器的私钥由服务器自身存储。由于服务器是不可信的,因此服务器的私钥可能已经泄露给攻击者。

其次,对客户端而言:①客户端的公钥为安全起见,在每次进行密钥协商时,都要重新生成。②客户端的私钥由客户端自身进行保密性存储。本文要求客户端本身是可信的(参见以下说明 3),因而客户端的私钥一定是安全的。



说明3“服务器的公钥可信地公开”和“客户端所使用的移动智能终端是可信的”是本文仅有的安全假设。

本文要求服务器的公钥可信地公开,前面已经说明,这可以通过证书或者硬编码到移动智能终端实现。注意服务器的数量并不多,那么对应证书的数量也并不多,因而这也是容易实现的。

2.2 协议详细设计

在详细分析协议之前,先给出协议的符号使用说明如下:约定用 s 指代服务器,用 a, b 分别指代通话双方客户端Alice和客户端Bob。每次即时通信之前,服务器和客户端需要重新生成自身的RSA公私钥对,约定用 ke_i 指代实体 i 的公钥,用 kd_i 指代实体 i 的私钥,例如; ke_s 是服务器Server的公钥, kd_a 是客户端A的私钥。使用 $HASH(x)$ 来指代对 x 的哈希操作;用 $E(ke_i, x)$ 指代对 x 用公钥 ke_i 作加密(或者签名验证)操作,用 $D(kd_i, x)$ 指代对 x 用私钥 kd_i 作解密(或者数字签名)操作。如2.1节的说明2所述,服务器已经生成了公私钥对 ke_s 和 kd_s ,其中公钥 ke_s 利用证书或者硬编码等方式真实、新鲜地公开给所有的通信终端;私钥 kd_s 由服务器 s 自己保存,但是私钥 kd_s 是不安全的,可能已经泄露给攻击者。

协议分为两大阶段。第一阶段:终端A和B分别将自身的公钥真实、新鲜地传送给对方(出于安全考虑,在每一次会话密钥协商时,即时通信双方都会重新生成公私钥对。由于公钥不需要考虑机密性,因而只需要将所生成的公钥真实、新鲜地传送给对方即可)。第二阶段:客户端A和B自主协商会话密钥,并确保会话密钥的真实性、新鲜性和机密性。

协议的详细步骤如下:

步骤1 通过步骤①~④,客户端A将公钥 ke_a 发送给服务器,并获取服务器对于 ke_a 的真实、新鲜的签名 sig_a 。

① 在发起会话密钥协商时,客户端A重新生成新的RSA公私钥对 ke_a 和 kd_a ,并将公钥 ke_a 发送给服务器。

② 服务器在收到 ke_a' (由于攻击者的存在,服务器实际接收到的结果与客户端A在步骤①发送的 ke_a 并不一定相同,因此这里用 ke_a' 代替)之后,使用自身的私钥 kd_s 对 ke_a' 进行数字签名生成 $sig_a = D(kd_s, h_a)$ 。

③ 服务器将数字签名 sig_a 和所接收到的 ke_a' 返回给客户端A。

④ 客户端A实际接收到 sig_a' 和 ke_a'' (由于攻击者的存在,客户端A实际接收到的结果与服务器在步骤③发送的 sig_a 和 ke_a' 不一定相同,因此这里用 sig_a' 和 ke_a'' 代替)之后,验证数字签名 sig_a' ,并比较 ke_a'' 是否与步骤①中生成的 ke_a 一致。如果验证和比较通过,则说明服务器收到的客户端A所发送的公钥 ke_a 是真实、新鲜的,且服务器对 ke_a 的签名 sig_a 也是真实、新鲜的。

步骤2 利用步骤1所获得的服务器对客户端A公钥 ke_a 的真实、新鲜的签名 sig_a ,将客户端A的公钥 ke_a 真实、新鲜地传送给客户端B。

① 客户端A生成随机数 m_a ,并利用私钥 kd_a 对 m_a 计算生成 $Dm_a = D(kd_a, m_a)$ 。

② 客户端A将自己的公钥 ke_a 、由步骤1获得的服务器对于 ke_a 的签名 sig_a ,以及 Dm_a ,即 $\langle ke_a, sig_a, Dm_a \rangle$,传送给客户端B。

③ 客户端B在实际接收到 $\langle ke_a', sig_a', Dm_a' \rangle$ (由于攻击者的存在,客户端B实际接收到的结果与客户端A在步骤③

发送 $\langle ke_a, sig_a, Dm_a \rangle$ 并不一定相同,因此这里用 $\langle ke_a', sig_a', Dm_a' \rangle$ 代替)之后,首先会验证签名 sig_a' 。如果验证通过,客户端B将利用 ke_a' 对 Dm_a' 计算 $m_a' = E(ke_a', Dm_a')$,并将 m_a' 传送给客户端A。

④ 客户端A在接收到 m_a'' (由于攻击者的存在,客户端A实际接收到的结果与客户端B在步骤③所发送的 m_a' 并不一定相同,因此这里用 m_a'' 代替)之后,验证所接收到的 m_a'' 是否与步骤①中生成的 m_a 一致。如果两者一致,则说明客户端B真实且新鲜地接收到了客户端A的公钥 ke_a ;否则客户端B接收到的公钥是错误的。

步骤3 采用与步骤1、2对称的操作,客户端B将公钥 ke_b 真实、新鲜地传送给客户端A。

步骤4 客户端A随机生成会话密钥前半部分 aes_1 ,并真实、新鲜、保密地传送给客户端B。

① 客户端A随机生成AES会话密钥的前半部分 aes_1 ,并利用私钥 kd_a 对 aes_1 进行数字签名生成 $sig_{aes1} = D(kd_a, h_{aes1})$ 。

② 客户端A利用客户端B的公钥 ke_b 将 $\langle aes_1, sig_{aes1} \rangle$ 加密生成 $E_{aes1} = E(ke_b, aes_1, sig_{aes1})$ 并传送给客户端B。

③ 客户端B在接收到 $E_{aes1}' = E(ke_b', aes_1', sig_{aes1}')$ (由于攻击者的存在,客户端B实际接收到的结果与客户端A在步骤②发送的 $E_{aes1} = E(ke_b, aes_1, sig_{aes1})$ 并不一定相同,因此这里用 $E_{aes1}' = E(ke_b', aes_1', sig_{aes1}')$ 代替)之后,利用私钥 kd_b 解密 E_{aes1}' ,获取 $\langle aes_1', sig_{aes1}' \rangle$ 并对 sig_{aes1}' 进行验证。如果验证通过,则说明真实、新鲜、保密地获取了 aes_1 。

步骤5 采用与步骤4类似的操作将客户端B随机生成的会话密钥的后半部分 aes_2 真实、新鲜、保密地传送给客户端A。

步骤6 客户端A和客户端B计算得到最终的会话密钥 $AES = HASH(aes_1) \oplus HASH(aes_2)$ 。

协议协商完毕。

2.3 协议安全性分析

1) 步骤1的安全性。

步骤1的目的是将客户端A新生成的公钥 ke_a 传送给服务器,并获取服务器对于 ke_a 真实、新鲜的签名 sig_a ,攻击者试图通过攻击使得上述目标无法达成。

由于服务器和网络同时是不可信的,因此协议必须同时检测到两者所发起的伪造、篡改和回放攻击。由此有如下三种情形:a) 服务器不进行攻击,其他网络攻击者对 ke_a 及其签名 sig_a 进行(伪造、篡改或者回放)攻击;b) 网络攻击者不进行攻击,服务器对 ke_a 及其签名 sig_a 进行(伪造、篡改或者回放)攻击;c) 服务器和网络攻击者同时对 ke_a 及其签名 sig_a 进行(伪造、篡改或者回放)攻击。上述三种情形均可以达到让客户端A无法获取服务器对于 ke_a 真实、新鲜签名的目的。

对于上述三种攻击情形,容易证明:对于客户端A,其在步骤1、④要么会验证服务器所传过来的对公钥 ke_a 的签名 sig_a 失败;要么会发现客户端B所实际接收到的公钥 ke_a' 与客户端A实际发送的公钥 ke_a 并不一致。无论哪种情形,客户端A都会发现攻击(限于篇幅,具体过程从略)。因此,步骤1能够确保客户端A将新生成的公钥 ke_a 传送给服务器,并获取服务器对于 ke_a 真实、新鲜的签名 sig_a 。

2) 步骤2的安全性。

步骤2的目的在于将客户端A的公钥 ke_a 真实、新鲜地发



送给客户端B,攻击者试图通过攻击以阻止上述目的的达成。

类似地,由于服务器和网络均是不可信的,协议需要检测到两者可能发起的伪造、篡改和回放攻击,由此也有三种情形需要考虑:a)服务器不进行攻击,网络攻击者对 ke_a 进行(伪造、篡改和回放)攻击;b)网络攻击者不进行攻击,服务器对 ke_a 进行(伪造、篡改和回放)攻击;c)服务器和网络攻击者同时对 ke_a 进行(伪造、篡改和回放)攻击,从而达到阻止客户端A将公钥 ke_a 真实、新鲜地发送给客户端B的目的。

对于上述三种攻击型情形,容易证明:客户端A要么在步骤2.③验证签名 sig_a' 失败,要么在步骤2.④发现其实际接收到的随机数 m_a'' 与它在步骤2.①所最初生成的随机数 m_a 并不一致,从而发现攻击(限于篇幅,具体过程从略)。因此,步骤2能够确保客户端A将其公钥 ke_a 真实、新鲜地发送给客户端B。

3) 步骤3的安全性。

由于步骤3是步骤1、2的对称过程,因而其安全性可以类似分析,这里从略。到此,通信双方均真实、新鲜地得到了对方所新生成的公钥。

4) 步骤4的安全性。

步骤4的目的是客户端A随机生成会话密钥前半部分 aes_1 ,并真实、新鲜、保密地发送给客户端B。

类似地,根据服务器和网络攻击者是否发起攻击,也有三种情形需要考虑。对于这三种攻击情形,容易证明:无论是哪种情形,客户端A将会在步骤4.③对它所实际接收到的签名 sig_{aes1}' 验证失败,从而发现攻击。因此,如果步骤4.③通过,则客户端A将其随机生成的会话密钥前半部分 aes_1 真实、新鲜、保密地发送给了客户端B。

5) 步骤5的安全性。

步骤5是步骤4的对称过程,因而其安全性可以类似分析,这里从略。至此,客户端B和客户端A分别接收到了对方真实、新鲜和保密发送过来的会话密钥的前半部分 aes_1 和后半部分 aes_2 。

协议安全性分析完毕。

2.4 会话密钥安全属性分析

需要强调的是,本文基于传统的非对称密码体制,而并非是无证书密钥协商,因而文献[11]中2.1节关于身份基认证密钥协商协议对安全属性的定义并不适合本文。但若借鉴其思想和定义,则可以进行类似安全属性分析并得出结论如下:

1) 满足已知密钥安全性。由于最终协商的会话密钥 $AES = HASH(aes_1) \oplus HASH(aes_2)$,而 aes_1 和 aes_2 是每次密钥协商时,分别由客户端A和客户端B随机生成的,因此,即使攻击者获得了某次客户端A和B所协商的会话密钥,他也无法求出其他协商时生成的会话密钥。

2) 满足完美前向安全性。若客户端A和B当前的私钥 kd_a 和 kd_b 都泄露,攻击者可以获得客户端A和B本次协商的会话密钥。但是,注意到在每次会话密钥协商时,客户端A和B都会分别重新生成新的公私钥对,不失一般性,不妨假设当前客户端A和B的公私钥对分别是 ke_a/kd_a 和 ke_b/kd_b ;假设在 kd_a 和 kd_b 泄露之前某次密钥协商时客户端A和B的公私钥对分别为 ke_a'/kd_a' 和 ke_b'/kd_b' ,那么有 $ke_a' \neq ke_a$ 和 $kd_a' \neq kd_a$,以及 $ke_b' \neq ke_b$ 和 $kd_b' \neq kd_b$ 。这样,即使攻击者获得了过去的 $E_{aes1}' = E(ke_b', aes_1', sig_{aes1}')$,由于攻击者所获得的客户端B的当前私钥 kd_b 和过去的公钥 ke_b' 之间并不匹配,他也无法正

确解密获得过去的 aes_1' 。因此,攻击者无法获得在 kd_a 和 kd_b 泄露之前所协商的会话密钥。

3) 满足PKG前向安全性。本文协议中不存在私钥产生中心(Private Key Generator, PKG)。但是,本文遵从主流即时通信软件采用图1所示的即时通信模型。若将服务器视作PKG,前述2.1节说明2已经说明,本文协议默认服务器是不可信的,默认其私钥已经泄露,且默认服务器在密钥协商过程中也会发起攻击,在此情况下协议仍能可信地协商会话密钥,因此,满足PKG前向安全性。

4) 满足抗密钥泄露伪装攻击。假设客户端A的私钥 kd_a 泄露,攻击者在不知道客户端B的私钥 kd_b 的情况下,无法冒充客户端B正常进行会话密钥协商(所有客户端B进行数字签名的步骤都无法通过),因而无法向客户端A冒充客户端B,满足抗密钥泄露伪装攻击。

5) 满足抗未知密钥共享。以步骤4.②为例,客户端A必须使用客户端B的公钥对所生成的会话密钥的前半部分 aes_1 和签名 sig_{aes1} 进行加密,如果采用其他客户端的公钥,则客户端B在随后将无法正确验证签名 sig_{aes1}' ,从而协商失败。因此,如果会话密钥协商成功,客户端A不会认为是和其他客户端C的共享会话密钥,满足抗未知密钥共享。

5) 满足无密钥控制。最终协商的会话密钥 $AES = HASH(aes_1) \oplus HASH(aes_2)$ 。由于哈希函数 $HASH$ 是单向函数,因而无论是客户端A还是客户端B都无法逆向选择性生成 aes_1 或者 aes_2 以达到控制所协商会话密钥中的一部分或者全部的目的。

2.5 即时通信完整性和拒绝服务攻击

1) 即时通信的完整性。

即时通信安全的另一个重要属性是完整性。事实上,本协议设计除了关注即时通信信息的机密性之外,也可以用以保证即时通信的完整性。注意到协议的第一阶段是将客户端A和B的公钥真实、新鲜地发送给对方,因此只要会话密钥能够协商成功,则客户端A和B一定分别真实、新鲜地获得了对方的公钥 ke_b 和 ke_a 。那么在后续的即时通信过程中,为了同时确保通信信息的机密性和完整性,只要先对通信信息进行数字签名,再用对方公钥加密传输即可。限于篇幅,具体实施步骤从略。据作者尽可能的了解,目前主流即时通信软件并没有考虑即时通信信息完整性的问题,而即时通信的完整性在包含远程命令发送等场景下是很有意义的。

2) 协议拒绝服务攻击。

协议流程中使用了一些密码学运算操作是比较耗费资源的,因而攻击者可能针对上述位置发送恶意攻击包而对终端造成拒绝服务(Denial of Service, DoS)攻击。限于篇幅,本协议目前未考虑拒绝服务攻击,而将其留作下一步的工作。可采用的一种解决方案^[23]是:一旦发现类似DoS攻击的企图(如通过验证失败的阈值),验证方在如签名验证等耗费计算资源的位置,在进行真实计算之前,先发送难题(Puzzle)给发送方,只有发送方解决了难题并回复正确结果之后,验证方才进行真正的密码学计算。Puzzle的求解难度可以随着DoS攻击的风险而逐步提高,从而迫使攻击方需要耗费更多、甚至不可接受的资源来达成攻击。另一方面,也可以采用文献[24]的方法,从DoS攻击下的资源损失以及损失的概率分布的角度来对安全协议的DoS风险进行量化评估和改进。



2.6 原型系统测试与分析

实验终端采用两台三星手机,CPU 1 GHz,Android 4.3 操作系统;服务器采用一台东芝笔记本电脑,CPU 为 Intel i5 2.5 GHz,内存 8 GB,Windows 7(64 位)操作系统。整个实验是在真实的互联网中完成的:服务器通过电信网络连接到 Internet 当中,任何接入 Internet 的机器都可以对其进行访问;两台三星手机作为即时通信双方,分别通过 3G 网络进行多省跨省远程即时语音/视频通信实验(如武汉与西安、杭州与西安等)。

1) 安全性测试。利用 Wireshark 抓包,可以发现攻击者只能够获取加密后的语音/视频数据包,无法解密之后进行正常的语音/视频播放。对于加密语音通信,抓包可见正常解密后的语音波形和攻击者从网络获取的加密语音波形两者完全不同。对加密语音波形播放时只有无意义的噪声。对于加密视频通信,正常解密后的即时通信视频可以正常播放,而攻击者从网络获取的加密视频即时通信视频只能获得无意义的“花屏”播放结果。安全测试达到预期结果。

2) 效率测试。协议使用了较多密码学运算(如签名和验证等),这可能会影响密钥协商的运行效率。真实互联网环境下远程跨省的多次实验结果表明,只要密钥协商能够成功,则密钥协商一定可以在 2 s 之内完成,这是用户可以接受的。另一方面,大量的测试表明,在不加解密的情况下语音/视频即时通信的时延分别约为 0.5 s 和 0.8 s,加解密后的语音/视频时延分别约为 0.8 s 和 1.3 s,即加解密引起的时延分别约为 60% 和 62.5%。上述加解密导致的时延可以通过进一步多线程、优化语音视频算法、优化传输数据包大小以及优化体系架构等方法解决。

3 结语

即时语音/视频通信是目前移动互联网各类应用的重要基础,但是如何保证即时语音/视频通信的安全性却仍然是一个开放问题。我们设计并实现了一种不可信互联网环境下安全保密即时通信方法,在真实互联网环境下的原型系统测试表明,整个密钥协商过程可在 1~2 s 完成,整个系统能够有效保证即时通信信息的安全性,方法是高效和安全的。

在实际使用中,文中的非对称、对称、哈希算法等可以对应更换为国家商密的 SM2、SM1/SM4、SM3 等算法或者军用算法,以确保密码算法的安全可控,以及国家安全的特殊需要;同时,本文方法也可以与已有的信息系统安全技术(如可信计算等)相结合,以进一步增强系统的安全。最后需要指出的是,虽然本文的研究背景是商业即时语音/视频通信,但由于图 1 所示架构的普遍性,以及即时通信的普遍性和重要性,只要是符合图 1 所示的架构的(如军用无人机侦查和警用监控等),亦可以应用本文的方法。

参考文献 (References)

- [1] 孟蕊. 即时通信用户规模增长第一, 手机端发展超整体水平 [EB/OL]. [2016-05-01]. http://www.cnnic.cn/hlwfzyj/fxszl/fxswz/201307/t20130718_40676.htm. (MENG R. Instant messaging user scalge grows the fastest, and the development of mobile phones go beyond the overall levels [EB/OL]. [2016-05-01]. http://www.cnnic.cn/hlwfzyj/fxszl/fxswz/201307/t20130718_40676.htm.)
- [2] 沈坤. 即时通信行业稳步发展, 移动即时通信成为厂商争夺重点 [EB/OL]. [2016-05-01]. <http://www.cnnic.cn/hlwfzyj/fxs...> zl/fxswz/201107/t20110719_33459.htm. (SHEN K. Instant messaging is developing steadily, and mobile instant messaging has become the hot area of competitions for manufactures [EB/OL]. [2016-05-01]. http://www.cnnic.cn/hlwfzyj/fxszl/fxswz/201107/t20110719_33459.htm.)
- [3] 麟晓海,薛质. 微信加密通信原理分析[J]. 信息安全与技术, 2014, 5(1): 13~16. (QU X H, XUE Z. The analysis and research of micro letter encryption on the mobile client and reverse break mode [J]. Information Security and Technology, 2014, 5(1): 13~16.)
- [4] 段冰,谷大武. Skype 与 QQ 软件的安全通信技术研究[J]. 信息安全与通信保密, 2007(11): 58~60. (DUAN B, GU D W. Study on the secure communication technology of Skype and QQ [J]. Information Security and Communications Privacy, 2007(11): 58~60.)
- [5] 宁国强. 一种安全即时通信系统的研究与设计[D]. 长沙: 湖南大学, 2010: 35~42. (NING G Q. Design and implementation of a secure instant messaging system [D]. Changsha: Hunan University, 2010: 35~42.)
- [6] 张立坤. 即时通信安全机制研究[D]. 济南: 山东大学, 2009: 42~77. (ZHANG L K. Research of instant messaging [D]. Jinan: Shandong University, 2009: 42~77.)
- [7] PINTO R L. Secure instant messaging [D]. Frankfurt: Frankfurt University, 2014: 55~62.
- [8] PATIL S, KOBSA A. Enhancing privacy management support in instant messaging [J]. Interacting with Computers, 2010, 22(3): 206~217.
- [9] XIA M, WU Z, WANG H. Secure instant messaging enterprise-like networks [J]. Computer Network: The International Journal of Computer and Telecommunications Networking, 2012, 56(1): 448~461.
- [10] DOUGLAS R S. 密码学原理与实践[M]. 冯登国,译. 3 版. 北京:电子工业出版社,2009: 123~15. (DOUGLAS R S. Cryptography Theory and Practice [M]. FENG D G, translated. 3rd ed. Beijing: Publishing House of Electronics Industry, 2009: 123~125.)
- [11] 王圣宝,曹珍富,董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报, 2007, 30(10): 1842~1852. (WANG S B, CAO Z F, DONG X L. Provably secure identity-based authenticated key agreement protocols in the standard model [J]. Chinese Journal of Computers, 2007, 30(10): 1842~1852.)
- [12] 汪小芬,陈原,肖国镇. 基于身份的认证密钥协商协议的安全分析与改进[J]. 通信学报, 2008, 29(12): 16~21. (WANG X F, CHEN Y, XIAO G Z. Analysis and improvement of an ID-based authenticated key agreement protocol [J]. Journal on Communications, 2008, 29(12): 16~21.)
- [13] 赵建杰,谷大武. eCK 模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34(1): 47~54. (ZHAO J J, GU D W. Provably secure two-party authenticated key exchange protocol in eCK model [J]. Chinese Journal of Computers, 2011, 34(1): 47~54.)
- [14] 张福泰,孙银霞,张磊,等. 无证书公钥密码体制研究[J]. 软件学报, 2011, 22(6): 1316~1332. (ZHANG F T, SUN Y X, ZHANG L, et al. Research on certificateless public key cryptography [J]. Journal of Software, 2011, 22(6): 1316~1332.)
- [15] 高海英. 可证明安全的基于身份的认证密钥协商协议[J]. 计算机研究与发展, 2012, 49(8): 1685~1689. (GAO H Y. Provably secure ID-based authenticated key agreement protocol [J]. Journal of Computer Research and Development, 2012, 49(8): 1685~1689.)



- 1689.)
- [16] 赵波, 张换国, 李晶, 等. 可信 PDA 计算平台系统结构与安全机制[J]. 计算机学报, 2010, 33(1): 82–92. (ZHAO B, ZHANG H G, LI J, et al. The system architecture and security structure of trusted PDA [J]. Chinese Journal of Computers, 2010, 33(1): 82–92.)
- [17] DAM M, GUANCIALE R, KHAPOUR N, et al. Formal verification of information flow security for a simple ARM-based separation kernel [C]// CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013: 223–234.
- [18] DAVI L, DMITRIENKO A, EGELE M, et al. MoCFI: a framework to mitigate control-flow attacks on smartphones [C]// NDSS 2012: Proceedings of the 19th Annual Network and Distributed System Security Symposium. Washington, DC: Internet Society, 2012: 222–237.
- [19] YANG Z, YANG M, ZHANG Y, et al. AppIntent: analyzing sensitive data transmission in Android privacy leakage detection [C]// CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013: 1043–1054.
- [20] ZHOU X, DEMETRIOU S, HE D, et al. Identity, location, disease and more: inferring your secrets from Android public resources [C]// CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013: 1017–1028.
- [21] EGELE M, KRUEGEL C, KIRDA E, et al. PiOS: detecting privacy leaks in iOS applications [C]// NDSS 2011: Proceedings of the 18th Annual Network and Distributed System Security
- Symposium. Washington, DC: Internet Society, 2011: 189–206.
- [22] LANGE M, LIEBEGELD S, LACKORZYNSKI A, et al. L4Android: a generic operating system framework for secure smartphones [C]// SPSM '11: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. New York: ACM, 2011: 39–50.
- [23] 卫剑帆, 陈钟, 段云所, 等. 一种认证协议防御拒绝服务攻击的设计方法[J]. 电子学报, 2005, 33(2): 288–293. (WEI J F, CHEN Z, DUAN Y S, et al. A new countermeasure for protecting authentication protocols against denial of service attack [J]. Acta Electronica Sinica, 2005, 33(2): 288–293.)
- [24] CAO Z, GUAN Z, CHEN Z, et al. Towards risk evaluation of denial-of-service vulnerabilities in security protocols [J]. Journal of Computer Science and Technology, 2010, 25(2): 375–387.

This work is partially supported by the National Natural Science Foundation of China (61502438, 61502362), Key Projects of Hubei Provincial Natural Science Foundation (2015CFA061), Zhejiang Provincial Natural Science Foundation (LY15F020015), 2015 Hubei Provincial Research Project of Construction Department.

ZHANG Fan, born in 1977, Ph. D., associate professor. His research interests include information system security, software security.

ZHANG Cong, born in 1968, Ph. D., professor. His research interests include multimedia communication and security.

ZHAO Zemao, born in 1965, Ph. D., professor. His research interests include privacy protection, software security.

XU Mingdi, born in 1980, Ph. D., associate research fellow. His research interests include information system security, trusted computing.

(上接第 391 页)

- [4] PATIL S, KASHYAP A, SIVATHANU G, et al. FS: an in-kernel integrity checker and intrusion detection file system[C]// LISA '04: Proceedings of the 18th USENIX Conference on System Administration. Berkeley, CA: USENIX Association, 2004: 67–78.
- [5] QUYNH N A, TAKEFUJI Y. A novel approach for a file-system integrity monitor tool of Xen virtual machine [C]// ASIACCS '07: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007: 194–202.
- [6] 王照羽. 基于 Xen 硬件虚拟化的磁盘文件操作监控系统[D]. 西安: 西安电子科技大学, 2013: 5–7. (WANG Z Y. Monitoring system for disk file operations in Xen Full virtualization [J]. Xi'an: Xidian University, 2013: 5–7.)
- [7] 王铸, 黄涛, 文莎. 基于虚拟机的文件完整性监控系统[J]. 中州大学学报, 2009, 26(5): 121–123. (WANG Z, HUANG T, WEN S. A file integrity monitoring system based on virtualization [J]. Journal of Zhongzhou University, 2009, 26(5): 121–123.)
- [8] 王婷婷. 基于硬件辅助虚拟化的虚拟机监控研究与实现[D]. 北京: 北京邮电大学, 2015: 3–4. (WANG T T. Research and implementation of virtual machine based on hardware-assisted virtualization [J]. Beijing: Beijing University of Posts and Telecommunications, 2015: 3–4.)
- [9] JIN H, XIANG G, ZOU D, et al. A guest-transparent file integrity monitoring method in virtualization environment [J]. Computers & Mathematics with Applications, 2010, 60(2): 256–266.
- [10] PAYNE B D, DE A CARBONE M D P, LEE W. Secure and flexible monitoring of virtual machines[C]// ACSAC 2007: Proceedings of the Twenty-Third Annual Computer Security Applications
- Conference. Washington, DC: IEEE Computer Society, 2007: 385–397.
- [11] HABIB I. Virtualization with KVM [J]. Linux Journal, 2008(166): Article No. 8.
- [12] Intel. Intel 64 and IA-32 architectures software developer manuals [EB/OL]. [2015-03-20]. <https://software.intel.com/en-us/articles/intel-sdm>.
- [13] AMD. AMD64 architecture programmer's manual volume 2: system programming [EB/OL]. [2015-03-20]. <http://developer.amd.com/resources/developer-guides-manuals/>.
- [14] 熊海泉, 刘志勇, 徐卫志, 等. VMM 中 Guest OS 非陷入系统调用指令截获与识别[J]. 计算机研究与发展, 2014, 51(10): 2348–2359. (XIONG H Q, LIU Z Y, XU W Z, et al. Interception and identification of guest OS non-trapping system call instruction within VMM [J]. Journal of Computer Research and Development, 2014, 51(10): 2348–2359.)

This work is partially supported by the National Natural Science Foundation of China (61272447).

ZHAO Cheng, born in 1991, M. S. candidate. His research interests include cloud computing, virtualization technology.

CHEN Xingshu, born in 1969, Ph. D., professor. Her research interests include cloud computing, big data, information security, trusted computing.

JIN Xin, born in 1976, Ph. D. candidate. His research interests include cloud computing, virtualization technology, trusted computing.