مطالعات علوم کاربردی در مهندسی

دوره ۳، شماره ۱، بهار ۱۳۹۶

صفحات ۱۷۱- ۱۵۸

Online ISSN: ٢٤٧٦-٤٥٠٧

Print ISSN: ٢٥٣٨-٢٠٥٥

www.irijournals.com

تکنیک جدید احراز هویت در صوت شبکه به کمک تلفیق منحنی بیضوی با سرور بلیط

محمد شرف فراهانی

کارشناس ارشد مهندسی کامپیوتر-نرم افزار دانشگاه فردوسی مشهد.

چکیده

در دنیای امروز سیستمهای صوت و تصویر مبتنی بر اینترنت (**VOIP**) روز به روز در حال گسترش می باشد و در این راستا پروتکل شروع جلسه (**SIP**) کاربرد بسیار زیادی داشته و بسیار مهم میباشد. پروتکل شروع جلسه به کمک سیگنالینگ اعمال کنترلی خود را انجام میدهد و برای تحقق این امر از پروتکل احراز هویت ابر متن کمک میگیرد. پروتکل **SIP** تحت استاندارد **IETF** در نسخه **RFC 3261** بصورت کامل شرح داده شده است. با توجه به اینکه کاربردهای پروتکل **SIP** در تجهیزات **VOIP** بسیار زیاد شده است لذا اکثر حملات به سمت این پروتکل متمرکز شده است. در این مقاله ما سعی میکنیم که مکانیزم احراز هویت این پروتکل را مقاومتر نماییم و نقاط ضعف انرا رفع نماییم. به کمک روش رمزنگاری منحنی بیضوی **ECC** و تلفیق آن با یک سرور کمکی بلیط باعث شده که امنیت را بالا برده و مقاومت در مقابل حملات را افزایش دهیم. سپس در انالیز نشان میدهیم که این روش از روشهای قبلی مناسبتر است.

واژه‌های کلیدی: احراز هویت، منحنی بیضوی، پروتکل شروع جلسه، چکیده ابر متن.

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

۱. مقدمه

با توجه به گسترده شدن کاربردهای اینترنت در خدمات صوت و تصویر (VOIP) و استفاده این کاربردها از پروتکل شروع جلسه (SIP) بعنوان سیگنالینگ لذا اهمیت امنیت در آن کاملا حس میشود. تا کنون بر روی قسمتهای مختلف این پروتکل مطالعات زیادی صورت گرفته است و قسمتی از این مطالعات مربوط به تشخیص هویت کاربران میباشد.

در حالت کلی SIP برای تشخیص کاربران از پروتکل احراز هویت خلاصه ابر متن استفاده میکند که تحت RFC 2617 شرح داده شده است. این پروتکل نقاط ضعف زیادی مانند عدم توانایی جلوگیری از حملات spoofing و offline password guessing دارد(دی جنیاتاکسی،۲۰۰۶)[1]. لذا جهت حل مشکل در سال ۲۰۰۵ اقای یانگ[2] در مقاله خود پیشنهاد کرد که از پروتکل تعویض کلید دایفی هلمن کمک گرفته شود و سپس در همان سال توسط دورالینک[3] روش فوق با روش منحنی بیضوی اصلاح شد ولی خیلی سریع مشخص شد که روش اولیه یانگ نمیتواند در مقابل حمله تکرار مقاومت نماید و اسیب پذیر است و در سال ۲۰۰۶ نیز مشخص شد که روش دورالینک نیز در مقابل حمله سرقت تصدیق نمی تواند مقاومت نماید.(اچ ال یاه۲۰۱۲[4])

در سال ۲۰۰۶ روش بهتری توسط رینگ[5] طراحی شد که در آن از تابع hash جهت شناسایی کاربران SIP استفاده شد ولی این روش هم در مقابل حمله جعل هویت اسیب پذیر است و همچنین سربار محاسباتی زیادی داشت , لذا توسط اقای وانگ[6] روش SAKA که یک روش امن تصدیق هویت بر مبنای کلید عمومی بدون گواهی (CL_PKC) بود پیشنهاد شد. اما این روش نیز محاسبات زیادی داشته و کند بود.(جی روزنبرگ ،۲۰۰۲[7])

در سال ۲۰۰۹ روش دیگری توسط تیسه[8] پیشنهاد شد. تیسه پیشنهاد کرد که از رشته چالش nonce میتوان برای احراز هویت کمک گرفت اما آقای Lee در مقاله خود نشان داد که این پروتکل در مقابل حمله حدس زدن رمز عبور ضعیف است. در سال ۲۰۱۴ آقایان یه[9]، چن[10]، شیه[11] در مقاله خود پیشنهاد دادند که از یک کارت هوشمند در احراز هویت پروتکل SIP استفاده شود و اطلاعات بر روی این کارت بصورت رمز نگهداری شود. اما این روش نیز خیلی کارایی نداشت چرا که نمیتوان برای چند سیستم VOIP کاربران را مجبور کرد که چند کارت هوشمند نگهداری کنند و همچنین در صورت سرقت کارت هوشمند , سارق میتوانست به اطلاعات دستیابی داشته و یا حتی مبادرت به حمله جعل هویت نماید.(ام هندلی ،۱۹۹۶[12])

در روش منحنی بیضوی به دلیل کوتاهتر شدن طول کلید و کمتر شدن محاسبات و در نتیجه سریع شدن متد ما با افزایش امنیت روبرو می شویم. در این مقاله نشان داده میشود که بدون کارت هوشمند نیز میتوان به امنیت بالاتری رسید.

در قسمت ۲ ما ابتدا تعدادی از کارهای وابسطه به SIP را شرح میدهیم و سپس در قسمت ۳ روش پیشنهادی خودمان ارائه میگردد و در قسمت ۴ این روش هم انالیز امنیت و هم انالیز کارایی میشود. در نهایت در قسمت ۵ نتایج اعلام میگردد.

[1] D. Geneiatakis
[2] yang
[3] doralink
[4] H.-L. Yeh
[5] ring
[6] Wang
[7] J. Rosenberg
[8] Tsai
[9] Yeh
[10] Chen
[11] Shih
[12] M. Handley

۲. روش تحقیق

در این قسمت ما بصورت مختصر عملکرد رمزنگاری منحنی بیضوی ECC و پروتکل شروع جلسه SIP و پروتکل احراز هویت چکیده ابر متن HTTP Digest Authentication را شرح می دهیم.

۲-۱. رمزنگاری منحنی بیضوی

رمزنگاری منحنی بیضوی یا ECC توسط نیل کوبلیتز و وکتور میلر در سال ۱۹۸۵ طراحی شد. برای بررسی آن ابتدا باید مسئله لگاریتم گسسته بررسی شده و سپس به عملکرد منحنی بیضوی برسیم.(دورنالینک،۲۰۰۲[1])

۲-۱-۱. لگاریتم گسسته

لگاریتم گسسته خود یک لگاریتم معمولی است که روی گروه دایره ای عمل میکند یعنی در لگاریتم معمولی جواب ما داخل مجموعه اعداد حقیقی است اما در یک لگاریتم گسسته $Log_p(h)$ به x میرسد که x جواب معادله داخل یک گروه دایره ای است.

مسئله لگاریتم گسسته دنبال پیدا کردن عدد صحیح x است که این عدد باید در محدوده $0 \leq x \leq n-1$ باشد. میتوانیم انرا بصورت زیر نمایش دهیم:

$$g^x = h \ (mod \ \ p) \ \ \forall g \in Z_p^* \qquad (1)$$

الگوریتمهایی مثل DSA و دیفی هلمن و الگامال بر پایه لگاریتم گسسته بنا نهاده شده اند.(ال کانگ ،[2]۲۰۰۶)

۲-۱-۲. لگاریتم گسسته بر روی منحنی بیضوی

منحنی بیضوی E_p بقسمی که p ناحیه ما و مخالف عدد ۲و۳ باشد و نقطه (x,y) هم عضو p` باشد معادله زیر را خواهیم داشت:

$$y^2 = x^3 + ax + b \qquad (2)$$

aوb باید دو عدد صحیح غیر منفی و کمتر از p باشد و در رابطه زیر نیز صدق کند:

$$4a^3 + 27b^2 \ \ (mod\, p\,) \ \ \neq 0 \qquad (3)$$

لذا $E_p(a,b)$ بصورت فوق اصلاح میشود:

$$y^2 = x^3 + ax + b \ \ (mod \ \ p) \qquad (4)$$

[1] A. Durlanik

[2] L. Kong

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

حال لگاریتم گسسته منحنی بیضوی به این صورت بوده که ابتدا عدد p باید ثابت نگه داشته شود و سپس یک منحنی بیضوی بصورت Q=X.P محاسبه شود. X.P یعنی نقطه P روی منحنی بیضوی به اندازه X بار با خودش جمع شود.
(هوانگ،[1] ۲۰۰۲)

۲-۱-۳. منحنی بیضوی بر روی ناحیه محدود

عملیاتی که بصورت پایه ای استفاده میشود شامل جمع نقطه ای و ایجاد نقطه مضاعف می باشد.
جمع دو نقطه A و B که بصورت W=A+B است نیاز به یک عمل معکوس و ۳ عمل ضرب دارد و اگر A,B نقاطی روی منحنی بیضوی باشند حاصل جمع بصورت زیر محاسبه میشود:
اگر A≠ -B باشد پس باید یک خط بین A وB رسم کنیم و این خط منحنی را در W- قطع میکند حال برای محاسبه W باید مقدار x در نقطه را تغییر نداده و y را تبدیل به y– نماییم.

اگر A= -B باشد لذا خط بین این دو یک خط عمودی بوده و به سمت بینهایت میرود و نقطه ما واقع در بینهایت است که به آن نقطه O میگوییم.
برای نقطه مضاعف یعنی W=2A ابتدا خط مماس بر نقطه A را رسم میکنیم. این خط محور را در W– قطع میکند . حال باید مقدار y را منفی نماییم و با این روش به W میرسیم(ای جی یون ۲۰۰۹[2])

بررسی عملکرد پروتکل SIP

SIP یک پروتکل سیگنالینگ پیشنهاد شده توسط IETF است و این پروتکل تامیین کننده جلسات ارتباطی صوتی و ویدئویی بصورت بلادرنگ می باشد. پروتکل شروع جلسه SIP توسط IETF در RFC 3261 توصیف شده است. سازگاری با ساختار اینترنت و سادگی پیاده سازی از جمله دلایل عمده محبوبیت این پروتکل میباشد. SIP یک پروتکل کنترل سیگنالینگ لایه کاربرد جهت ایجاد و تغییر و خاتمه دادن به جلسات, با حضور یک یا چند کاربر است. در این پروتکل گروهی از سرورها استفاده میشود که میتوان موارد زیر را ذکر کرد : سرور پراکسی – سرور ثبت – سرور اصلاح مسیر
همچنین عامل های کاربران درگیر کار با این سرورها هستند. یک جلسه SIP را میتوان بصورت زیر نشان داد:
مرحله ۱) A ابتدا خود را در سرور register ثبت می نماید
مرحله ۲) A یک پیغام invite به سمت سرور proxy ارسال می کند.
مرحله ۳) بعد از رسیدن پیغام invite به سرور , سرور proxy آدرس B را از طریق DNS موجود در سرور redirect پیدا می کند.
مرحله ۴) سرور proxy درخواست invite را به سمت B و همزمان پیغام 100 trying را به سمت A ارسال میکند.
مرحله ۵) B بعد از دریافت پیغام invite انرا با 200 OK پاسخ می دهد.
مرحله ۶) در پایان یک گواهی تصدیق ACK از A به سمت B ارسال میشود.
مرحله ۷) در این مرحله یک ارتباط RTP بین A,B برقرار میشود.
مرحله ۸) در پایان هر کدام از کاربران میتوانند به جلسه خاتمه دهند و برای این کار یک پیغام BYE به سمت طرف مقابل ارسال میکند و طرف مقابل نیز جواب آنرا با 200 OK می دهد و جلسه خاتمه پیدا می کند.

[1] M.S. Hwang

[2] E.J. Yoon

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

پروتکل احراز هویت خلاصه ابر متن

عملکرد پروتکل احراز هویت خلاصه ابر متن را می توان بصورت زیر شرح داد:

مرحله ۱) کاربر UA پیغام request را ارسال می کند. این پیغام شامل شناسه کاربر می باشد.

مرحله ۲) سرور SIP یک رشته nonce تولید و پیغام چالش شامل (realm, nonce) را به UA ارسال می کند.

مرحله ۳) UA با مشاهده پیغام مرحله ۲ , رمز را وارد و تابع hash زیر را محاسبه کرده h(nonce,id,password,realm) و پیغام response را به سرور ارسال می کند.)

مرحله ۴) از طرف دیگر سرور نیز خود تابع hash را فراخوانی کرده و مقدار `Response را محاسبه می کند. حال اگر این `respone=response باشد پیغام invite به UB ارسال می کند.

این پروتکل دارای نقاط قوت و ضعفی نیز میباشد که میتوان بصورت زیر نام برد.

نقاط قوت:

- Password بصورت مستقیم در digest استفاده نشده و بصورت hash ارسال میشود.
- رشته nonce سمت کاربر تحت RFC 2617 تولید می شود که در مقابل حمله chosen plaintext attacks مقاوم است.
- رشته nonce سمت سرور دارای برچسب زمانی است و در نتیجه جلو حمله replay را میگیرد.
- سرور تا مدتی رشته های nonce را نگهداری میکند که در نتیجه جلو رشته های nonce تکراری گرفته میشود.

نقاط ضعف:

- خیلی از نکات امنیتی REC 2617 بصورت optional هستند لذا اگر حفاظت کامل رعایت نشود کاربر از امنیت کمتری برخوردار است.
- پروتکل احراز هویت خلاصه ابر متن در مقابل حمله مرد در میان مقاوم نیست .(آی دالگیک ۱۹۹۹[1])

۳. یافته ها

تا کنون تکنیکهای زیادی برای احراز هویت در SIP پیشنهاد گردیده که در مقدمه به بعضی از انها اشاره شد. در مقاله آقای yeh در سال ۲۰۱۴ از یک کارت هوشمند جهت بالاتر بردن امنیت استفاده شده اما حمل کارت هوشمند خود امنیت را کاهش می دهد زیرا امکان گم کردن کارت و یا کپی برداری از روی آن وجود دارد و همچنین کاربران نمیتوانند برای چند سیستم SIP چندین کارت هوشمند نگهداری کنند.

در روش پیشنهادی ما سطح امنیت بالا بوده و نیازی هم به کارت هوشمند ندارد.

در این روش به کمک یک سرور کمکی با نام سرور بلیط میتوان عمل ذخیره سازی روش آقای یه را در آن انجام داد و مشکل امنیت کارت هوشمند نیز حل میشود.

برای بررسی مدل ابتدا پارامترهای زیر را تعریف میکنیم:

[1] I. Dalgic

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

جدول۱: پارامترهای استفاده شده در روابط ریاضی

توضیح	پارامتر
یک نقطه تصادفی روی منحنی بیضوی	R_A
تابع منحنی بیضوی روی ناحیه محدود	$E_p(a,b)$
کلمه رمز کاربر	PWx
تابع or انحصاری	$\oplus$
کلید کاربر B	K_B
کلید کاربر A	K_A
کلید جلسه	K
تابع hash	H(..)
برچسب زمان	T
رشته تولیدی توسط تابع hash	Nr
کلید رمز کاربر	Kida

۳-۱. فاز ثبت اولیه

در این مرحله ابتدا کاربر یوزر و پسورد خور را وارد کرده و سپس در عامل سمت کاربر مقادیر زیر محاسبه میشود:

$$N_r = h(id \parallel PW_x) \quad (5)$$

$$PW_y = h(PW_x \oplus N_r) \quad (6)$$

سپس پیغام ثبت شامل id و PWy به سمت سرور ارسال میشود. در قسمت سرور محاسبات زیر انجام میشود :

$$B_A = h(id \oplus PW_y) \quad (7)$$

$$K_{IDA} = q.s * H1(id)G_p \quad (8)$$

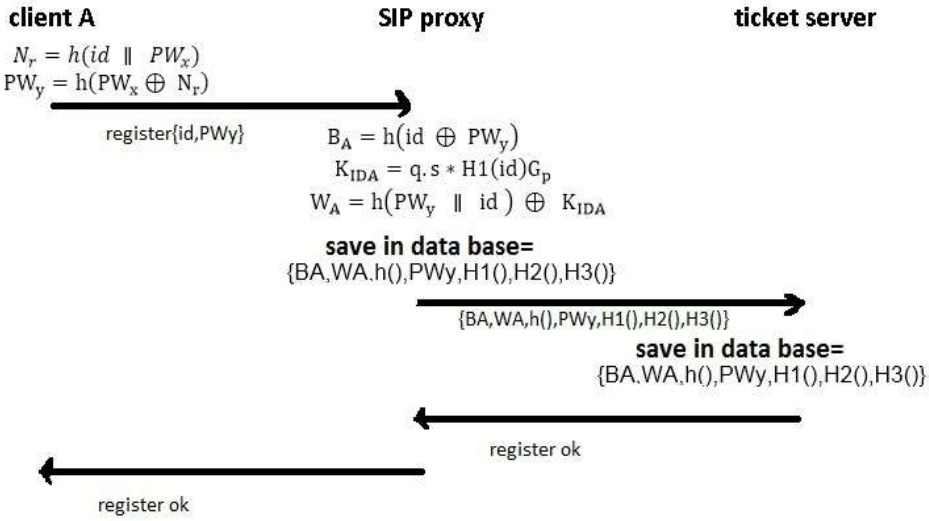
$$W_A = h(PW_y \parallel id) \oplus K_{I\ DA} \quad (9)$$

در پایان سرور پارامترهای مخفی زیر را در پایگاه داده خود ذخیره کرده و یک کپی از انرا از طریق یک کانال امن به سمت سرور بلیط ارسال میکند و این سرور پارامترها را ذخیره میکند. {BA,WA,h(),PWy,H1(),H2(),H3()}

سپس تایید اجرای این عمل را سرور بلیط به سرور پراکسی داده و سرور پراکسی به کاربر میدهد.

شکل ۱ روش ثبت اولیه را کامل نشان میدهد.

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸



شکل 1: نحوه ثبت اولیه کاربر در سرور اصلی و سرور بلیط

۳-۲. فاز احراز هویت دوطرفه

کاربر جهت شروع ارتباط به سرور وارد فاز احراز هویت دوطرفه میشود.

ابتدا کاربر مقادیر زیر را محاسبه و به سمت سرور بلیط مقدار PWy را ارسال میکند

$$N_r = h(id \parallel PW_x) \quad (10)$$

$$PW_y = h(PW_x \oplus N_r) \quad (11)$$

در سرور بلیط چنانچه مقدار PWy در پایگاه داده آن پیدا شد. سرور پارامترها ی زیر را برای کاربر ارسال میکند

{BA,WA,h(),H1(),H2(),H3()}

حال در قسمت کاربر باید محاسبات زیر انجام شود :

$$B'_A = h(id \oplus PW_y) \quad (12)$$

$$PW_y = h(PW_x \oplus N_r) \quad (13)$$

سپس کاربر تایید میکند که آیا B`a مساوی Ba هست یا نه. اگر مساوی است پس کاربر V و K(IDA) را بصورت زیر محاسبه میکند:

$$V = h(PW_y \parallel id) \quad (14)$$

$$K_{IDA} = W_A \oplus V \quad (15)$$

در مجموع کاربر نقطه تصادفی $R_A = (R_A^x, R_A^y)$ را در Ep(a,b) انتخاب میکند. که R_A^x و R_A^y همان نقاط x و y هستند که بعد از تولید کلید احراز هویت K(IDA) ایجاد شدند.

در برچسب زمانی T1 , کاربر محاسبه میکند :

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

t1=H2(T1) (16)

MA=RA+t1*K(IDA) (17)

$R_A^x * P = R_A^*$ (18)

سپس بسته درخواست به سمت سرور پراکسی ارسال میشود

در پراکسی محاسبات زیر انجام میشود:

$$t_1 = H_2(T_1) \quad (19)$$

$$R_A' = M_A - qs * t_1 * U_{IDA} \quad (20)$$

$$U_{IDA} = (U^x, U^y) \quad (21)$$

$$R_A' = (R_A^x, R_A^y) \quad (22)$$

$$R_A^{x'} * P = R_A^* \quad (23)$$

$$R_s = (R_s^x, R_s^y) \quad E_p(a,b) \quad (24)$$

$$M_s = R_s + t_2 * qs * U_{IDA} \quad (25)$$

$$K = H_3(U^x \parallel R_A^x \parallel R_s^x) \quad (26)$$

$$M_k = (K + R_s^x) * p \quad (27)$$

حال سرور بسته چالش را به سمت کاربر ارسا میکند.

در قسمت کاربر باید مقادیر زیر محاسبه شود و بعنوان پاسخ به سرور ارسال گردد:

$$t_2 = H_2(T_2) \quad و \quad R_s' = M_s - t_2 * K_{IDA} \quad (28)$$

حال برای بدست آوردن

$$R_s' = (R_s^{x'}, R_s^{y'}) \quad (29)$$

از مقادیر بالا استفاده میشود. در مجموع حال میتوان $U_{IDA} = (U^x, U^y)$ را بدست آورد و کاربر مقادیر زیر را محاسبه کند:

$$K^* = H_3(U^x \parallel R_A^x \parallel R_s^{x'}) \quad (30)$$

$$M_k^* = (K^* + R_s^{x'}) * P \quad (31)$$

و همچنین کاربر بررسی میکند که آیا مقدار $M_k^* ? = M_k$. اگر شرط برقرار بود کاربر مقدار h(userid||realm||K) را محاسبه و بسته پاسخ را تولید و به سمت پراکسی ارسال میکند. در سرور نیز این مقادیر محاسبه شده و با مقدار وارده مقایسه میشود. اگر برابر بود تایید به کاربر داده شده و کلید جلسه نیز

$$K = H3(U^x \parallel R_A^x \parallel R_s^x) \quad (32)$$

خواهد بود. شکل ۲ نحوه عملکرد را بصورت کامل نشان میدهد.

۴. تحلیل روش پیشنهادی

در این قسمت امنیت و کارایی روش پیشنهادی احراز هویت SIP ارائه شده ما بررسی میگردد. در شکل ۱ عملکرد روش پیشنهادی مشخص شده است. در ادامه امنیت و کارائی آن بررسی می گردد.

۴-۱. بررسی امنیت

در این قسمت مقاومت در برابر انواع حملات بررسی میشود

۴-۱-۱.مقاومت در مقابل حمله جعل هویت

اثبات: برای یک حمله موفقیت آمیز از نوع حمله جعل عویت , حمله کننده باید پسورد کاربر PWx را بداند تا بتواند از مرحله فاز login عبور کند و پیغام تایید را تفسیر کند. ولی با توجه به روابط زیر :

$$PW_y = h(PW_x \oplus N_r) \quad (29)$$

$$B_A = h(id \oplus PW_y) \quad (30)$$

$$M_A = R_A + t_1 * K_{IDA} \quad (31)$$

$$R_A^* = R_A^* * P \quad (32)$$

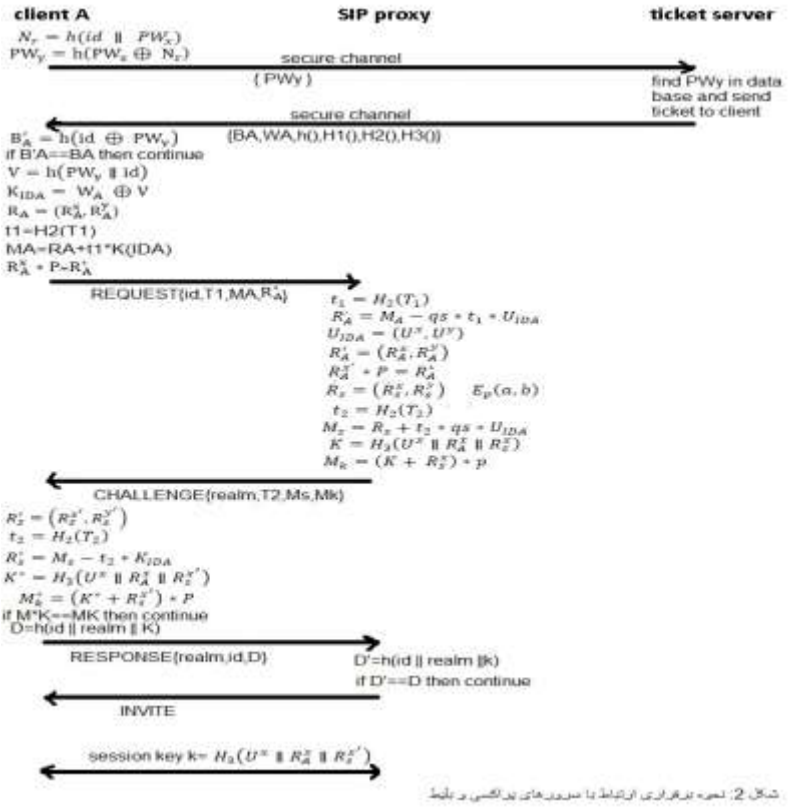
مشخص است که به کمک یک تابع hash یکطرفه و ضرب اسکالر منحنی بیضوی دادهها ارسال شده است و حمله کننده نمیتواند خود را بعنوان یک کاربر واقعی قرار دهد .

۴-۱-۲. مقاومت در مقابل حمله داخلی

یک امر عادی که معمولا کاربران به آن عمل میکنند این است که اگر نرم افزار بخواهد پسورد را ذخیره کند , کاربر برای راحتی خود انرا تائید میکند. اگر یک کاربر داخلی اطلاعات پسورد کاربران را داشته باشد شاید بخواهد جعل هویت کرده و به اطلاعات سایرین دسترسی پیدا کند.

اثبات : پروتکل پیشنهادی ما برای ثبت از کد رمز شده $PW_y = h(PW_x \oplus N_r)$ محاسبه میشود از طریق یک کانال امن ارتباط برقرار میکند. این روش از سرقت پسورد جلوگیری میکند چرا که هیچگاه خود پسورد داخل سیستم نگهداری نشده است.

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸



شکل 2: نحوه برقراری ارتباط با سرورهای پراکسی و بلیط

۴-۱-۳. مقاومت در مقابل حمله نشست های موازی

اثبات:پروتکل ما از کد رمز {Ma,R*a,…, time stamp,RA(RA(x),RA(y))} استفاده میکند به عبارت دیگر حمله نشستهای موازی در این مدل موثر نیست.

۴-۱-۴. مقاومت در مقابل حمله پخش

اثبات: اگر حمله کننده بخواهد همان پیغام را دوباره به سمت کاربر یا سرور مجدا ارسال کند , مشخص است که کاربر نمیتواند موفق شود زیرا عدد تصادفی Ma و R*a که داخل رمز مخفی قرار دارد در هر دفعه متفاوت است. بعلاوه سرور میتواند فقط کاربرانی را احراز هویت کند که

$R_A^* = P * R_A^{x'}$. اگر حمله پخش بخواهد جعل هویت انجام دهد. حمله کننده نمی تواند در مقابل مکانیزم چالش و پاسخ عمل تکراری انجام دهد لذا پروتکل امن است.

۴-۱-۵. مقاومت در مقابل حمله حدس زدن رمز عبور

کاربر فقط بصورت امن میتواند پسورد خود را عوض کند و ضمنا این ثبت در سرور بلیط نیز ثبت شده است. در طرح ما پسورد فقط توسط یک hash یکطرفه با یک عدد تولید شده توسط تابع hash با نام Nr منتقل میشود و داخل سرور اصلی و سرور بلیط ذخیره شده است بنابراین حمله کننده نمتواند پسورد را داخل پیامها حدس بزند.

۴-۲. کارایی

جدول زیر پروتکل ما را در مقابل چند پروتکل دیگر مقایسه میکند

جدول ۲:مقایسه چند مدل با روش پیشنهادی ما.

attack	HTTP digest	Tsai	Yang et al.	H_L_Yeh et al.	Our scheme
Crack/miss smart card resistant	Yes	Yes	Yes	No	Yes
Masquarade attack resistant	no	No	Yes	Yes	Yes
Insider attack resistant	no	No	No	Yes	Yes
Parallel session attack resistant	No	No	Yes	Yes	Yes
Replay attack resistant	Yes	No	Yes	Yes	Yes
Password guessing attack resistant	no	No	Yes	Yes	Yes

همچنین برای مقایسه زمان اجرا باید پارامترهای زیر را ابتدا تعریف کنیم:

جدول ۳: پارامترهای استفاده شده در محاسبه زمان

وظیفه	متغیر
زمان تولید عمل چند جمله ای منحنی بیضوی	t_{EC}
زمان محاسبه تابع یک طرفه hash	t_h
زمان ضرب اسکالر منحنی بیضوی	t_{mu}

در این حالت کل محاسبات مورد نیاز ما برابر است با

$$2t_{EC} + 15t_h + 3t_{mu} \qquad (33)$$

اگر زمان تولید چند جمله ای منحنی بیضوی را مساوی زمان ضرب اسکالر منحنی بیضوی بگیریم لذا در نهایت جدول زیر بدست می آید

جدول۴: ارزیابی زمانهای مصرفی

Operation	HTTP digest	Tsai	Yang et al.	H_L_Yeh et al.	Our scheme
Hash	1	7	7	13	15
Exponential	0	0	4	0	0
ECC computation	0	0	0	12	5

۵. بحث ونتیجه گیری

در این مقاله ما ابتدا روشهای موجود و جدید را بررسی کردیم و سپس طرح جدیدی درست کردیم که به کمک یک سرور بلیط قبتوانیم کارت هوشمند را از طرح Yeh که مربوط به سال ۲۰۱۴ است حذف کنیم.این روش باعث حذف نگهداری کارت هوشمند شده که خود این نگهداری پر خطر است و از طرف دیگر به دلیل هماهنگی با دو سرور مستقل , احتمال نفوذ کمتر شده و سپستم امن تر است. لازم به ذکر است که محیط SIP شبکه اینترنت است که بسیار نا امن می باشد و مدل ما میتواند نسبت به مدلهای قبلی بهتر عمل نماید ولی در اینده میتوان روشهای سریعتر و پیچیده تر طراحی کرد تا پروتکل امن تر شود.

منابع

1. C.C. Yang, R.C. Wang, W.T. Liu, Secure authentication scheme for session initiation protocol, Comp. Secur. 24 (2005) 381–386.
2. Conference on New Trends in Information and Service Science, 2009, pp. 642–647.
3. D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, Survey of security vulnerabilities in session initial protocol, IEEE Commun. Surv. Tutor. 8 (2006) 68–81.
4. Dalgic, H. Fang, Comparison of H.323 and SIP for IP Telephony Signaling, in Proc. Of Photonics East, SPIE, Boston, Massachusetts, Sept. 1999.
5. Durlanik, I. Sogukpinar, SIP authentication scheme using ECDH, World Enformatika Soc. Trans. Eng. Comput. Technol. 8 (2005) 350–353.
6. E.J. Yoon, E.K. Ryu, K.Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 50 (2004) 612–614.
7. E.J. Yoon, K.Y. Yoo, Cryptanalysis of DS-SIP authentication scheme using ECDH, International
8. H.-L. Yeh, et al., Robust smart card secured authentication scheme on SIP using Elliptic Curve Cryptography, Comput.Stand. Interfaces , Elsevier. 36 (2014) 397-402.
9. J. Rosenberg, H. Schulzrinne, G. Camarillo, SIP: session initiation protocol, request for comments: 3261, Internet Engineering Task Force, June 2002.

10. L. Kong, V.A. Balasubramaniyan, M. Ahamad, L. Kong, V.A. Balasubramaniyan, M. Ahamad, A lightweight scheme for securely and reliably locating SIP users, The 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe 2006), 2006, pp. 9–17.
11. M. Handley, H. Schulzrinne, E. Schooler, C. Tech, J. Rosenberg, L. Bell, SIP: session initiation protocol, IETF RFC2543, Mar. 1999..
12. M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (2000) 28–30.
13. W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 22 (1976) 644–654.

مطالعات علوم کاربردی در مهندسی

دوره ۳، شماره ۱، بهار ۱۳۹۶، صفحات ۱۷۱- ۱۵۸

A New Voice Authentication Technique through Integration of Elliptic Curve with Ticket Server

Mohammad Sharaf Farahani

M.Sc of computer engineering- software, Ferdowsi University of Mashhad.

Abstract

The Voice over Internet Protocol (VOIP) systems are growing more rapidly in today's world and Session Initiation Protocol (SIP) has widespread use and is very important in this regard. Session Initiation Protocol uses signaling to perform its control actions and uses the hypertext authentication protocol to achieve this. The SIP protocol under the IETF standard has been described in detail in the RFC 3261 version. Considering that the SIP protocol is being used widely in VOIP equipment, most of the attacks have been focused on this protocol.

Our attempt in this article is to strengthen the authentication mechanism of this protocol and to remove its weaknesses. Using the Elliptic curve cryptography (ECC) method and integrating it with an auxiliary ticket server, we improve the security and increase resistance against the attacks. We will show in our analysis that this approach is better than the previous approaches.

Keywords: authentication, Elliptic Curve, Session Initiation Protocol, hypertext abstract.