第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0147—03 文献标识码：A 中图分类号：TP393

一种基于 CPK 的传输协议

万 伟，王晋东，张恒巍
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：为提高 VxWorks 中数据传输的效率，结合组合公钥算法的原理和加密通信方法，设计一种高效、安全的嵌入式安全传输(EST)协议。EST 协议能够在 VxWorks 环境下快速建立端到端的通信，实现保密通信，满足实时操作系统的安全需求。给出该协议的设计与实现及相应结果分析，证明了该协议的可行性、有效性。

关键词：组合公钥；VxWorks 操作系统；SSL 协议；安全断言标记语言；可扩展的访问控制高标识语言

CPK-based Transmission Protocol

WAN Wei, WANG Jin-dong, ZHANG Heng-wei
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 In order to improve the efficiency of data transfer under VxWorks, based on Combined Public Key(CPK) and encrypted communication, this paper designs an efficient and secure Embedded Secure Transmission(EST) protocol. It can set up an end-to-end secure channel quickly and realizes authentication and encrypted data transfer, which satisfies the demand of real-time system. It presents the design and implementation of the protocol. The results analysis shows that the protocol is efficient and feasible.

【Key words】 Combined Public Key(CPK); VxWorks OS; SSL protocol; Security Assertion Markup Language(SAML); eXtensible Access Control Markup Language(XACML)

1 概述

嵌入式系统不断应用于工业领域，VxWorks 是一种嵌入式实时操作系统，凭借其高可靠性、强实时性优点，在嵌入式实时操作系统领域占据一席之地。VxWorks 采用与 BSD4.4 TCP/IP 兼容的实时网络协议栈，在其通信协议组件中有 SSL 组件，但 SSL 在嵌入式环境下建立安全通道较慢，其算法的性能、密钥长度等都影响安全性和运行效率。为了提高 SSL 通信效率，文献[1]对各种数据算法进行组合，以达到快速认证和应用数据的加密目的。文献[2]针对嵌入式系统的特点对算法进行更换，并精简相关的结构。这些算法在一定程度上提高了嵌入式系统的认证效率，但这些改进并不能有效解决其效率问题。组合公钥(Combined Public Key, CPK)体制凭借安全性高、灵活性好的特性可以很好地解决这个问题。通过对 CPK 算法原理的研究，发现在这种机制下用户可以与任意用户进行快速的身份认证和会话密钥协商。

本文结合 CPK 的算法原理和加密通信方法，设计并实现了一种协议，在达到相同安全性的前提下，使报文交互的次数大大减少。

2 CPK 体制原理

CPK 算法依据椭圆曲线上离散对数难题的数学原理构建公私钥矩阵[3]，它只需较短的密钥就可以达到较好的安全性，具有以下特性：

若 $(x_1, p_1),(x_2, p_2)$ 是$(a,\ b,\ G,\ n,\ p)$中的公私钥对，则 (x_1+x_2, p_1+p_2) 也是一对公私钥对。将这种组合方法推广到 m 个密钥对的组合，如下所述：

$(x_i, y_i), i=1,2,\cdots,m$ 为$(a,\ b,\ G,\ n,\ p)$中的公私钥对，令 $X=\sum_{i=1}^{m} x_i, Y=\sum_{i=1}^{m} y_i$，则 X 与 Y 构成一个组合的公私钥对(X, Y)。

CPK 利用这种组合性，通过规模很小的矩阵产生海量的公私钥对，达到密钥管理规模化的目的。在给定椭圆曲线密码参数的基础上，可构建公私钥矩阵。它们都是由基点 G 生成的元素，即 $X_{ij}=(x_{ij}, y_{ij})$。公钥矩阵记为

$$\boldsymbol{PSK}=\boldsymbol{SSK}=\begin{pmatrix}(x_{11},y_{11}) & (x_{12},y_{12}) & \cdots & (x_{1h},y_{1h})\\ (x_{21},y_{21}) & (x_{22},y_{22}) & \cdots & (x_{2h},y_{2h})\\ \vdots & \vdots & & \vdots\\ (x_{m1},y_{m1}) & (x_{m2},y_{m2}) & \cdots & (x_{mh},y_{mh})\end{pmatrix}$$

私钥矩阵记为

$$\boldsymbol{SSK}=\begin{pmatrix}r_{11} & r_{12} & \cdots & r_{1h}\\ r_{21} & r_{22} & \cdots & r_{2h}\\ \vdots & \vdots & & \vdots\\ r_{m1} & r_{m2} & \cdots & r_{mh}\end{pmatrix}$$

利用标识映射值，在矩阵中选取对应的位置生成公私钥对。设映射的坐标为：$(i_1, j_1),(i_2, j_2),\cdots,(i_t, j_t)$，则得到的公钥为 $PK=(x_{i1,y1},y_{i1,j1})+(x_{i2,j2},y_{i2,j2})+\cdots+(x_{it,jt},y_{it,jt})$，得到的私钥为 $SK=(r_{i1,j1}+r_{i2,j2}+\cdots+r_{it,jt})\bmod n$，因为 $PK=SK\times G$。由此可见，基于 CPK 算法的标识可用于网络的身份认证。

3 嵌入式安全传输协议研究与设计

嵌入式安全传输(Embedded Secure Transmission, EST)协议主要包括握手、应用数据传输和通告消息，分别完成身份认证、应用数据的机密性和完整性、传递相关的通告功能。

3.1 EST 的握手协议

第 1 阶段，建立 EST 会话，进行身份认证和密钥交换，

作者简介：万 伟(1983－)，男，硕士研究生，主研方向：嵌入式网络安全；王晋东，副教授；张恒巍，讲师
收稿日期：2009-08-30 **E-mail：**infodo2009@163.com

并协商将要采用的加密和压缩算法。当上层调用 EST 协议时，由发起方生成一个初始消息，包含收/发身份标识、会话号、压缩和加密算法、随机数 Random、公钥加密 Randomx、发方签名。报文消息格式结构如下：

```
Struct{
IdSource id_source;
IdDestiantion id_destination;
SessionNum session_num;
Compress compress;
Encryption  encryption;
Random random;
ProtectedRandomx protectedrandomx;
SignID  sign_id;
}
Initialization;
```

通信双方的标识(ID)可以是 ID 证书中用户标识或应用程序进程号，方便上层识别。在多任务操作系统 VxWorks 下，任务由唯一的 ID 标识。会话号(Session Num)用于标识连接号，连接过程可能出现断开，在再次连接时，可快速地用上一次规定的通信规则，不进行身份的再次认证，如须改变，则发送规则改变消息；其次是限制一定时间内通信双方的认证次数，防止恶意连接。加密算法(Encryption)是加密算法设置；压缩算法(Compress)采用 GZIP 或不用压缩算法；Random 作为标识报文的新鲜性；Randomx 用收方的公钥加密 Rx(PK)；Sig(Id)是对发方自身的签名。

发送初始消息时，对公钥加密的 Rx 同时对自身签名并发给接收方；会话号将自动从 1 计数，最大值为 1 500。发送初始消息后，进行密钥的生成 key＝MD5(R||Rx||Session Num)，并等待确认。

第 2 阶段，收方收到初始消息，先对其身份进行认证，用发方的公钥验证对方的签名，并记录当前会话号和将要用到的加密、压缩算法。用私钥解密得到随机数 Rx，同样计算会话密钥，然后给发起方发送确认消息。它包含用会话密钥对 Rx 加密和对随机数 R 签名，由发方检验，证明收方已取得正确的密钥并保证消息的新鲜性。

第 3 阶段，发方检验正常后，返回一个预传送数据消息，然后传送加密数据。如果验证不符合，则发送错误握手报文通知发方重新进行身份认证，并且有认证最大次数限制。

3.2 EST 的传送协议

EST 协议可以从上层接收未解释的任意长度的数据。握手的消息、应用数据和通告消息都通过 EST 传送协议发给对方。应用数据传输分以下步骤进行：

(1)将每个来自上层的消息分成 200 Byte 或更小的块。在 WTLS 协议中建议分块不超过 16 KB。在信息吞吐量较小、要求低延时的 VxWorks 系统中，大数据块要在下层重新分割，这样无疑会增加系统的负担，所以，较小数据块是最好的选择。文献[4]把分块降到 256 Byte。它的计算过程是：MD5 产生 MAC 值 128 bit，EST 报头是 8 Byte，数据最大分段＝MTU-EST -MAC -TCP-IPHS＝296-8-16-20-20=232。经实验证明，取分段为 200 Byte，既保证线路的利用率，又保证其他控制信息的传输。

(2)对每个分段进行压缩，并得到压缩后的长度。对于不足 1 KB 的数据不压缩，这样可以省去解压缩的时间。对于解压出现错误的报文，按分段号查找再重传。

(3)选用 SHA-1 和 MD5 计算数据块 MAC 值。它包括随机数、源和目的 Id、会话号、压缩的长度、压缩分段，计算定义如下：

MAC= MD5(Random||id_source||SHA (||Session_num ||EST Compressed.length||ESTCompressed.fragment))

(4)对加上 MAC 的消息加密。用分组密码加密之前要填充，使总长度是密码块长度的倍数，即原数据+MAC+填充块是密码块长度整数倍；支持流密码算法 RC4_128。在通用的设备上[5]，可选多种加密算法，而对于资源受限的嵌入式系统，把多种算法纳入系统是不可取的。

(5)生成一个 EST 数据报头，包含以下字段：

TaskId	TaskPriority	HLEN	Type	P/F
Segment Number		Last Segment Number		
Data Portion				

其中，Type(4 bit)表示 EST 报文有 5 种报文类型，包括压缩报文标志该报文是否是压缩类型；重传报文在得到中断报文通知后发送报文，能根据分段号快速连接到断开的地方；临时透明报文在与一方进行通信时，可能要与其他用户通信，则发送透明类型报文；分段报文是最后传输的一个分段，通知某网络任务这个分段是最后一个，如果无错误则及时释放缓存空间；中断报文指在传输过程中，如果系统出现异常，则发送中断传输报文，该报文无数据部分，系统根据任务号和分段号找到对应的任务，放弃传输或重新连接操作等。HLEN(11 bit)指示数据报头的长度；P/F(1 bit)指示是否需要一个双重的回应，对不足一个分段的报文，要求对方一个回应；TaskId(8 bit)对应的是系统的任务，Segment Number(16 bit)则是对相应任务号的子号；Last Segment Number(16 bit)指对应任务已正常收到的分段号。TaskPriority(8 bit)表示这个数据分段的优先级。VxWorks 中 tNetTask 的默认优先级[6]是 50，建立网络服务的任务要设在 50 以上，低于 tNetTask 的优先级。在封闭或组装时会让优先级高的任务先占用网络信道，保证 VxWorks 系统多任务的正常调度。

相反，如果从底层收到一个数据报，则进行解密、验证和组包之后，交给上层处理。

3.3 EST 协议通告消息

EST 协议相对简单，发现错误的一方向对方发送通告消息，一方收到后则进行相应的处理或双方进行共同处理，若是严重错误则关闭本次连接。消息通告类型如下：

(1)改变密钥消息：传输一定量的数据段或有特定的需要，则对会话密钥更改，由发方传送一个改变密钥消息，收方则利用会话号进行快速连接，收方用发方的公钥对新随机数加密并传给发方，然后双方进行密钥计算。

(2)规则改变消息：根据会话号找到对应的通信规格，并改变加密算法和压缩类型。

(3)错误 MAC 消息：如果接收到错误 MAC，则返回错误 MAC 消息，重新计算 MAC 值。

(4)解密错误消息：如果收到的数据不能正常解密，可能是长度错误或填充有误，则进行重传。

(5)预传送数据消息：它告知对方认证通过，准备传送应用数据。

(6)握手错误消息：如果在 EST 协议的认证阶段出现错误，则发送错误握手报文，重新进行双方的身份认证，并在一定时间内有认证的最大次数。这个错误也可能是由一方或

双方的任务被取消引起的。

(7)关闭连接消息：如果要关闭本次连接，则收发双方销毁本次连接的会话和加密密钥，并释放系统资源。

4 EST 协议安全性与性能分析

4.1 EST 协议安全性分析

(1)密钥的安全性

CPK 密钥管理体制是离散对数难题型的基于标识的密钥生成与管理的体制，而 CPK 系统规定私钥的分发是静态的且只在系统内部参与运算，即使系统的合法用户也不能从 CPK 系统中读出私钥，杜绝了攻击者获得私钥。

(2)对应用数据的保护

数据分段时采用 MAC 作为消息验证算法，阻止重放攻击和截断连接攻击。为防止重放或篡改攻击，MAC 从序列号、ID 号、消息长度同时对数据加密。

(3)对握手协议的攻击

攻击者可能试图改变握手协议中的消息，达到非法认证的目的。但在 EST 中，没有私钥无法解开握手信息包中的数据，而私钥在 CPK 系统中是安全的。

4.2 EST 协议性能分析

对 SSL 而言，在达到相同安全性的前提下，EST 报文交互 3 次完成。SSL 无法解决客户到客户的连接，加大了服务器的负载，而 EST 协议使认证负担均衡落到各接收端，大大减轻了服务器负担，且能更好地适应无中心网络的认证。

实验中采用 ARM9 S3C2410 芯片的嵌入式平台，在 VxWorks 5.5 系统的客户端与服务器之间创建一个 TCP 连接，然后打开 EST 连接，最后传输 EST 应用数据。

(1)握手过程的性能分析

对 SSL 和 EST 协议中密钥交换和产生 MAC 进行测试，见表 1。

表 1 认证时间的测量 ms

通信方式	SSL 执行时间	EST 执行时间
端到端认证	28.00(620 B)	10.00(528 B)
产生 MAC	0.79	0.68

在端到端的认证过程中，由于在 SSL 进行认证和签名的报文交互繁多，因此 SSL 协议认证的时间大大增加。EST 对相同用户信息的交换较快，耗时只有 SSL 的 35.7%。EST 产生 MAC 的用时明显比 SSL 少，只有 SSL 的 86.1%。

(2)应用数据加密性能分析

在相同的系统下，用 AES 对本地应用数据加密，见表 2。

表 2 应用数据加密的测试

数据大小	SSL 执行时间	EST 执行时间
128 B	1.16 ms	1.43 ms
512 B	4.11 ms	3.97 ms
8 KB	56.51 ms	51.62 ms
4.6 MB	37.26 s	30.67 s

可见，EST 对少量的应用数据加密稍慢；随着数据量增大，这种差距变小；在 8 KB 时，EST 处理较快，而加密较大文件时，耗时比 SSL 少。

(3)EST 与 SSL 的运行效率

在 ARM9 平台上处理多用户认证，并对 EST 和 SSL 在处理时间上进行比较，见图 1。

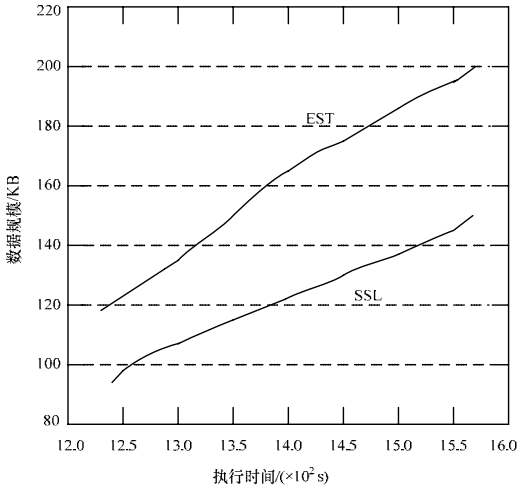

图 1 EST 与 SSL 协议的运行效率比较

当处理 140 KB 数据时，EST 与 SSL 用时分别为 1.3 s 和 1.5 s，前者是后者用时的 86.7%；而在 1.4 s 时，EST 处理 163 KB，SSL 处理 122 KB，前者是后者处理的 134%。在开始阶段，由于通信双方在进行身份认证时的交互次数少，同时 ECC 算法运算较快，因此 EST 协议比 SSL 协议处理快。随着时间和通信用户的增加，EST 对快速增加的数据能很好地处理，而 SSL 协议则是很平稳地处理，所以，EST 比 SSL 能更好地适应嵌入式中身份认证频繁而数据量不大的应用环境。

5 结束语

本文基于 CPK 原理实现了一种新的安全传输协议，解决了嵌入式系统中认证交互繁琐的问题。下一步将研究如何适应通用设备中大块数据的高速传输。

参考文献

[1] Sang H S, Zimmerman R, Hansson J. An Adaptable Security Manager for Real-time Transactions[C]//Proceedings of the 12th Euromicro Conference on Real-time Systems. Stockholm, Sweden: [s. n.], 2000: 63-70.

[2] 白志中, 罗斌骞, 夏靖波, 等. 基于 SSL 协议的嵌入式 Web 系统安全性研究与实现[J]. 电光与控制, 2006, 13(3): 60-64.

[3] 南湘浩. CPK 标识认证[M]. 北京: 国防工业出版社, 2006.

[4] Wright G R, Stevens W R. TCP/IP 详解(卷 1): 协议[M]. 北京: 机械工业出版社, 2000.

[5] Ertaul L, Chavan N. Security of Ad Hoc Networks and Threshold Cryptography[C]//Proc. of International Conference on Wireless Networks, Communications and Mobile Computing. [S. l.]: IEEE Press, 2005: 69-74.

[6] Wind River. VxWorks 网络程序员指南[M]. 北京: 清华大学出版社, 2003.

编辑 张正兴