第 34 卷 第 3 期 计 算 机 工 程 2008 年 2 月
Vol.34 No.3 Computer Engineering February 2008
·安全技术· 文章编号：1000—3428(2008)03—0189—02 文献标识码：A 中图分类号：TP309

无线移动网络密码协议的安全性

喻 慧
（名人科技实验室，深圳 518008）

摘 要：描述了一组无线移动网络中密码协议的过程，利用 GNY 逻辑对密码协议进行分析，鉴于 EAP-TLS 密码协议会受到中间人攻击，提出了解决方法，找出协议中存在的安全缺陷，发现了对密码协议的安全威胁，并给出攻击者可能的攻击。
关键词：EAP-TLS 密码；GNY 逻辑；密码协议

Security of Cryptographic Protocols of Wireless and Mobile Networks

YU Hui
(Celebrity Laboratory of Science and Technology, Shenzhen 518008)

【Abstract】 This paper describes a family of cryptographic protocols in wireless and mobile networks, analyzes protocols with GNY logic. Seeing that EAP-TLS cryptographic is suffered from man-in-the-middle attack, solution is proposed, security deficiency and the security threats are found, and probable attacks are obtained.
【Key words】 EAP-TLS cryptographic; GNY logic; cryptographic protocol

作为安全服务基础的密码协议，由于自身的复杂性，因此存在安全缺陷。逻辑分析在目前密码协议形式化分析中使用广泛，其中GNY逻辑是BAN类型逻辑中较为成功的一例。GNY逻辑中的命题包括：$A \triangleleft X$，主体A接收到公式X；$A \ni X$，A拥有公式X；$A|\sim X$，A曾经发送过X；$A|\equiv \#(X)$，A相信公式X是新鲜的；$A|\equiv \phi(X)$，A相信公式X是可辨认的；$A|\equiv A \overset{Kab}{\longleftrightarrow} B$，$A$相信$K_{ab}$是他和主体$B$之间的秘密密钥；$A|\equiv \overset{KU_b}{\longrightarrow} B$，$A$相信$KU_b$是$B$的公开密钥；$A|\equiv B|\Rightarrow C$，$A$相信$B$是命题$C$的权威。使用GNY逻辑分析密码协议：(1)确定协议的初始状态假设；(2)利用协议解析器将协议步骤翻译成逻辑描述；(3)根据初始假设、协议的逻辑描述和推理规则进行推理，得出各方持有的最终拥有集和信念集。本文指出了GNY逻辑的主要命题和协议分析过程[1-2]，分析了EAP-TLS[3-5]密码协议。

1 EAP-TLS 认证和密钥交换协议消息的描述

EAP-TLS 认证机制的无线客户端和服务器先申请一个标准的 X.509 证书并安装，认证时彼此交换证书，并协商出一个会话密钥，一旦认证通过，服务器将会话密钥发送给客户端并通知无线访问点，允许该客户端使用网络服务。在 EAP TLS 认证协议中，各主体间交换的消息内容如下：

(1)在EAP-Response/Identity消息中包含客户呼叫(M_{ch})消息，其中M_{ch}消息包括客户的TLS协议版本号、会话标识符、随机数和客户支持的加密算法集。

(2)在消息EAP Request中包含以下消息：服务器呼叫(M_{sh})，服务器证书(M_{sc})，服务器密钥交换(M_{ske})，服务器证书请求(M_{scr})，服务器呼叫结束(M_{shd})。

(3)在消息EAP Response中包含以下消息：客户证书(M_{cc})，客户密钥交换(M_{cke})，客户证书校验(M_{ccv})，客户改变加密描述(M_{cccs})，客户完成(M_{cf})。

(4)在消息EAP Succ/Fail中包含服务器改变加密描述(M_{sccs})和服务器完成(M_{sf})消息。

假定A为请求者，B为认证者，CA为可信证书权威，A和B拥有相同的证书权威，公开密钥证书为X.509 格式，K_a,K_b分别为A和B的Diffie-Hellman临时密钥交换公开参数，使用Diffie-Hellman密钥交换算法来产生预主秘密(K_{pms})，K_{pms}通过伪随机数产生器(PRF)转换为主秘密(K_{ms})。X.509 证书中包含RSA公开密钥，使用RSA公开密钥密码算法进行签名。随机数(R_{tn})由时间戳(T_a或T_b)联接随机字节(R_a或R_b)而成。

M_{ccv}中的握手消息为

$$M_{hs}=T_a,R_a,T_b,R_b,CA,B,T_{kb},KU_b,\ \{H(CA,B,T_{kb},KU_b)\}KR_{CA},P,G,K_b,\ \{H(P,G,K_b,T_a,N_a,T_b,N_b)\}KR_b,CA,A,T_{ka},KU_a,\ \{H(CA,A,T_{ka},\ KU_a)\}KR_{CA},K_a$$

$$H(T_a,N_a,T_b,N_b,P,G,K_b)=MD5(T_a,R_a,T_b,R_b,P,G,K_b)+SHA\text{-}1(T_a,R_a,\ T_b,\ R_b,P,G,K_b)$$

$$H(M_{hs})=MD5(M_{hs})+SHA\text{-}1(M_{hs})$$

完成消息为

$$MF=H(K_{ms},H(M_{hs}))=PRF(K_{ms},\ \text{“}FL\text{”}\ ,MD5(M_{hs})+\ SHA\text{-}1\ (M_{hs}))$$

客户完成消息为

$$MF_c=H(K_{ms},H(M_{hs},\{H(M_{hs})\}KR_a))=\ PRF\ (K_{ms},\ \text{“}MF_c\text{”}\ ,MD5(M_{hs},\{H\ (M_{hs})\}KR_a)+\ SHA\text{-}1(M_{hs},\{H(M_{hs})\}KR_a))$$

服务器完成消息为

$$(MF_s)=H(K_{ms},H(M_{hs},\{H(M_{hs})\}\ KR_a,MF_c))=PRF(K_{ms},\ \text{“}MF_s\ \text{”},MD5\ (M_{hs},\{H(M_{hs})\}KR_a,MF_c)\ +SHA\text{-}1(M_{hs},\{H(M_{hs})\}KR_a,MF_c)$$

2 EAP-TLS 认证和密钥交换协议的安全性分析

将 EAP-TLS 认证协议概括为：

消息 1 $AP \rightarrow A$: AP；

消息 2 $A \rightarrow B$: A；

消息 3 $B \rightarrow A$: $START$；

消息 4 $A \rightarrow B$: T_a,R_a；

消息 5 $B \rightarrow A$: T_b, R_b, CA, B, T_{kb}, KU_b, $\{H(CA,B,T_{kb},KU_b)\}KR_{CA},P,G,K_b$, $\{H(T_a,R_a,T_b,R_b,P,G,K_b)\}KR_b$；

消息 6 $A \rightarrow B$: CA, A, T_{ka}, KU_a, $\{H(CA, A, T_{ka}, KU_a)\}$ K

作者简介：喻 慧(1983－)，女，学士，主研方向：信息安全
收稿日期：2007-04-12 **E-mail：**kerry_yuhui@163.com

R_{CA},K_a,{$H(M_{hs})$}KR_a,$H(K_{ms}$,$H(M_{hs}$,{$H(M_{hs})$}KR_a))；

消息 7 $B \rightarrow A$: H (K_{ms}, $H(M_{hs}$, {$H(M_{hs})$} KR_a, H (K_{ms}, $H(M_{hs}$,{$H(M_{hs})$}KR_a))))。

经过解析器解析，得到如下协议描述：

1 $A\triangleleft$: *AP；

2 $B\triangleleft$: *A；

3 $A\triangleleft$: *$START$；

4 $B\triangleleft$: *T_a,*R_a；

5 $A\triangleleft$: *T_b,*R_b,CA,B,*T_{kb},*KU_b, *{*$H(CA,B,T_{kb},KU_b)$} KR_{CA}~>$CA|\equiv \xrightarrow{Ku_b} B$
P,G,*K_b,*{*$H(T_a,R_a,T_b,R_b,P,G,K_b)$}$KR_b$ ~> $B|\equiv \xrightarrow{KR_b} B$；

6 $B\triangleleft$: CA, A, *T_{ka}, *KU_a, *{*$H(CA, A, T_{ka}, KU_a)$}KR_{CA} ~>$CA|\equiv \xrightarrow{Ku_a} A$
K_a,{*H(*M_{hs})}KR_a ~>$A|\equiv \xrightarrow{KR_a} A$
H(K_{ms},*$H(M_{hs}$,{$H(M_{hs})$}KR_a))；

7$A\triangleleft$:*H(*K_{ms},*H(*M_{hs},*{*$H(M_{hs})$}KR_a,*$H(K_{ms}$,*$H(M_{hs}$,{$H(M_{hs})$}KR_a))))~>$B|\equiv A\ni K_{ms}$。

协议分析如下：

主体A和主体B分别拥有并相信CA的公钥证书；主体A和主体B分别拥有并相信各自的公钥证书和私钥，并相信彼此是诚实且有能力的；认证权威CA相信A, B的公钥证书，A, B信任CA能够正确对A, B的公钥证书进行签名，主体A能够产生K_{pms}和K_{ms}；主体B能够产生K_{pms}和K_{ms}；主体A拥有时间戳T_a、有效期T_{ka}和K_a并相信T_a是新鲜的，主体B拥有时间戳T_b、有效期T_{kb}和K_b并相信T_b是新鲜的；主体A拥有CA并相信CA和B可辨认的，主体B相信主体A是可辨认的，主体B拥有并相信CA,P,G是可辨认的。

对于消息 1：运用T_1和P_1得，$A\ni AP$，即A拥有了AP。

对于消息 2：运用T_1和P_1得，$B\ni A$，即B拥有了A。

对于消息 3：运用T_1和P_1得，$A\ni$START，即A拥有了START。

对于消息 4：运用T_1和P_1得，$B\ni T_a$,$B\ni R_a$，即B拥有了T_a和R_a。

对于消息 5：由于消息前提为初始假设，因此其是有效的，A相信CA签名并发送了B的公钥证书，但只从该数字签名也得不出A相信该证书是B的公钥证书；同时该消息隐含着公钥证书的功能是把公钥证书拥有者和公钥捆绑在一起，$H(CA,B,T_{kb},KU_b)$是B的标识符和公钥等的消息摘要，但由于B值以明文形式发送，容易被窃听并截获，从而会受到假冒认证者的攻击，因此B的真实身份和公钥证书能被假冒。

$H(T_a,R_a,T_b,R_b,P,G,K_b)$是新鲜的，则可得$B$在当前会话中发送了该消息，即$B$在当前会话中存在，$B$的身份被认证；$H(T_a,R_a,T_b,R_b,P,G,K_b)$是$(T_a,R_a,T_b,R_b,P,G,K_b)$的消息摘要，$A$通过比较所接收到的$H(T_a,R_a,T_b,R_b,P,G,K_b)$与自己所计算出的$(T_a,R_a,T_b,R_b,P,G,K_b)$的散列值，并由$B$的签名可得，$B$在当前会话中发送了$P$, G, K_b；以上推断也是以A接收到的消息 1 中的B值是主体B的真实身份为前提的。

对于消息 6：由于消息前提为初始假设，因此其是有效的，运用T_1和P_1得，$B\ni CA$, $B\ni A$, $B\ni T_{ka}$, $B\ni KU_a$,$B\ni K_a$，即B拥有了CA, A, T_{ka}, KU_a, K_a，由$B\ni P$, $B\ni G$, $B\ni K_b$，可以得出K_{pms}和K_{ms}；根据T_6和P_1得$B\ni H(CA,A,T_{ka},KU_a)$；根据R_1得，B相信他此时所接收的消息是可辨认的，包括$B|\equiv\#(CA,A,T_{ka},KU_a)$，又由于$B\ni$($CA$, A, T_{ka}, KU_a)，根据R_5得$B|\equiv\#(H(CA,A,T_{ka},KU_a))$，因此$B$拥有$H(CA,A,T_{ka},KU_a)$并相信它是可辨认的。

$B|\equiv CA\ |\sim(\ CA,A,T_{ka},KU_a)$，$B|\equiv CA\ |\sim${$H(CA,\ A,T_{ka}$, KU_a)}KR_{CA}，即B相信CA签名并发送了A的公钥证书，但由于没有证据证明$H(CA,B,T_{kb},KU_b)$是新鲜的，不能推断出CA在当前会话中签名并发送了A的公钥证书，只从该数字签名得不出B相信该证书是A的公钥证书；同时该消息隐含着公钥证书的功能是把公钥证书拥有者和公钥捆绑在一起，$H(CA,A,T_{ka},KU_a)$是A的标识符和公钥等的消息摘要，B通过比较所接收到的$H(CA,A,T_{ka},KU_a)$与自己所计算出的(CA,A,T_{ka},KU_a)的散列值，并且可信任的CA对它进行了签名可得出KU_a是A的公钥，即B相信该证书是A的公钥证书；B通过比较该消息中的A值与消息 2 中接收到的A值比较可得出，该公钥证书拥有者A就是消息 2 中所声称的A，即A通过身份认证，以上推断是以B接收到的消息 2 中的A值是主体A的真实身份为前提的。

对于消息 7：由于消息前提是消息 6 的推论，因此其是有效的，得

$A|\equiv B|\equiv A\ni K_{ms}$, $A|\equiv A\ni K_{ms}$

K_{ms}和此前所接收到的全部握手消息的消息摘要为

$H(K_{ms},H(M_{hs},\{H(M_{hs})\}KR_a,H(K_{ms},H(M_{hs},\{H(M_{hs})\}KR_a))))$

A通过比较所接收到的该消息与自己所计算出散列值以及B对$H(T_a,R_a,T_b,R_b,P,G,K_b)$的签名可得$A|\equiv B|\sim K_{ms}$。根据相关理论，得$A|\equiv B\ni K_{ms}$。

A 和 B 最终的拥有集和信念集为

$A\ni KU_b$; $A\ni P$; $A\ni G$; $A\ni K_b$; $A|\equiv B\ni K_{ms}$

$A|\equiv \xrightarrow{KU_b} B$; $A|\equiv B|\equiv \xrightarrow{KR_b} B$

$B\ni KU_a$;$B\ni K_a$;$B\ni K_{ms}$;$B|\equiv A\ni K_{ms}$

$B|\equiv \xrightarrow{KU_b} A$; $B|\equiv A|\equiv \xrightarrow{KR_a} A$

EAP-TLS协议通过公钥证书进行相互认证，使用Diffie-Hellman密钥交换算法来产生会话密钥，通过完成消息来检验双方是否同时拥有K_{pms}和K_{ms}。以上推断都是以A和B各自接收到的消息 1 和消息 2 中的B和A值是主体B的真实身份为前提的，而A值和B值都以明文形式发送，容易被窃听并截获，会受到中间人攻击；并且认证双方最后并没有达到K_{pms}和K_{ms}为秘密信念的目的。如果A值和B值可以被加密(如A_K)，就可以避免中间人攻击。

3 结束语

基于 GNY 逻辑，本文分析了无线移动网络密码协议，针对所发现的安全缺陷，对协议进行了改进。

参考文献

[1] Burrows M, Abadi M, Needham R. A Logic of Authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[2] Gong L, Needham R, Yahalom R. Reasoning About Belief in Cryptographic Protocols[C]//Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, CA: [s. n.], 1990: 234-248.

[3] Dierks T. The TLS Protocols[S]. RFC 2246, 1999-01.

[4] Aboba B, Simon D. PPP EAP TLS Authentication Protocol[S]. RFC 2716, 1999-10.

[5] Tian L. Extending Formal Security Protocol Specification Languages for Use with New Verification Techniques[EB/OL]. (2006-01-02). http://www.ece.ul.ie/Research/DataComms/papers/2006%20-%20WSEAS%20Transactions%20-%20Extending%20Formal%20Security%20Protocol%20Specification%20Language%20for%20use%20with%20New%20Verification%20Techniques.pdf.