ICWR2022
May 11-12, 2022; Tehran, Iran
8th International Conference on Web Research

Security Analysis and Improvement of Sureshkumar et al. Authentication Scheme

Mohammad Reza Servati*[1], Masoumeh Safkhani[2]

[1] M.Sc. student of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran
Mohammadreza.servati@sru.ac.ir

[2]Associate Professor of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran
Safkhani@sru.ac.ir

Abstract

The widespread development of wireless networks and cloud computing has provided numerous benefits to individuals in the community. These networks have applications in the fields of health and medicine, including medical wireless sensor networks. One of the concerns in these networks is security. In the context of activities in this area, the issue of security and privacy remains one of the challenges, and only a small number of schemes have been able to achieve good security from the proposed schemes. Sureshkumar et al. recently presented an authentication scheme for IoT-based smart medical services, claiming that it is resistant to known attacks. This paper demonstrates that Sureshkumar et al. authentication's scheme is vulnerable to traceability, integrity contradiction, and de-synchronization attacks. This paper also examines the security of Sureshkumar et al. authentication's protocol using the Scyther tool, which verifies the accuracy of the presented attacks. In this paper, we also make recommendations to improve Sureshkumar et al., so that this protocol can provide complete security against all active and passive attacks, particularly the attacks presented in this paper.

Keywords: IoT, Wireless Sensor Networks, Mutual Authentication, Security Protocols, Gateway Node, Sensor Node, Cloud, IoT, Scyther

ICWR2022
May 11-12, 2022; Tehran, Iran
8th International Conference on Web Research

تحلیل امنیتی و بهبود طرح احراز اصالت شورسکومار و همکاران

محمدرضا ثروتی*[1]، معصومه صفخانی[2]

[1] دانشجوی کارشناسی ارشد دانشکده مهندسی کامپیوتر، گروه نرم افزار، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
Mohammadreza.servati@sru.ac.ir

[2] دانشیار دانشکده مهندسی کامپیوتر، گروه نرم افزار، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
Safkhani@sru.ac.ir

چکیده

توسعه گسترده شبکه‌های بی‌سیم و محاسبات ابری مزایای زیادی برای افراد جامعه داشته است. از کاربردهای این شبکه‌ها می‌توان در حوزه سلامت و پزشکی را نام برد که شامل شبکه حسگر بی‌سیم پزشکی[1] است. در این شبکه‌ها یکی از نگرانی‌های موجود، امنیت است، در چشم‌انداز فعالیت‌های صورت گرفته در این حوزه موضوع امنیت و حریم خصوصی به عنوان یکی از چالش‌ها باقی مانده است، و تعداد کمی از طرح‌های پیشنهاد شده توانسته‌اند امنیت مطلوبی را داشته باشند. اخیراً، شورسکومار و همکاران[2] یک طرح احراز اصالت برای خدمات پزشکی هوشمند مبتنی بر اینترنت اشیاء و سامانه ابری ارائه کردند و ادعا نمودند طرح آنها در برابر حملات شناخته‌شده امن است. در این مقاله نشان داده می‌شود که طرح احراز اصالت شورسکومار و همکاران در برابر حمله ردیابی، حمله نقض یکپارچگی و حمله غیر همزمان سازی آسیب‌پذیر است. در این مقاله هم‌چنین امنیت پروتکل احراز اصالت شورسکومار و همکاران توسط ابزار Scyther تحلیل می‌گردد که درستی حملات ارائه شده را راستی آزمایی می‌نماید. هم‌چنین ما در این مقاله، طرح احراز اصالت شورسکومار و همکاران را با توصیه‌هایی بهبود می‌دهیم، به گونه‌ای که قادر به برقراری امنیت کامل در برابر حملات فعال و غیرفعال به خصوص حملات ارائه‌شده در این مقاله باشد.

کلمات کلیدی

اینترنت اشیاء، شبکه‌های حسگر بی‌سیم، احراز اصالت متقابل، پروتکل‌های امنیتی،گره دروازه، گره حسگر، ابر، IoT، Scyther

۱_مقدمه

مراقبت پزشکی الکترونیکی، یک زمینه در حال رشد است که شبکه‌های اینترنت اشیاء، شبکه‌های حسگر بی‌سیم[3] و تلفن‌های همراه به خوبی توانسته‌اند نقش به‌سزایی در این پیشرفت داشته باشند و پزشکان بتوانند با دستیابی به اطلاعات از طریق حسگرهای موجود ارزیابی خود را داشته باشند [1]. در این شبکه‌ها، حسگرهای موجود علائم حیاتی بیمار را اندازه‌گیری می‌کنند و اطلاعات به‌دست آمده را توسط حسگرهای هوشمند ارسال می‌نمایند. این اطلاعات حساس در ابر ذخیره می‌گردد. تمامی کاربران اعم از بیمار، پزشک و مراکز پزشکی می‌توانند به این اطلاعات از نقاط مکانی مختلف و در فواصل زمانی متفاوت دسترسی داشته باشند. البته دسترسی غیرمجاز یا قرار گرفتن اطلاعات شخصی بیمار در دسترس مراکز تحقیقاتی یا شرکت های بیمه می‌تواند حریم خصوصی بیمار را به مخاطره بیندازد [2]. همچنین وجود حسگرهای بی‌سیم این امکان را به بیمار می‌دهد که بتواند در هر موقعیتی نظیر خارج از بیمارستان یا درون بیمارستان یا در خانه که باشد اطلاعات و علائم حیاتی خود را به دست پزشک متخصص و مراکز درمانی برساند [3]. مراقبت پزشکی الکترونیکی مستلزم تأیید احراز اصالت متقابل است تا اطلاعات و خدمات ارائه شده مورد سوء استفاده قرار نگیرند. به همین منظور پروتکل‌های احراز اصالت بسیاری برای تأمین یک دسترسی امن پیشنهاد شده است. پروتکل‌های ارائه شده باید از ویژگی‌هایی نظیر ناشناس بودن، حفظ حریم خصوصی، حفظ محرمانگی و حفظ یکپارچگی برخوردار باشند تا در برابر حملات شناخته شده نظیر حملات ردیابی، جعل هویت، حملات غیرهمزمان سازی و... مقاومت لازم را داشته باشند.

۲_کارهای مرتبط

در سال‌های اخیر پروتکل‌های احراز اصالت متفاوتی ارائه شده است که در آن میان تعداد بسیاری به دلیل عدم امنیت در برابر حملات شناخته شده، تغییر و بهبود پیدا کردند. در سال ۲۰۱۷، لیو و چانگ[۴] در [4]، طرح احراز اصالتی برای شبکه‌های بی‌سیم در حوزه مراقبت پزشکی را ارائه کردند. ضعف این طرح در برابر حمله تکرار و حمله حدس‌زدن گذرواژه برون خط و حمله جعل هویت توسط لی و همکارانش[۵] در سال ۲۰۱۷ [5] مشخص گردید. در سال ۲۰۱۶ کال و آوستی[۶] [6]، طرح دیگری را پیشنهاد دادند و ادعا کردند که طرح پیشنهادی آنها ایمن است، در سال ۲۰۲۰ رانا و همکاران[۷] [7]، نشان دادند که پروتکل پیشنهادی آنها در برای حمله جعل هویت مقاومت ندارد و ایمن نیست و پروتکل [6] را بهبود دادند. هم‌چنین در سال ۲۰۱۹ وینود کومار و همکاران[۸] [8] پروتکل احراز اصالتی برای اینترنت وسایل نقلیه مبتنی بر ابر پیشنهاد دادند و مدعی شدند که پروتکل آنها مقاوم است، ولی در سال ۲۰۲۰ صفخانی و همکاران [9] نشان دادند که پروتکل آنها در برابر حمله جعل برچسب و قرائت‌گر مقاوم نیست. هم‌چنین در سال ۲۰۱۹ شوای و همکاران[۹] [10] پروتکلی برای خانه هوشمند پیشنهاد دادند و مدعی شدند که پروتکل آنها در برابر حملات مقاوم است ولی در سال ۲۰۲۰ فاکرون و همکارانش[۱۰] [11] اثبات کردند که پروتکل شوای و همکارانش در برابر حمله کلید نشست موازی آسیب‌پذیر است. در سال ۲۰۱۹، شورسکومار و همکاران در [12] یک طرح احراز اصالت سبک‌وزن ارائه دادند و ادعا نمودند که در برابر تمام تهدیدات امنیتی مقاوم است، ولی در این مقاله نشان می‌دهیم که طرح احراز اصالت فوق در برابر حمله نقض یکپارچگی، حمله غیر هم‌زمان‌سازی و حمله ردیابی آسیب‌پذیر است. ما هم چنین طرح احراز اصالت فوق را با استفاده از ابزار خودکار Scyther تحلیل می‌نماییم که نتایج به دست آمده حملات فوق را بار دیگر نشان می‌دهد. ما به منظور رفع این آسیب‌پذیری‌ها توصیه‌هایی هم برای بهبود پروتکل ارائه می‌دهیم. جزئیات پروتکل بهبود یافته و اثبات‌های امنیتی مربوطه به دلیل محدودیت صفحه در این مقاله ذکر نمی‌گردد و در تحقیقات آتی مد نظر قرار خواهد گرفت.

۳_طرح احراز اصالت شورسکومار و همکاران

این طرح توسط شورسکومار و همکاران [12] به‌منظور احراز اصالت متقابل در راستای نظارت از راه دور بر بیمار ارائه شده‌است. در این طرح، احراز اصالت و توافق کلید بین چهار هستینه پزشک (U_i)، گره دروازه (GW) و گره حسگر (SN) و مدیر سامانه SA انجام می‌گیرد. طرح شورسکومار و همکارانش [12] شامل شش مرحله‌ی تنظیمات، ثبت‌نام گره حسگر و دروازه، ثبت‌نام کاربر، مرحله ورود، مرحله احراز اصالت و مرحله به‌هنگام‌رسانی گذرواژه است که در راستای آسیب‌پذیری طرح، تنها به تجزیه و تحلیل مراحل ورود و احراز اصالت کاربر و ثبت نام کاربر می‌پردازیم. علائم و نمادهای استفاده‌شده در این مقاله در جدول (۱) نشان داده‌شده‌است. در ادامه مقاله، بخش‌های مقاله به شرح زیر سازمان‌دهی شده است: طرح شورسکومار و همکاران [12] در قسمت ۳ به صورت مختصر شرح داده می‌شود. در قسمت ۴ امنیت طرح شورسکومار و همکاران و چگونگی اعمال حملات مختلف بر علیه آن مورد بررسی قرار می‌گیرد. هم‌چنین در این قسمت طرح احراز اصالت شورسکومار و همکاران در ابزار تحلیل امنیتی Scyther مدل شده که نتایج به دست آمده از ارزیابی آن بار دیگر بر درستی حملات وارد شده صحه می‌گذارد. در قسمت ۵ توصیه‌هایی جهت بهبود طرح شورسکومار و همکاران بیان می‌گردد و در نهایت مقاله با نتیجه‌گیری در قسمت ۶ به پایان می‌رسد.

۳-۱مرحله ثبت‌نام کاربر

در این مرحله، کاربر باید در گره دروازه (GW) اقدام به ثبت‌نام کند که مراحل ثبت‌نام به شرح زیر است:

۱) کاربر (U_i) شناسه کاربری (ID_i)و گذرواژه (PW_i) را برای خود انتخاب می‌کند.کاربر (U_i) مقدار $b_i = H(B_i)$ را به واسطه اطلاعات زیست‌سنجی خود محاسبه می‌کند و هم‌چنین مقادیر $HPW_i = h(PW_i \| b_i)$ و مقادیر $HID_i = h(ID_i \| b_i)$ را محاسبه می‌کند و اطلاعات ثبت‌نام $\{HID_i, HPW_i, GW_{ID_j}\}$ را برای SA ارسال می‌کند.

۲) با دریافت مقادیر ثبت‌نام از مرحله یک شروع به محاسبه مقادیر روابط (۱)،(۲)،(۳) و (۴) زیر می‌نماید:

$$A_1 = h(HID_i \| HPW_i).P \quad (۱)$$
$$A_2 = h(HID_i \| S_{GW_j}).P \quad (۲)$$
$$A_3 = A_2 \oplus A_1 \quad (۳)$$
$$A_4 = S_{GW_j}.P \quad (۴)$$

SA *مقادیر* $SC = \langle A_3, A_4, h(.), P \rangle$ را در کارت هوشمند ذخیره می‌کند و از طریق کانال امن برای کاربر ارسال می‌کند. لازم به ذکر است که مقادیر روابط (۱)، (۲) و (۴) روی خم بیضوی محاسبه شده‌اند.

جدول(۱): نمادهای استفاده‌شده در طرح احراز اصالت شورسکومار و همکاران [12]

نماد	شرح
U_i	کاربر
SN	گره حسگر
GW	گره دروازه
ID_i	شناسه منحصربه‌فردکاربر
PW_i	گذرواژه کاربر
B_i	اطلاعات زیست‌سنجی
Sk	کلید بلندمدت مخفی مشترک بین گره دروازه و حسگر وکاربر
$H(.)$	تابع چکیده‌ساز
Id_{SN_i}	شناسه گره حسگر
ΔT	زمان
$\oplus$	عملیات یای انحصاری بیتی
$\|\|$	عملیات الحاق
SA	مدیر سامانه
ECC	رمزنگاری خم بیضوی
P	نقطه پایه در خم بیضوی

۳-۲مرحله ورود و احراز اصالت

۱) کاربر (U_i)،کارت هوشمند خود را وارد ترمینال می‌کند و سپس شناسه کاربری (ID_i) و اطلاعات زیست‌سنجی (B_i) و گذرواژه (PW_i) خود را وارد می‌کند.

۲) کارت هوشمند مقادیر روابط (۵)، (۶)، (۷) و (۸) زیر را محاسبه می‌کند:

$$b_i = H(B_i) \quad (۵)$$
$$HID_i = h(ID_i \,||b_i) \quad (۶)$$
$$HPID = h(HID_i||PW_i) \quad (۷)$$
$$A_5^* = h(HID_i||HPID_i).P \quad (۸)$$

سپس بررسی می‌کند که آیا تساوی $A_5^* = A_5$ با رابطه‌ی (۸) برقرار است یا خیر، اگر این تساوی برابر نباشد، جلسه توسط کارت هوشمند خاتمه می‌یابد در غیر این صورت یک عدد تصادفی انتخاب می‌کند و مقادیر روابط (۹)، (۱۰)، (۱۱)، (۱۲) و (۱۳) زیر را محاسبه می‌کند:

$$HPW_i = h(PW_i \,||b_i) \quad (۹)$$
$$A_1^* = h(HID_i||HPW_i).P \quad (۱۰)$$
$$A_2^* = A_3 \oplus A_1^* \text{ و } A_7 = h(A_2^*||T_1) \quad (۱۱)$$
$$A_8 = r_u.P \text{ و } A_9 = A_8 \oplus A_2^* \quad (۱۲)$$
$$A_{10} = A_6 \oplus A_9 = A_4 \oplus A_8 \quad (۱۳)$$

که در این روابط T_1 مهر زمان[11] جاری است.

۳) کارت هوشمند (SC) پیام $M_1 = \langle A_7.A_9.A_{10}.T_1 \rangle$ را به گره دروازه GW_j ارسال می‌کند. در این زمان کاربر مرحله ورود برای دستیابی به اطلاعات بیمار را آغاز می‌کند.

۴) گره دروازه GW_j اولین پیام را از طرف کاربر U_i دریافت می‌نماید. در راستای مقاومت در برابر حمله تکرار، یک مهر زمان جاری T_2 تولید می‌کند و بررسی می‌کند که شرط $|T_2 - T_1| < \Delta T$ برقرار است یا خیر (ΔT، برابر با بیشترین تأخیر زمان ارسال است). اگر این زمان قابل قبول نباشد درخواست توسط گره دروازه رد می‌شود و همچنین گره دروازه مقادیر روابط (۱۴)، (۱۵) و (۱۶) را محاسبه می‌کند:

$$A_4^* = S_{GW_j}.P \quad (۱۴)$$
$$A_8^* = A_{10} \oplus A_4^* \quad (۱۵)$$
$$A_2^{**} = A_9 \oplus A_8^* \text{ ، } A_7^* = h(A_2^{**}||T_1) \quad (۱۶)$$

و بررسی می‌کند که تساوی مقابل $A_7^* = A_7$ برقرار است یا خیر. اگر این تساوی درست باشد GW_j یک عدد تصادفی r_g را انتخاب می‌کند و سپس مقادیر روابط (۱۷)، (۱۸)، (۱۹) و (۲۰) را حساب می‌کند:

$$A_{11} = r_g.A_8^* = r_g.r_s.P \text{ ، } A_{12} = r_g.P \quad (۱۷)$$
$$A_{13} = h(S_{SN_K}).A_{12} \quad (۱۸)$$
$$A_{14} = h(GW_{ID_j}||S_{SN_K}).P \quad (۱۹)$$
$$A_{15} = h(A_{14}||T_2) \text{ ، } A_{16} = A_8^* \oplus A_{13} \quad (۲۰)$$

گره دروازه پیام $M_2 = \langle A_{12}.A_{11}.A_{15}.A_{16}.T_2 \rangle$ را برای گره حسگر ارسال می‌کند.

۵) در این مرحله ابتدا گره حسگر به محض دریافت پیام، شرط زمانی $|T_3 - T_2| < \Delta T$ را بررسی می‌کند. در صورت برقراری شرط، مقادیر روابط (۲۱) و (۲۲) را محاسبه می‌کند:

$$A_{14}^* = h(GW_{ID_j}||S_{SN_k}).P \quad (۲۱)$$
$$A_{15}^* = h(A_{14}^*||T_2) \quad (۲۲)$$

و سپس چک می‌کند $A_{15}^* = A_{15}$ که با رابطه‌ی (۲۲) برقرار است یا خیر، اگر این تساوی درست باشد یک عدد تصادفی r_s انتخاب می‌کند و مقادیر روابط (۲۳)، (۲۴)، (۲۵) و (۲۶) زیر را محاسبه می‌کند:

$$A_{17} = r_s.A_{12} \text{ و} \quad (۲۳)$$
$$A_{18} = h(A_{17}||S_{SN_K}||T_3) \quad (۲۴)$$
$$A_{13}^* = h(S_{SN_K}).A_{12} \text{ ، } A_8^{**} = A_{16} \oplus A_{13}^* \quad (۲۵)$$
$$A_{20} = r_s.P \text{ ، } A_{19} = r_s.A_8^{**}. \quad (۲۶)$$

در نهایت گره حسگر کلید نشست را به صورت $sk = r_s.A_{11}$ محاسبه می‌کند و پیام $M_3 = \langle A_{19}.A_{18}.A_{20}.T_3 \rangle$ را ارسال می‌کند.

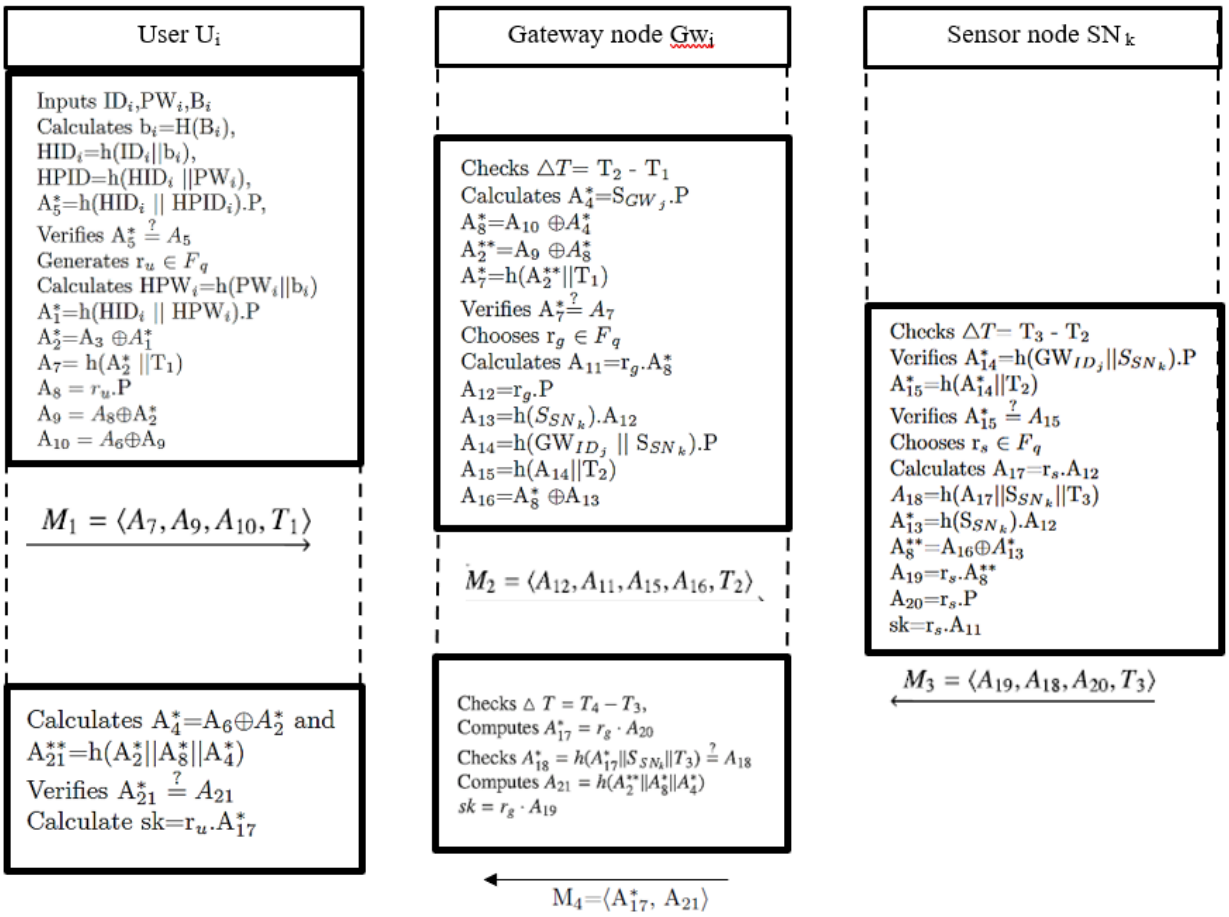
۶) بعد از دریافت پیام از گره حسگر، گره دروازه صحت زمان را بررسی می‌کند $|T_4 - T_3| < \Delta T$، در اینجا زمان جاری T_4 است. اگر این زمان قابل قبول باشد، گره دروازه مقادیر زیر را محاسبه می‌کند در غیر این صورت درخواست رد می‌شود. $A_{17}^* = r_g A_{20}$ را محاسبه می‌کند و همچنین درستی رابطه $A_{18}^* = A_{18}$ را با رابطه‌ی (۲۷) را چک می‌کند.

$$A_{18}^* = h(A_{17}^*||S_{SN_K}||T_3) \quad (۲۷)$$

اگر این تساوی برقرار بود گره دروازه مقدار رابطه‌ی (۲۸) زیر را محاسبه می‌کند.

$$A_{21} = h(A_2^{**}||A_8^*||A_4^*) \quad (۲۸)$$

و پیام $M_4 = \langle A_{17}^*.A_{21} \rangle$ را برای کاربر ارسال می‌کند و گره حسگر کلید نشست را به صورت $sk = r_g A_{19}$ محاسبه می‌کند. بعد از دریافت پیام M_4 از گره دروازه کاربر مقادیر $A_4^* = A_6 \oplus A_2^*$ و $A_{21}^* = h(A_2^*||A_8^*||A_4^*)$ را محاسبه می‌کند و چک می‌کند آیا رابطه $A_{21}^* = A_{21}$ برقرار است یا خیر. اگر این تساوی درست باشد، کاربر کلید نشست را به صورت $sk = r_u A_{17}^*$ محاسبه می‌کند. روند انجام ورود و احراز هویت پروتکل شورسکومار و همکاران [12] در شکل (۱) نشان داده شده است.



شکل ۱: مرحله ورود و احراز هویت در طرح شورسکومار و همکاران [۱۲]

٤_تجزیه‌وتحلیل امنیتی طرح شورسکومار و همکاران

در این بخش به تحلیل امنیتی طرح احراز اصالت شورسکومار و همکاران می‌پردازیم و نشان می‌دهیم که پروتکل احراز اصالت شورسکومار و همکاران [12] قادر به برقراری امنیت کامل نیست و در برابر حمله ردیابی، حمله نقض یکپارچگی و حمله غیر همزمان‌سازی آسیب‌پذیر است.

٤-١ حملات اعمال شده

۱) حمله ردیابی

عدم ردیابی ویژگی امنیتی است که تضمین می‌کند که سرور یا دشمن نمی‌توانند متوجه شوند که چه کاربری با گره دروازه و حسگر در حال ارتباط است. این مفهوم می‌تواند برای گره دروازه و حسگر هم مطرح شود. در این حمله، شخص حمله‌کننده یا مهاجم مراحل زیر را انجام می‌دهد و به واسطه اطلاعات به دست آمده می‌تواند شخص را ردیابی کند. ابتدا دشمن پیام M_1= $\langle A_7. A_9. A_{10}. T_1 \rangle$ را شنود کرده و بدست می‌آورد و از شرح پروتکل می‌دانیم که روابط (۱۳) و (۴) برقرار است و همچنین مقادیر روابط (۲۹)، (۳۰) و (۳۱) به طریق زیر محاسبه می‌شود:

$$A_2^* = h(HID_i || S_{Gw_j}).P \quad (۲۹)$$

$$A_6 = A_4 \oplus A_2^* \quad (۳۰)$$

$$A_6 = h(HID_i || S_{Gw_j}).P \oplus S_{GW_j}.P \quad (۳۱)$$

اگر دشمن دو مقدار A_{10} و A_9 شنود شده در پروتکل را با هم یای انحصاری کند به مقدار رابطه‌ی (۳۰) می رسد که یک مقدار ثابت مرتبط با هویت کاربر است. در واقع با انجام عملیات بالا می‌توان پی‌برد که یک اطلاعات ثابت مرتبط با یک کاربر به دست می‌آید که با آن می‌توان کاربر را ردیابی کرد. دراین صورت کاربر دارای خاصیت گمنامی نخواهد بود و حمله کننده می‌تواند با اطلاعات شنود شده فرد را شناسایی کند. احتمال موفقیت این حمله برابر یک و پیچیدگی آن یک بار اجرای پروتکل است.

۲) حمله نقض یکپارچگی

در پروتکل‌های امنیتی هرگونه تغییر در یک پیام باید در سمت دریافت کننده پیام حس شود، اگر این چنین نباشد در این صورت نقض یکپارچگی رخ داده است. برای حمله نقض یکپارچگی در طرح شورسکومار و همکاران کافی است که دشمن مراحل زیر را انجام دهد:

دشمن پیام M_1= $\langle A_7. A_9. A_{10}. T_1 \rangle$ را شنود می‌کند، اگر دشمن مقادیر A_{10} و A_9 رد و بدل شده را متوقف کند و با مقادیر دلخواه یای انحصاری کند به رابطه (۳۲) خواهد رسید:

$$A'_9 = A_9 \oplus \Delta \quad و \quad A'_{10} = A_{10} \oplus \Delta \qquad (۳۲)$$

و به‌جای مقادیر A_9 و A_{10} مقادیر رابطه (۳۲) را بفرستد، توسط گره دروازه و گره حسگر این تغییر تشخیص داده نمی‌شود، در حالی که تمام پیام‌های پروتکل باید قابلیت ارزیابی یکپارچگی داشته باشند، یعنی طرف دیگر پروتکل باید متوجه هر گونه تغییر در پیام ارسالی شود. دلیل این امر هم آن است که درستی این پیام‌ها در سمت گیرنده‌ی پیام به هیچ‌وجه بررسی نمی‌شود. احتمال موفقیت این حمله برابر یک و پیچیدگی آن یک بار اجرای پروتکل است.

۳) حمله غیر همزمان‌سازی

در حمله غیر همزمان سازی دشمن با انجام اقداماتی سعی می‌کند که دو طرف ارتباط را از همزمانی خارج نماید. این کار می‌تواند به صورت مثال با انجام اقداماتی انجام گیرد که منجر به این می‌شود که مقادیر مخفی مشترک در طرفین ارتباط به مقادیر متفاوتی بهنگام شوند که منجر به خروج از همزمانی یکدیگر می‌شود. برای انجام حمله غیر همزمان‌سازی بر علیه طرح شورسکومار و همکاران کافی است دشمن به صورت زیر عمل کند:

۱) دشمن $M_2 = \langle A_{12}.A_{11}.A_{15}.T_2 \rangle$ را شنود می‌کند، در این جا مقدار A_{11} برابر است با $A_{11} = r_g.A_8^*$.

۲) سپس با توجه به مراحل پروتکل می‌بینیم که یکپارچگی A_{11} توسط گره حسگر بررسی نمی‌شود، بنابراین اگر به جای مقدار A_{11} در پیام، مهاجم مقدار A_{11} را با یک مقدار دلخواه یای انحصاری بیتی کند، در این صورت مقدار A_{11} مانند $A'_{11} = A_{11} \oplus \Delta$ خواهد شد و اگر این مقدار ارسال شود، کلید محاسبه شده در سمت گره حسگر به صورت رابطه (۳۳) خواهد بود:

$$sk = r_s.A'_{11} = r_s.(A_{11} \oplus \Delta) \qquad (۳۳)$$

سپس A_{19} را برای گره دروازه ارسال می‌کند. همانطور که می‌دانیم مقدار $A_{19} = r_s.A_8$ و $A_{20} = r_s.P$ است.

۳) حال اگر دشمن A_{19} را نیز همچنین به مقدار A'_{19} تغییر دهد و برای گره دروازه ارسال کند، در نهایت کلید در گره دروازه به صورت $sk = r_g.A'_{19}$ خواهد بود، که این کلید با کلید محاسبه شده در سمت گره حسگر متفاوت است.

۴) اگر دشمن A_{17} را هم به A'_{17} تغییر دهد، کلید در سمت کاربر می‌شود $sk = r_u.A'_{17}$ که در این صورت کلید در سه سمت پروتکل تفاوت خواهد داشت. در نتیجه کلید در این سه طرف پروتکل یکسان نیست و عملاً چنان‌چه برای رمز کردن اطلاعات به کار رود دیگر این اطلاعات قابل رمزگشایی نخواهد بود. چون در سمت گیرنده کلید رمزگشایی متفاوت از کلید رمزگذاری است. بنابراین پروتکل فوق در برابر حمله همزمان سازی مقاوم نیست. احتمال موفقیت این حمله برابر یک و پیچیدگی آن یک بار اجرای پروتکل است.

٤-۲ تحلیل امنیتی طرح شورسکومار و همکاران

ابزار Scyther : Scyther [13]، یکی از ابزارهای شبیه‌سازی پروتکل برای تأیید امنیت است که در آن پیاده‌سازی پروتکل بر اساس تعریف نقش انجام می‌شود. در شبیه‌سازی پروتکل شورسکومار و همکاران، سه نقش گره دروازه، کاربر و گره حسگر است و در مرحله ورود و احراز اصالت ۴ پیام $\{M1.M2.M3.M4\}$، از طریق کانال‌های (dy) رد و بدل می‌شوند. طرح شورسکومار و همکاران را در ابزار امنیتی Scyther به زبان spdl [۱۲] پیاده سازی کردیم. همان طور که در شکل (۲) نشان داده شده است نتایج حاصل از ارزیابی نشان می‌دهد که طرح احراز اصالت شورسکومار و همکاران در سمت کاربر سه ادعای امنیتی [۱۳] Alive، Weakagree و Nisynch را برآورده نمی‌کند که بار دیگر بر حملات ارائه شده در این مقاله صحه می‌گذارد. در ابزار خودکار تحلیل امنیتی Scyther انواع مختلفی از ادعاهای امنیتی وجود دارد که برخی از مهم‌ترین آنها در زیر تعریف شده‌اند [14].

Secret: این ادعا به این معنی است که در پروتکل مورد بررسی، مقدار مخفی مورد نظر به صورت مخفی نگاه داری می‌شود و افراد غیر مجاز قادر به دسترسی به آن نیستند.

Alive: بدین معنی است که اگر نقشی یک اجرا را تمام کرده باشد، نقش دیگر قبلاً شروع به اجرا شدن کرده باشد و نتایج تجزیه تحلیل صحت این ادعا را توجیه می‌کند. این ادعای امنیتی در واقع بررسی می‌کند که یک طرف پروتکل با طرف مورد نظر خودش در ارتباط است. به عبارت دیگر یک پروتکل برای آغازگر A زنده بودن عامل B دیگر را تضمین می‌کند اگر: هرگاه (A که به عنوان آغازگرعمل می‌کند) اجرای پروتکل را، ظاهراً با پاسخ دهنده B، کامل می‌کند، B قبلاً پروتکل را اجرا کرده است.

Weakagree: این ادعا به این معنی است وقتی یک نقش یک اجرا را تمام کرد، نقش دیگر قبلاً شروع به اجرا شده باشد و نقش اول به ظاهر با نقش دوم در ارتباط است و نتایج تجزیه و تحلیل صحت این ادعا را توجیه می‌کند. به عبارت دیگر Weakagree به یک توافق ضعیف تمایل دارد، که درآن طرف‌های ارتباطی باید مطمئن شوند که در واقع با یکدیگر در ارتباط هستند تا از جعل هویت یکی از آن‌ها توسط مهاجم جلوگیری کنند.

Nisynch: این ادعا به این معنی است که رویدادهای دریافت و ارسال توسط نقش‌ها و به ترتیب و دارای محتوای اصلی مد نظر اجرا می‌شوند و نتایج تجزیه و تحلیل صحت این ادعا را توجیه می‌کند.

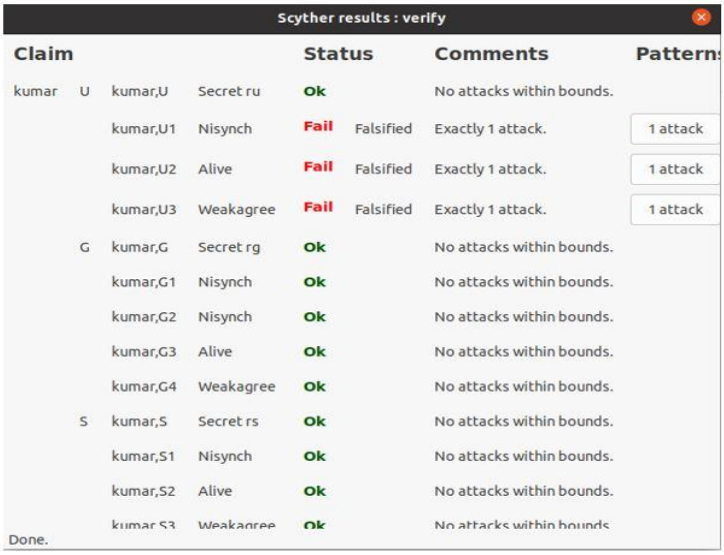
Niagree: این ادعای امنیتی به این معنی است که فرستنده و گیرنده درمورد مقادیر مخفی مبادله شده توافق دارند و نتایج تجزیه و تحلیل صحت این ادعا را توجیه می‌کند.

۵_ توصیه‌هایی جهت بهبود امنیت طرح شورسکومار و همکاران

در این قسمت توصیه می‌شود برای مقاوم کردن پروتکل شورسکومار در برابر حملات ارائه شده در این مقاله نکات زیر در نظر گرفته شوند:

۱) برای مقاوم کردن پروتکل شورسکومار در برابر حمله تکرار توصیه می‌شود که در پیام M_4 یک مهر زمانی مثلاً T_4 اضافه‌شود.

۲) برای مقاوم کردن پروتکل شورسکومار و همکاران در برابر حمله غیرهمزمان سازی توصیه می‌گردد که در قسمت کاربر و گره دروازه تغییراتی



شکل ۲: نتایج ارزیابی امنیتی طرح احراز اصالت شورسکومار و همکاران در ابزار Scyther [۱۲]

را در مقادیر برخی پیام‌ها داشته باشیم. یکی از پیشنهادها این است که در بخش کاربر پیام A_{10} را برای جلوگیری از حمله ردیابی می‌توان حذف کرد. با این حذف مقدار A_9 هم باید به صورت $A_9 = A_8 \oplus A_4^*$ تغییر یابد. همین طور مقدار A_7 هم باید به $A_7 = h(A_8||A_4^*||T_1)$ تغییر پیدا کند که دیگر نتوان مقدار A_9 را هم تغییر داد و در صورت تغییر A_9 نتوان A_7 متناظر با آن را تولید کرد. چرا که مقدار A_9 به مقدار A_8 و A_4^* بستگی دارد. A_4^* که یک مقدار مخفی مشترک بین کاربر و گره دروازه است که با تغییر A_9 مقدار A_8 محاسبه شده در سمت گره دروازه تغییر می‌کند و در نتیجه مقدار A_7 محاسبه شده در سمت گره دروازه با مقدار A_7 دریافتی برابر نخواهد بود و حمله غیر همزمان‌سازی شرح داده شده در این مقاله بر این پروتکل بهبود یافته قابل اعمال نخواهد بود.

۳) برای مقاوم سازی پروتکل شورسکومار و همکاران در برابر حمله نقض یکپارچگی می بایست در پروتکل بهبود یافته یکپارچگی پیام‌های مرتبط با A^*_{17} و A_{19} و A_{21} در سمت گیرنده پیام‌ها بررسی شود تا حمله نقض یکپارچگی شرح داده شده در این مقاله بر این بهبود پروتکل قابل اعمال نباشد.

٦_ نتیجه گیری

در این مقاله، طرح احراز اصالت شورسکومار و همکاران که برای استفاده برای نظارت از راه دور بر بیمار ارائه شده بود مورد تحلیل و بررسی امنیتی قرار گرفت و نشان داده شد که این طرح در برابر حمله نقض یکپارچگی، حمله غیر همزمان سازی و حمله ردیابی آسیب‌پذیر است و قادر به ارائه امنیت کامل نیست. احتمال موفقیت تمام حملات ارائه شده در این مقاله برابر یک و پیچیدگی آن‌ها تنها یک‌بار اجرای طرح است. سپس امنیت آن را با استفاده از ابزار تحلیل امنیتی Scyther ارزیابی نمودیم که نتایج حاصل از آن هم عدم برقراری امنیت کامل این طرح را نشان می‌دهد. در انتها هم توصیه‌هایی برای بهبود پروتکل کومار و همکاران بیان گردید. امکان شرح کامل پروتکل بهبود یافته و اثبات امنیتی آن به دلیل محدودیت صفحه امکان پذیر نشد.

۷- مراجع

[1] Ghoneim, A., Muhammad, G., Amin, S. U., Gupta, B., "*Medical Image Forgery Detection for Smart Healthcare*", IEEE Communications Magazine, Vol. 56, No. 4, pp. 33-37, 2018.

[2] Abidi, B., Jilbab, A., Haziti, M. E., "*Wireless sensor networks in biomedical: Wireless body area networks*", In Europe and MENA cooperation advances in information and communication technologies, pp. 321-329. Springer, Cham, 2017.

[3] Gai, K., Qiu, M., "*Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers*", IEEE Transactions on Industrial Informatics, Vol. 14, No. 8, pp. 3590-3598, 2018.

[4] Liu, C.-H., and Chung, Y.-F., "*Secure user authentication scheme for wireless healthcare sensor networks*", Computers & Electrical Engineering, Vol. 59, pp. 250-261, 2017.

[5] Li, C. T., Wu, T. Y., Chen, C. L., Lee, C. C., Chen, C. M., "*An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system*", *Sensors*, Vol.17, No.7, pp. 1-18, 2017.

[6] Kaul, S. D., Awasthi, A. K., "*Security enhancement of an improved remote user authentication scheme with key agreement*", Wireless Personal Communications, Vol. 89, No. 2, pp. 621-637, 2016.

[7] Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S. A., Zikria, Y. B.,"*A secure and lightweight authentication scheme for next generation IoT infrastructure*", Computer Communications, Vol. 165, pp. 85-96, 2021.

[8] Kumar, V., Ahmad, M., Mishra, D., Kumari, S. and Khan, M.K., "*RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing*", Vehicular Communications, Vol. 22, p.100213, 2020.

[9] Safkhani, M., Camara, C., Peris-Lopez, P., Bagheri, N., "*RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud*

computing", Vehicular Communications, Vol. 28, p. 100311, 2021.

[10] Fakroon, M., Alshahrani, M., Gebali, F., Traore, I., "*Secure remote anonymous user authentication scheme for smart home environment*", Internet of Things, Vol. 9, p. 100158, 2020.

[11] Sureshkumar, V., Amin, R., Vijaykumar, V. R., Sekar, S. R., "*Robust secure communication protocol for smart healthcare system with FPGA implementation*", Future Generation Computer Systems, Vol. 100, pp. 938-951, 2019.

[12] Cremers, C. J., "*The Scyther Tool: Verification, falsification, and analysis of security protocols*", In International conference on computer aided verification, Springer, pp. 414-418, 2008.

[13] Lowe, G., "*A hierarchy of authentication specifications*", In Proceedings 10th Computer Security Foundations Workshop, IEEE, pp. 31-43, 1997.

زیرنویس‌ها

[1] MWSNS (Medical Wireless Sensors Networks)

[2] Sureshkumar et al.

[3] Wireless Sensor Network (WSN)

[4] Liu and Chung

[5] Li et al.

[6] Kaul and Awasthi

[7] Rana et al.

[8] Vinod Kumar et al.

[9] Shuai et al.

[10] Fakroon et al.

[11] Timestamp

[12] Security Protocol Description Language

[13] Security Claim