ارائه پروتکلی جامع و سبک وزن برای احرازهویت دو طرفه دستگاه‌های VoIP مبتنی بر کارت هوشمند

مهدی نیکوقدم[۱]، هاله امین‌طوسی[۲]

[۱]دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری، دانشگاه فردوسی مشهد

[۲]استادیار دانشکده مهندسی، دانشگاه فردوسی مشهد، amintoosi@um.ac.ir

چکیده

همزمان با فراگیری استفاده از فناوری صوت بر روی IP (VoIP) برای انتقال داده‌های چند رسانه‌ای نظیر صوت و تصویر، پروتکل برقراری نشست (SIP)، در مرکز توجه بسیاری از تحقیقات قرار گرفته است. برای برقراری یک کانال ارتباطی امن بین دو طرف ارتباط با استفاده از SIP، احرازهویت طرفین از اهمیت بالا یی برخوردار است. در سال‌های اخیر، پژوهش‌های زیادی در زمینه پروتکل‌های احرازهویت انجام شده است که از جمله می‌توان طرحی سبک وزن برای احرازهویت در VoIP را که توسط ژنگ و همکاران ارائه شده نام برد. در این مقاله ابتدا اثبات خواهیم کرد طرح ژنگ در برابر حملات افشای پارامترهای تصادفی و منع سرویس مقام نیست و نیاز امنیتی محرمانگی رو به جلو را تامین نمی‌کند. در ادامه، پروتکلی سبک وزن وکارآمد ارائه کرده‌ایم و نشان داده‌ایم که پروتکل پیشنهادی در مقابل حملات مختلف مقاوم است و قادر به تامین نیازمندی‌های امنیتی اساسی همانند محرمانگی روبه جلو و گمنامی کاربر می باشد. همچنین عملکرد پروتکل پیشنهادی را به لحاظ پیچیدگی محاسباتی مورد بررسی قرار داده و نشان داده ایم که روش پیشنهادی در مقایسه با اغلب روشهای مشابه، دارای پیچیدگی محاسباتی کمتری می‌باشد. در نهایت، صحت پروتکل پیشنهادی را با ابزارهای رسمی Scyther و Proverif اثبات نموده‌ایم.

کلیدواژه

احرازهویت، Proverif ،Scyther ،VoIP ،SIP

مقدمه

سازمان Internet Engineering Task Force در سال ۱۹۹۹ پروتکلی برای برقراری جلسه که مبتنی بر استاندارد RFC۲۵۴۳ بود را ارائه داد[۱] که از آن، برای ارتباطات صوت بر روی IP یا VoIP[۱] نیز استفاده می‌شود. پروتکل برقراری جلسه یا SIP[۲] یکی از محبوب‌ترین پروتکل‌های علامت‌دهی است که برای برقراری، مدیریت و خاتمه ارتباط بین طرفین به کار می‌رود. این پروتکل، یک پروتکل لایه کاربرد بوده و با توجه به وظیفه آن، که برقراری و مدیریت جلسه است در لایه پایین تر، از TCP که پروتکلی اتصال‌گرا و قابل اعتماد است استفاده می‌کند. از رقبای SIP می‌توان به پروتکل‌های H.۳۲۳، MGCP و Megaco اشاره کرد.

به طور خلاصه، عملکرد پروتکل SIP در سیستم VoIP شامل ۴ مرحله ثبت‌نام، برقراری تماس، تبادل داده و خاتمه تماس می‌باشد[۲].

در مرحله ثبت نام، قبل از شروع جلسه، هر کدام از طرفین ارتباط پیغام REGISTER را برای سرویس‌دهنده ثبت‌نام ارسال نموده و مشخصات مکان کنونی خود را ثبت می‌کنند. سپس در مرحله برقراری تماس برای شروع مکالمه، کاربری که قصد تماس گرفتن را دارد یک پیغام INVITE برای سرویس‌دهنده‌ای که در آن ثبت‌نام کرده ارسال می‌کند و اعلام می‌کند که می‌خواهد با این شماره تماس بگیرد. سپس خدمات‌دهنده، مکان کاربر طرف مقابل یعنی مقصد تماس را پیدا کرده و پیام INVITE را برای او ارسال می‌کند. وقتی که پیام INVITE به کاربر مقصد می‌رسد، پیام‌های TRYING، RINGING و OK مبادله شده و در نهایت، مقصد ارتباط، پیام ACK را برای کاربر شروع‌کننده ارتباط می‌فرستد.

در مرحله تبادل داده‌ها، نوبت به پروتکل RTP[۳] خواهد رسید و داده‌ها به صورت انتها به انتها بین مبدا و مقصد مبادله می‌شوند. در نهایت در مرحله خاتمه تماس، بعد از مبادله اطلاعات، هر یک از طرفین می‌توانندپیام BYE را به عنوان درخواست خاتمه

---

[۱] Voice over Internet Protocol

[۲] Session Initiation Protocol

[۳] Real-time Transport Protocol

تماس برای طرف مقابل ارسال کنند و در جواب آن زمانی که پیغام OK را دریافت کنند ارتباط خاتمه می‌یابد.

مهم‌ترین بحث امنیتی در مورد پروتکل SIP، بحث احراز هویت است که در تمامی مراحل ذکر شده در بالا دارای اهمیت بسزایی است. در مرحله ثبت‌نام، در زمان برقراری تماس، باید با استفاده از مکانیزم‌های احرازهویت، از ثبت‌نام کاربران غیر مجاز جلوگیری شود. همچنین، در زمان برقرای تماس باید با پیام INVITE، هر یک از طرفین، ارتباط هویت واقعی طرف مقابل را شناسایی کند. در نهایت در مرحله خاتمه تماس، در زمان اتمام یک جلسه با پیام BYE یاCANCEL، باز هم باید هویت کاربر فرستنده این چنین پیامی برای طرف مقابل تائید شود.

از طرفی در بحث برقراری تماس از طریق شبکه VoIP، یکی از مسائلی که اهمیت بسزایی دارد بحث کم شدن تاخیر در تماس می‌باشد. به همین دلیل، ایجاد کلید نشست در ابتدای کار به طوری که طرفین بتوانند در ادامه ارتباط از طریق این کلید نشست، با هم ارتباط داشته باشند اهمیت به سزایی دارد.

با توجه به مطالبی که در بالا گفته شد، فرایند تصدیق هویت و توافق کلید در پروتکل SIP از نظر امنیتی از اهمیت بالایی برخوردار است. به همین دلیل، تحقیقات و پژوهش‌های زیادی در احراز هویت و توافق کلید در شبکه‌های VoIP انجام شده است[۸-۶][۵][۴][۳].

در این مقاله، ابتدا به بررسی و تحلیل طرح احزار هویت و تبادل کلید ژنگ و همکاران[۹] می‌پردازیم و نشان میدهیم که این طرح در برابر حمله افشای پارامترهای تصادفی[۱۳-۱۰] و حمله منع سرویس مقاوم نیست و نیاز امنیتی محرمانگی رو به جلو[۱۰] را تامین نمی‌کند. در ادامه، پروتکلی امن و کارا برای احراز هویت و تبادل کلید در VoIP ارائه خواهیم نمود و با استفاده از تحلیل رسمی و غیررسمی نشان خواهیم داد که پروتکل پیشنهادی در مقابل حملات مختلف، مقاوم است. همچنین نشان خواهیم داد که پروتکل پیشنهادی به لحاظ پیچیدگی زمانی، عملکرد بهتری نسبت به پروتکل های مشابه دارد.

ساختار مقاله به شرح زیر است: در ابتدا در بخش کارهای پیشین به بررسی کارهای گذشته می‌پردازیم. سپس در بخش بررسی و تحلیل طرح ژنگ و همکاران، طرح ژنگ و همکاران[۹] را مورد بررسی و تحلیل قرار می‌دهیم. در ادامه در بخش پروتکل پیشنهادی، پروتکلی بهبود یافته و امن برای احراز هویت و تبادل کلید ارائه خواهیم داد که در برابر حملات مختلف مقاوم است. در ادامه ابتدا در بخش تحلیل امنیتی پروتکل پیشنهادی به تحلیل امنیتی غیررسمی پروتکل پیشنهادی خواهیم پرداخت و در بخش اثبات رسمی امنیت پروتکل پیشنهادی با استفاده از ابزارهای Scyther و Proverif، پروتکل پیشنهادی خود را با ابزارهای رسمی Scyther [۱۴] و Proverif [۱۵] مورد تحلیل و بررسی قرار خواهیم داد. همچنین در تحلیل و مقایسه پیچیدگی زمانی و سخت افزاری طرح پیشنهادی و دیگر طرح‌های مشابه، پروتکل پیشنهادی را از نظر پیچیدگی زمانی با دیگر پروتکل‌های مشابه مقایسه خواهیم کرد. در نهایت، به نتیجه‌گیری و کارهای آینده می‌پردازیم.

کارهای پیشین

در سال ۲۰۰۵ دورلانیک و همکاران[۱۶] یک رویکرد جدید برای احرازهویت امن SIP با استفاده از رمزنگاری منحنی بیضوی ارائه نمودند. یون و همکاران[۱۷] در سال ۲۰۱۰ نشان دادند که طرح احرازهویت دورلانیک و همکاران در برابر حمله حدس رمزعبور[۴] و حمله Denning-Sacco و حمله دزدیده شدن تایید کننده‌ها [۵] مقاوم نیست. آن‌ها همچنین یک طرح احرازهویت امن و مناسب برای برای شبکه‌های VoIP ارائه دادند.

در سال ۲۰۱۴ ژَنگ و همکاران[۱۸] طرحی برای احرازهویت و توافق کلید در SIP مبتنی بر رمز عبور و کارت هوشمند ارائه دادند که نیاز به ذخیره‌سازی رمز عبور کاربران در خدمات‌دهنده ندارد. همچنین در سال ۲۰۱۴، فراش[۱۹] روشی امن برای احرازهویت و توافق کلید در SIP ارائه کرد و ادعا کرد که در برابر اکثر حملات مقاوم است. اما در سال ۲۰۱۵ کوماری و همکاران[۲۰] طرحی دو فاکتوره ارائه دادند که بر پایه مسئله سخت منحنی بیضوی[۶] استوار بود. همچنین آن‌ها اثبات کردند که طرح فراش[۱۹] گمنامی و حریم خصوصی کاربر را فراهم نمی‌کند و در برابر حمله لو رفتن پارامترهای تصادفی یک جلسه و حمله حدس رمز عبور، آسیب پذیر است.

پس از مدتی ژنگ و همکاران[۲۱] نشان دادند که روش ارائه شده قبلی آنها[۱۸] در برابر حمله جعل هویت مقاوم نیست و پروتکل توسعه‌یافته‌ای با استفاده از کارت هوشمند ارائه دادند. در سال ۲۰۱۵ ژیانگ و همکاران[۲۲] نشان دادند که طرح[۱۸] در برابر حمله داخلی آسیب پذیر است و برای حل این مشکل طرح جدیدی را ارائه نمودند.

در سال ۲۰۱۵ تو و همکاران[۲۳] نشان دادند که طرح ژنگ و همکاران[۱۸] در برابر حمله جعل هویت مقاوم نیست و یک طرح بهبود یافته ارائه دادند و ادعا کردند که هزینه محاسباتی

---

[۴] off-line password guessing attacks

[۵] stolen-verifier attacks

[۶] elliptic curve discrete logarithm problem

طرح آن‌ها حدود ۷۵درصد هزینه محاسباتی طرح ژنگ و همکاران است. در سال ۲۰۱۶، فراش و همکاران[۲۴] ادعا کردند که طرح تو و همکاران هنوز هم در برابر حمله جعل هویت مقاوم نیست و همچنین در برابر حمله تغییر رمزعبور آسیب‌پذیر است و طرح بهبود یافته‌ای ارائه دادند. در سال ۲۰۱۷ چادری و همکاران[۲۵] ثابت کردند که طرح[۲۳] در برابر حملات جعل هویت خدمات‌دهنده و حمله تکرار و همچنین حمله منع سرویس مقاوم نیست و نیاز امنیتی گمنامی کاربر را تامین نمی‌کند. آنها همچنین ادعا کردند که طرح فراش و همکاران[۲۴] گمنامی کاربر را تامین نمی‌کند و مستعد حمله تکرار است. همچنین میشرا و همکاران[۲۶] طرح تو و همکاران[۲۳] را مورد بررسی قرار داده و ضعف امنیتی آن را دربرابر حمله مرد میانی نشان دادند. همچنین برای رفع این ضعف امنیتی، پروتکلی ارائه کرده و آن را از نظر سربار محاسباتی با طرح تو و همکاران[۲۳] مقایسه نمودند. در سال ۲۰۱۶، فراش و عطاری [۲۷] طرحی برای احرازهویت SIP ارائه دادند که در سال ۲۰۱۷ توسط لو و همکاران[۲۸] مورد بررسی قرار کرفت و نشان داده شد که طرح فراش و عطاری[۲۷] در برابر حمله حدس رمزعبور مقاوم نیست. نویسندگان سپس یک طرح بر اساس رمزنگاری منحنی بیضوی ارائه دادند و ادعا کردند که در برابر حملات مختلف مقاوم است. همچنین در سال ۲۰۱۶، لو و همکاران[۲۹] طرحی برای احراز هویت SIP ارائه دادند که در سال ۲۰۱۸ توسط سورش کومار و همکاران[۳۰] مورد تحلیل قرار گرفت و نشان داده شد که قادر به تامین گمنامی کاربر نیست و در برابر حملات جعل هویت کاربر و جعل هویت خدمات‌دهنده آسیب پذیر است. لذا آن‌ها طرحی بهبود یافته برای احرازهویت و توافق کلید ارائه دادند. سپس در سال ۲۰۱۹، سوراو و همکاران[٤] محدودیت‌های طرح سورش کومار و همکاران[۳۰] را نشان دادند و طرحی بهبود یافته بدون افزایش هزینه محاسباتی ارائه نمودند. همچنین در سال ۲۰۱۶ ژنگ و همکاران[۳۱] طرحی برای احراز هویت sip ارائه دادند که روانبخش و همکاران[۱۰] اثبات کردند که ژنگ و همکاران نیاز امنیتی محرمانگی رو به جلو را تامین نمی‌کنند. کیو و همکاران[۳۲] در سال ۲۰۱۸ طرحی در مورد تامین نیاز امنیتی محرمانگی رو به جلو در پروتکل‌های SIP ارائه دادند که ژنگ و همکاران[۹] در سال ۲۰۱۹ ضمن بررسی ایرادات امنیتی طرح کیو و همکاران[۳۲]، طرح بهبود یافته‌ای ارائه دادند. در این مقاله اثبات خواهیم کرد که طرح ژنگ و همکاران[۹]، در برابر حمله افشای پارامترهای تصادفی [۷] و حمله منع سرویس ، مقاوم نیست و نیاز امنیتی محرمانگی رو به جلو [۸] را تامین نمی‌کند.

بررسی و تحلیل طرح ژنگ و همکاران

در این بخش، روش ارائه شده توسط ژنگ و همکاران[۹] بطور خلاصه ارائه شده و ضعف های امنیتی آن بیان می گردد. جدول ۱ نمادهای بکار رفته در پروتکل ارائه شده در طرح ژنگ و همکاران[۹] را نشان می‌دهد.

جدول ۱. نمادهای به کار رفته در طرح [۹]

توضیحات	نماد
کاربر	U
خدمات‌دهنده	S
شناسه کاربر	ID
رمزعبور انتخابی کاربر	PW
کلید محرمانه خدمات‌دهنده	S_p
کلید نشست ایجاد شده بین طرفین	sk
عملگر XOR	$\oplus$
عملگر الحاق دو رشته	$\|\|$

در طرح ژنگ و همکاران[۹]، کاربر ابتدا شناسه ID و رمز عبور PW و عدد r را برای خود انتخاب می‌کندو پارامترهای VPw و HId را بر طبق روابط (۱) و (۲) محاسبه نموده و پارامترهای VPw و HId بر روی کانال امن برای خدمات‌دهنده ارسال می‌کند.

$$VPw=h(PW||ID||r) \quad (۱)$$
$$HId=h(ID\oplus r) \quad (۲)$$

خدمات‌دهنده با دریافت پارامترهای VPw و Hid، پارامترهای N و R را طبق روابط (۳) و (۴) می‌سازد سپس پارامترهای N و HId را درون حافظه خود و پارامتر R را درون کارت هوشمند ذخیره می‌کند و در نهایت کارت هوشمند را برای کاربر بر روی کانال امن ارسال می‌کند.

$$N=VPw\oplus h(S_p||HId) \quad (۳)$$
$$R=h(S_p \oplus VPw) \quad (۴)$$

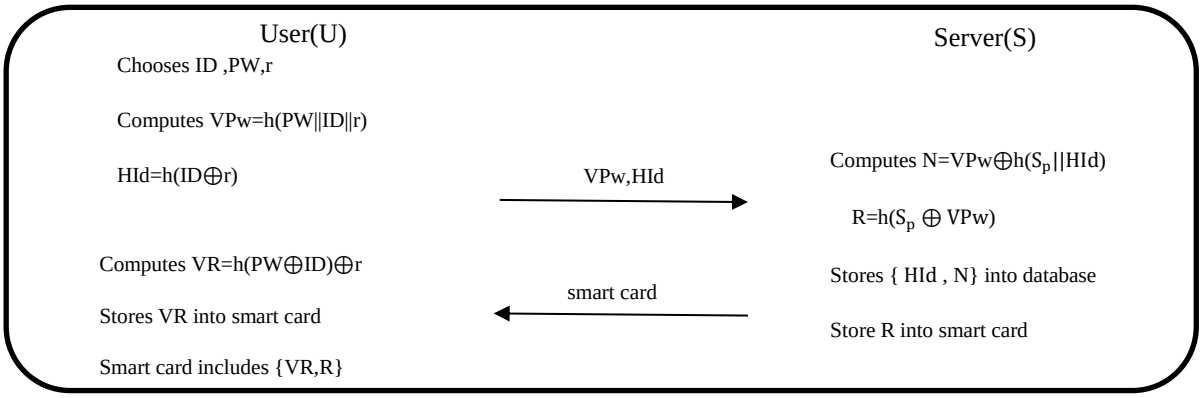
کاربر به محض دریافت کارت هوشمند، پارامتر VR را از رابطه (۵) محاسبه می‌کند و درون کارت هوشمند قرار می‌دهد. در نهایت در مرحله ثبت‌نام، پارامترهای VR و R درون کارت هوشمند قرار دارند. مراحل گفته شده در شکل ۱ نشان داده شده اند.

$$VR=h(PW\oplus ID)\oplus r \quad (۵)$$

در مرحله احراز هویت، ابتدا کاربر، شناسه و رمز عبور خود را وارد می‌کند و سپس پارامتر r' از رابطه (۶) و همچنین پارامترهای

---

[۷] Known-session-specific Temporary Information Attack
[۸] perfect forward secrecy



شکل۲ .مرحله ثبت‌نام طرح ژنگ و همکاران [۹]

HId' وVPw' از روابط (۷) و (۸) توسط کارت هوشمند محاسبه می‌شود.

$$=VR\oplus h(PW\oplus ID)r' \quad (۶)$$
$$HId'=h(ID\oplus r') \quad (۷)$$
$$VPw'=h(pw||ID||r') \quad (۸)$$

در ادامه، عدد تصادفی r_a را انتخاب و روابط (۹) و (۱۰) را محاسبه می‌کند و در نهایت پارامترهای $Auth_u$وCوHId' را برای خدمات‌دهنده ارسال می‌نماید.

$$C=h(R\oplus VPw')\oplus r_a \quad (۹)$$
$$Auth_u = h(r_a \oplus HId' \oplus VPw') \quad (۱۰)$$

حال خدمات‌دهنده، ابتدا پارامترN را از کارت هوشمند استخراج می‌کند و سپس VPw'' و R' و r'_a را طبق روابط (۱۱)، (۱۲) و (۱۳) محاسبه می‌کند. سپس با مقایسه $?= h(r'_a \oplus Auth_u \oplus HId' \oplus VPw'')$ هویت کارت هوشمند و کاربر برای خدمات دهنده احراز می‌شود. حال خدمات‌دهنده عدد تصادفی r_b را انتخاب می‌کند و کلید نشست را طبق رابطه (۱۴) می‌سازد.

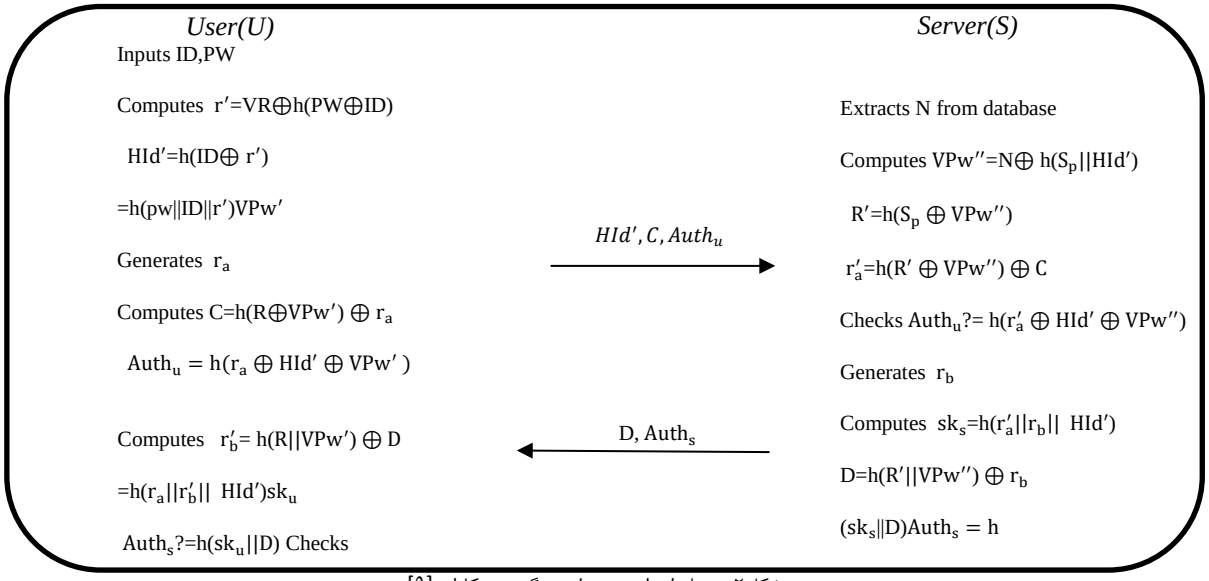
در انتها پارامترهای D و$Auth_s$ *را برای کارت هوشمند ارسال می‌کند*.سپس روابط (۱۵)(۱۶) را محاسبه می‌کند. و در انتها پارامترهای D و$Auth_s$ *را برای کارت هوشمند ارسال می‌کند.*

$$=N\oplus h(S_p||HId')VPw'' \quad (۱۱)$$
$$=h(S_p \oplus VPw'')R' \quad (۱۲)$$
$$=h(R' \oplus VPw'') \oplus Cr'_a \quad (۱۳)$$
$$=h(r'_a||r_b||\ HId')sk_s \quad (۱۴)$$
$$D=h(R'||VPw'') \oplus r_b \quad (۱۵)$$
$$(sk_s||D)Auth_s = h \quad (۱۶)$$

کارت هوشمند به محض دریافت پارامترهای D و$Auth_s$ ابتدا پارامترr'_b را از رابطه (۱۷) محاسبه نموده و سپس کلید نشست را از رابطه (۱۸) محاسبه می‌کند و سپس با مقایسه $?=h(sk_u||D)Auth_s$ خدمات‌دهنده را احرازهویت می‌نماید.

$$= h(R||VPw') \oplus Dr'_b \quad (۱۷)$$
$$=h(r_a||r'_b||\ HId')sk_u \quad (۱۸)$$

شمای کلی مرحله احراز هویت طرح ژنگ و همکاران در شکل ۲ قابل مشاهده است.



شکل۲ .مرحله احرازهویت طرح ژنگ و همکاران [۹]

حملات وارده به طرح ژنگ و همکاران [۲۰]

حمله افشای پارامترهای تصادفی[۹]: بر طبق مقالات[۱۳-۱۰] حمله ای وجود دارد که بر طبق آن، اگر اعداد تصادفی پروتکل لو بروند و به دست مهاجم بیفتند، مهاجم نباید قادر باشد به کلید نشست برسد. در پروتکل ژنگ وهمکاران[۹] ، اگر فرض بر این باشد که اعداد موقتی یا تصادفی r_a و r_b به دست مهاجم بیفتد، از آنجایی که HId' بر روی کانال عمومی رد و بدل میشود، مهاجم می‌تواند به کلید نشست sk_s=$h(r'_a||r_b||\ HId')$ برسد چرا که به تمامی پارامترهای آن دسترسی دارد.

عدم تامین نیاز امنیتی محرمانگی رو به جلو: در حمله محرمانگی رو به جلو فرض بر ان است که اگر پارامترهای طولانی مدت مانند کلید خصوصی خدمات دهنده لو برود و دست مهاجم بیفتد، مهاجم نتواند به کلید نشست برسد[۱۰]. در ادامه، اثبات خواهیم کرد که اگر کلید محرمانه خدمات‌دهنده لو برود مهاجم می‌تواند به کلید نشست برسد.

مرحله ۱: فرض کنید کلید محرمانه خدمات‌دهنده یعنی S_p لو برود. از آنجایی که HId' بر روی کانال عمومی رد و بدل می‌شود مهاجم می‌تواند با استفاده از آن در پایگاه داده جستجو کند و Nمعادل آن را به دست بیاورد.

مرحله۲: طبق فرض مهاجم S_p را دارد و همچنین HId' که بر روی کانال عمومی قرار دارد، از طرفی طبق مرحله۱ مهاجم پارامتر N را دارد. حال از آن‌جایی که در رابطه $N=h(S_p||HId')\oplus VPw''$ مهاجم تمامی پارامترها را دارد، می‌تواند VPw'' را محاسبه کند.

مرحله۳: طبق فرض، مهاجم کلید محرمانه یعنی S_p را دارد، همچنین پارامتر VPw'' را طبق مراحل ۱ و ۲ به دست آورده، در نتیجه در رابطه $R'=h(S_p \oplus VPw'')$ می‌تواند پارامتر R' را محاسبه کند.

مرحله۴: از آنجایی که پارامتر C بر روی کانال عمومی رد و بدل می‌شود و همچنین طبق مراحل ۱ و ۲ و۳ مهاجم از رابطه $Cr'_a=h(R' \oplus VPw'') \oplus Dr'_a$ می‌تواند به r'_a که برابر با r_a هست دست پیدا کند.

مرحله۵: از آنجایی که $R'=R$ و $VPw''=VPw'$ ، همچنین به علت اینکه پارامتر D بر روی کانال عمومی ارسال می‌شود طبق مراحل ۱ تا ۴ و همچنین رابطه $h(R||VPw') \oplus Dr'_b$ = مهاجم می‌تواند تمامی پارامترهای کلید نشست یعنی sk_u=$h(r_a||r'_b||\ HId')$ را به دست آورده و آن را بسازد.

حمله منع سرویس: از آنجایی که در پروتکل هیچ مُهر زمانی استفاده نشده است، در زمانی که پیغام $Auth_u$ و C_i و HId' فرستاده می‌شود، خدمات دهنده، اطلاعاتی را در پایگاه داده جستجو می‌کند در نتیجه مهاجم میتواند با تکرار این پیغام، باعث این شود که خدمات دهنده مشغول شده و اصطلاحاً حمله منع سرویس اتفاق بیفتد.

پروتکل پیشنهادی

در این بخش، به معرفی پروتکل پیشنهادی خواهیم پرداخت. پروتکل پیشنهادی، شامل سه مرحله ثبت‌نام، احرازهویت و تغییر رمزعبور است که در ادامه هر یک را به تفضیل توضیح خواهیم داد. جدول ۲ نمادهای به کار رفته در پروتکل پیشنهادی را نمایش می‌دهد.

جدول۲. نمادهای به کار رفته در طرح پیشنهادی

توضیحات	نماد
کاربر	U
خدمات‌دهنده	S
شناسه کاربر	ID_i
رمزعبور انتخابی کاربر	PW_i
کلید محرمانه خدمات‌دهنده	x
کلید نشست ایجاد شده بین طرفین	SK
عملگر XOR	$\oplus$
تابع درهم ساز یک طرفه	h(.)
رمزنگاری و رمزگشایی	E(.)/D(.)
عملگر الحاق دو رشته	||

مرحله ثبت‌نام

در ابتدا کاربر، شناسه ID، رمز عبور PW_i و عدد تصادفی a_i را انتخاب می‌کند. سپس پارامتر MPW_i را از رابطه (۱۹) محاسبه می‌کند. در نهایت پارامترهای ID_i, MPW_i, a_i را بر روی کانال امن، برای خدمات‌دهنده ارسال می‌کند.

$$=h(ID_i||h(PW_i \oplus a_i)) \oplus PW_i MPW_i \qquad (۱۹)$$

خدمات‌دهنده به محض دریافت پارامترهای ID_i و MPW_i و a_i، ابتدا عدد تصادفی b_i را تولید می‌کند. سپس روابط (۲۰) تا (۲۴) را محاسبه نموده و در ادامه، پارامترهای HID_i و b_i و H_i را با طبق رابطه (۲۴) با کلید محرمانه خودش رمز می‌کند. در انتها،

[۹] Known-session-specific Temporary Information Attack

پارامترهای b_i وq_i وD_i وH_i را درون کارت هوشمند ذخیره نموده و کارت هوشمند را بر روی کانال امن برای کاربر ارسال می‌نماید.

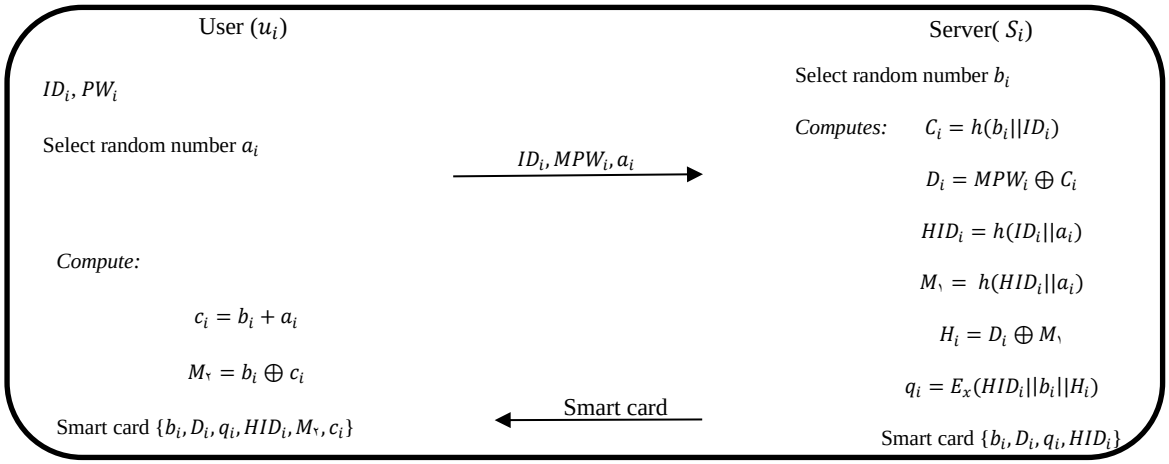
$$C_i = h(b_i||ID_i) \quad (۲۰)$$
$$D_i = MPW_i \oplus C_i \quad (۲۱)$$
$$HID_i = h(ID_i||a_i) \quad (۲۲)$$
$$H_i = D_i \oplus M_۱ \quad (۲۳)$$
$$q_i = E_x(HID_i||b_i||H_i) \quad (۲۴)$$

کاربر به محض دریافت کارت هوشمند، روابط (۲۵) و (۲۶) را محاسبه نموده و پارامترهای c_i و$M_۲$ را درون کارت هوشمند ذخیره می‌کند. به این ترتیب، همانطور که در شکل ۳ مشاهده می‌شود، مرحله ثبت‌نام به پایان می‌رسد.

$$c_i = b_i + a_i \quad (۲۵)$$
$$M_۲ = b_i \oplus c_i \quad (۲۶)$$

مرحله احرازهویت:

در مرحله احرازهویت، کاربر، کارت هوشمند خود را وارد دستگاه کارت‌خوان نموده، شناسه و رمز عبور PW_i^* وID_i^* خود را وارد می‌کند. سپس کارت هوشمند، روابط (۲۷) تا (۳۰) را محاسبه و با مقایسه $D_i^* ?= D_i$ مشخص می‌شود که کارت به سرقت نرفته است و در اختیار صاحب اصلی آن است. سپس، روابط (۳۱) تا (۳۳) محاسبه شده و درنهایت، کارت هوشمند، پارامترهای $M_۱$ وG_i، b_i،q_i را برای خدمات‌دهنده بر روی کانال عمومی ارسال می‌کند



شکل ۳.مرحله ثبت‌نام طرح پیشنهادی

$$a_i = c_i - b_i \quad (۲۷)$$
$$=h(ID_i^*||h(PW_i^* \oplus a_i)) \oplus PW_i^* MPW_i^* \quad (۲۸)$$
$$C_i^* = h(b_i||ID_i^*) \quad (۲۹)$$
$$D_i^* = MPW_i^* \oplus C_i^* \quad (۳۰)$$
$$HID_i = h(ID_i||a_i) \quad (۳۱)$$
$$G_i = HID_i \oplus c_i \quad (۳۲)$$
$$M_۱ = h(HID_i||a_i) \quad (۳۳)$$

خدمات دهنده به محض دریافت پیام، ابتدا تازگی پیام را مورد بررسی قرار می‌دهد سپس پارامتر q_i را از آنجایی که با کلید خدمات‌دهنده، سپس، عدد تصادفی $N_۱$ را انتخاب نموده، سپس روابط (۳۷)و(۳۸)و(۳۹)و(۴۰) را محاسبه می‌کند و در نهایت پارامترهای $M_۴$ و$M_۵$ را برای کارت هوشمند ارسال می‌کند.

$$=h(N_۱||M_۱)M_۲ \quad (۳۷)$$
$$=H_i \oplus M_۱ D_i \quad (۳۸)$$
$$= D_i \oplus N_۱ M_٤ \quad (۳۹)$$
$$h(N_۱||D_i)M_۵ = \quad (۴۰)$$

کارت هوشمند به محض دریافت پیام، ابتدا تازگی پیغام را بررسی می‌کند و سپس روابط (۴۰) و (۴۱) را محاسبه می‌کند و در صورتی که $M_۵$ ارسالی با $M_۵$ محاسبه شده برابر باشد در این صورت، اصالت پیغام ارسالی محرز می‌شود و هویت خدمات‌دهنده تایید خواهد شد.

$$= D_i \oplus M_٤ N_۱ \quad (۴۱)$$
$$h(N_۱||D_i)M_۵' = \quad (۴۲)$$

حال، کارت هوشمند، عدد تصادفی $N_۲$ را انتخاب و روابط (۴۳) تا (۴۶) را محاسبه میکند. سپس عدد تصادفی $N_۳$ را انتخاب و رابطه (۴۷) محاسبه می‌شود. پس از آن، بر طبق رابطه (۴۸)، کلید نشست در سمت کارت هوشمند/کاربر ساخته می‌شود. در نهایت، پارامترهای$M_۸$، $M_۱۰$، $M_۹$ را کارت هوشمند از طریق کانال عمومی و ناامن برای خدمات‌دهنده ارسال می‌کند.

$$M_٦ = h(N_۲||M_٤) \quad (٤۳)$$
$$M_۷ = N_۱ \oplus N_۲ \quad (٤٤)$$
$$M_۸ = M_۷ \oplus N_۱ \quad (٤٥)$$
$$h(N_۲||M_۵)M_۹ = \quad (٤٦)$$
$$M_{۱۰} = N_۲ \oplus N_۳ \quad (٤۷)$$
$$SK=h(M_٦||N_۲||HID_i||N_۳) \quad (٤۸)$$

تایید خواهد شد.کارت هوشمند به محض دریافت پیام، ابتدا تازگی پیغام را بررسی می‌کند و سپس روابط (۴۰) و (۴۱) را محاسبه می‌کند و در صوتی که $M_۵$ ارسالی با $M_۵$ محاسبه شده برابر باشد در این صورت، اصالت پیغام ارسالی محرز می‌شود و هویت خدمات‌دهنده تایید خواهد شد.

خدمات‌دهنده به محض دریافت پیام، ابتدا تازگی پیام را بررسی نموده و سپس روابط (۴۹) و (۵۰) و (۵۱) را محاسبه می‌کند. در صورتی که M_9 ارسال شده با M_9 ساخته شده برابر باشد در این صورت صحت پیام ارسال شده تایید، و کارت هوشمند/کاربر احراز هویت می‌شود.

$$M_7 = M_8 \oplus N_1 \quad (49)$$
$$N_2 = N_1 \oplus M_7 \quad (50)$$
$$M_9' = h(N_2||M_5) \quad (51)$$

خدمات‌دهنده، روابط (۵۲) و (۵۳) را محاسبه می‌کند و درنهایت همانطور که در شکل ۴ مشاهده می‌شود، کلید نشست را از رابطه (۵۴) محاسبه خواهد کرد.

$$N_3 = N_2 \oplus M_{10} \quad (52)$$
$$M_6 = h(N_2||M_4) \quad (53)$$
$$SK = h(M_6||N_2||HID_i||N_3) \quad (54)$$

مرحله تغییر رمز عبور:

در این مرحله، ابتدا کاربر شناسه و رمز عبور قدیمی خود را وارد می‌کند. کارت هوشمند، روابط (۲۷) تا (۳۰) را محاسبه می‌کند و در صورتی که $D_i^* ? = D_i$ برقرار باشند، مشخص می‌شود که کارت هوشمند به سرقت نرفته است. حال کاربر، درخواست تغییر رمزعبور را داده، رمزعبور جدید را وارد می‌کند و روابط (۵۵) تا (۵۸) محاسبه خواهد شد. در نهایت، D_i^{**} جایگزین D_i درون کارت هوشمند می‌شود.

$$a_i = c_i - b_i \quad (55)$$
$$= h(ID_i^{**}||h(PW_i^{**} \oplus a_i)) \oplus PW_i^{**} MPW_i^{**} \quad (56)$$
$$C_i^* = h(b_i||ID_i^*) \quad (57)$$
$$D_i^{**} = MPW_i^{**} \oplus C_i^* \quad (58)$$

تحلیل امنیتی غیررسمی پروتکل پیشنهادی:

تامین نیاز امنیتی محرمانگی رو به جلو: در این نیاز امنیتی، فرض بر این است که اگر پارامترهای طولانی مدت مانند کلید محرمانه خدمات دهنده لو برود، باز هم مهاجم نباید قادر باشد به کلید نشست دست پیدا کند. از آنجایی که درون کلید نشست، پارمترهای N_3 و N_2 وجود دارد که حتی با لو رفتن کلید محرمانه خدمات دهنده، امکان رسیدن به آن‌ها وجود ندارد در نتیجه نیاز امنیتی محرمانگی رو به جلو تامین می‌شود.

حمله افشای پارامترهای تصادفی: در این حمله، فرض بر این است که اگر مهاجم بتواند به پارامترهای تصادفی دست پیدا کند، نباید این امکان وجود داشته باشد که به کلید نشست دست پیدا کند. حال اگر پارامترهای تصادفی N_3 و N_2 و N_1 لو بروند، مهاجم امکان رسیدن به کلید نشست را ندارد چراکه در کلید نشست، پارامتر HID_i وجود دارد که تنها در صورت لو رفتن کلید محرمانه خدمات دهنده می‌توان به آن رسید. در نتیجه امکان چنین حمله‌ای وجود ندارد.

حمله جعل هویت خدمات دهنده: فرض کنید مهاجم در پیام دوم M_4^* و M_5^* را با با هدف جعل هویت خدمات‌دهنده جایگزین M_4 و M_5 کند. از آنجایی در که پیام دریافت شده، M_4 و M_5 از طریق $M_5' = ? M_5$ احراز هویت می‌شود، از آنجایی که M_5' از D_i ساخته می‌شود که خود کاربر آن را می‌سازد در نتیجه امکان جعل هویت خدمات‌دهنده وجود ندارد.

حمله داخلی: در حمله داخلی فرض بر این است که مهاجم، خود، یکی از افراد داخلی سیستم خدمات دهنده است و سعی در رسیدن به رمزعبور خدمات‌دهنده دارد. از آنجایی که کاربر شناسه و رمزعبور خود را به طور مستقیم به سمت خدمات دهنده ارسال نمی‌کند و آن را در پوشش $=h(ID_i||h(PW_i \oplus MPW_i$ $a_i)) \oplus PW_i$ برای خدمات دهنده ارسال می‌کند، در نتیجه امکان چنین حمله ای وجود ندارد.

حمله جعل هویت کاربر: از آنجایی که در دو مرحله، پیام‌های رسیده شده از طریق کاربر به خدمات‌دهنده از طریق مقایسه $M_1' = ? M_1$ و $M_9' = ? M_9$ احراز هویت می‌شود، اگر فرض شود که در پیام اول، مهاجم q_i' را در بین راه جایگزین q_i کند، چون امکان باز شدن q_i' جعلی با کلید محرمانه خدمات‌دهنده وجود ندارد در نتیجه در همین مرحله ارتباط قطع می‌شود. به شکل مشابه، اگر مهاجم پارامترهای جعلی M_1^* و M_9^* و M_8^* را جایگزین M_1 و M_9 و M_8 کند، از آنجایی که در ساخت پارامتر M_9 از پارامتر M_5 استفاده می‌شود، که خدمات‌دهنده از پارامتر M_5 که خود آن را می‌سازد در ساخت M_9 استفاده می‌کند، در نتیجه امکان جعل هویت کاربر وجود نخواهد داشت.

حمله تکرار: در این حمله، مهاجم پیام‌های انتقالی بین دو موجودیت را به دست آورده و آن‌ها را در زمان دیگری ارسال می‌کند. طرفین ارتباط، متوجه تازگی پیام‌ها نشده و با این پیام، به مانند یک پیام جدید رفتار می‌شود و مراحل توافق کلید جلسه طی می‌شود. در پروتکل پیشنهادی، به علت وجود مُهرهای زمانی و بررسی آن‌ها در ابتدای هر گام و همچنین به علت وجود اعداد تصادفی امکان حمله تکرار وجود نخواهد داشت.

تامین نیاز امنیتی گمنامی و حریم خصوصی کاربر[33]: از آنجایی که در مرحله ثبت نام، خدمات‌دهنده برای کاربر، شناسه موقت $HID_i = h(ID_i||a_i)$ را ساخته و در اختیار او قرار می‌دهد و در ادامه کار، در تمامی مراحل، از شناسه موقت استفاده می‌شود، لذا امکان رسیدن به شناسه اصلی از روی کانال عمومی نیست و در نتیجه، گمنامی کاربر تامین می‌شود.

User (u_i)

Server(S_i)

مرحله ۱

Inserts smartcard

Enters ID_i^*, PW_i^*

Computes:

$$a_i = c_i - b_i$$

$$=h(ID_i^* || h(PW_i^* \oplus a_i)) \oplus PW_i^* MPW_i^*$$

$$C_i^* = h(b_i || ID_i^*)$$

$$D_i^* = MPW_i^* \oplus C_i^*$$

$$D_i^* ? = D_i$$

Selects time stamp $T_۱$

$$HID_i = h(ID_i || a_i)$$

$$G_i = HID_i \oplus c_i$$

$$M_۱ = h(HID_i || a_i)$$

$M_۱, G_i, b_i, q_i, T_۱$ ⟶

مرحله ۲

Selects time stamp $T_۲$

$|T_۲ \_ T_۱| <=$ delta T

$(q_i)=(HID_i^*, H_i^*, b_i^*) DEC_X$

Computes:

$$c_i = HID_i \oplus G_i$$

$$a_i = c_i - b_i$$

$$=h(HID_i^* || a_i) M_۱'$$

Check $M_۱' =? M_۱$

Selects random number $N_۱$

Computes:

$$=h(N_۱ || M_۱) M_۳$$

$$= H_i \oplus M_۱ D_i$$

$$= D_i \oplus N_۱ M_٤$$

$$h(N_۱ || D_i) M_٥ =$$

مرحله ۳

$M_٥, M_٤, T_۲$ ⟵

Selects time stamp $T_۳$

$|T_۳ \_ T_۲| <=$ delta T

Computes:

$$= D_i \oplus M_٤ N_۱$$

$$h(N_۱ || D_i) M_٥' =$$

Check $M_٥' =? M_٥$

Selects random number $N_۲$

Computes:

$$M_٦ = h(N_۲ || M_٤)$$

$$M_۷ = N_۱ \oplus N_۲$$

$$M_۸ = M_۷ \oplus N_۱$$

$$h(N_۲ || M_٥) M_۹ =$$

Selects random number $N_۳$

Computes:

$$M_۱۰ = N_۲ \oplus N_۳$$

SK=$h(M_٦ || N_۲ || HID_i || N_۳)$

$M_۸, M_۹, M_۱۰, T_۳$ ⟶

مرحله ۴

Selects time stamp $T_٤$

$|T_٤ \_ T_۳| <=$ delta T

Computes:

$$M_۷ = M_۸ \oplus N_۱$$

$$N_۲ = N_۱ \oplus M_۷$$

$$h(N_۲ || M_٥) M_۹' =$$

Check $M_۹' =? M_۹$

$$N_۳ = N_۲ \oplus M_۱۰$$

$$M_٦ = h(N_۲ || M_٤)$$

SK=$h(M_٦ || N_۲ || HID_i || N_۳)$

شکل ۴.مرحله احرازهویت طرح پیشنهادی

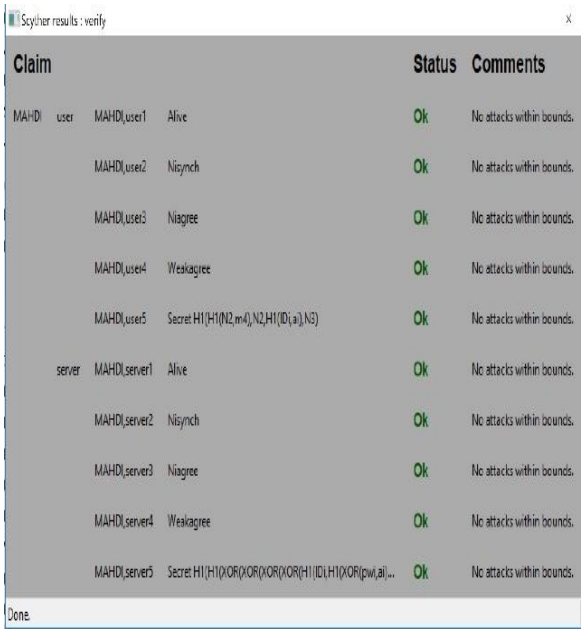
حمله منع سرویس: در حمله منع سرویس، مهاجم سعی می‌کند با ارسال پیام‌های متوالی و بی ارزش، خدمات دهنده را مشغول کند به طوری که خدمات‌دهنده، امکان سرویس‌دهی به کاربر را نداشته باشد. در پروتکل پیشنهادی، به علت وجود اعداد تصادفی و همچنین وجود مُهرهای زمانی و بررسی تازگی پیام در ابتدای هر گام، امکان وجود چنین حمله‌ای وجود ندارد. همچنین به علت اینکه پروتکل پیشنهادی سبک وزن است و هیچ جستجویی در پایگاه داده خدمات دهنده و یا محاسبه پیچیده‌ای در سمت خدمات‌دهنده وجود ندارد، در نتیجه امکان حمله منع سرویس وجود ندارد.

اثبات رسمی امنیت پروتکل پیشنهادی با استفاده از ابزارهای Scyther و Proverif

Scyther[۱۴] و Proverif [۱۵] ابزارهایی قدرتمند و مؤثر به‌منظور تجزیه‌وتحلیل، شناسایی حمله‌های احتمالی و آسیب‌پذیری‌های پروتکل‌های امنیتی هستند. این دو ابزار رسمی، پروتکل را به طور خودکار تحلیل نموده و رفتار آن را درمقابل اکثر حمله‌های ممکن، مورد بررسی دقیق قرار می‌دهند. در شکل ۷ کدهای نوشته‌شده برای ابزار scyther را مشاهده می‌نمایید.

شکل ۵، خروجی بررسی پروتکل پیشنهادی توسط scyther را نمایش میدهد. ویژگی Niagree تضمین میکند که طرفین ارتباط مطمئن هستند که پیام‌ها به طور امن و با ترتیبی درست بین آن‌ها رد و بدل شده است. ویژگی Nisynch تضمین می‌کند که پیام‌های رد و بدل شده بین طرفین قابل رمزگشایی و ارسال دوباره نباشد. ویژگی Alive تضمین می‌کند که ترتیب مراحل پروتکل به وسیله طرفین ارتباط، تایید شده است. ویژگی Weakagree تضمین می‌کند که در پروتکل، امکان جعل هویت وجود نداشته باشد. ویژگی secret نیز تضمین خواهد کرد که پارامتر مربوطه امن خواهد ماند. همانگونه که در شکل ۵ نشان داده شده است پروتکل احراز هویت معرفی شده در مقاله، قادر است تمامی ویژگی های فوق را تامین نماید.

ProVerif ابزاری قدرتمند برای تحلیل پروتکل‌های امنیتی است که از ابتکاراتی مانند رمزنگاری/رمزگشایی و درهم سازی یک طرفه و ساخت تابع‌های مختلف پشتیبانی می‌کند. همچنین حملات مختلف وارده به یک پروتکل امنیتی را بررسی می نماید. شکل۶ نتیجه بررسی پروتکل پیشنهادی را نمایش می‌دهد که حاکی از امن بودن پروتکل پیشنهادی و کلید نشست است. همچنین شکل ۸ کدهای نوشته شده برای ابزار ProVerif می‌باشد.



شکل۵. خروجی تحلیل پروتکل با استفاده از ابزار Scyther

```
RESULT inj-event( AuthServerSj(IDi)) == > injevent)

beginServerSj(IDi)) is true.

RESULT inj-event( AuthUserUi(ID_۱۸۹۰)) == > injevent)

beginUserUi(IDi_۱۸۹۰)) is true.

RESULT not attacker (SK[]) is true.
```

شکل۶.خروجی ابزار ProVerif

با توجه به مطالب گفته شده، جدول سه نشان‌دهنده مقایسه امنیتی پروتکل پیشنهادی با دیگر طرح‌های مشابه را نشان می‌دهد. طرح پیشنهادی نسبت به طرح‌های مشابه، از نظر امنیتی قوی‌تر می‌باشد و در مقابل حملات مختلف مقاوم است و نیازهای امنیتی مختلف را تامین می‌کند.

```
usertype TimeStamp;
const P;
secret x,Y;
secret IDi,pwi,ai,bi,Ci,x,m٤;
macro mpwi=XOR(H١(IDi,H١(XOR(pwi,ai))),pwi);
macro Ci = H١(bi, IDi);
macro Di= XOR(mpwi, Ci);
macro HIDi= H١(IDi, ai);
macro m١=H١(HIDi,ai);
hashfunction H١;
secret XOR: Function;
macro Hi=XOR(Di,m١);
macro qi={HIDi,bi,Hi}x;
macro ci=add(bi,ai);
macro m٢=XOR(bi ,ci);
secret add: Function;
secret sub: Function;
protocol MAHDI(user,server)
{
role user            {

var N١,m٥,m٤;
macro ai=add(bi,ci);
macro Ai= H١(b١, Pi);
macro mpwi١=XOR(H١(IDi,H١(XOR(pwi,ai))),pwi);
macro Ci١ = H١(bi, IDi١);
macro Di١= XOR(mpwi١, Ci);
match(Di١,Di);
macro HIDi١= H١(IDi, ai);
macro Gi=XOR(HIDi١,ci);
macro m١=H١(HIDi١,ai);
send_١(user,server, (m١,Gi,bi,qi));
recv_٢(server, user,(m٥,m٤));
macro N١=XOR(Di,m٤);
macro m٥٥=H١(N١,Di);
match(m٥,m٥٥);
fresh N٢;
macro m٦=H١(N٢,m٤);
macro m٧= XOR(N١,N٢);
macro m٨=XOR(N١,m٧);
macro m٩=H١(N٢,m٥٥);
fresh N٣;
macro m١٠=XOR(N٢,N٣);
macro sk=H١(m٦,N٢,HIDi,N٣);
send_٣(user,server, (m٨,m٩,m١٠));
claim (user, Alive ) ;
claim (user, Nisynch );
claim(user,Niagree);
claim(user,Weakagree);
claim(user, Secret, sk);
                    };
```

```
role  server
                              {
var N٢, N٣;
recv_١(user,server, m١,Gi,bi,qi);
macro ai=sub(bi,ci);
macro m١٢=H١(HIDi١,ai);
match(m١٢,m١);
fresh N١;
macro m٣=H١(N١,m١٢);
macro Di=XOR(Hi,m١٢);
macro m٤=XOR(Di,N١);
macro m٥=H١(N١,Di);
send_٢(server, user,(m٥,m٤));
recv_٣(user,server, (m٨,m٩,m١٠));
macro m٧=XOR(m٨,N١);
macro N٢=XOR(N١,m٧);
macro m٩٩=H١(N٢,m٥);
match(m٩٩,m٩);
macro N٣= XOR(N٢,m١٠);
macro m٦=H١(N٢,m٤);
macro sk=H١(m٦,N٢,HIDi,N٣);
claim (server, Alive ) ;
claim (server, Nisynch );
claim(server,Niagree);
claim(server,Weakagree);
claim(server, Secret, sk);
                              };
};
```

شکل۷. کدهای شبیه سازی پروتکل پیشنهادی با ابزار Scyther

```
(*** Channels ***)
free SCh: channel [private]. (*Confidential Channel*)
free PCh: channel. (*Open/insecure Channel*)
(*** Constants and Variables ***)
free IDi : bitstring.
free SIDj : bitstring.
free x : bitstring [ private ].
free BIOi : bitstring [ private ].
free PWi : bitstring [ private ].
(*** Constructor ***)
fun h(bitstring ) :bitstring.
fun H(bitstring ) :bitstring.
fun XOR(bitstring, bitstring): bitstring.
fun ENC(bitstring, bitstring): bitstring.
fun DEC(bitstring, bitstring): bitstring.
fun CONCAT( bitstring ,bitstring):bitstring.
fun add(bitstring,bitstring):bitstring.
fun sub(bitstring,bitstring):bitstring.
 **)Destructors & related Equations(**
equation forall u: bitstring, v: bitstring;
XOR (XOR(u,v) ,v)=u.
reduc forall w: bitstring, key: bitstring;
DEC (ENC (w, Pub), Prs)=w.
event beginUserUi ( bitstring ).
event AuthUserUi ( bitstring ).
event beginServerSj ( bitstring ).
event AuthServerSj ( bitstring ).
(**********p r o c e s s e s*******)
(**************** User Ui ******************)
let UserUi=
(**** Registration *******)
new ai:bitstring;
let MPWi=XOR(h(CONCAT(IDi,h(XOR(PWi,ai)))),PWi) in
out (SCh , (IDi, MPWi, ai));
in (SCh , (xbi:bitstring,xDi:bitstring,xqi:bitstring,xHIDi:bitstring));
let ci=add(xbi,ai)in
let M۲=XOR(xbi,ci) in
(***** Login and Authentication ********)
event beginUserUi ( IDi );
let ai=add(xbi,ci)in
let MPWi=XOR(h(CONCAT(IDi,h(XOR(PWi,ai)))),PWi) in
let Ci=h(CONCAT(xbi,IDi))in
let Di=XOR(MPWi,Ci)in
if (xDi=Di) then
                    let HIDi=h(CONCAT(IDi,ai))in
                    let Gi=XOR(HIDi,ci)in
                    let M۱=h(CONCAT(HIDi,ai))in
                    out(PCh,(M۱,Gi,xbi,xqi));
                    in(PCh,(xM۵:bitstring,xM۴:bitstring));
                    let N۱=XOR(Di,xM۴) in
                    let M۵=h(CONCAT(N۱,Di))in
                    if (M۵=xM۵)then
                    new N۲:bitstring;
                    let M۶=h(CONCAT(N۲,M۴)) in
                    let M۷=XOR(N۱,N۲)in
                    let M۸=XOR(M۷,N۱) in
                    let M۹=h(CONCAT(N۲,M۵)) in
new N۲:bitstring;
                    let M۱۰=XOR(N۲,N۳)in
                    let sk=h(CONCAT(CONCAT(CONCAT(M۶,N۲),HIDi),N۳))in
                    out(PCh,(M۸,M۹,M۱۰));
(** **Server (Sj) *******)
(** Server Sj **)
let ServerSj=
(****** Registration *********)
event beginServerSj ( SIDj );
new bi:bitstring;
let Ci=h(CONCAT(IDi,bi)) in
let Di=XOR(xMPWi,Ci)in
let HIDi=h(CONCAT(IDi,xai))in
let M۱=h(CONCAT(HIDi,xai ))in
let Hi=XOR(Di,M۱)in
let qi=ENC(CONCAT(HIDi,CONCAT(bi,Hi)),x)in
out (SCh,(bi,Di,qi,HIDi));
(***** Login and Authentication ********)
in(PCh,(xM۱:bitstring,xGi:bitstring,xbi:bitstring,xqi:bitstring));
let ci=XOR(HIDi,Gi) in
let ai=sub(bi,ci)in
let M۱=h(CONCAT(HIDi,ai))in
            if (xM۱=M۱) then
            new N۱:bitstring;
            let M۳=h(CONCAT(N۱,M۱))in
            let Di=XOR(Hi,M۱)in
            let M۴=XOR(Di,N۱)in
            let M۵=h(CONCAT(N۱,Di))in
            out(PCh,(M۵,M۴));
in(PCh,(xM۸:bitstring ,xM۹:bitstring ,xM۱۰:bitstring))
let M۷=XOR(M۸,N۱) in
let N۲=XOR(N۱,M۷) in
let M۹=h(CONCAT(N۲,M۵)) in
            if (xM۹=M۹)then
            let N۲=XOR(N۲,xM۱۰) in
            let M۶=h(CONCAT(N۲||M۴))in
            let sk=h(CONCAT(CONCAT(CONCAT(M۶,N۲),HIDi),N۳))in
            else
            .
process
( ( ! UserUi ) |  ( !ServerSj ))
(** Queries **)
free sk: bitstring [ private ].
query attacker (SK).
query IDi: bitstring ; inj event ( AuthUserUi  (IDi )) ==> inj
event ( beginUserUi ( IDi )).
query IDi: bitstring ; inj event ( endServerSj ( IDi) ) ==> inj
event ( beginServerSj ( IDi )).
```

شکل۸. کدهای نوشته شده با ابزار ProVerif

با توجه به مطالب گفته شده، جدول سه نشان‌دهنده مقایسه امنیتی پروتکل پیشنهادی با دیگر طرح‌های مشابه را نشان می‌دهد. طرح پیشنهادی نسبت به طرح‌های مشابه، از نظر امنیتی قوی‌تر می‌باشد و در مقابل حملات مختلف مقاوم است و نیازهای امنیتی مختلف را تامین می‌کند. این امر نشان از برتری روش پیشنهادی نسبت به روش‌های مشابه دارد.

جدول۳. مقایسه امنیتی روش پیشنهادی با طرح‌های مشابه

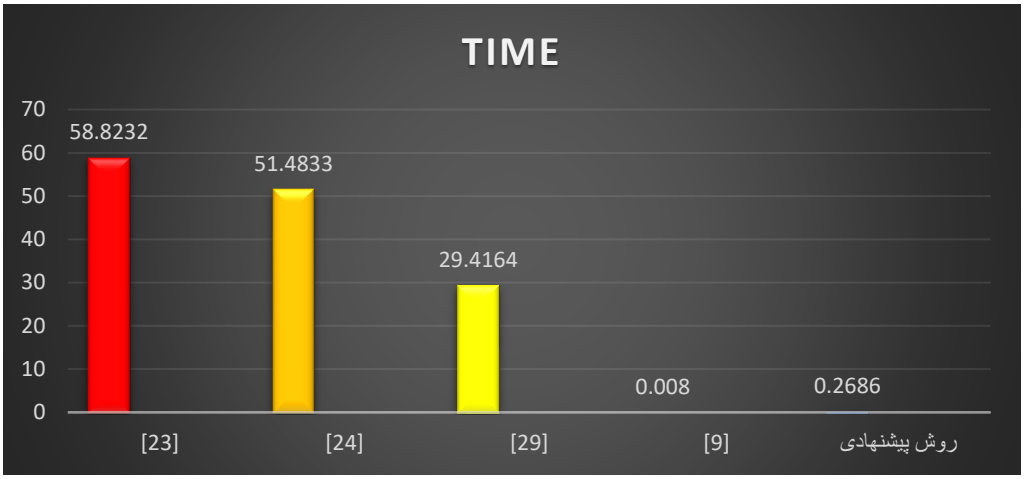
طرح پیشنهادی	[۹]	[۲۹]	[۲٤]	[۲۳]	نیازمندی امنیتی
بله	خیر	بله	بله	بله	**محرمانگی رو به جلو**
بله	بله	خیر	خیر	خیر	**گمنامی کاربر**
بله	بله	بله	خیر	خیر	**مقاومت در برابرحمله تکرار**
بله	بله	خیر	بله	خیر	**مقاومت در برابر حمله جعل هویت خدمات دهنده**
بله	بله	خیر	بله	خیر	**مقاومت در برابر حمله جعل هویت کاربر**
بله	خیر	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	**مقاومت در برابر حمله افشای پارامترهای تصادفی**
بله	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	خیر	**مقاومت در برابر منع سرویس**

تحلیل و مقایسه پیچیدگی زمانی و سخت افزاری طرح پیشنهادی و دیگر طرح‌های مشابه

بر طبق مقالات[۳٤] و[۳٥]، پیچیدگی زمانی هر ضرب نقطه ای روی منحنی بیضوی، ۷.۳٥۲۹ میلی ثانیه و هر درهم ساز یک طرفه ۰.۰۰۰۴ میلی ثانیه است. همچنین پیچیدگی زمانی هر جمع نقطه‌ای روی منحنی بیضوی، ۰.۰۰۹ میلی ثانیه و مدت زمان هر رمزنگاری/رمزگشایی ۰.۱۳۰۳ میلی ثانیه می‌باشد. اگر h و mu و ad و en/d را به ترتیب نمادهای درهم ساز یکطرفه و ضرب نقطه‌ای روی منحنی بیضوی و جمع نقطه‌ای روی منحنی بیضوی و همچنین رمزنگاری/رمزگشایی در نظر بگیریم، جدول ۴ نشان دهنده مقایسه پیچیدگی زمانی طرح پیشنهادی و طرح‌های مشابه است. همانطور که شکل ۹ نشان می‌دهد، طرح پیشنهادی از نظر سربار زمانی، بهتر و یا نزدیک به طرح‌های مشابه عمل می‌کند. اهمیت این مساله زمانی مشخص می شود که برتری روش پیشنهادی را در زمینه مقاومت در برابر حملات شناخته شده در برابر سایر روشهای مورد مقایسه، درنظر بگیریم. به عبارت دیگر، طرح پیشنهادی قادر است با پیچیدگی زمانی کمتر از اغلب روشهای مشابه، نیازمندیهای امنیتی را به طور کامل تامین نماید.

جدول۴. مقایسه پیچیدگی زمانی

طرح پیشنهادی	[۹]	[۲۹]	[۲٤]	[۲۳]	
٥h+۱en/d	٥h	۳h	٤mu+۱ad+٥h	٤mu+٦h	زمان مرحله ثبت‌نام
۱٥h+۱en/d	۱٥h	٤mu+۹h	۳mu+٥h	٤mu+۷h	زمان مرحله احراز هویت
۲۰h+۲en/d	۲۰h	٤mu+۱۲h	۷mu+۱ad+۱۰h	۸mu+۱۳h	زمان کل
۰,۲٦۸٦	۰,۰۰۸	۲۹,٤۱٦٤	٥۱,٤۸۳۳	٥۸,۸۲۳۲	زمان (میلی ثانیه)

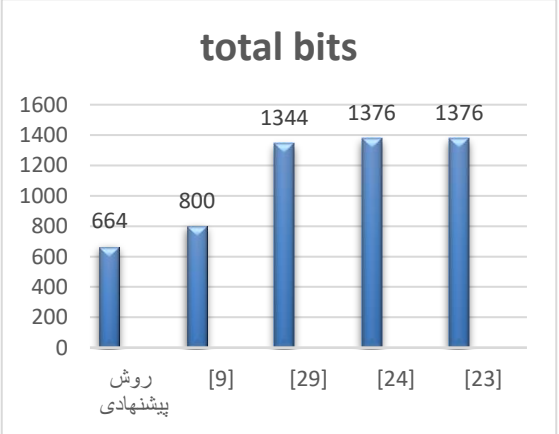


شکل۹. نمودار مقایسه پیچیدگی زمانی طرح پیشنهادی و طرح‌های مشابه

برای مقایسه طرح‌های مختلف میتوان تعداد بیت های موجود در پیامهای مبادله شده در مرحله احراز هویت را نیز درنظر گرفت. بر اساس مقالات[37][36][10]، هر تابع درهم ساز یک طرفه ۱۶۰ بیت، ضرب اسکالر ۳۲۰ بیت، پارامتر رمزنگاری شده ۱۲۰ بیت ، شناسه ۱۶۰ بیت و مُهر زمانی ۳۲ بیت نیاز دارد. با مراجعه به جدول مقایسه‌ای ۵ و شکل ۱۰، مشاهده می شود که پروتکل پیشنهادی حاوی کمترین تعداد بیت رد و بدل شده بر روی کانال در مرحله احراز هویت است .

جدول۵. مقایسه سخت افزاری

طرح	تعداد پیام‌های رد و بدل شده	تعداد بیت‌های رد و بدل شده
پیشنهادی	۳	۶۶۴
[۹]	۲	۸۰۰
[۲۹]	۳	۱۳۴۴
[۲٤]	۳	۱۳۷۶
[۲۳]	۳	۱۳۷۶



شکل۱۰. نمودار مقایسه تعداد بیت‌های رد و بدل شده

نتیجه‌گیری و کارهای آینده

در این مقاله، پروتکلی کارآمد و سبک‌وزن برای ارتباط امن دستگاه‌هایVoIP مبتنی بر کارت هوشمند ارائه گردید. تحلیل‌های امنیتی پروتکل نشان داد که طرح ارائه شده در برابر حملات مختلف مقاوم است و نیازهای امنیتی گوناگون را تامین می‌کند همچنین صحت امنیتی پروتکل باکمک ابزار Scyther و نیز Proverif بررسی و تایید گردید. همچنین در آینده می‌توان طرحی ارائه گردد که فقط مبتنی بر رمز عبور باشد، یعنی نیازی به کارت هوشمند احساس نشود، همچنین می‌توان پروتکل پیشنهادی را از نظر زمانی بهبود بخشید.

مراجع

[۱] Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L Http authentication: Basic and digest access authentication. In: IETF RFC۲٦۱۷, ۱۹۹۹.

[۲] Yeh H., Chen T., Shih W., Robust smart card secured authentication scheme on SIP using Elliptic Curve Cryptography. Computer Standards & Interfaces; ۲۰۱٤, vol. ۳٦, no.۲, pp: ۳۹۷-٤۰۲.

[۳] Zhang L, Tang S, Zhu S, An energy e_cient authenticated key agreement protocol for SIP-based green VoIP networks, J Netw Comput Appl, ۲۰۱٦, vol. ٥۹, pp. ۱۲٦-۱۳۳.

[٤] Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure

privacy preserving authentication protocol for sip. Peer-to-Peer Networking and Applications, ٢٠١٧, vol. ١٠, no. ١, pp. ١-١٥.

[٥] Sourav S., Odelu V., Prasath R., Enhanced Session Initiation Protocols for Emergency Healthcare Applications. In: Thampi S., Madria S., Wang G., Rawat D., Alcaraz Calero J. (eds) Security in Computing and Communications (SSCC), Communications in Computer and Information Science, ٢٠١٨, vol ٩٦٩, pp ٢٧٨-٢٨٩.

[٦] Arshad H, Nikooghadam M. An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. Multimedia Tools and Applications ٢٠١٦, vol. ٧٥, no.١, pp.١٨١-١٩٧.

[٧] H. Arshad and M. Nikooghadam, ‘‘Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol,’’ J. Supercomput., ٢٠١٥, vol. ٧١, no. ٨, pp. ٣١٦٣–٣١٨٠.

[٨] Dhillon, P.K.; Kalra, S. Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. Multimed.Tools Appl. ٢٠١٩, vo. ٧٨, no. ١٦, pp.٢٢١٩٩-٢٢٢٢٢.

[٩] Zhang Y, Xie K, Ruan O An improved and efficient mutual authentication scheme for session initiation protocol. PLoS ONE, , ٢٠١٩, vol.١٤, vo.٣.

[١٠] Ravanbakhsh, N., Mohammadi, M. Nikooghadam, Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme, M. Multimed Tools Appl, ٢٠١٩, vol. ٧٨, no. ٩, pp. ١١١٢٩-١١١٥٣.

[١١] Amin R, Islam S, Biswas G, Giri D, Khan MK, Kumar N. A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments. Secur Commun Netw. ٢٠١٦, vol. ٩, no.١٧, pp.٤٦٥٠-٤٦٦٦.

[١٢] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, ‘‘A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications,’’ J. Med. Syst., ٢٠١٩, vol. ٤٣, p. ١٠.

[١٣] Ostad-Sharif, A, Abbasinezhad-Mood, D, Nikooghadam, M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst. ٢٠١٩, vol. ٣٢, no. ٥.

[١٤] Cremers, C, Scyther - Semantics and Verification of Security Protocols. Ph.D. dissertation, Eindhoven University of Technology, ٢٠٠٦.

[١٥] Blanchet B, Cheval V, Allamigeon X, Smyth B. ProVerif: Cryptographic protocol verifier in theformalmodel.(Availableat:http://prosecco.gforge.inria.fr/personal/bblanche/proverif/).

[١٦] A.Durlanik, I. Sogukpinar. SIP authentication scheme using ECDH. World Enformatika Society Transaction on Engineering Computing and Technology, ٢٠٠٥, vol. ٨, pp.٣٥٠-٣٥٣.

[١٧] EJ Yoon, KY Yoo, et al..A secure and efficient SIP authentication scheme for converged VoIP networks. Computer Communications, ٢٠١٠, vol. ٣٣, pp.١٦٧٤-١٦٨١.

[١٨] Zhang L., Tang S., Cai Z.. Efficient and flexible password authenticated key agreement for Voice over Internet Protocol Session Initiation Protocol using smart card. International Journal of Communication Systems ٢٠١٤.

[١٩] Farash MS. Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. Peer-to-Peer Networking and Applications. ٢٠١٦, vol. ٩, no. ١, pp: ٨٢–٩١.

[٢٠] Kumari S, Chaudhry S, Wu F, Li X, Farash M, Khan M. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications. ٢٠١٥, vol. ١٠. no. ١, pp. ٩٢-١٠٥.

[٢١]Zhang L, Tang S, Cai Z. Cryptanalysis and improvement of password-authenticated key agreement for session initiation protocol using smart cards. Security and Communication Networks. , ٢٠١٤, vol. ٧, no. ١٢, pp.٢٤٠٥-٢٤١١.

[٢٢]Jiang Q, Ma J, Tian Y, Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al. Int J Commun Syst, ٢٠١٥, vol.٢٨, no. ٧, pp:١٣٤٠-١٣٥١.

[٢٣]Tu, H., Kumar, N., Chilamkurti, N., Rho, S., An improved authentication protocol for session initiation protocol using smart card. Peer-to-Peer Networking and Applications, ٢٠١٥, vol. ٨, no. ٥, pp. ٩٠٣-٩١٠.

[٢٤]Farash MS. Security analysis and enhancements of an improved authentication for ses sion initiation protocol with provable security. Peer-to-Peer Networking and Applications , ٢٠١٦, vo. ٩, no. ١, pp: ,٩١-٨٢.

[٢٥]Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for sip. Peer-to-Peer Networking and Applications, ٢٠١٧, vol. ١٠, no. ١, pp. ١٥-١.

[٢٦]Mishra D, Das AK, Mukhopadhyay S, A secure and ecient ECC-based user anonymity preserving session initiation authentication protocol using smart card. Peer-to-peer Netw Appl, ٢٠١٦, vol. ٩, no. ١, pp. ١٧١,١٩٢.

[٢٧]Farash MS, Attari MA. An anonymous and untraceable password-based authentication scheme for session initiation protocol using smart cards. International Journal of Communication Systems, ٢٠١٦, vol. ٢٩. no. ١٣, pp. ١٩٥٦-١٩٦٧.

[٢٨]Lu Y, Li L, Peng H, Yang Y, An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimedia Tools and Applications, ٢٠١٧, vol. ٧٦, no. ٢, pp. ١٨٠١-١٨١٥.

[٢٩]Lu Y, Li L, Peng H, Yang Y, A secure and efficient mutual authentication scheme for session initiation protocol. Peer-to-Peer Netw Appl, ٢٠١٦, vol. ٩, no. ٢, pp. ٤٤٩-٤٥٩.

[٣٠]V. Sureshkumar, R. Amin, and R. Anitha, A robust mutual authentication scheme for session initiation protocol with key establishment, Peer-toPeer Netw. Appl. , ٢٠١٨, vol. ١١, no. ٥, pp. ٩٠٠-٩١.

[٣١]Zhang L, Tang S, Zhu S, An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. J Netw Comput Appl, ٢٠١٦, vol.٥٩, pp.١٢٦–١٣٣.

[٣٢]Qiu S, Xu G, Ahmad H. An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy. PLOS ONE, ٢٠١٨, vol. ١٣, no, ٣.

[٣٣]M. Nikooghadam, R. Jahantigh, and H. Arshad, ‘‘A lightweight authentication and key agreement protocol preserving user anonymity,’’ Multimedia Tools Appl., ٢٠١٧, vol.٧٦, no.١١, pp. ١٣٤٠١–١٣٤٢٣.

[٣٤]Xu, L., Wu, F., Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. Journal of medical systems, ٢٠١٥, vol. ٣٩, no. ١٠.

[٣٥]Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Obaidat, M. S., Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. Journal of medical systems, ٢٠١٥, vol. ٣٩, no.١١, pp. ١٣٧.

[٣٦]Xu L,Wu F Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. J Med Syst, ٢٠١٥, vol. ٣٩, no. ٢, pp:١–٩.

[٣٧]Kumari S, Karuppiah M, Das AK, Li X, Wu F, Gupta V. Design of a secure anonymity preserving authentication scheme for session initiation protocol using elliptic

curve cryptography. J Ambient Intell Human Comput,, ۲۰۱۸, vol. ۹, no.۳, pp ٦٤۳–٦٥۳.

Secure Lightweight Mutual Authentication Scheme for VoIP based on Smart Card

Mahdi Nikooghadam, Haleh Amintoosi

Abstract

With the widespread use of Voice over IP (VoIP) technology to transmit multimedia such as voice and video, Session Initiation Protocol (SIP) has been the focus of many research. To establish a secure communication channel between the two parties using SIP, authentication of the parties is of the utmost importance. Many research has been done on authentication protocols in recent years, including the lightweight VoIP authentication scheme presented by Zhang et al. In this article, we first prove that Zhang's authentication scheme is not robust against known-session-specific temporary information attack and does not meet the security requirement of perfect forward secrecy. In addition, we present a lightweight and efficient authentication protocol and show that the proposed protocol is resistant to various attacks and is capable of meeting essential security requirements such as perfect forward secrecy and user anonymity. We have also examined the performance of the proposed protocol in terms of computational complexity and have shown that the proposed method has less computational complexity compared to most similar methods. Finally, we prove the correctness of the proposed protocol with Scyther and Proverif tools.

Keywords:

Authentication, VoIP, SIP, Scuther, Provreif