دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۲ (۵۶-۶۴)
https://monadi.isc.org.ir

ارائه‌شده در بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه تربیت مدرس و پژوهشگاه ارتباطات و فناوری اطلاعات، ۲۵ و ۲۶ مهرماه ۱۴۰۳

نقض خاصیت یکپارچگی در یک پروتکل حافظ حریم خصوصی انتها به انتها در سامانه‌های پایش سلامت مبتنی بر اینترنت اشیا★

فاطمه غلامی سبزوار و معصومه صفخانی*

گروه نرم‌افزار، دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
اینترنت اشیا
حفظ حریم خصوصی
حمله نقض یکپارچگی
زنجیره قالب‌های سلسله مراتبی
سامانه‌های مراقبت بهداشتی

نوع مقاله: پژوهشی

چکیده

حفظ حریم خصوصی در سامانه‌های مراقبت بهداشتی، همواره مورد توجه بیماران و پزشکان بوده است. برای حل این مشکل پروتکل‌های بسیاری طراحی شده است. در این مقاله به بررسی طرح پیشنهادی نصر اصفهانی و همکاران پرداختیم و این طرح را از نظر امنیتی مورد بررسی قرار داده‌ایم. طرحی که آن‌ها پیشنهاد داده‌اند از یک زنجیره قالب‌های سلسله مراتبی سه لایه، برای ذخیره و نگهداری اطلاعات مهم پزشکی بیماران، به صورت متمرکز و ایمن، استفاده می‌کند. همچنین به کمک اثبات ناتراوا (ZKP) و روش امضای حلقه، نشان داده‌اند که طرح آنها امنیت داده‌های پزشکی را در برابر هم حملات داخلی و هم حملات خارجی حفظ می‌کند. طبق سناریوهای احتمالی، پروتکل نصر اصفهانی و همکاران توانسته است در برابر بسیاری از حملات، مانند حمله ذخیره‌سازی و حمله تکرار عملکرد خوبی را داشته‌باشد اما در برابر حمله نقض یکپارچگی آسیب‌پذیر است. احتمال موفقیت حملات ارائه شده در این مقاله برابر یک و پیچیدگی آن تنها یک‌بار اجرای پروتکل است.

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

مفهوم اینترنت اشیا (IoT [1]) توسط یک کارآفرین بریتانیایی به‌نام کوین آشتون [2] در سال ۱۹۹۹ معرفی شد. اینترنت اشیا به‌عنوان یک فناوری محبوب، مورد توجه افراد زیادی قرارگرفته‌است. این فناوری شامل انواع دستگاه‌های هوشمند مانند دوربین‌ها، حسگرها و دستگاه‌های تلفن همراه است که قادرند اطلاعات را جمع‌آوری کرده، آنها را به صورت زمان واقعی ضبط کرده و برای هدف مشخصی به کار بگیرند. اینترنت اشیا در بخش‌های مختلفی از جمله در حوزه بهداشت، کاربردهای گسترده‌ای داشته است.

با افزایش بیماری‌ها در سراسر جهان، استفاده از اینترنت اشیا توانسته است به صورت قابل توجهی به صنعت بهداشت کمک نماید. حسگرهای متصل به بدن، علائم حیاتی بیماران را به صورت لحظه‌ای اندازه‌گیری و نظارت کرده و به این ترتیب ارائه‌دهندگان خدمات بهداشت امکان رصد کامل وضعیت بیماران را خواهند داشت. این امکان موجب می‌شود که روش‌های بهتری برای درمان به کار گرفته شود که منجر به کاهش مدت درمان و افزایش سرعت بهبود بیماران می‌شود. عواملی نظیر هزینه‌های مالی و زمانی مرتبط با مراجعه بیماران به مراکز بهداشت اثرات منفی بر دسترسی بیماران دارد. با ظهور اینترنت اشیا در حوزه بهداشت، بیماران قادرند از راه دور و بدون حضور فیزیکی در مراکز درمانی، خدمات پزشکی را دریافت نمایند. نظارت از راه دور امکان می‌دهد که ارائه‌دهندگان خدمات بهداشت، به سرعت وضعیت بیمار را تشخیص دهند و تمهیدات

★از کمیته علمی بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول.
آدرس‌های رایانامه: Fatemeh.glm@sru.ac.ir (فاطمه غلامی سبزوار)، Safkhani@sru.ac.ir (معصومه صفخانی)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] Internet of Things [2] Kevin Ashton

لازم را برای درمان وی به کار بگیرند.

یکی از چالش‌های اصلی کاربران در استفاده از اینترنت اشیا، مسائل امنیتی و حفظ حریم خصوصی بیماران است. به دلیل ارتباط بی‌سیم دستگاه‌ها آنها در مقابل انواع حملات سایبری آسیب‌پذیر هستند. به‌علاوه، به دلیل محدودیت منابع آنها، پروتکل‌های امنیتی قوی لازم هستند تا جلوی دسترسی غیرمجاز و دستکاری در داده‌های کاربر را بگیرند. حفظ حریم خصوصی یک نیاز امنیتی حیاتی در این سیستم‌ها است زیرا این دستگاه‌ها مقدار زیادی از داده‌های شخصی کاربران را جمع آوری می‌کنند و کنترل زیادی بر زندگی افراد دارند. اگر افراد غیرمجاز به این اطلاعات دسترسی پیدا کنند، خسارات جبران‌ناپذیر را وارد می‌کنند، حتی در مواقعی موجب از دست رفتن جان افراد می‌شوند.

سامانه‌های مبتنی بر اینترنت اشیا، با قابلیت نظارت و اطلاع رسانی فعالیت‌ها، می‌توانند نقش حیاتی را در برنامه‌های مبتنی بر انسان ایفا کنند. همچنین امکان کنترل مصرف منابع را دارند و زندگی امروزی را آسان‌تر کرده‌اند.

ارتباط این کاربردها با شبکه اینترنت، امکان بروز حملات متعدد را افزایش می‌دهد. امنیت و حریم خصوصی مهم‌ترین چالش سامانه‌های مبتنی بر اینترنت اشیا است. انواع مختلفی از نیازهای امنیتی مورد نیاز در این سامانه‌ها، از جمله محرمانگی، احراز اصالت متقابل و مدیریت صحیح کلیدهای جلسه است. به ویژه، احراز اصالت نیاز امنیتی مهمی برای برقراری ارتباط قابل اطمینان و انتقال اطلاعات امن در سامانه‌های مبتنی بر اینترنت اشیا است. عمده روش‌های احراز اصالت موجود، مبتنی بر تابع چکیده ساز[1]، رمزنگاری مبتنی بر داده‌های زیست‌سنجی، مبتنی بر کارت هوشمند و رمزنگاری منحنی بیضوی (ECC[2]) طراحی‌شده‌اند. استفاده از اینترنت اشیا به ویژه در سیستم‌های بهداشت از راه دور توانسته برای جامعه پزشکی سودمند باشد. حسگرهای جاساز شده در بدن بیماران، اطلاعات مرتبط با سلامتی مانند گلوکز خون، ضربان قلب، دما و فشار خون را اندازه‌گیری می‌کنند و آنها را به دروازه‌ها انتقال می‌دهند. دروازه‌ها این اطلاعات مهم و خصوصی را برای بهبود بیماران جمع‌آوری و ذخیره می‌کنند که می‌توانند در هر زمان توسط کاربران با دسترسی مجاز به سامانه، مورد بررسی قرار گیرند. با توجه به نگرانی‌ها در مورد دسترسی غیرمجاز به اطلاعات سلامت بیماران و دستکاری در داده‌ها ما در ادامه این مقاله به بررسی کامل امنیتی طرح نصر اصفهانی و همکاران [۱] پرداخته‌ایم.

۲ کارهای مرتبط

در سال‌های گذشته، مقالات زیادی در مورد حفظ امنیت و حریم خصوصی سامانه‌های پزشکی ارائه داده شده است. یویانگ و همکاران در [۲] یک مدل حفظ حریم خصوصی را در شبکه‌های بهداشت هوشمند ارائه می‌دهند که بر پایه زنجیره قالب‌ها طراحی شده است و قابلیت اعتبارسنجی و پیگیری داده‌های حساس پزشکی را دارد. حسین کوشا در [۳] حفظ حریم خصوصی کاربر را مورد توجه قرار داده است و از معماری زنجیره قالب‌ها برای کنترل دسترسی کاربران به داده‌های سلامت استفاده کرده است.

شیا و همکاران در [۴] طرحی به‌نام MeDShare را ارائه داده‌اند که با استفاده از زنجیره قالب‌ها امکان حفظ حریم خصوصی داده و کنترل دسترسی ارائه‌دهندگان خدمات ابری را فراهم می‌کند.

دیباک و همکاران در [۵] یک روش احراز اصالت ناشناس مبتنی بر داده زیست‌سنجی برای حفظ حریم خصوصی در سامانه پزشکی را ارائه می‌دهد.

دویدی و همکاران در [۶] راه‌حل‌هایی را برای امنیت بیشتر و ناشناسی داده‌ها در سیستم‌های از راه دور به کمک فناوری زنجیره قالب‌ها برای حفظ حریم خصوصی پزشکی ارائه می‌دهد.

گوتیرز و همکاران در [۷] سعی کردند که طرحی را ارائه دهند که با استفاده از هوش‌مصنوعی، علاوه بر اینکه انتقال داده‌ها به صورت امن در سامانه سلامت از راه دور مبتنی بر زنجیره قالب‌ها صورت بگیرد، مصرف انرژی هم کاهش یابد.

فتحی و همکاران در [۸] یک پروتکل RFID[3] حفظ حریم خصوصی بیماران و احراز اصالت بر اساس رمزنگاری الجمال[4] ارائه داده‌اند. همچنین با استفاده از ابزار AVISPA[5] نشان داده‌اند که طرح پیشنهادی‌شان در برابر انواع حملات فعال و غیرفعال ایمن است. شانگ و همکاران در [۹] طرح احراز اصالتی مبتنی بر کارت هوشمند در محیط چند سروره، برای احراز اصالت کاربران ارائه داده‌اند.

خدیجا و همکاران در [۱۰] سامانه‌ای امن را برای نگهداری داده‌های پزشکی مبتنی بر زنجیره قالب‌ها، ارائه داده‌اند.

زیشان و همکاران در [۱۱] یک طرح بهبود یافته برای شبکه‌های بی‌سیم حسگرهای بهداشتی (WHSN[6]) ارائه نموده‌اند.

یانگ و همکاران نیز در [۱۲] یک طرح احراز اصالت جدید در شبکه‌های بی‌سیم حسگرهای بهداشتی (WBANs) ارائه دادند که امنیت بالایی در مقابل انواع حملات دارد.

بخش‌های مقاله به شرح زیر سازمان‌دهی شده است: طرح نصر اصفهانی و همکاران [۱] در قسمت ۳ به صورت مختصر شرح داده می‌شود. در قسمت ۴ امنیت طرح نصر اصفهانی و همکاران [۱] و چگونگی حمله صورت گرفته بر آن مورد بررسی قرار می‌گیرد. در قسمت ۵ این مقاله با نتیجه‌گیری به پایان می‌رسد.

[1] Hash function
[2] Elliptic Curve Cryptography
[3] Radio-Frequency Identification
[4] El-Gamal
[5] A tool for Validating Internet Security Protocols and Applications
[6] Wireless Body Area Networks

۳ طرح نصر اصفهانی و همکاران

پروتکل احراز اصالت مبتنی بر اینترنت اشیا که توسط نصر اصفهانی و همکاران ارائه شده است و در شکل ۱ قابل مشاهده است، به منظور حفظ اطلاعات محرمانه پزشکی بیماران در معرض تهدیدات داخلی و خارجی قرار دارد. این پروتکل شامل مراحل ثبت‌نام و تبادل کلید و مرحله اعتبارسنجی و احراز اصالت می‌باشد.

در جدول ۱ علامت و نمادهای استفاده‌شده در این مقاله نشان داده شده است.

در مرحله ثبت‌نام و تبادل کلید، مرکز توزیع کلید (KDC[1]) گواهی‌نامه‌های کلید عمومی برای کاربران برنامه، نقاط دسترسی (APs) و دروازه‌ها (GWs) ایجاد می‌کند و کلیدهای عمومی و خصوصی را صادر می‌کند. همچنین، مرکز توزیع کلید یک فهرست ابطال گواهینامه را برای بررسی اعتبار دروازه‌ها ارسال می‌کند.

در مرحله اعتبار سنجی و احراز اصالت، اطلاعات حسگرها به صورت امن در اختیار کاربر برنامه قرار می‌گیرد. مدیر شبکه هر حسگر، اصالت‌های مستعار، مجوز یک‌بار مصرف و یک کلید مشترک را در جدولی به‌نام tablesensors ذخیره می‌کند.

پروتکل امنیتی نصر اصفهانی و همکاران تمامی نهادهای سامانه را غیرقابل‌اعتماد فرض می‌کند و امنیت را به صورت انتها به انتها در تمام پروتکل حفظ می‌کند. این پروتکل شامل اجزایی از جمله حسگرها، دروازه‌ها، برنامه‌های کاربر و کاربران نهایی است که به انتقال داده‌های پزشکی بیماران به صورت امن در سامانه بهداشتی مبتنی بر اینترنت اشیا کمک می‌کند.

۱.۳ مرحله احراز اصالت

(گام ۱) حسگر، یک عدد تصادفی با نام N_S تولید می‌کند و از آن برای ساخت AID_S به صورت

$$AID_S = h(N_S \| ID_S \| T_{seq} \| ID_U)$$

استفاده می‌کند. همچنین $N_X = (K_(S - NM) \oplus N_U)$ را نیز محاسبه می‌کند.

(گام ۲) حسگر، مقادیر $(N_X, AID_S, T_{seq}, ID_U)$ را برای دروازه ارسال می‌کند.

(گام ۳) دروازه، احراز اصالت خودش را به صورت اثبات ناتراوا به این ترتیب انجام می‌دهد که، یک پیام رمزگذاری شده که شامل چند بخش مختلف است را تولید می‌کند. به جز بخش اول، که شامل اطلاعات احراز اصالت است، برای بقیه بخش‌ها اگر بیت چالشی تولید شده توسط برنامه کاربر صفر باشد $(cha_i = ۰)$ در نتیجه $Res_i = Iso_i$، در غیر این‌صورت پاسخ $Res_i = Sol_{Gi}$ را بر می‌گرداند. در آخر

[1] Key Distribution Centre

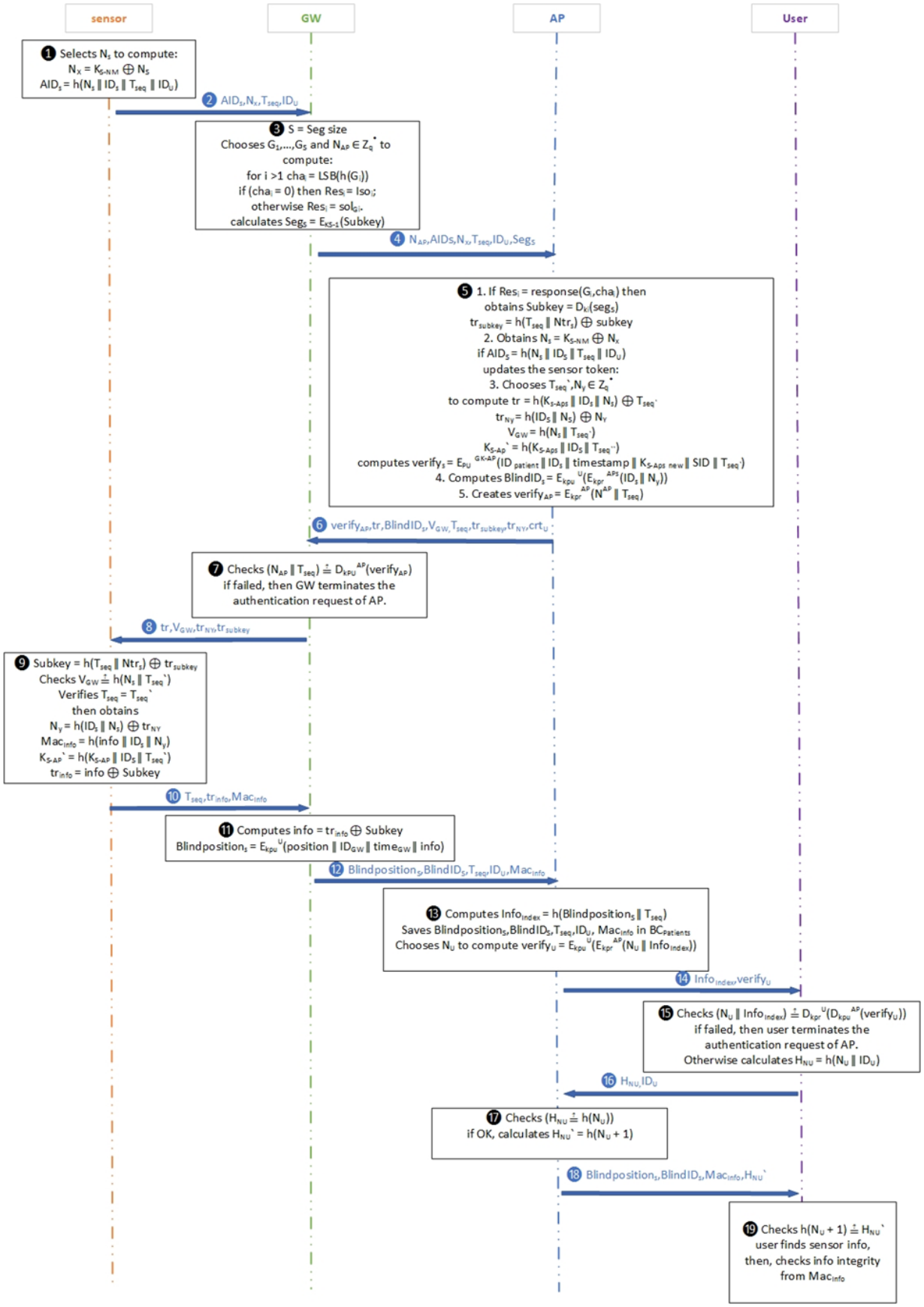
جدول ۱. علائم و نمادهای مورد استفاده در این مقاله

نماد	شرح
U	کاربر
GW	دروازه
AP	برنامه کاربر
NM	مدیر شبکه
K_{pr}^{AP}, K_{pu}^{AP}	کلید عمومی و خصوصی برنامه
K_{pr}^{U}, K_{pu}^{U}	کلید عمومی و خصوصی کاربر
K_{pr}^{NM}, K_{pu}^{NM}	کلید عمومی و خصوصی مدیر شبکه
S	امضای دروازه
$Timestamp$	مهر زمانی
$\|$	عملیات الحاق رشته‌ها
h	تابع چکیده ساز رمزنگاری
$position$	مکان دروازه
ID_S	شناسه حسگر
ID_U	شناسه کاربر
$Subkey$	کلید جلسه مشترک
Mac_{info}	کد احراز اصالت پیام
K_{S-NM}	کلید مشترک حسگر و مدیر شبکه
T_{seq}	مجوز یک‌بار مصرف
N_U, N_{AP}	اعداد تصادفی تولید شده توسط برنامه و کاربر
crt_U	گواهینامه کاربر
t_C	زمان فعلی
ΔT	تاخیر زمانی
Sol_G	یک پاسخ برای مسئله‌ی سخت
$n_h, r_j, N_Y, N_S, N_{AP}$	اعداد تصادفی
Seg_i	iامین بخش پیام احراز اصالت دروازه
G_i	iامین گراف هم‌ریخت برای ارتباط
Cha_i	iامین بیت چالشی انتخاب شده توسط اثبات کننده
Res_i	iامین پاسخ برای چالش
Cha_i	روی گراف G_i
Sol_G	پاسخ مسئله سخت بر روی گراف G_i
K_i	iامین کلید رمزنگاری

مقدار Seg_S را که، S اندازه هر بخش است، به صورت $Seg_S = E_(K_{s-۱})(Subkey)$ محاسبه می‌کند. برای جزئیات بیشتر خواننده می تواند به [۱] مراجعه کند.

(گام ۴) دروازه، مقادیر $(N_AP, AID_S, T_{seq}, ID_U, N_X, Seg_S)$ را برای برنامه کاربر ارسال می‌کند.

(گام ۵) در این گام برنامه کاربر پاسخ Res_i را بررسی می‌کند. در



شکل ۱. طرح نصر اصفهانی و همکاران [۱]

صورت تأیید پاسخ، مقدار $Subkey$ را با رمزگشایی Seg_S به صورت $Subkey = D_{K_i}(Seg_i)$ به دست می‌آورد. برای جزئیات بیشتر خواننده می تواند به [۱] مراجعه کند. سپس مقدار N_S را به صورت $N_S = K_{S-NM} \oplus N_X$ به دست می‌آورد. سپس صحت AID_S را با توجه به عبارت

$$AID_S = h(N_S \| ID_S \| T_{seq} \| ID_U)$$

بررسی می‌کند و در صورت صحیح بودن، مجوز حسگر را به این ترتیب به‌روز رسانی می‌کند:

- ابتدا یک مقدار تصادفی $N_Y \in Z_q^*$ را انتخاب می‌کند و مقادیر زیر را محاسبه می‌کند:

$$tr = h(K_{S-APs} \| ID_S \| N_S) \oplus T_{seq}$$
$$tr_{NY} = h(ID_S \| N_S) \oplus N_Y$$

و دروازه $V = h(T_{seq} \| N_S)$ را محاسبه می‌کند و کلید مشترک جدید بین خود و حسگر را به صورت

$$K'_{S-APs} = h(K_{S-APs} \| T'_{seq} \| ID_S)$$

می‌سازد.

- برنامه کاربر، مقدار شناسه حسگر $BlindID_S$ را با رابطه‌ی

$$BlindID_S = E_{K_{pu}^U}(E_{K_{pr}^{APs}}(ID_S \| N_Y))$$

برای کاربر رمزگذاری می‌کند که تنها کاربر با کلید خصوصی خود می‌تواند آن را باز کند.

- در آخر برنامه کاربر $verify_{AP}$ را برای احراز اصالت خود، به صورت

$$verify_{AP} = E_(K_{pr}^{APs})(N_{AP} \| T_{seq})$$

می‌سازد.

(گام ۶) برنامه کاربر، مقادیر

$$(verify_{AP}, tr, BlindID_S, T_{seq}, tr_{subkey}, V_{GW}, tr_{NY}, crt_U)$$

را به دروازه ارسال می‌کند.

(گام ۷) دروازه، با رمزگشایی $verify_{AP}$، صحت عبارت زیر را برای احراز اصالت برنامه کاربر، بررسی می‌کند و در صورت عدم‌تأیید، جلسه را پایان می‌دهد.

$$(N_{AP} \| T_{seq}) = D_{K_{pu}^{AP}}(verify_{AP})$$

(گام ۸) دروازه، مقادیر $(tr, tr_{subkey}, V_{GW}, tr_{NY})$ را برای حسگر ارسال می‌کند.

(گام ۹) حسگر، مقدار $Subkey$ را با توجه به رابطه

$$Subkey = h(T_{seq} \| Ntr_S) \oplus tr_{subkey}$$

به دست می‌آورد و سپس بعد از تأیید صحت مجوز جدید، مقدار عدد تصادفی N_Y را به صورت

$$N_Y = h(ID_S \| N_S) \oplus tr_{NY}$$

به دست می‌آورد و Mac_{info} را به صورت

$$Mac_{info} = h(info \| ID_S \| N_Y)$$

می‌سازد. سپس کلید جدید مشترک خود با برنامه کاربر را به صورت

$$K'_{S-APs} = h(K_{S-APs} \| T'_{seq} \| ID_S)$$

می‌سازد. سپس $tr_{info} = info \oplus Subkey$ را محاسبه می‌کند.

(گام ۱۰) حسگر، مقادیر $(tr_{info}, Mac_{info}, T_{seq})$ را برای دروازه ارسال می‌کند.

(گام ۱۱) دروازه، اطلاعات حسگر با مقدار $info$ را با توجه به رابطه $info = Subkey \oplus tr_{info}$ به دست می‌آورد و سپس $Blindposition_S$ را به صورت زیر محاسبه می‌کند.

$$Blindposition_S = E_{K_{pu}^U}(position \| ID_{GW} \| time_{GW})$$

(گام ۱۲) دروازه، مقادیر

$$(Blindposition_S, BlindID_S, T_{seq}, ID_U, Mac_{info})$$

را برای برنامه کاربر ارسال می‌کند.

(گام ۱۳) برنامه کاربر، $Info_{index}$ را به این صورت

$$Info_{index} = h(Blindposition_S \| T_{seq})$$

محاسبه کرده و سپس $verify_U$ را برای احراز اصالت کاربر، به صورت

$$verify_U = E_{Kpu}(E_{K_{pr}^{AP}}(N_U \| Info_{index}))$$

که در آن N_U یک عدد تصادفی است، می‌سازد. در آخر مقادیر دریافتی

$$(Blindposition_S, BlindID_S, T_{seq}, ID_U, Mac_{info})$$

را در زنجیره قالب‌ها ذخیره می‌کند.

(گام ۱۴) برنامه کاربر، مقادیر $verify_U$ و $Info_{index}$ را برای کاربر ارسال می‌کند تا فرایند احراز اصالت خود را به کمک کاربر انجام دهد.

(گام ۱۵) کاربر، با بازکردن امضا با کلید عمومی امضا کننده $verify_U$ صحت عبارت

$$(N_U \| Info_{index}) = D_{Kpr}(E_{K_{pu}^{AP}}(verify_U))$$

را بررسی می‌کند و در صورت تأیید درستی، عبارت زیر را محاسبه می‌کند

$$HN_U = h(N_U).$$

(گام ۱۶) برنامه کاربر، در ابتدا یکسان بودن $HN_U = h(N_U)$ را بررسی می‌کند و در صورت تأیید، مقدار HN_U جدید را به صورت $HN'_U = h(N_U + ۱)$ محاسبه می‌کند.

(گام ۱۷) برنامه کاربر، مقادیر

$$(Blindposition_S, BlindID_S, Mac_{info}, HN'_U)$$

را برای کاربر ارسال می‌کند.

(گام ۱۸) کاربر صحت $h(N_U + ۱) = HN'_U$ را بررسی می‌کند و در صورت تأیید، اطلاعات حسگر را پیدا می‌کند و همچنین یکپارچگی اطلاعات را از روی مقدار Mac_{info} بررسی می‌کند.

۴ تجزیه و تحلیل امنیتی طرح نصر اصفهانی و همکاران

مهاجم به ترتیب زیر می‌تواند از طریق تغییر Subkey یکپارچگی پروتکل نصر اصفهانی و همکاران را نقض کند.

(۱) مهاجم مقدار Seg_s را به Seg'_s تغییر می‌دهد و در گام ۴ با توجه به شکل ۲، برای برنامه کاربر ارسال می‌کند.
(۲) با توجه به رابطه $Subkey = D_{K_i}(Seg_i)$ در گام ۵، با تغییر Seg_S، مقدار $Subkey$ به $Subkey'$ تغییر می‌یابد.
(۳) سپس برنامه کاربر، به‌اشتباه، مقدار tr'_{subkey} را به جای tr_{subkey} با توجه به رابطه

$$tr'_{subkey} = h(T_{seq}\|Ntr_S) \oplus Subkey'$$

محاسبه می‌کند و برای دروازه ارسال می‌کند.
(۴) دروازه، بعد از انجام احراز اصالت برنامه کاربر، مقدار $tr'_s ubkey$ را به سمت حسگر ارسال می‌کند.
(۵) در گام ۹، حسگر مقدار $tr'_s ubkey$ را از دروازه دریافت می‌کند و در نتیجه مقدار $Subkey'$ جدید را با توجه به رابطه‌ی

$$Subkey' = h(T_{seq}\|Ntr_S) \oplus tr'_{subkey}$$

به دست می‌آورد.
(۶) سپس به کمک $Subkey'$ که محاسبه کرده بود، مقدار tr'_{info} را از رابطه‌ی $tr'_{info} = info \oplus Subkey'$ به اشتباه محاسبه می‌کند و در گام ۱۰ برای دروازه ارسال می‌کند.
(۷) گره دروازه، مقدار tr'_{info} را از سمت حسگر دریافت می‌کند و به این ترتیب، مقدار $info'$ را با توجه به رابطه

$$info' = tr'_{info} \oplus Subkey'$$

به‌اشتباه به دست می‌آورد و همچنین $Blindposition'_S$ را به جای $Blindposition_S$ از رابطه‌ی

$$Blindposition'_S = E_{Kpu}(position\|ID_GW\|time_{GW}\|info')$$

محاسبه کرده و در گام ۱۲ برای برنامه کاربر می‌فرستد.
(۸) برنامه کاربر، بدون بررسی صحت اطلاعات دریافتی، مقدار نادرست $Blindposition'_S$ را در زنجیره قالب‌ها ذخیره می‌کند و در گام ۱۸ برای کاربر ارسال می‌کند. در نتیجه برنامه کاربر، از تغییرات مقدار $Blindposition'_S$ آگاهی نداشته و اقدام به ذخیره کردن اطلاعات بدون بررسی می‌کند که این مورد، یکپارچگی پروتکل نصر اصفهانی و همکاران را نقض می‌کند.

در ادامه حمله نقض یکپارچگی از طریق تغییر $Blindposition_S$ توسط مهاجم به ترتیب زیر انجام‌می‌شود:

(۱) در گام ۱۳ با توجه به شکل ۲، برنامه کاربر، مقدار نادرست $Blindposition'_S$ محاسبه شده توسط گره دروازه، را طبق مراحل قبل دریافت کرده و به این ترتیب با توجه به رابطه‌ی

$$Info'_index = h(Blindposition'_S\|T_{seq})$$

به‌جای $Info_{index}$، مقدار $Info'_{index}$ را محاسبه می‌کند.
(۲) به این ترتیب برنامه کاربر، مقدار تغییریافته‌ی $verify_U$ را با توجه به رابطه‌ی

$$verify_U = E_{Kpu}(E_{K^{AP}_{pr}}(N_U\|Info'_{index}))$$

برای تأیید احراز اصالت کاربر به اشتباه می‌سازد و در گام ۱۴ برای وی ارسال می‌کند.
(۳) سپس در گام ۱۵ عبارت

$$(N_U\|Info'_{index}) = D_{Kpr}(E_{K^{AP}_{pu}}(verify_U))$$

توسط کاربر رمزگشایی می‌شود و برنامه به اشتباه احراز اصالت می‌شود. در نتیجه مهاجم خود را به عنوان یک نهاد معتبر جا می‌زند و احراز اصالت می‌شود. در نتیجه با این سناریوی حمله نقض یکپارچگی، کاربر اطلاعات نادرست را از یک نهاد غیر معتبر دریافت می‌کند.

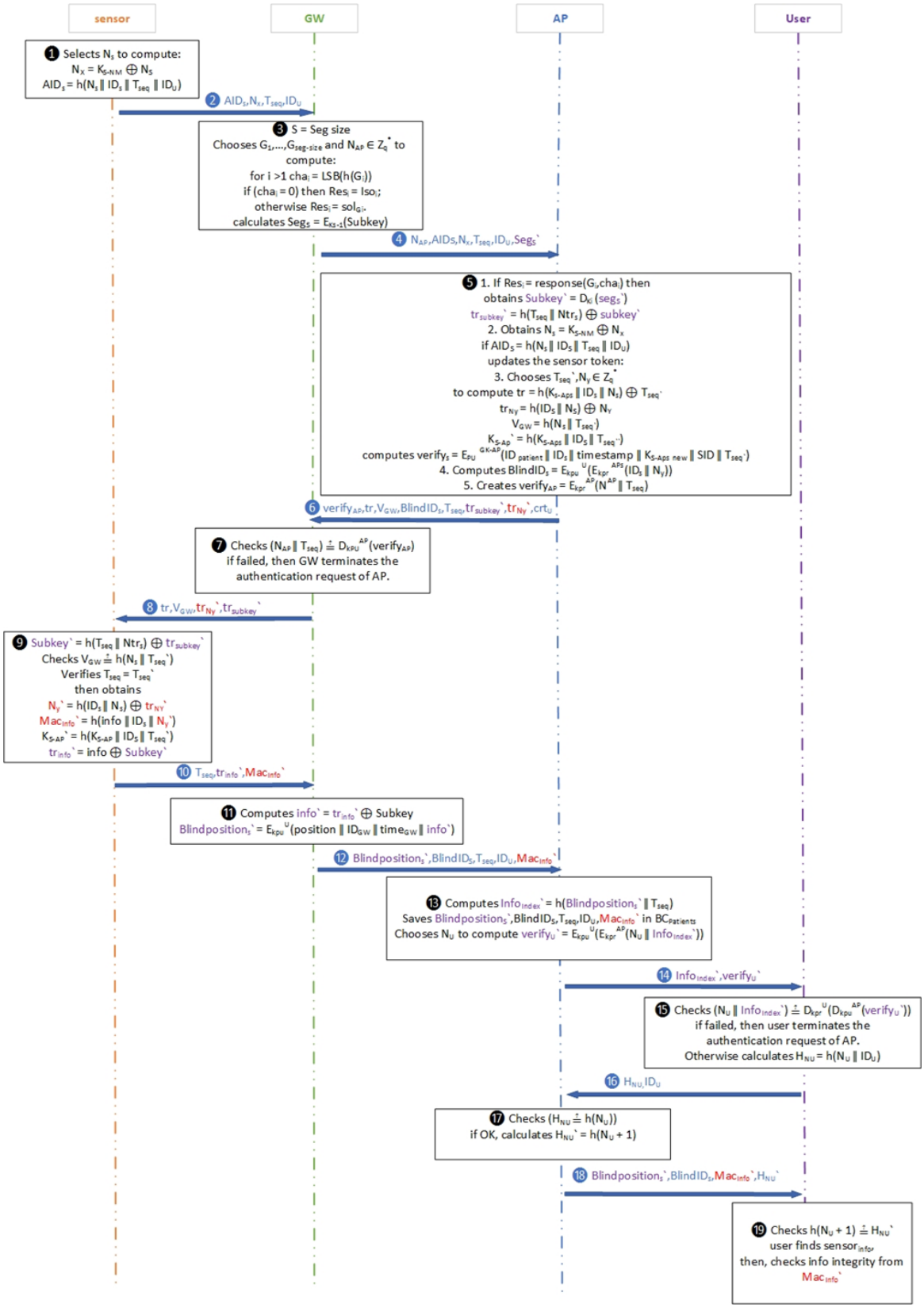
هم چنین به ترتیب زیر هم، با سناریوی دیگری هم می‌توان حمله نقض یکپارچگی را بر پروتکل نصر اصفهانی و همکاران وارد نمود.

مهاجم به ترتیب زیر از طریق تغییر Mac_{info} یکپارچگی پروتکل نصر اصفهانی و همکاران را نقض می‌کند:

(۱) مهاجم مقدار tr'_{NY} را در گام ۶ به جای tr_{NY} برای دروازه ارسال می‌کند که $tr'_{NY} = tr_{NY} \oplus \Delta$ است. Δ یک مقدار دلخواه غیر صفر است.
(۲) دروازه، بعد از اطمینان از احراز اصالت برنامه کاربر، مقدار tr'_{NY} را برای حسگر ارسال می‌کند.
(۳) حسگر با دریافت مقدار tr'_{NY} مقدار N'_Y را به جای N_Y با توجه به $N'_Y = h(ID_S\|N_S) \oplus tr'_{NY}$ محاسبه می‌کند.
(۴) با محاسبه‌ی مقدار N'_Y به همین ترتیب، مقدار Mac'_{info} را به صورت

$$Mac'_{info} = h(info\|ID_S\|N'_Y)$$

محاسبه می‌کند و در گام ۱۰ برای برای دروازه ارسال می‌کند.
(۵) دروازه بدون بررسی، مقدار Mac'_{info} را برای برنامه کاربر ارسال می‌کند.
(۶) در گام ۱۳ برنامه کاربر، نیز بدون بررسی، مقدار نادرست Mac'_{info} را ذخیره می‌کند و بعد از انجام احراز اصالت متقابل با کاربر در گام ۱۸ اطلاعات نادرست Mac'_{info} را برای کاربر ارسال می‌کند.
(۷) کاربر در انتها متوجه می‌شود که اطلاعات نادرستی را دریافت کرده است. ولی روشن است که گره‌های دروازه و برنامه کاربر مقدار Mac'_{info}



شکل ۲. سناریوهای مختلف نقض یکپارچگی پیام‌های مبادله شده در طرح نصر اصفهانی و همکاران که رنگ‌های قرمز و بنفش هر کدام متعلق به یک سناریوی مختلف هستند.

دریافتی را بدون بررسی و آگاهی از صحت آن، به طرف دیگر پروتکل ارسال می‌کنند تا در نهایت پیام نادرست به دست کاربر می‌رسد و به این ترتیب یکپارچگی پیام در پروتکل نصر اصفهانی و همکاران، نقض می‌شود.

سناریوهای مختلف حمله نقض یکپارچگی وارد بر پروتکل نصر اصفهانی و همکاران، در شکل ۲ با رنگ‌های قرمز و بنفش نشان داده شده است.

۵ نتیجه‌گیری

در این مقاله ما طرح احراز اصالت و حفظ حریم خصوصی انتها به انتهای نصر اصفهانی و همکاران را بررسی کردیم. طبق بررسی‌هایی که انجام دادیم، نشان دادیم که طرح فوق در مقابل حمله نقض یکپارچگی آسیب‌پذیر است، همچنین خاصیت یکپارچگی و صحت اطلاعات را که یکی از نیازهای امنیتی مهم در سامانه‌های پزشکی است، نقض می‌کند. احتمال موفقیت مهاجم در سناریوهای نقض یکپارچگی ارائه شده در این مقاله برابر صد در صد است و با یک بار اجرای پروتکل، امکان انجام حملات بیان شده وجود خواهد داشت. در نتیجه حملات نقض یکپارچگی اطلاعات اشتباه دریافت و ذخیره خواهد شد که ممکن است سلامت بیماران را با مشکل جدی مواجه نماید.

۶ تشکر و قدردانی

این مقاله با حمایت دانشگاه تربیت دبیر شهید رجایی تحت قرارداد شماره ۵۹۷۳/۲۰ انجام شده است.

مراجع

[1] Nasr Esfahani, Maryam, Ghahfarokhi, Behrouz Shahgholi, and Etemadi Borujeni, Shahram. Blockchain-based end-to-end privacy-preserving scheme for iot-based healthcare systems. *The Journal of Supercomputing*, 80(2):2067–2127, 2024.

[2] Qu, Youyang, Chen, Shiping, Gao, Longxiang, Cui, Lei, Sood, Keshav, and Yu, Shui. Personalized privacy-preserving medical data sharing for blockchain-based smart healthcare networks. in *ICC 2022-IEEE International Conference on Communications*, pp. 4229–4234. IEEE, 2022.

[3] Hossein, Koosha Mohammad, Esmaeili, Mohammad Esmaeil, Dargahi, Tooska, Khonsari, Ahmad, and Conti, Mauro. Bchealth: A novel blockchain-based privacy-preserving architecture for iot healthcare applications. *Computer Communications*, 180:31–47, 2021.

[4] Xia, QI, Sifah, Emmanuel Boateng, Asamoah, Kwame Omono, Gao, Jianbin, Du, Xiaojiang, and Guizani, Mohsen. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, 5:14757–14767, 2017.

[5] Deebak, Bakkiam David, Al-Turjman, Fadi, Aloqaily, Moayad, and Alfandi, Omar. An authentic-based privacy preservation protocol for smart e-healthcare systems in iot. *IEEE Access*, 7:135632–135649, 2019.

[6] Dwivedi, Ashutosh Dhar, Srivastava, Gautam, Dhar, Shalini, and Singh, Rajani. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):326, 2019.

[7] Escorcia-Gutierrez, José, Mansour, Romany F, Leal, Esmeide, Villanueva, Jair, Jimenez-Cabas, Javier, Soto, Carlos, and Soto-Díaz, Roosvel. Privacy preserving blockchain with energy aware clustering scheme for iot healthcare systems. *Mobile Networks and Applications*, pp. 1–12, 2023.

[8] Salem, Fatty M and Amin, Ruhul. A privacy-preserving rfid authentication protocol based on el-gamal cryptosystem for secure tmis. *Information sciences*, 527:382–393, 2020.

[9] Li, Xiong, Niu, Jianwei, Kumari, Saru, Liao, Junguo, and Liang, Wei. An enhancement of a smart card authentication scheme for multi-server architecture. *Wireless Personal Communications*, 80:175–192, 2015.

[10] Rais, Khadija, Derdour, Makhlouf, and Amroune, Mohamed. A blockchain-based model for efficient, privacy-preserving online medical diagnoses. in *2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1–5. IEEE, 2022.

[11] Ali, Zeeshan, Ghani, Anwar, Khan, Imran, Chaudhry, Shehzad Ashraf, Islam, SK Hafizul, and Giri, Debasis. A robust authentication and access control protocol for securing wireless healthcare sensor networks. *Journal of Information Security and Applications*, 52:102502, 2020.

[12] Yang, Xu, Yi, Xun, Nepal, Surya, Khalil, Ibrahim, Huang, Xinyi, and Shen, Jian. Efficient and anonymous authentication for healthcare service with cloud based wbans. *IEEE Transactions on Services Computing*, 15(5):2728–2741, 2021.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 2 (pp. 56–64)
https://monadi.isc.org.ir

Presented at the ISCISC 2024 in Tarbiat Modares University & Research Institute for Information and Communication Technology, Tehran, Iran

Violation of integrity in an end-to-end privacy-preserving protocol in IoT-based health monitoring systems★

Fatemeh Gholami Sabzevar and Masoumeh Safkhani *

Software Group, Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran

ARTICLE INFO.

Keywords:
Internet of Things (IoT)
Privacy preservation
Integrity violation attack
Hierarchical template chain
Healthcare systems

Type: Research paper

ABSTRACT

Privacy preservation in healthcare monitoring systems has always been a concern for both patients and doctors. To address this issue, many protocols have been designed. In this article, we examine the proposed scheme by Nasr Esfahani and colleagues, evaluating it from a security perspective. Their proposed scheme uses a three-layer hierarchical template chain to store and maintain critical medical information of patients in a centralized and secure manner. Additionally, by using Zero-Knowledge Proof (ZKP) and ring signature methods, they demonstrate that their scheme protects medical data against both internal and external attacks. According to potential scenarios, the Nasr Esfahani et al. protocol has shown good performance against many attacks, such as storage attacks and replay attacks, but it is vulnerable to integrity violation attacks. The success probability of the attacks presented in this article is one, and the complexity is only a single execution of the protocol.

© 2024 ISC

★ The ISCISC 2024 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: Fatemeh.glm@sru.ac.ir (Fatemeh Gholami Sabzevar), Safkhani@sru.ac.ir (Masoumeh Safkhani)
© 2024 ISC. All rights reserved.