استاندارد ملی ایران

۲۱۹۳۵-۱

چاپ اول

۱۳۹۵

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

INSO
21935-1
1st Edition

2017

Identical with
ISO/IEC 30107-1
:2016

فناوری اطلاعات- آشکارسازی حمله ارائه زیست‌سنجشی- قسمت ۱: چارچوب

Information technology — Biometric presentation attack detection — Part 1: Framework

ICS: 35.240.15

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، موجودیتها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1]، کمیسیون بین المللی الکتروتکنیک(IEC)[2] و سازمان بین المللی اندازه شناسی قانونی(OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سامانه‌های مدیریت کیفیت و مدیریت محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تائید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تائید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج افزاره بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1 - International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات– آشکارسازی حمله ارائه زیست‌سنجشی- قسمت ۱: چارچوب»

رئیس :	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (کارشناسی ارشد مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (کارشناسی ارشد مدیریت تکنولوژی)	مدیرکل نظام مدیریت امنیت اطلاعات- سازمان فناوری اطلاعات ایران
اعضاء : (اسامی به ترتیب حروف الفبا)	
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:
معروف، سینا
(کارشناسی مهندسی کامپیوتر- سخت‌افزار)

سمت و/ یا محل اشتغال:
کارشناس تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات– آشکارسازی حمله ارائه زیست‌سنجشی- قسمت ۱: چارچوب» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شماره ۵ تهیه و تدوین شده، در چهارصد و هشتاد و یکمین اجلاسیه کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۱۲/۲۲ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 30107-1: 2016, Information technology — Biometric presentation attack detection— Part 1: Framework

مقدمه

فناوری‌های زیست‌سنجشی به‌منظور تشخیص افراد بر مبنای مشخصه‌های زیستی و رفتاری آنان استفاده می‌شوند و در نتیجه اغلب به‌صورت مؤلفه‌ای در سامانه‌های امنیتی استفاده می‌شوند. فناوری زیست‌سنجشی که به سامانه امنیتی کمک می‌کند ممکن است به‌منظور تشخیص افرادی به‌کار رود که به‌عنوان دوست یا دشمن شناخته‌شده‌اند یا برای سامانه ناشناس هستند.

از آغاز این فناوری‌ها، امکان خرابکاریِ تشخیص توسط دشمنانِ معین، به‌صورت گسترده اذعان شده است، به‌طوری‌که نیازمند اقدامات متقابل برای آشکارسازی و شکست تلاش‌های خرابکارانه‌ی تشخیص یا حملات ارائه است. تخریب کارکرد موردنظر فناوری زیست‌سنجشی می‌تواند در هر نقطه‌ای درون سامانه امنیتی و توسط هر موضوعی رخ دهد؛ چه دشمن درونی سامانه و چه دشمن خارجی. این مجموعه استاندارد (ISO/IEC 30107) محدودیت‌هایی در دامنه‌ی کاربرد دارد، بااین‌حال، تمرکز بر فنون آشکارسازی خودکار حملات ارائه، توسط موضوعات گیراندازی[1] زیست‌سنجشی در نقطه‌ی ارائه و جمع‌آوری مشخصه‌های زیست-سنجشی مرتبط انجام می‌شود. این فنون خودکار را روش‌های «آشکارسازی حمله ارائه» (PAD) [2] می‌خوانیم.

قابلیت خرابکاری در سامانه‌های زیست‌سنجشی در محل جمع‌آوری داده توسط افراد معین به‌صورت موضوعات گیراندازی زیست‌سنجشی، استفاده از زیست‌سنجی را در برنامه‌های کاربردی که توسط عامل سامانه نظارت‌نشده‌اند، مانند جمع‌آوری از دور در شبکه‌های غیرقابل اطمینان، محدود کرده است، به همین دلیل به‌طور مثال راهنماهای اصالت‌سنجی الکترونیکی استفاده از زیست‌سنجه‌ها را به‌صورت عامل اصالت-سنجی پیشنهاد نمی‌دهند. در برنامه‌های کاربردی غیرحضوری[3] مانند اصالت‌سنجی از دور در شبکه‌های باز، روش‌های آشکارسازی حمله ارائه به‌صورت خودکار می‌تواند برای کاهش مخاطرات حمله، کاربردی باشد. استانداردها، روال‌های مطلوب[4] و فنون ارزشیابی شده‌ی مستقل، می‌توانند امنیت را در همهٔ سامانه‌هایی که از زیست‌سنجی استفاده می‌کنند، بهبود بخشند، خواه آن سامانه‌ها از گیراندازی نظارت‌شده یا نظارت‌نشده داده استفاده کنند. این شامل آن‌هایی می‌شود که از تشخیص زیست‌سنجشی به‌منظور امن کردن تراکنش‌های برخط استفاده می‌کنند.

مانند آن‌چه که در تشخیص زیست‌سنجشی هست، فنون PAD هم در معرض خطاها هستند: هم مثبت کاذب[5] و هم منفی کاذب[6]: در حالت مثبت کاذب به‌صورت نادرست روال‌های عادی را به‌عنوان حملات رده-بندی می‌کند و بنابراین به کارایی سامانه آسیب وارد می‌کند و در حالت منفی کاذب، حملات ارائه را به‌صورت نادرست، به‌عنوان روال طبقه‌بندی می‌کند که بازدارنده‌ی تجاوز امنیتی نیست؛ بنابراین، تصمیم

1 - Capture
2 - Presentation Attack Detection
3 - Unattended
4 - Best practices
5 - False positive
6 - False negative

برای استفاده از پیاده‌سازیِ خاص PAD به الزامات برنامه‌های کاربردی و درنظر گرفتن مصالح با توجه به امنیت و کارایی بستگی خواهد داشت.

هدف این استاندارد ارائه اصولی برای PAD با تعریف اصطلاحات و بنانهادن چارچوبی است که در آن رویدادهای حمله ارائه می‌توانند مشخص شوند و به‌گونه‌ای آشکارسازی شوند که بتوانند برای تصمیم‌گیری‌های سامانه زیست‌سنجشی و عملکرد فعالیت‌های ارزیابی طبقه‌بندی شوند، با جزئیات توصیف و مخابره شوند. این اصول برای استانداردهای سایر پروژه‌ها در کارگروه‌ها و زیرکارگروه‌های ISO/IEC آن مفید است. این استاندارد ملی فن مشخصی را به‌صورت ابزار PAD استاندارد معرفی نمی‌کند.

دو قسمت دیگر از استاندارد ISO/IEC 30107 وجود دارد. قسمت ۲ قالب‌های داده را برای انتقال نوع رویکرد استفاده‌شده در آشکارسازی حمله ارائه زیست‌سنجشی و انتقال نتایج روش‌های آشکارسازی حمله ارائه تعریف می‌کند. قسمت ۳ اصول و روش‌هایی برای ارزیابی عملکرد الگوریتم‌ها یا سازوکارهای آشکارسازی حمله ارائه بنا می‌کند.

فناوری اطلاعات– آشکارسازی حمله ارائه زیست‌سنجشی- قسمت ۱: چارچوب

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه اصطلاحات و تعاریفی است که در مشخصات، شناخت و ارزشیابی روش‌های آشکارسازی حمله ارائه مفید هستند.

این استاندارد برای موارد زیر کاربرد ندارد:

- استانداردسازی روش‌های آشکارسازی PAD مشخص؛
- اطلاعات جزئی در مورد اقدامات متقابل (مثل فنون ضد کلاه‌برداری)، الگوریتم‌ها یا حسگرها و
- امنیت کلی در سطح سامانه یا ارزیابی آسیب‌پذیری

حملاتی که باید در استاندارد ISO/IEC 30107 در نظر گرفته شوند آن‌هایی هستند که در مدت ارائه و جمع‌آوری مشخصه‌های زیست‌سنجشی در حسگر رخ می‌دهند.

هر حمله دیگری خارج از دامنه‌ی کاربرد استاندارد ISO/IEC 30107 در نظر گرفته می‌شود.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به‌صورت الزامی به آن‌ها ارجاع داده‌شده است. بدین ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مرجعی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده‌شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO/IEC 2382- 37:2012, Information technology — Vocabulary — Part 37: Biometrics.

یادآوری- نسخه‌ی الکترونیکی استاندارد ISO/IEC 2382- 37:2012 می‌تواند به‌صورت رایگان از وبگاه ISO/IEC Information Technology Task Force (ITTF) بارگیری شود:
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین‌شده در استاندارد ISO/IEC 2382-37:2012، اصطلاحات و تعاریف زیر نیز به کار می‌رود:

۱-۳

محصول مصنوعی

artefact

شیء یا بازنماییِ مصنوعی که رونوشتی از مشخصه‌های زیست‌سنجی یا الگوهای زیست‌سنجشی ساختگی ارائه می‌کند.

۲-۳

زنده‌بودن

liveness

کیفیت یا حالت زنده‌بودن که با مشخصه‌های کالبدی، واکنش‌های‌های غیرارادی یا کارکردهای کاراندام‌شناختی[1] (فیزیولوژیکی) یا واکنش‌های‌های ارادی یا رفتارهای موضوع مورد نظر آشکار می‌شود.

مثال ۱: جذب نور[2] توسط پوست یا خون مشخصه‌های کالبدی هستند.

مثال ۲: واکنش‌های عنبیه به نور و فعالیت (ضربان) قلب، واکنش‌های‌های غیرارادی هستند (کارکردهای کاراندام‌شناختی نیز خوانده می‌شوند).

مثال ۳: دو عملِ فشار دادن انگشت‌های دست و ارائه زیست‌سنجشی در پاسخ به سخنی راهنمایی کننده، اعمال ارادی هستند (که رفتارهای موضوع نیز خوانده می‌شوند).

۳-۳

آشکارسازی زنده‌بودن

liveness detection

سنجش و تحلیل مشخصه‌های کالبدی یا واکنش‌های‌های ارادی و غیرارادی برای تعیین اینکه نمونه‌ی زیست‌سنجشی در موقع گرفتن، از یک مورد زنده گرفته شده است.

یادآوری ۱- روش‌های آشکارسازی زنده‌بودن، زیرمجموعه‌ای از روش‌های آشکارسازی حمله ارائه هستند.

1 - Non-conformant
2 - Illumination

۴-۳

ارائه عادی

normal presentation

تعامل موضوع گیراندازی زیست‌سنجشی و زیرسامانه گیراندازی داده زیست‌سنجشی به شیوه‌ای که مـوردنظرِ خط‌مشی سامانه زیست‌سنجشی است.

یادآوری ۱- زمانی که به «ارائه هنجار» استناد می‌کنیم، اصطلاح «هنجار» مشابه «امر عادی» است. هر نـوع ارائـه کـه حملـه نیست به‌صورت «ارائه هنجار» در نظر گرفته می‌شود.

۵-۳

حمله ارائه

presentation attack

ارائه به زیرسامانه گیراندازی داده زیست‌سنجشی با هدف مداخله در عملیات سامانه زیست‌سنجشی است.

یادآوری ۱- حمله ارائه می‌تواند با استفاده از روش‌های مختلفی انجام شود، به‌عنـوان مثـال، محصـول مصـنوعی، قطـع عضـو، بازپخش و غیره.

یادآوری ۲- حملات ارائه ممکن است دارای چند هدف باشد به‌طور مثال جعل هویت یا تشخیص داده نشدن.

یادآوری ۳- سامانه‌های زیست‌سنجشی ممکن است قادر به تمایز بین حملات ارائه زیست‌سنجشی بـا هـدف مزاحمـت بـرای سامانه‌های عملیاتی و ارائه‌های غیر انطباقی[1] نباشد.

۶-۳

آشکارسازی حمله ارائه

presentation attack detection (PAD)

تعیین خودکار حمله ارائه است.

یادآوری ۱- PAD نمی‌تواند نیت موضوع را استنباط کند. در حقیقت ممکـن اسـت نتیجـه گـرفتن از ایـن تفـاوت در فراینـد گیراندازی داده یا نمونه‌ی به دست آمده، غیرممکن باشد.

1 - Non-conformant

۷-۳

ابزار حمله ارائه

presentation attack instrument (PAI)

مشخصه زیست‌سنجشی یا شیء استفاده‌شده برای حمله ارائه است.

یادآوری ۱- مجموعه‌ی PAI شامل محصولات مصنوعی می‌شود، همچنین ممکن است شامل مشخصه‌های بدون جان زیست-سنجشی (ناشی از جنازه مردگان) یا مشخصه‌های زیست‌سنجشی تغییر داده‌شده (به‌عنوان مثال اثر انگشتان تغییر داده‌شده) باشد که در حمله استفاده می‌شوند.

۴ کوته‌نوشت‌ها

آشکارسازی حمله ارائه	Presentation Attack Detection	PAD
ابزار حمله ارائه	Presentation Attack Instrument	PAI

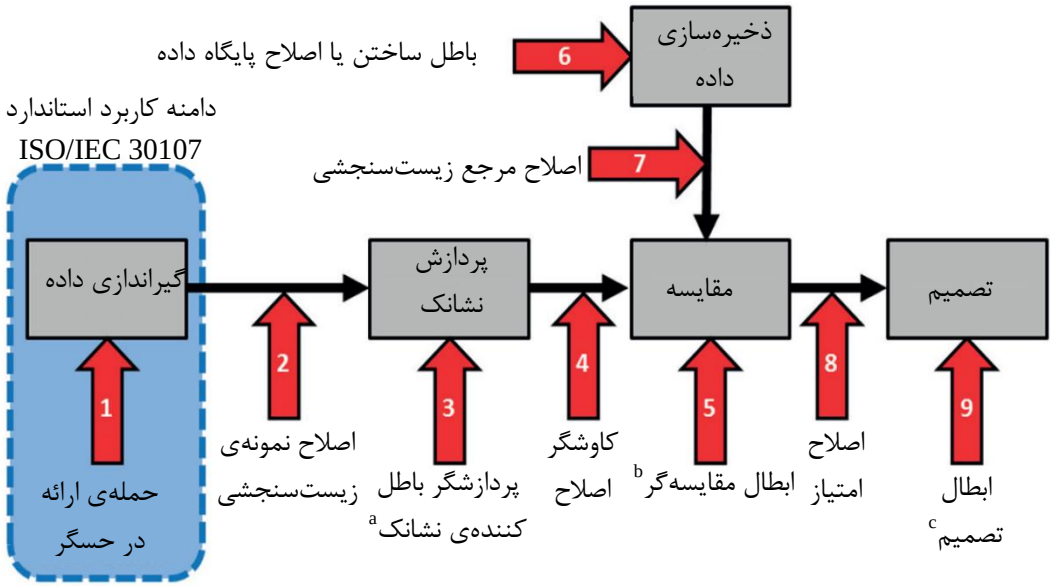
۵ شناخت حملات ارائه

۵-۱ عمومی

با اینکه حملات در سامانه زیست‌سنجشی می‌توانند در هر جا رخ دهند و توسط هر کنشگری[1] انجام شوند، استاندارد ISO/IEC 30107 بر حملات با مبنای زیست‌سنجشی روی زیرسامانه گیراندازی داده توسط موضوعات گیراندازی زیست‌سنجشی حمله‌کننده تمرکز دارد که به‌منظور خرابکاری در عملیات موردنظر سامانه انجام می‌شود. حملات توسط کنشگران دیگر و در نقاط دیگر سامانه، در مستندات قبلی مانند [۲] در نظر گرفته‌شده بودند. استاندارد ISO/IEC 30107 به محافظت از زیرسامانه گیراندازی داده‌ها (شامل خود حسگر) از اصلاح، جایگزینی یا حذف و یا به محافظت کردن ارتباطات بین زیرسامانه گیراندازی داده و زیرسامانه‌های دیگر نمی‌پردازد.

شکل ۱ چند حمله عمومی را در مقابل سامانه زیست‌سنجی نشان می‌دهد. استاندارد ISO/IEC 30107 تنها بر حملات مشخص‌شده توسط پیکانه[2] «۱» تمرکز دارد که در آن مشخصه‌ی زیست‌سنجشی یا PAI به حسگری اشاره دارد که به‌صورت مناسب درون سامانه زیست‌سنجشی عمل می‌کند.

1 - Actor
2 - Arrow



[a] - Override Signal Processor
[b] - Override Comparator
[c] - Override Decision

شکل ۱- نمونه‌هایی از نقاط حمله در سامانه زیست‌سنجی (اقتباس از [۱])

حملات ارائه می‌تواند توسط دو نوع موضوع خرابکاری گیراندازی زیست‌سنجشی انجام شود: بدخواه[1] زیست-سنجشی که در آن موضوع خرابکاری گیراندازی زیست‌سنجی تمایل دارد به‌صورت فردی دیگر تشخیص داده شود یا پنهان‌کننده زیست‌سنجشی که در آن موضوع خرابکاری گیراندازی زیست‌سنجشی تمایل دارد تا از تشخیص داده شدن به‌صورت فرد شناخته‌شده برای سامانه فرار کند.

بدخواهان زیست‌سنجشی ممکن است حمله را به دو طریق مختلف انجام دهند. در نوع اول، موضوع داده خرابکاری تمایل دارد به‌صورت فردی مشخص که برای سامانه معلوم است، شناخته شود. در نوع دوم، موضوع داده خرابکاری تمایل دارد به‌صورت هر فرد شناخته‌شده برای سامانه تشخیص داده شود بدون آن‌که به‌صورت فردی مشخص باشد.

در مقابل، پنهان کنندگان زیست‌سنجشی تمایل به پنهان نمودن مشخصه‌های زیست‌سنجشی خود دارند تا مانع مدل‌سازی مشخصه‌های افراد شناخته‌شده شوند، به‌طور مثال، با استفاده از عضو مصنوعی یا از طریق تغییر چهره یا تغییر مشخصه‌های زیست‌سنجی طبیعی.

۵-۲ ابزارهای حمله ارائه

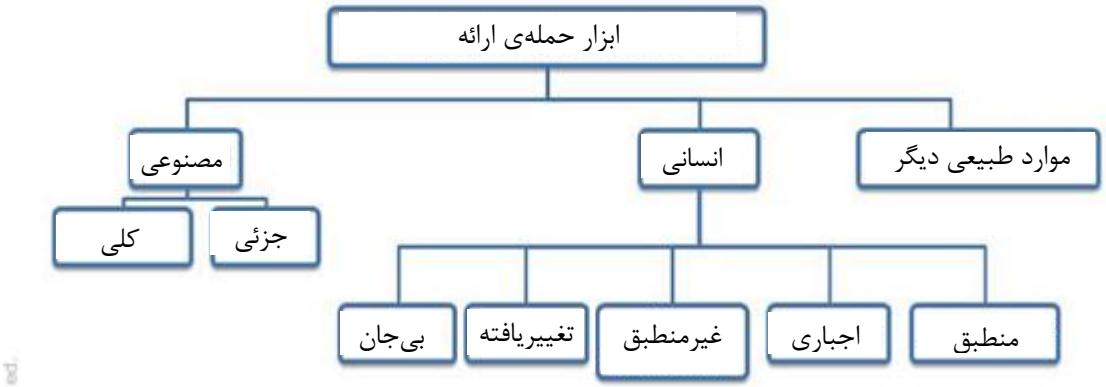
شیء یا مشخصه استفاده‌شده در حمله ارائه، PAI است. عموماً حملاتی که از PAI ها در حسگر استفاده می-

1 - Imposter

کنند در یکی از این دو گروه جای می‌گیرند: مشخصه‌های مصنوعی یا مشخصه‌های مبتنی بر انسان. یادآوری می‌شود که دسته‌ی سومی نیز از موارد طبیعی دیگر مانند PAI های بر مبنای حیوان و بر مبنای گیاهان وجود دارد.

علاوه بر این، اصطلاحات منطبق و غیرمنطبق در این بند و به خصوص در جدول ۱ استفاده شده‌اند، اما این اصطلاحات بر کدبندیِ PAD تأثیر ندارد، چراکه معنای آن‌ها با تعامل حسگر-موضوع مرتبط است و سنجش آن به‌صورت عینی دشوار است و بنابراین نمی‌تواند کدبندی شود. مثالی برای این تعامل منطبق قرار دادن گوشه‌ی انگشت به‌جای الگوی اثر انگشت روی افزاره است.

یادآوری می‌شود که حمله آشکارسازی شده ممکن است به دلیل موضوعات دسترس‌پذیری یا قابلیت استفاده از موضوع باشد و به دلیل تلاش برای حمله به سامانه نباشد.



شکل ۲ – انواع حملات ارائه

شکل ۲ این دسته‌ها را در ردیف سوم نشان می‌دهد. جدول ۱ مثالی از هر نوع PAI ویژه در ردیف انتهایی شکل ۲ را نشان می‌دهد. این شکل می‌تواند برای توصیف PAI مشخص با استفاده از صفت ستون دوم و پیرو آن از طریق کلمه ستون اول، استفاده شود. به‌عنوان مثال، قسمتی از بدن جسد انسان می‌تواند مثالی از «PAI انسانی بی‌جان» باشد.

جدول ۱- مثال‌هایی از ابزارهای مصنوعی و انسانی حملات ارائه

مصنوعی	کامل	انگشت چسبناک[a]، تصویر صورت
	جزئی	چسب بر انگشت، عینک آفتابی، عدسی‌های تماسی مصنوعی/ نمونه
انسان	بی‌جان	قسمتی از جسد انسان، انگشت/دست جداشده
	تغییریافته	شکستن اعضا، تعویض اثر انگشت بین دست‌ها و انگشت پا با جراحی
	غیرمنطبق	سیمای صورت، نوک یا گوشه‌ی انگشت
	اجباری[b]	بی‌هوش، تحت اجبار
	منطبق	تلاشِ صفر تلاش[c] بدخواه

[a] Gummy finger

[b] انتظار می‌رود تمامی ارائه‌های اجباری آشکارسازی شده باشد. تعدادی از روش‌ها ممکن است قادر به سنجش شاخص اجباری، مانند تحلیل تنش صوتی، نرخ بیشینه پالس یا تحلیل حالت چهره (ترس) باشند.

[c] Zero Effort

۶ چارچوب برای روش‌های آشکارسازی حمله ارائه

۶-۱ انواع آشکارسازی حمله ارائه

همان‌طور که در جدول ۲ نشان داده‌شده، روش‌های PAD به دو رده تقسیم می‌شوند: آن‌هایی که بر مبنای داده گرفته‌شده توسط زیرسامانه گیراندازی داده هستند و آن‌هایی که بر مبنای سنجش‌های امنیتی سطح سامانه هستند. یادآوری می‌شود که روش‌های PAD خواستار رابطه‌ی یک‌به‌یک با دسته‌های PAI نیستند (شکل ۲).

جدول ۲- مثال‌هایی از روش‌های آشکارسازی حملات ارائه

از طریق زیرسامانه گیراندازی داده	آشکارسازی محصول مصنوعی	آشکارسازی خصوصیاتی که نشان‌دهنده‌ی محصول مصنوعی هستند. مثال‌ها: ۱- مقاومت ظاهری الکتریکی «انگشت» بر حسگری که خارج بازه‌ی نوعی است. ۲- نسخه‌های سطحی و زیرپوستی اثرانگشت به‌طور چشم‌گیری متفاوت هستند
	آشکارسازی زنده‌بودن	برای این تعریف به زیربند ۳-۳ مراجعه شود. برای مثال‌ها، به زیربند ۶-۲-۱ و ۶-۲-۲ مراجعه شود.
	آشکارسازی تغییر	آشکارسازی مشخصه‌هایی از تلاش برای تغییر دادن خصوصیات زیست‌سنجی. مثال: جای زخم بر اثرانگشت
	آشکارسازی نامنطبق	آشکارسازی نابهنجاری‌هایی که توصیه نمی‌شود در ارائه مناسب رخ دهد، مثال: آشکارسازی که سطح نور با حالت استفاده‌ی عادی سازگار نیست.
	آشکارسازی اجبار	مثال: تحلیل تنش از حالت صدا یا صورت
	آشکارسازی تاریکی	آشکارسازی اینکه خصوصیاتی به‌صورت جزئی یا کامل از «دید» حسگر مسدود شده‌اند. مثال: آشکارسازی متعلقات پوشاننده‌ی قسمتی از صورت مانند روسری یا کلاه.
از طریق پایش در سطح سامانه	شمارنده‌ی آشکارسازی تلاش شکست‌خورده	مثال: حمله مشکوک ارائه، اگر دنباله‌ای از تلاش‌های شکست‌خورده‌ی مشابه وجود داشته باشد.
	جغرافیایی	ترکیب جغرافیا/زمان. مثال: حمله ارائه مشکوک اگر مکان یا زمان استفاده برای تشخیص همتا غیرممکن یا غیر استفاده است.
	زمانی	
	بررسی تصویر	مثال: قضاوت توسط کارور[a] انسانی (سامانه تحلیل تصویر)
[a] Operator		

یادآوری- تاریکی شامل ارائه موضوعی شامل ابزار مشخصه‌های زیست‌سنجشی کاهش‌یافته به دلیل نبود بعضی جزئیات مشخصه‌ها است، به‌عنوان مثال، چهره‌ای که به‌صورت جزئی توسط کلاه یا روسری پنهان‌شده است. در بعضی موارد، آشکارسازی تاریکی ممکن است در آشکارسازی محصول مصنوعی در نظر گرفته‌شده باشد.

۶-۲ نقش چالش-پاسخ[1]

مفهوم چالش-پاسخ به‌صورت گسترده در طرح‌های اصالت‌سنجی استفاده می‌شود، بعضی از آن‌ها شامل جنبه‌های زیست‌سنجشی هستند و مابقی آن‌ها هیچ مشارکت زیست‌سنجشی ندارند. این بند، ساختاری برای تعیین مفهوم کلی چالش-پاسخ ارائه می‌کند و در بعضی از جزئیات بر کاربرد زیست‌سنجشی با استفاده از چالش-پاسخ، رابطه‌ی بین زنده‌بودن و چالش-پاسخ تمرکز خواهد داشت.

1 - Challenge-Response

در این محتوا، چالش، فعالیتی هدف‌دار است که پاسخی قابل‌انتظار در زمان وجود شرایط هدف دارد.

۶-۲-۱ چالش-پاسخ مربوط به زنده‌بودن

چالش-پاسخ می‌تواند به‌عنوان ابزاری برای تعیین ارائه موضوعی به‌کار رود که خصوصیات زنده‌بودن را در به‌دست آوردن زیرسامانه گیراندازی داده‌های زیست‌سنجشی دارد. به‌عنوان مثال، انتظار می‌رود اندازه‌ی مردمک عنبیه‌ی چشم انسان زنده در مقابل تغییر روشنایی نور مرئی تغییر کند (چالش) که نشان‌دهنده‌ی زنده‌بودن وی است.

چارچوب دسته‌بندی تمامی جنبه‌های چالش-پاسخ متناسب با زنده‌بودن در جدول ۳ نشان داده‌شده است. یادآوری می‌شود که ستون آخر نمی‌تواند برای برخورد اولیه با موضوع یا برای تعیین ثبت زنده‌بودن به‌کار رود، درحالی‌که ستون‌های دیگر می‌توانند استفاده شوند.

جدول ۳- آشکارسازی زنده‌بودن با استفاده از چالش-پاسخ به‌عنوان یک ابزار

	۱. پاسخ غیرارادی	۲. پاسخ ارادی	۳. ترکیب چیزی که شما هستید و می‌دانید
چالش	محرک هدف‌دار که بر شناختن خصوصیات زیست‌سنجشی تمرکز دارد	اشارات (شنیداری، دیداری) راهنمای عملی مخصوص که توسط سامانه زیست‌سنجشی گرفته شده باشد	رهنمودهای مشخص کننده‌ی ارائه زیست‌سنجی با استفاده از اطلاعات از پیش استفاده‌شده
پاسخ	به‌صورت طبیعی، غیرارادی و غیرقابل واپایش توسط موضوع	بر مبنای ادراک انسان زنده و اقدام واپایش‌شده‌ی ارادی	بر مبنای ادراک انسان زنده و گیراندازی زیست‌سنجشی شخص
مثال‌ها	تغییرات نور : تغییر اندازه‌ی مردمک	اشاره با علامت سر: زاویه‌ی سر در راستایی صحیح تغییر می‌کند. اشاره با بستن چشم‌چپ: بسته شدن عنبیه چپ	ترتیب انگشت (توسط سامانه به‌صورت تصادفی تغییر می‌کند): نشان دادن و مقایسه انگشت‌های صحیح ترتیب شماره: اعلام و مقایسه شماره صحیح

۶-۲-۲ زنده‌بودن نامرتبط با چالش-پاسخ

گروهی از رویکردهای آشکارسازی زنده‌بودن از نظر زیست‌سنجشی وجود دارد که توسط چالش-پاسخ توانمند نشده‌اند و به عنوان آشکارسازی «مشاهدات شبیه‌سازی نشده‌ی زنده‌بودن» به آن اشاره می‌شود (همچنین می‌توان به‌عنوان آشکارسازی «غیرفعال» زنده‌بودن به آن اشاره کرد). زنده‌بودن به‌صورت خاص از آنچه که توسط حسگر در برخی از دوره‌های زمانی مناسب دریافت می‌شود، مشخص‌شده است و در آن هیچ شبیه‌سازی هدف‌داری مرتبط با زنده‌بودن وجود ندارد. مثال‌های این دسته عبارت‌اند از:

- عرق کردن انگشت (به‌مرور زمان)
- حرکت / بسامد عنبیه (در زمانی کوتاه)
- پالس (به‌مرور زمان) و
- نور چند طیفی (جذب بسامد نور خون/بافت)

۶-۲-۳ چالش-پاسخ نامرتبط با زیست‌سنجی

بعضی از طرح‌های اصالت‌سنجی که به‌صورت زیست‌سنجشی انجام شدنی نیستند از مفاهیم چالش-پاسخ برای تحکیم تضمین اصالت‌سنجی‌شان عموماً از اصالت‌سنجی چندعاملی (به‌استثنای عامل زیست‌سنجشی) استفاده می‌کنند. چالش در این مورد می‌تواند به‌صورت اصالت‌سنجی افزاره/کارت با استفاده از گواهی‌نامه‌های رقمی یا درخواست پاسخ به سؤالات امنیتی (راز[1]) شکل بگیرد.

۶-۳ فرایند آشکارسازی حمله ارائه (PAD)

آشکارسازی حمله ارائه ممکن است با گام‌های زیر انجام شود که مشابه فرایندهای تشخیص زیست‌سنجشی هستند.

گام ۱- داده خام برای PAD از موضوعی با استفاده از زیرسامانه گیراندازی داده زیست‌سنجشی، گرفته شود.

یادآوری می‌شود که حسگرهای مورداستفاده ممکن است از حسگرهای استفاده‌شده برای گیراندازی مشخصه‌های زیست‌سنجشی و گیراندازی داده‌های زیست‌سنجشی متفاوت باشند و PAD ممکن است به‌صورت هم‌زمان نباشد، باوجود این‌که واگرایی[2] در زمان سنجش بین گیراندازی زیست‌سنجشی و داده PAD می‌تواند منجر به آسیب‌پذیری شود.

گام ۲- استخراج ویژگی‌ها از داده‌های PAD.

گام ۳- مقایسه‌ی ویژگی‌های PAD با معیارها.

گام ۴- نتیجه (آشکارسازی، عدم آشکارسازی، امتیاز و ....) خروجی مقایسه است. این داده به‌صورت تنها یا ترکیبی با داده‌های دیگر، تصمیم نهایی سامانه زیست‌سنجشی را ازنظر پذیرش یا رد نمودن نمونه اعلام می‌کند.

بااینکه این سه‌گام باید به‌این‌ترتیب انجام شوند، اما ممکن است به‌صورت پیوسته در زمان یا مکان انجام نشوند.

معیار تصمیم‌گیری استفاده‌شده در گام ۳ ممکن است برای تمامی موضوعات مشترک یا برای هر موضوع

1 - Secret
2 - Divergence

مشخص باشد. به‌طور مثال، هنگامی‌که واکنش‌های غیرارادی یا کارکردهای کاراندام‌شناختی یا واکنش-های‌های ارادی یا حرکت موضوع برای آشکارسازی حملات واردشده استفاده می‌شوند، اگر تمامی موضوعات به‌طورکلی سنجیده شوند، ممکن است معیار حمله ارائه برای آن‌ها مشترک باشد؛ درحالی‌که اگر آن‌ها به‌دقت سنجیده شوند، ممکن است معیار برای هر موضوع مشخص باشد.

بنابراین در مواردی که معیارها برای هر موضوع مشخص است، فرایند ثبت‌نام معیار ضروری است.

۶-۴ آشکارسازی حمله ارائه در معماری سامانه زیست‌سنجشی

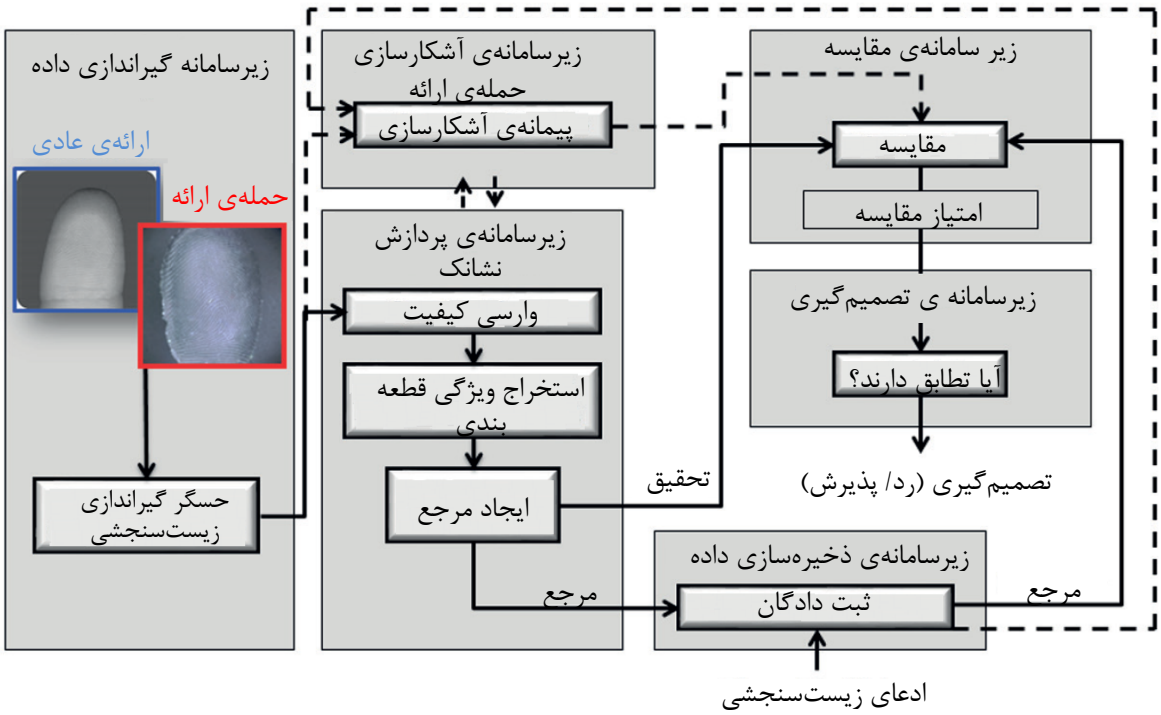
۶-۴-۱ مرور کلی اصطلاحات چارچوب کلی زیست‌سنجشی

بااینکه در استاندارد ISO/IEC 30107 تنها حملاتی موردنظر است که در محل گیرانداز داده زیست-سنجشی رخ می‌دهند، عملکرد PAD ممکن است در هر مکان یا زمانی در سامانه زیست‌سنجی رخ دهد.

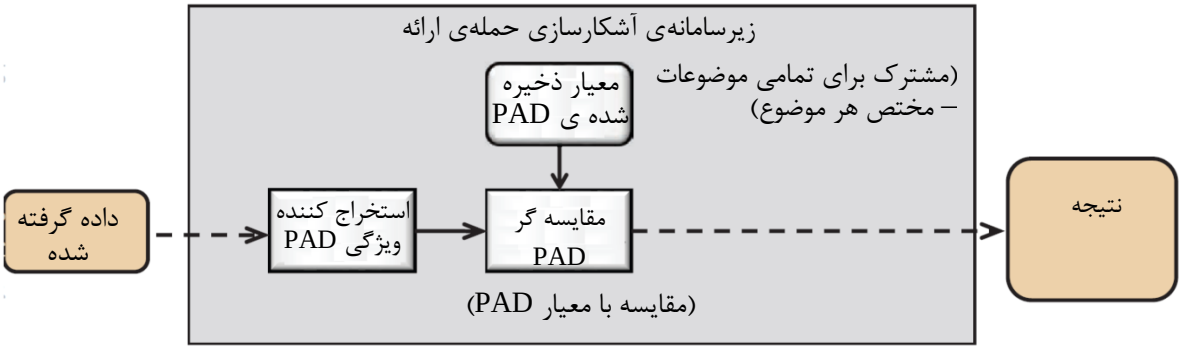
شکل ۳ زیرسامانه PAD درج‌شده در چارچوب کلی زیست‌سنجشی را نشان می‌دهد اما زیرسامانه PAD (و فرایندهای منحصربه‌فرد آن) می‌تواند به شیوه‌های مختلف درون هر چارچوب کلی قرار گیرد. زیرسامانه‌ای که حملات ارائه را آشکارسازی می‌کند ممکن است در دنباله‌ی زیرسامانه گیراندازی داده (یا درون آن) و یا دنباله‌ی زیرسامانه پردازش نشانک[1] (به‌صورت خط‌چین در شکل ۳ نشان داده‌شده است) قرار بگیرد. علاوه بر این، PAD می‌تواند بعد از زیرسامانه‌های مقایسه یا تصمیم (نشان داده نشده است) یا در نقاط مختلف در سامانه نیز رخ دهد. همچنین، ممکن است بین فرایند جمع‌آوری داده برای استفاده در تعیین هویت و فرایند آشکارسازی حمله ارائه، همپوشانی فیزیکی، زمانی یا کارکردی وجود داشته باشد. برای بحث بیشتر در مورد این تغییرات با توجه به مکان و زمانی که فرایندهای PAD ممکن است رخ دهد، به زیربندهای ۶-۴-۲ و ۶-۴-۳ مراجعه شود.

شکل ۴ جزئیات اضافی زیرسامانه‌های PAD را ارائه می‌دهد. بعضی زیرسامانه‌های PAD ممکن است برای استخراج ویژگی PAD موردنیاز نباشد. مقایسه‌گر PAD و معیار ذخیره‌شده‌ی PAD در این زیرسامانه‌ها ضروری هستند. معیار PAD برای تمامی موضوعات مشترک است یا برای هر موضوع مشخص است.

1 - Signal



شکل ۳- چارچوب کلی زیست‌سنجشی با آشکارسازی حمله ارائه (پیکربندی‌های دیگر نیز ممکن است)



شکل ۴- مؤلفه‌های زیرسامانه کلی آشکارسازی حمله ارائه

۶-۴-۲ ملاحظات پردازش PAD متناسب با دیگر زیرسامانه‌های زیست‌سنجشی

درنظرگرفتن جمع‌آوری و پردازش داده PAD و داده نمونه‌ی زیست‌سنجشی هم در زمان و هم در مکان به‌صورت مستقل آموزنده است. دو شکل داده ممکن است موجود باشد یا ممکن است یکی در غیاب دیگری موجود باشد. پردازش PAD می‌تواند توسط سامانه زیست‌سنجشی به‌صورت هم‌زمان، قبل یا بعد هر زیرسامانه انجام شود. مؤلفه‌های زیرسامانه PAD ممکن است حتی به‌صورت جداگانه و/یا هم‌زمان با بیش از

یک زیرسامانه رخ دهد. خروجی PAD ممکن است به چندین نمونه زیست‌سنجی گیراندازی‌شده بستگی داشته باشد و الزاماً شاخص دودویی ساده نیست.

مثال ۱: افزاره گیراندازی داده ممکن است برای تولید داده نمونه زیست‌سنجشی و داده PAD برای هر رویداد گیراندازی داده، طراحی‌شده باشد. بسته به طراحی سامانه، این افزاره‌ی گیراندازی داده ممکن است داده نمونه‌ی زیست‌سنجشی را بدون توجه به نتیجه‌ی کارکرد PAD، یا تنها در موردی که PAD هیچ حمله‌ای را آشکارسازی نمی‌کند، تولید کند. همچنین ممکن است که داده PAD بدون استفاده از نمونه‌ی زیست‌سنجی ایجاد شود. در این مثال، خروجی PAD شاخص دودویی ساده حمله آشکارسازی شده است.

مثال ۲: ممکن است داده PAD گیراندازی‌شده در طول کارکرد پردازنده‌ی نشانک بعد از اینکه نمونه‌ی زیست‌سنجشی به‌دست آمد، تحلیل‌شده باشد. در این مورد، نمونه‌ی زیست‌سنجشی یا ویژگی‌های زیست‌سنجشی یا مدل حاصل از زیرسامانه پردازش نشانک ممکن است با ماتریس PAD تعیین‌شده در هنگام پردازش نشانک همراه شود.

مثال ۳: داده PAD ممکن است جمع‌آوری‌شده باشد اما تا زمان زیادی در پردازش، تحلیل نشده باشد. در این مثال، نشانک موردنیاز برای پردازش PAD با نمونه، ویژگی یا مدل زیست‌سنجی ذخیره‌شده است.

یادآوری- درحالی‌که سامانه‌ای ممکن نیست همیشه از پایش بلادرنگ استفاده کند، نظارت ویدئویی و دیگر ضبط‌ها می‌تواند سازوکاری مؤثر برای آشکارسازی پس از رویداد و تحلیل برای ضبط ارائه‌های زیست‌سنجشی و رویدادهای پیرامون آن باشد، درست همان‌طور که اکنون برای ماشین‌های خودکار گویا، در هنگام استفاده‌ی محرمانه از داده کارت به‌منظور دزدیدن حساب‌ها استفاده می‌شود. این امر سبب افزایش آشکارسازی روش (موفق یا غیر موفق) استفاده‌شده یا اجبار کردن موضوع می‌شود و امکان گیراندازی دیگر نمونه‌های زیست‌سنجشی را به وجود می‌آورد که این نمونه‌ها در تحلیل پس از رویداد استفاده می‌شوند (به‌طور مثال نظارت ویدئویی برای جمع‌آوری اطلاعات چهره درزمانی که دسترسی اصلی به وجوه خودپرداز (ATM)[1] با اثرانگشت بود) که می‌تواند عامل بازدارنده را برای حملات به این سامانه‌ها افزایش دهد. این‌ها راه‌حل‌های دنیای واقعی هستند که به‌منظور پیشگیری و آشکارسازی سوء رفتار سامانه‌ها استفاده‌شده و ممکن است بهترین روش برای سامانه‌های زیست‌سنجشی باشند.

۳-۴-۶ پیامدهای مکانی PAD با توجه به تبادل داده

مؤلفه‌های زیرسامانه PAD می‌توانند در مکان‌های مختلفی باشند (کارخواه[2] در برابر کارساز[3]، انتهای جلویی[4] در برابر انتهای پُشتی[5]) یا افزاره‌ی تلفن همراه در برابر نرم‌افزار برنامه‌ی کاربردی/ ابری). محصولاتی که PAD پشتیبانی می‌کند می‌توانند به شکل‌ها و موقعیت‌های متفاوت باشند.

رئوس مطالب چندین رویکرد در ادامه آورده شده است. یادآوری می‌شود که بعضی از قالب‌های PAD مرتبط (وابسته) به تبادل داده نیستند.

- آشکارسازی حمله ارائه ممکن است روی همان افزاره‌ای انجام شود که محل حسگر گیراندازی داده

1 - Automated Teller Machine
2 - Client
3 - Server
4 - Front end
5 - Back end

است. ممکن است با افزاره پیچیده‌ای که توانایی محاسبه انجام PAD را دارد، به نتایج PAD در هر تبادل داده نیاز نباشد (به‌طور مثال، به‌منظور فرستادن به ماشین پشت-انتهایی، کارساز یا برنامه‌ی کاربردی). خروجی نمونه‌ی زیست‌سنجی یا حقوق دسترسی (نبود هریک از این‌ها) ممکن است برای ارائه نتایج کافی باشد.

- از طرف دیگر حتی اگر تمامی مؤلفه‌های زیرسامانه PAD در افزاره‌ی گیرانـدازی داده اجرا شوند، برنامه‌های کاربردی با مخاطره‌ی بالاتر ممکن است برای کسب اطلاعات بیشتر پیرامون اثرات متقابل حسگر آن‌ها و جمع‌آوری داده، هم در مورد تلاش‌های شکست‌خورده و هم چگونگی ارزشمندی نمونه زیست‌سنجشی بر مبنای داده PAD در دسترس، تمایل داشته باشند.

- داده PAD ممکن است در افزاره‌ای قابل‌اطمینان گرفته شود و به کارساز یا برنامه‌ی کاربردی (نرم‌افزار اجرایی توسعه‌یافته توسط قسمتی دیگر) ارسال شود تا هویت ادعاشده و حقوق دسترسی را تعیین نهایی کند. بسته به برنامه‌های کاربردی، داده PAD موجود در داده تبادلی برای نشست، ممکن است داده خام باشد که در همان قالب گرفته شده، فرستاده شود یا ممکن است افزاره‌ی محلی استخراج ویژگی انجام دهد و امتیاز یا دیگر داده‌های استخراج‌شده را ارسال کند.

۷ موانع حملات ارائه زیست‌سنجشی بدخواه در سامانه زیست‌سنجشی

برای موفقیت‌آمیز بودن حمله ارائه زیست‌سنجشی بدخواه باید اقدامات زیر صورت گیرد:

i- نمونه‌ی حمله ارائه باید توسط زیرسامانه گیراندازی داده حاصل شود،

ii- نمونه‌ی حمله ارائه باید به‌صورت موفق به‌منظور تولید مرجع یا کاوند[1]، پردازش شود.

iii- مقایسه‌ی کاوند-مرجع بر مبنای حمله ارائه باید با مرجع زیست‌سنجی هدف منطبق باشد.

iv- باید این امکان وجود داشته باشد که حمله در محل تحت روش‌های اجرایی امنیت سطح سامانه انجام شود.

v- توصیه می‌شود در صورت وجود، زیرسامانه PAD نمونه‌ی ارائه داده‌شده را به‌صورت حمله طبقه‌بندی نکند.

بسته به نوع سامانه زیست‌سنجشی و مهارت حمله ارائه، ممکن است از موفقیت حمله ارائه در هرکدام از این گام‌ها جلوگیری شود. به‌طور مثال (متناظر با ترتیب گام‌های بالا):

i- محصول مصنوعی ممکن است به دلیل طراحی حسگر گیراندازی زیست‌سنجشی و ویژگی‌هایی که برای به دست آوردن نمونه‌ها استفاده کرده، کسب نشود، همانند اثرانگشت سیلیکونی جعلی بر افزاره‌ی اثرانگشت خازنی.

ii- نمونه‌ی محصول مصنوعی ممکن است ناشی از کیفیت ناکافی در زمان پردازش نشانک فرض شود.

iii- از دست دادن راستی به دلیل چاپ رونوشت تصویر زیست‌سنجشی درست، ممکن است سبب شود امتیاز مقایسه، خارج از مقدار آستانه‌ی تشخیص واقع شود.

iv- جعل هویت تصویر چهره با استفاده از اندازه‌ی طبیعی سر مانکن به‌احتمال زیاد توسط یک کارور مشاهده‌شده است.

1 - Probe

کتاب‌نامه

[1] Ratha N.K., Connell J.H., Bolle R.M. E nhancing s ecurity a nd privacy i n biometrics-based authentication systems. IBM Syst. J. 2001, 40 (3)

[2] Elliott Stephen J., & Kukula Eric P. A Definitional Framework for the Human-Biometric Sensor Interaction Model", Proc. of SPIE Vol. 7667 76670H-7