INSO

21825
1st.Edition

2017

Identical with
ISO-IEC-20648
(2016)

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران
۲۱۸۲۵

چاپ اول

۱۳۹۶

فناوری اطلاعات – ویژگی امنیت لایه انتقال (TLS) برای سامانه‌های ذخیره‌سازی

Information technology — TLS specification for storage systems

ICS: 35.030 35.220.01

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

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی‌و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
«فناوری اطلاعات – ویژگی امنیت لایه انتقال (TLS) برای سامانه‌های ذخیره‌سازی»

رئیس:	سمت و/ یا محل اشتغال:
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس
دبیر:	
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات، گرایش تکنولوژی ارتباطات)	مشاور مرکز آپا دانشگاه تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
ترابی، مهرنوش (فوق لیسانس مهندسی فناوری اطلاعات- تجارت الکترونیک)	کارشناس استاندارد
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
صالحی، فاطمه (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس مسئول پرداخت الکترونیک شرکت فناوری اطلاعات و ارتباطات پاسارگاد (فناپ)
قندهاری، آزاده (فوق لیسانس کامپیوتر، نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی واحد ساوه و کارشناس مرکز تحقیقات مخابرات ایران
کماسی، مهدی (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس شرکت گسترش سرمایه‌گذاری ایران خودرو
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس

معروف، سینا — کارشناس سازمان فناوری اطلاعات ایران

(لیسانس، مهندسی کامپیوتر، سخت افزار)

ویراستار:

فرهاد شیخ احمد، لیلا — کارشناس استاندارد

(فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات – ویژگی امنیت لایه انتقال (TLS) برای سامانه‌های ذخیره‌سازی» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در پانصد و هفتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۹۶/۲/۱۹ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان 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 وخدمات، 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 20648:2016, Information technology — TLS specification for storage systems

مقدمه

در فناوری اطلاعات و ارتباطات (CT)[1]، یکی از بهترین دفاع‌ها در برابر حملات مخابراتی، استقرار خدمات امنیتی پیاده‌سازی‌شده با سازوکارهای مشخص‌شده در استانداردهایی است که به طور کامل در حوزه عمومی بررسی می‌شود و با دقت توسط آزمایشگاه‌های طرف سوم، فروشندگان و کاربران محصولات تجاری مورد آزمایش قرار می‌گیرد. سه خدمتی که اغلب به الزامات امنیتی کاربران شبکه می‌پردازد، محرمانگی، یکپارچگی پیام و اصالت‌سنجی است.

گروه مهندسی اینترنت (IETF)[2] با امنیت لایه انتقال (TLS)[3] خود دارای استانداردی است که قادر به جلوگیری از دستکاری[4]، جعل پیام[5] و استراق سمع[6] توسط رمزگذاری[7] واحدها یا بخش‌های داده از یک انتهای لایه انتقال به انتهای دیگر است. علاوه بر این، TLS پروتکل مستقل از برنامه کاربردی است به این معنی که پروتکل‌های سطح بالاتر مانند پروتکل انتقال ابَرمتن (HTTP)[8] می‌تواند به صورت شفاف در بالای پروتکل TLS قرار گیرد.

جزئیات افزوده در مورد ویژگی پروتکل TLS پایه برای اطمینان از امنیت و قابلیت همکاری ضروری است. این ویژگی جزئیات در قالب الزامات خاص و راهنمایی برای استفاده از امنیت لایه انتقال (TLS) در رابطه با سامانه‌های ذخیره‌سازی را ارائه می‌کند.

1 - Communications Technology
2 - The Internet Engineering Task Force
3 - Transport Layer Security
4 - Tampering
5 - Message forgery
6 - Eavesdropping
7 - Encrypting
8 - The Hypertext Transfer Protocol

فناوری اطلاعات – ویژگی امنیت لایه انتقال (TLS) برای سامانه‌های ذخیره‌سازی

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزاماتی برای استفاده از پروتکل امنیت لایه انتقال (TLS) در رابطه با فناوری ذخیره‌سازی داده‌ها است. الزامات این استاندارد به منظور تسهیل قابلیت همکاری امن کارخواه‌ها[1] و کارسازهای[2] ذخیره‌سازی و فناوری‌های غیر ذخیره‌سازی در نظر گرفته شده است که ممکن است نیازهای قابلیت همکاری مشابهی داشته باشند.

این ویژگی به افراد دخیل در مالکیت، اجرا یا استفاده از افزاره‌های ذخیره‌سازی داده مربوط است. این افراد علاوه بر مدیران و مدیران سامانه هستند که مسئولیت‌های خاص برای امنیت اطلاعات و / یا امنیت ذخیره‌سازی، عملیات ذخیره‌سازی دارند یا افراد مسئول برنامه‌های امنیتی و تدوین سیاست امنیتی سازمان هستند که مدیران ارشد، کارفرمایان محصول و خدمت ذخیره‌سازی و سایر مدیران غیرفنی یا کاربران را نیز شامل می‌شود. همچنین این ویژگی به افراد دخیل در طرح‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیتی ذخیره‌سازی مربوط است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

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

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی‌است:

2-1 ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

یادآوری- استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سیستم های (سامانه های) مدیریت امنیت اطلاعات-مرور کلی و واژگان با استفاده از استاندارد ISO/IEC 27000 : 2014تدوین شده است.

2-2 IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,

1 - Clients
2 - Servers

یادآوری- استاندارد ملی ایران شماره ۱۷۱۱۵: سال ۱۳۹۴، فناوری اطلاعات -الزامات تشکیل و اعتبار سنجی مسیر گواهی دیجیتالی با استفاده از استاندارد RFC 5280: 2008, Internet X.509 : 1- تدوین شده است.

2-3 IETF, 2008 IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, IETF, 2008

2-4 IETF RFC 5746, Transport Layer Security (TLS) Renegotiation Indication Extension, IETF, 2010

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود.

۳-۱

مجموعه رمز

cipher suite

به ترکیبی از اصالت‌سنجی، رمزگذاری و الگوریتم‌های کد اصالت‌سنجی پیام استفاده‌شده برای انجام تنظیمات امنیتی برای اتصال به شبکه گفته می‌شود.

یادآوری ۱- مجموعه‌های رمز به طور معمول با امنیت لایه انتقال (TLS)[1] و پروتکل های شبکه لایه سوکت‌های امن (SSL)[2] استفاده می‌شود.

۳-۲

گواهی دیجیتال (رقمی)

digital certificate

ساختار داده امضاشده با امضای دیجیتالی (رقمی) بر اساس کلید عمومی است که متعلق بودن کلید به موضوع تعیین‌شده در ساختار را اظهار می‌کند.

1 - Transport Layer Security
2 - Secure Sockets Layer

۳-۳

پنهان کاری کامل پیش‌سو

perfect forward secrecy

شرایط امنیتی که هستار[1] ترک کننده نمی‌تواند هیچ کلید رمز به اشتراک گذاشته شده پس از آن را به دست آورد.

[منبع: بند ۳-۲۴ استاندارد ISO/IEC 11770-5: 2011]

۴-۳

پیشکار

proxy

واسطه‌ای است که هم به عنوان کارساز[2] و هم به عنوان کارخواه[3] به منظور ایجاد درخواست از طرف سایر کارخواه‌ها عمل می‌کند.

۵-۳

گواهی خود امضا

self-signed certificate

گواهی دیجیتالی (بند ۳-۲) است که توسط هستار یکسان که هویت او گواهی شده، امضا می‌شود.

یادآوری ۱- گواهی خود امضا یک گواهی امضاشده با کلید خصوصی خود است.

۶-۳

قدرت امنیتی

security strength

عدد مربوط به مقدار کار است (یعنی تعداد عملیات) که برای شکستن الگوریتم یا سامانه رمزگذاری لازم است.

عددی در ارتباط با مقدار کاری (یعنی تعداد عملیات) که برای شکستن یک الگوریتم یا سامانه رمزنگاشتی مورد نیاز است.

1 - Entity
2 - Server
3 - Client

یادآوری ۱- قدرت امنیتی بر حسب بیت مشخص می‌شود، و مقدار خاصی از مجموعه {۲۵۶، ۱۹۲، ۱۲۸، ۱۱۲، ۸۰} است. قدرت امنیتی b بیت به این معنی است که 2^b عملیات برای شکستن سامانه مورد نیاز است.

[منبع: بند ۳-۱۴، استاندارد ملی ایران شماره ۱۷۹۱۴-۲: سال ۱۳۹۳[1]]

1 - ISO/IEC 9797-2: 2011

۴ نمادها و اصطلاحات کوته نوشت

3DES	Triple Data Encryption Standard	استاندارد رمزگذاری داده سه‌گانه
AED	Authenticated Encryption with Additional Data	رمزگذاری اصالت‌سنجی‌شده با داده‌های افزوده
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
CA	Certificate Authority	مرجع صدور گواهی
CBC	Cipher Block Chaining	زنجیره بلوک رمز
CDMI	Cloud Data Management Interface	واسط مدیریت داده ابری
CRL	Certificate Revocation List	فهرست ابطال گواهی
CRLDP	CRL Distribution Point	نقطه توزیع CRL
DER	Distinguished Encoding Rules	قواعد کدگذاری متمایز
DHE	Ephemeral Diffie-Hellman	دیفه- هیلمن موقت
DSA	Digital Signature Algorithm	الگوریتم امضای دیجیتال
ECDHE	Elliptic Curve Ephemeral Diffie–Hellman	دیفه- هیلمن موقت منحنی بیضوی
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال منحنی بیضوی
EDE	Encryption-Decryption-Encryption	رمزگذاری، رمزگشایی، رمزگذاری
GCM	Galois/Counter Mode	حالت گالوا / شمارنده
HMAC	Hash-based Message Authentication Code	کد اصالت‌سنجی پیام مبتنی بر چکیده‌سازی
HTTP	Hypertext Transfer Protocol	پروتکل انتقال ابرمتن
HTTPS	Hypertext Transfer Protocol Secure	پروتکل انتقال ابرمتن امن
ICT	Information and Communications Technology	فناوری اطلاعات و ارتباطات
IETF	Internet Engineering Task Force	گروه مهندسی اینترنت
IP	Internet Protocol	پروتکل اینترنت

MAC	Message Authentication Code	کد اصالت‌سنجی پیام
MD5	Message Digest 5	خلاصه پیام ۵
OCSP	Online Certificate Status Protocol	پروتکل وضعیت گواهی برخط
PEM	Privacy Enhanced Mail	نامه بهبودیافته حریم خصوصی
PKCS	Public-Key Cryptography Standards	استانداردهای رمزنگاری کلید عمومی
PKI	Public Key Infrastructure	زیرساخت کلید عمومی
PSK	Pre-Shared Key	کلید پیش اشتراکی
RFC	Request For Comment	درخواست برای نظر
RSA	Rivest, Shamir, and Adelman algorithm	الگوریتم ریوست، شمیر و آدلمن
SHA	Secure Hash Algorithm	الگوریتم چکیده‌سازی امن
SMI-S	Storage Management Initiative – Specification	طرح مدیریت ذخیره‌سازی- ویژگی
SNIA	Storage Networking Industry Association	انجمن صنعت شبکه ذخیره‌سازی
SSL	Secure Socket Layer	لایه سوکت امن
TCP	Transmission Control Protocol	پروتکل واپایش ارسال
TLS	Transport Layer Security	امنیت لایه انتقال

۵ مرورکلی و مفاهیم

۵-۱ کلیات

سامانه‌ها و زیرساخت‌های ذخیره‌سازی داده به طور فزاینده از فناوری‌هایی مانند پروتکل TCP/IP برای مدیریت سامانه‌ها و داده‌ها و همچنین برای دسترسی به داده‌ها استفاده می‌کند. در بسیاری از موارد، تکیه بر اتصال مجزای تاریخ‌های قبلی، فناوری‌های تخصصی و امنیت فیزیکی مراکز داده برای محافظت از داده‌ها کافی نیست، به خصوص زمانی که داده‌ها حساس و / یا با ارزش بالا در نظر گرفته شده است. بنابراین، نیاز است که امنیت در لایه انتقال در برگرفته شود و در همان زمان، از قابلیت همکاری اطمینان حاصل شود.

امنیت لایه انتقال (TLS) و ملحقات آن، لایه سوکت امنیت (SSL)، برای محافظت موفق از طیف گسترده‌ای از ارتباطات در TCP/IP استفاده می‌کند. با اذعان به این واقعیت، صنعت ذخیره‌سازی استفاده از اتصال

TLS/SSL را در رابطه با دستور پروتکل انتقال ابرمتن (HTTP) برای ویژگی‌های متعدد اجبار کرده است. (به بند ۵-۲ مراجعه شود). متاسفانه، این ویژگی‌های ذخیره‌سازی طولانی و پیچیده هستند، این امر در نتیجه این است که چرخه‌های توسعه طولانی به دلیل آسیب‌پذیری‌های امنیتی یا حملات جدید، اجازه تغییرات سریع الزامات را نمی‌دهد.

اهداف این ویژگی عبارتند از:

- مشخص کردن عناصر TLS لازم برای امن کردن مدیریت ذخیره‌سازی و دسترسی به داده‌ها
- تسهیل به‌روزرسانی به موقع و پیشرفت‌های امنیتی برای ویژگی‌های ذخیره‌سازی
- اطمینان از این که کارخواه‌ها و سامانه‌های ذخیره‌سازی می‌توانند به صورت امن همکاری کنند
- پشتیبانی از فناوری‌های غیر ذخیره‌سازی که ممکن است نیازهای قابلیت همکاری TLS مشابهی داشته باشند

۵-۲ ویژگی‌های ذخیره‌سازی

به عنوان نقطه شروع، الزامات TLS از ویژگی‌های زیر استخراج شده است:

- استاندارد ملی ایران شماره ۱۷۸۲۶: سال ۱۳۹۲[1]، فناوری اطلاعات - واسط مدیریت داده ابری (CDMI)
- انجمن صنعت شبکه ذخیره‌سازی (SNIA)[2]، طرح مدیریت ذخیره‌سازی – ویژگی (SMI-S)، نسخه ۱-۶-۱

این الزامات پس از آن هماهنگ شده تا تفاوت‌های جزئی را از بین ببرد. الزامات نتیجه (به بند ۶ مراجعه شود) برای بازتاب وضعیت فعلی TLS و راهبردهای کاهش حمله به روز شده است.

۵-۳ مرورکلی TLS

۵-۳-۱ سابقه TLS

TLS پروتکلی است که امنیت ارتباطات را در شبکه‌ها فراهم می‌کند. این پروتکل به برنامه‌های کاربردی کارخواه/کارساز اجازه می‌دهد به روشی که برای جلوگیری از استراق سمع، دستکاری یا جعل پیام طراحی شده است، ارتباط برقرار کنند. TLS در بالای برخی از پروتکل‌های انتقال قابل اطمینان (به عنوان مثال، TCP) قرار گرفته و برای پوشینه‌دارسازی[3] پروتکل‌های سطح بالاتر مختلف استفاده می‌شود (به عنوان مثال، HTTP).

1 - ISO/IEC 17826: 2012
2 - Storage Networking Industry Association
3 - Encapsulate

نسخه ۱.۲ پروتکل TLS در IETF RFC 5246 مشخص شده است. نسخه‌های اولیه و با امنیت کمتر TLS نیز مشخص شده و در حال استفاده است. نسخه ۱.۰ TLS در IETF RFC 2246 و نسخه ۱.۱ TLS در RFC IETF 4346 مشخص شده است. ملحقات TLS، لایه سوکت‌های امن (SSL) و به ویژه نسخه ۳.۰ نیز در حال استفاده است اما امنیت آن کمتر است؛ SSL 3.0 در IETF RFC 6101 قدیمی، نسخه ۳.۰ پروتکل لایه سوکت‌های امن (SSL) مستند شده است.

۵-۳-۲ قابلیت TLS

TLS اصالت‌سنجی نقطه پایانی و ارتباطات حریم خصوصی در شبکه را با استفاده از رمزگذاری فراهم می‌کند. به طور معمول، تنها کارساز اصالت‌سنجی شده است (به عنوان مثال، هویت آن تضمین شده است) در حالی که کارخواه غیراصیل باقی می‌ماند؛ این به این معنی است که کاربر نهایی (که یک فرد یا یک برنامه کاربردی) سنجه تضمین با افرادی که در ارتباط هستند را دارد. اصالت‌سنجی دوجانبه (هویت‌های هر دو نقطه پایانی تایید شده است) با چند استثنا، نیاز به به کارگیری گواهی‌های دیجیتال در کارخواه دارد.

TLS شامل سه گام اصلی است:

الف- مذاکره همتا[1] برای پشتیبانی از الگوریتم

ب- تبادل و اصالت‌سنجی کلید

پ- رمزگذاری رمز متقارن[2] و اصالت‌سنجی پیام

در گام اول، کارخواه و کارساز در رابطه با مجموعه‌های رمزگذاری مذاکره می‌کنند (به ۵-۳-۳ مراجعه شود)، که رمزهای مورد استفاده، تبادل کلید، الگوریتم‌های اصالت‌سنجی و کدهای اصالت‌سنجی پیام (MAC) را تعیین می‌کند. الگوریتم‌های تبادل کلید و اصالت‌سنجی به طور معمول الگوریتم‌های کلید عمومی هستند. کدهای اصالت‌سنجی پیام از کد اصالت‌سنجی پیام کلید چکیده‌سازی، یا HMAC ساخته شده است.

۵-۳-۳ خلاصه ای از مجموعه‌های رمز

هر دوی TLS و SSL 3.0، ایجاد کلید، محرمانگی، امضا و الگوریتم چکیده‌سازی را در «مجموعه رمز» بسته‌بندی می‌کنند. شماره ۱۶ بیتی ثبت‌شده (۴ رقم مبنای شانزده) که شاخص مجموعه رمز نامیده می‌شود، برای هر مجموعه رمز تعریف‌شده تخصیص داده می‌شود. به عنوان مثال، توافق کلید RSA، امضای RSA، استاندارد رمزگذاری داده سه‌گانه (DES3) با استفاده از رمزگذاری، رمزگشایی، رمزگذاری (EDE) و زنجیره‌های بلوک رمز (CBC) محرمانگی و چکیده‌سازی الگوریتم چکیده‌سازی امن (SHA-1) یک مقدار شانزده‌تایی {0x00A} تخصیص داده و برچسب TLS_RSA_WITH_3DES_EBE_CBC_SHA را برای TLS ارائه می‌دهند.

1 - Peer
2 - Symmetric cipher encryption

برای اطمینان از سنجه قابلیت همکاری بین کارخواه‌ها و کارسازها، هر نسخه از TLS یک مجموعه رمز اجباری را مشخص می‌کند که برای پیاده‌سازی تمامی برنامه‌های کاربردی سازگار مورد نیاز است. موارد زیر مجموعه‌های رمز اجباری مرتبط با نسخه‌های مختلف TLS است:

- **TLS 1.0:** TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA {0x00, 0x13}

- **TLS 1.1:** TLS_RSA_WITH_3DES_EBE_CBC_SHA {0x00, 0x0A}

- **TLS 1.2:** TLS_RSA_WITH_AES_128_CBC_SHA {0x00, 0x0F}

کارخواه همیشه نشست TLS را آغاز می‌کند و مذاکره مجموعه رمز با ارسال یک پیام دست تکان دادن[1] می‌کند شروع می‌شود که مجموعه‌های رمزی (بر اساس مقدار شاخص) که قبول خواهد کرد را فهرست می‌کند. کارساز با یک پیام دست تکان دادن پاسخ می‌دهد که نشان می دهد کدام مجموعه رمز را از فهرست انتخاب کرده یا آن را «بی نتیجه[2]» گذاشته است. اگر چه کارخواه فهرست مجموعه رمز خود را با اولویت درخواست می‌کند، کارساز با شروع از افزودهین اولویت ممکن است هر یک از مجموعه‌های رمز ارائه‌شده توسط کارخواه را انتخاب کند. بنابراین، هیچ ضمانتی وجود ندارد که مذاکره، قوی‌ترین مجموعه را انتخاب کند. اگر هیچ مجموعه رمزی به طور متقابل پشتیبانی نشود، اتصال بی نتیجه است.

یادآوری- وقتی گزینه‌های مذاکره، از جمله گواهی‌های کلید عمومی اختیاری و داده‌های تصادفی که برای توسعه موارد کلیدزنی توسط الگوریتم‌های رمزنگاری استفاده می‌شود، کامل باشد، پیام‌ها برای جای دهی کانال ارتباطی در یک حالت امن تبادل می‌شود.

۵-۳-۴ گواهی‌های دیجیتال X.509

TLS از نسخه ۳ X.509 گواهی‌های کلید عمومی مطابق با *گواهی* و *رخنمای پسوند گواهی* تعریف‌شده در بخش ۴ RFC IETF 5280 استفاده می‌کند. این گواهی و رخ نمای[3] فهرست ابطال گواهی (CRL) زمینه‌های اجباری در گواهی و همچنین زمینه‌های اختیاری و پسوندهایی که ممکن است در گواهی گنجانده شده باشد را مشخص می‌کند. این گواهی‌های X.509 از یک امضای دیجیتال برای چسباندن کلید عمومی با هویت، استفاده می‌کنند. این امضاها اغلب توسط یک مرجع صدور گواهی (CA) صادر خواهد شد که با زیرساخت کلید عمومی (PKI) داخلی یا خارجی در ارتباط است؛ با این حال، رویکرد جایگزین از گواهی خود امضا استفاده می‌کند (گواهی دیجیتالی توسط جفت کلید بسیار مشابه امضا می‌شود که قسمت عمومی آن در داده‌های گواهی مشخص می‌شود). مدل‌های اعتماد در ارتباط با این دو رویکرد بسیار متفاوت است.

یادآوری- گواهی‌های خود امضا می‌تواند برای شکل‌دهی شبکه اعتماد (تصمیمات در مورد اعتماد در دست کاربران شخصی/ مدیران هستند)، مورد استفاده قرار گیرد. اما این مورد با امنیت کمتر است ، چرا که یک مرجع صدور مرکزی برای اعتماد

1 - handshake
2 - Abort
3 - Profile

وجود ندارد (به عنوان مثال، هیچ گونه تضمین هویت یا ابطالی وجود ندارد). این کاهش در کل امنیت که ممکن است حفاظت‌های کافی برای برخی محیط‌ها ارائه دهد، با کاهش پیچیدگی کلی پیاده‌سازی همراه است.

بخش ۶ IETF RFC 5280 نیاز به کارخواه‌ها و کارسازها را برای انجام اعتبارسنجی مسیر اولیه، اعتبارسنجی مسیر توسعه و اعتبار فهرست ابطال گواهی (CRL) شناسایی می‌شود. این اعتبارسنجی‌ها شامل موارد زیر است اما به آنها محدود نمی‌شود:

- گواهی، به طور معتبر گواهی را ایجاد کرده است

- امضا برای گواهی صحیح است

- تاریخ استفاده آن در مدت اعتبار (به عنوان مثال، منقضی نشده)

- گواهی ابطال نشده است (تنها به گواهی PKI اعمال می‌شود)

- زنجیره گواهی به طور معتبر ایجاد شده، با در نظر گرفتن بیشینه مجاز عمق زنجیره در مجموع تعداد گواهی همتا و گواهی‌های صادرکننده معتبر (تنها به گواهی‌های PKI اعمال می‌شود)

گواهی‌های دیجیتال X.509 در قالب‌های مختلف می‌آیند، اما موارد زیر اغلب به همراه TLS استفاده می‌شود:

- DER رمزگذاری‌شده X.509 به استاندارد ISO/IEC 9594-8: 2008 برای ویژگی و غلطنامه فنی مراجعه شود

- مبنای کدگذاری-۶۴ X.509 (اغلب PEM نامیده می‌شود). به بخش ۶-۸ IETF RFC 2045 مراجعه شود

۶ الزامات

۶-۱ الزامات پروتکل TLS

سامانه‌های ذخیره‌سازی عملکرد به عنوان کارسازها باید پروتکل TLS را پیاده‌سازی کنند؛ با این حال، استفاده از آن توسط کارخواه‌ها اختیاری است. نسخه TLS ۱.۲ (مشخص شده در IETF RFC 5246) یا نسخه‌های بعدی باید پیاده‌سازی شود. کارسازها نباید از SSL پشتیبانی کنند (به عنوان مثال، نسخه‌های غیر فعال ۱.۰، ۲.۰ و ۳.۰).

سامانه‌های ذخیره‌سازی باید در مقابل حملات در مذاکره مجدد مقاوم باشند (همان طور که IETF RFC 5246 مشخص شده)،

- گزینه ۱: مذاکره مجدد غیر فعال
- گزینه ۲:پیاده‌سازی پسوند نشانه مذاکره مجدد در IETF RFC 5246

۲-۶ مجموعه‌های رمز

مجموعه‌های رمز مورد نیاز برای قابلیت همکاری

سامانه‌های ذخیره‌سازی نباید از MD5 یا SHA-1 به عنوان HMAC پیش‌فرض استفاده کنند که با آنچه در مجموعه رمز مشخص شده متفاوت است. علاوه بر این، سامانه‌های ذخیره‌سازی باید از موارد زیر پشتیبانی کند:

- انتخاب و استفاده از جفت‌های الگوریتم امضا/چکیده‌سازی با استفاده از سازوکار *supported_signature_algorithms* در TLS 1.2
- استفاده از SHA-256 یا چکیده‌سازی‌های با قدرت افزوده

سامانه‌های ذخیره‌سازی باید از مجموعه‌های رمزی که کمینه ۱۱۲ بیت قدرت امنیتی دارند، استفاده کنند. علاوه بر این، مجموعه‌های رمز زیر باید توسط سامانه‌های ذخیره‌سازی و کارخواه‌هایی که به آنها دسترسی دارند، پشتیبانی شود:

- TLS_RSA_WITH_AES_128_CBC_SHA {0x00, 0x2F}
- TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}

یادآوری- استفاده از رمزگذاری حالت CBC، مخاطرات نظری مرتبط با حملات پدینگ اوراکل را دارد. حالت‌های رمزگذاری همچون GCM این مخاطرات را ندارد.

مجموعه‌های رمز توصیه‌شده برای امنیت ارتقایافته

مجموعه‌های رمز باید توسط سامانه‌های ذخیره‌سازی و کارخواه‌هایی که به آنها دسترسی دارند، پشتیبانی شود:

- TLS_RSA_WITH_AES_256_CBC_SHA256 {0x00, 0x3D}
- TLS_RSA_WITH_AES_128_GCM_SHA256 {0x00, 0x9C}
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 {0x00,0x67}

یادآوری- TLS-RSA به طور دقیق از تبادل کلید دیفه-هیلمن موقت (TLS_DHE) ضعیف‌تر است، چرا که رمز پیشرو دقیق را فراهم نمی‌کند. رمز پیشرو دقیق حتی اگر کلید خصوصی بلند مدتی تشکیل شده باشد، از نشست‌های ارتباطی گذشته حفاظت می‌کند.

از آنجا که استفاده از گواهی‌های دیجیتال می‌تواند به پیچیدگی اضافه کند، به خصوص برای اصالت‌سنجی دوگانه، رویکرد جایگزین با استفاده از کلیدهای اشتراک‌گذاشته شده قبلی مجاز است. به همین دلیل، توصیه می‌شود از مجموعه‌های رمز کلید از پیش به اشتراک گذاشته شده توسط سامانه‌های ذخیره‌سازی و کارخواه‌هایی که به آنها دسترسی دارند، استفاده شود.

- TLS_PSK_WITH_AES_128_CBC_SHA256{0x00,0Xae}
- TLS_PSK_WITH_AES_256_CBC_SHA384{0x00,0xAF}
- TLS_PSK_WITH_AES_128_GCM_SHA256{0x00,0xA8}

- TLS_PSK_WITH_AES_256_GCM_SHA384 {0x00,0xA9}

یادآوری- TLS_PSK_WITH_AES_128_GCM_SHA256 و TLS_PSK_WITH_AES_256_GCM_SHA384 از رمزگذاری اصالت‌سنجی‌شده با الگوریتم داده افزوده (AEAD) AEAD_AES_256_ GCM که در IETF RFC 5116 توصیف شده، استفاده می‌کنند.

در وضعیت‌هایی که امنیت ارتقایافته مورد نظر است یا مطابقت با الزامات خاص لازم است، توصیه می‌شود مجموعه‌های رمز زیر پشتیبانی شود:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256{0xC0,0x2B}
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 {0xC0,0x2C}

یادآوری- IETF RFC 6460 بیان می‌کند، مجموعه رمز TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ترجیح دارد؛ اگر چنین موردی پیشنهاد شود، باید قبل از مجموعه رمز TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ظاهر شود. این IETF RFC همچنین، سایر موضوعاتی که باید به آن پرداخته شود را تعیین می‌کند.

۶-۳ گواهی‌های دیجیتال

هنگامی که گواهی‌های دیجیتال توسط سامانه‌های ذخیره‌سازی و کارخواه‌هایی که به این سامانه‌ها، دسترسی دارند، استفاده می‌شود، گواهی‌های پشتیبانی‌شده باید نسخه ۳ X.509 گواهی کلید عمومی باشد که با گواهی و رخنمای پسوند گواهی که در بخش ۴ RFC IETF 5280 تعریف شده، مطابق است.

گواهی‌های کارساز باید توسط تمام کارسازهای ذخیره‌سازی با استفاده از TLS پشتیبانی شود. گواهی‌های کارخواه باید توسط کارخواه‌هایی که برای عملیات مدیریت و دسترسی داده‌ها به سامانه‌های ذخیره‌سازی دسترسی دارند، پشتیبانی شود.

برای گواهی‌های کارساز X.509 RSA / DSA، اندازه‌های کلید ۲۰۴۸ بیتی یا افزوده باید استفاده شود.

DER کد گذاری شده X.509، کدگذاری X.509 مبنای ۶۴ و قالب‌های گواهی PKCS#12 باید پشتیبانی شود.

اعتبار گواهی همان طور که در بخش ۶ IETF RFC 5280 توصیف شده باید توسط سامانه‌های ذخیره‌سازی و کارخواه‌هایی که گواهی‌های دیجیتال ارائه می‌دهند، انجام شود. علاوه بر این، یکی از رویکردهای زیر باید برای تعیین این که آیا مجوز باطل شده است مورد استفاده قرار گیرد:

- گزینه ۱: استفاده از فهرست‌های ابطال گواهی (CRL)

- CRL های پشتیبانی باید در DER کدگذاری‌شده X.509 یا قالب‌های X.509 کدگذاری‌شده مبنای ۶۴ باشد

- CRL های معتبر که به صورت محلی ذخیره شده (توزیع خارج دامنه کاربرد این استاندارد است) یا از منبع خارجی (به عنوان مثال، نقطه توزیع CRL یا CRLDP) بازیابی شده، باید استفاده شود

- گزینه ۲: استفاده از پروتکل وضعیت گواهی مانند OCSP به یکی از روش‌های زیر:

- استفاده از پروتکل وضعیت گواهی برخط (OCSP) به طور مستقیم همان طور که در IETF RFC 6960 توصیف شده است

- استفاده از OCSP از طریق پسوند درخواست *پاسخ وضعیت گواهی* به TLS به طور غیر مستقیم همان طور که در بخش ۸ RFC IETF 6066 توصیف شده است

۷ راهنمایی برای پیاده‌سازی و استفاده از TLS در ذخیره‌سازی داده

۷-۱ گواهی‌های دیجیتال

۷-۱-۱ مدل گواهی

گواهی‌های دیجیتال برای تعیین کارسازها (یا کارخواه‌های کمتر معمول) استفاده می‌شود و کلیدهای رمزنگاری را برای استفاده در ارتباطات ارائه می‌دهد. این گواهی‌ها می‌توانند گواهی‌های کلید عمومی یا گواهی‌های خود امضا باشد (همان طور که در ۵-۳-۴ اشاره شده). گواهی‌های کلید عمومی به طور معمول تضمین‌های هویت قابل اطمینان‌تری را ارائه می‌کند، اما نیاز به طرح‌ریزی اولیه و زیرساخت پشتیبان دارند (به عنوان مثال، مراجع صدور گواهی). گواهی‌های خود امضا برای استقرار بسیار آسان است اما تضمین هویت قابل اعتمادی ارائه نمی‌کنند. توصیه می‌شود سازمان‌ها بین این دو مدل بر اساس رخ‌نمای مخاطره و منابع در دسترس تصمیم آگاهانه‌ای بگیرند.

۷-۱-۲ زنجیره اعتماد

اعتمادی که در تضمین هویت توسط گواهی ارائه شده، در واقع به اعتماد هستار صدور گواهی بستگی دارد (به عنوان مثال، مرجع صدور گواهی). اغلب مرجع صدور گواهی قابل اعتماد، گواهی را برای سازمانی که پس از آن گواهی خود را صادر خواهد کرد، صادر می‌کند (این موضوع «زنجیره اعتماد» را ایجاد خواهد کرد). هنگام استفاده از گواهی‌های کلید عمومی، توصیه می‌شود سازمان‌ها به صراحت مراجع صدور گواهی که مجاز به صدور گواهی برای استفاده در سازمان هستند را تعیین کنند. توصیه می‌شود این CA های مورد اعتماد در کارخواه پیکربندی شود (به عنوان مثال، مرورگرهای وب).

۷-۱-۳ چرخه عمر گواهی

گواهی‌ها نیاز به صدور، نصب، جایگزینی و در نهایت حذف / ابطال دارند. حاکمیت موثر این چرخه عمر گواهی وابسته به سازمانی است که خط‌مشی‌ها و رویه‌ها را تدوین کرده است. تصمیم معمولا نادیده گرفته شده، عمر گواهی است. گواهی‌ها دارای تاریخ انقضا هستند تا بیشینه زمان اعتبار گواهی مشخص شود (بسیار شبیه به سایر شکل‌های تضمین هویت) و در پایان عمر خود، باید برای جلوگیری از خطاهای «گواهی منقضی شده» جایگزین شوند. هنگام تنظیم طول عمر، با دقت مخاطره، پیچیدگی درخواست و نصب گواهی

و تعداد گواهی‌های دخیل را در نظر بگیرید. برای مثال، اگر فرآیند نصب گواهی / درخواست نیاز به ۱.۵ نفر ساعت دارد و ۱۰۰۰۰ گواهی در سازمان وجود دارد، تنظیم طول عمر گواهی به ۱ سال نیاز به ۸ نفر کارمند تمام وقت (۱۰۰۰۰ * ۱.۵ تقسیم بر ۸ ساعت در هر روز کاری تقسیم بر ۲۳۰ روز کاری در سال) فقط برای جایگزینی گواهی دارد.

حذف گواهی‌ها از افزاره‌های در حال نوسازی یا خارج از واپایش سازمان، سنجه‌ای ضروری برای محافظت از سازمان در مقابل دسترسی‌های غیر مجاز است.

اگر گواهی به خطر بیافتد (به عنوان مثال، کلید خصوصی به یک فرد غیر مجاز نشان داده شود) یا اگر گواهی دیگر مورد نیاز نباشد، توصیه می‌شود گواهی برای جلوگیری از استفاده افزوده آن ابطال شود (به بند ۷-۱-۴ مراجعه شود).

۷-۱-۴ ابطال

گواهی‌ها زمانی که دیگر مفید نیستند یا به خطر افتاده اند نیاز به غیر معتبر شدن (ابطال) دارند (به عنوان مثال، کلید خصوصی مرتبط با گواهی در اختیار یک واحد غیر مجاز قرار گرفته باشد). به زبان ساده، ابطال گواهی فرایند اضافه کردن گواهی به فهرست ابطال گواهی (CRL) است. همان طور که در بند ۶-۳ توصیف شده، کارخواه‌ها و سایر کاربران گواهی نیاز به وارسی اعتبار گواهی (به عنوان مثال، وارسی این که گواهی ابطال نشده است) قبل از استفاده از گواهی دارند.

توصیه می‌شود به موضوعات مهم ابطال گواهی زیر پرداخته شود:

- توصیه می‌شود منابع اطلاعات ابطال، مرتبط و قابل اعتماد باشد

- توصیه می‌شود اطلاعات تا حد امکان «جدید» باشد، به ویژه هنگامی که داده‌های با ارزش بالا یا حساس دخیل باشد (به عنوان مثال، CRL می‌تواند تاریخ انقضای طولانی داشته باشد که نیاز به بازیابی نسخه بالاتری نسبت به نسخه فعلی CRL دارد)

- CRL های شبیه به زنجیره‌های گواهی می‌تواند بزرگ باشد بنابراین توصیه می‌شود مفاد کافی برای ذخیره و پردازش CRL ها زمانی که برای اعتبار سنجی استفاده می‌شود، ایجاد شود

- هنگام استفاده از OCSP به طور مستقیم، توصیه می‌شود کاربران درک کنند که ممکن است موضوعات حریم خصوصی وجود داشته باشد که حفاظت افزوده را ضروری می‌کند (به عنوان مثال، با استفاده از TLS با OCSP)

۷-۲ آگاهی امنیتی

آموزش کاربران (به عنوان مثال، در طول آموزش آگاهی امنیتی) در کار با گواهی ضروری است. برای مثال، زمانی که سازمان از کلید عمومی استفاده می‌کند، کاربران باید آموزش داده شوند که هرگز از سایتی که «هشدار گواهی» (صادر شده توسط CA غیر قابل اعتماد، منقضی‌شده، و غیره) تولید می‌کند، بازدید نکنند و

این هشدارها را گزارش کنند. لازم به ذکر است که گواهی‌های خود امضا به طور معمول هشداری را در مرورگر وب تولید می‌کنند و کاربران می توانند اگر دلایل دیگری برای اعتماد به هویت سایت داشته باشند (به عنوان مثال، ایجاد یک نشست HTTPS با افزاره ذخیره‌سازی توسط نشانی شبکه درگاه مدیریت آن) این هشدار را نادیده بگیرند.

۷-۳ مجموعه‌های رمز

همان طور که در بند ۵-۳-۳ شرح داده شده، مجموعه‌های رمز عنصر اصلی TLS هستند و بسیاری از رمزنگاری‌های مورد استفاده در نشست TLS را تعیین می‌کنند، بسیاری از مجموعه‌های رمز مختلف در TLS پشتیبانی شده است و برخی از آنها از سایر مجموعه‌ها قوی‌تر است. برای جلوگیری از کاهش امنیت در یک نشست TLS، از راهنمای مربوط به مجموعه رمز استفاده کنید:

- توصیه می‌شود هر دوی کارخواه و کارساز پیکربندی شود تا استفاده از مجوعه‌های رمز مشخص‌شده در بند ۶-۲ را الزام کند.
- توصیه می‌شود مجموعه‌های رمز ضعیف (به عنوان مثال، همه مجوعه‌های رمز SSL V2.0 که از رمزگذاری NULL استفاده می‌کنند و از MD5 برای چکیده‌سازی استفاده می‌کند و از حالت‌های ECB عملیات و غیره استفاده می‌کند) به صراحت از کارخواه‌ها و کارسازها خارج شود.
- توصیه می‌شود کارخواه‌ها قابل پیکربندی باشد تا تنها مجموعه‌های رمزی که کمینه سطح قدرت امنیتی را برآورده می‌کند، فهرست کند (به عنوان مثال، کمینه ۱۱۲ بیت)
- توصیه می‌شود کارسازها قابل پیکربندی باشد تا تنها مجموعه‌های رمزی که کمینه سطح قدرت امنیتی را برآورده می‌کند، بپذیرند و قویترین مجموعه رمز قابل قبول ارائه شده توسط کارخواه را انتخاب کنند
- در صورتی که کارخواه نمی‌تواند استفاده از مجموعه رمز توصیه‌شده را با کارساز مذاکره کند، توصیه می‌شود اتصال رد شود.

همان طور که در بند ۶-۳ اشاره شد، برای گواهی‌های با استفاده از RSA/DSA، اندازه کلید باید کمینه ۲۰۴۸ بیت باشد.

۷-۴ استفاده از TLS با HTTP

یک مخاطره جدی این است که مهاجم ممکن است قادر به راه اندازی کارساز نادرست یا قرار دادن یک پیشکار غیر مجاز در مسیر ارتباطات باشد تا اطلاعات حساس مانند اعتبار اصالت‌سنجی را اخذ کند. مقابله موثر برای این حمله، استفاده واپایش‌شده گواهی‌های کارساز با TLS است که با واپایش‌های کارخواه در پذیرش گواهی تطبیق داده شده است وفرض بر این است که کارساز کاذب قادر به بدست آوردن گواهی قابل قبول نخواهد بود. به طور خاص، این موضوع می‌تواند با پیکربندی کارخواه‌ها برای استفاده همیشگی TLS تحت اصالت‌سنجی HTTP انجام شود.

کارسازها ممکن است برای کارخواه‌ها از طریق استفاده از گواهی‌های کارساز صادرشده توسط یک مرجع صدور گواهی خاص، مجاز شوند (یا گواهی‌های خود امضا با سایرین، تضمین‌هایی مانند نشانی شبکه شناخته شده را شناسایی می‌کند) و واپایش‌های کارخواه که گواهی قابل قبول را مشخص می‌کند، تطبیق دهد. به طور جایگزین، کارسازها ممکن است با استفاده از کلیدهای پیش اشتراکی مجاز شوند (همان طور که در بند ۵-۷ توصیف شده است).

۵-۷ استفاده از کلید پیش اشتراکی

اصالت‌سنجی از طریق کلید پیش اشتراکی (PSK) آنچه که به طور عمومی به عنوان «منبع اصالت‌سنجی» شناخته شده را پیاده‌سازی می‌کند، اصالت‌سنجی بر اساس منبع ارتباطات با استفاده از کلید صحیح است. این روش در مقایسه با اصالت‌سنجی به طور بالقوه قوی که توسط کلید عمومی یا گواهی‌های خود امضا ارائه شده، روشی اصالت‌سنجی سبک‌تری است. همان طور که در IETF RFC 4279 اشاره شده، PSK می‌تواند در موارد زیر مناسب ترین روش باشد:

اجتناب از عملیات گواهی - عملیات رمزنگاری متقارن که بسیار کمتر وابسته به واحد پردازنده مرکزی (CPU)[1] است و بنابراین برای محیط‌های CPU محدود مناسب است.

مدیریت کلید ساده - در برخی از محیط‌ها ممکن است استفاده از PSK به جای سرمایه‌گذاری در زیرساخت‌ها و فرایندهای لازم برای پشتیبانی از گواهی بسیار راحت‌تر باشد.

با این حال سادگی به دست آمده در اجتناب از استفاده از گواهی‌ها هزینه دارد. در نظر بگیرید موردی که در آن کلید متعلق به یک کارساز به خطر افتاده است: اگر آن کلید خصوصی از یک گواهی PKI باشد، تمام چیزی که نیاز است، ابطال گواهی فعلی و صدور یک گواهی جدید است. اگر گواهی جدید توسط یک CA مورد اعتماد صادر شود، (یا کارخواه بر هشدارهای گواهی کلیک کند)، کارخواه می‌تواند برای اتصال به کارساز بدون مشکل ادامه دهد. با این حال، اگر کارساز از PSK برای اصالت به کارخواه‌ها استفاده کند، لازم است که یک کلید جدید برای کارساز تولید شود و سپس پیکربندی هر کارخواه برای استفاده از کلید جدید هنگام اصالت‌سنجی کارساز، اصلاح شود.

PSK همچنین برخی از انواع حملات را تا حدودی آسان‌تر می‌کند. به عنوان مثال، محیط گواهی، جعل هویت یک هستار را سخت‌تر می‌کند چرا که جعل نیاز به آگاهی از کلید خصوصی مرتبط با گواهی داده‌شده دارد. این موضوع، استفاده خصمانه از مرجع صدور گواهی‌های سرکش، حملات میان فردی و غیره را برای کار با این مسئله برمی‌انگیزد. در محیط PSK، اگر مهاجم بتواند کلید پیش اشتراکی را در اختیار گیرد، زمانی که اصالت‌سنجی صرفا با در اختیار داشتن کلید ارائه شده است ممکن است کارساز را به جای دیگری

1 - Central Processing Unit

جا زند. این موضوع لزوم حفاظت از PSK از دسترسی غیرمجاز یا افشا، حیاتی بودن شیوه‌های مدیریت کلید را تشدید می‌کند.

هنگام استفاده از PSK، توصیه می‌شود سازمان:

- تعداد کلیدهای مورد نیاز و دامنه کاربرد آن کلیدها را درک کند - برای مثال، هنگامی که کارساز را برای کارخواه‌ها اصالت‌سنجی می‌کند، ممکن است پیکربندی کلید مشابه در تمام کارخواه‌ها قابل قبول باشد. با این دامنه وسیع برای آن کلید، کلید زنی مجدد (با توجه به مدیریت دوره رمز یا به خطر افتادن کلید) نیاز به پیکربندی مجدد هر کارخواه خواهد داشت. اگر اصالت‌سنجی متقابل لازم باشد، یک جفت کلید منحصر به فرد (یکی در کارساز و یکی در کارخواه) برای هر کارخواه مورد نیاز است. اطمینان حاصل کنید که فرآیند تولید کلید از آنتروپی کافی استفاده می‌کند و باعث استفاده از کل فضای کلید می‌شود.
- طرح‌ریزی فرایند توزیع کلید - با PSK، کلیدها نیاز به توزیع بین کارخواه‌ها و کارسازها دارند و لازم خواهد بود به دقت از آن کلیدها از افشا در طول توزیع، محافظت شود.
- محافظت از کلیدهای ذخیره‌شده در کارخواه‌ها - با PSK، کارخواه‌ها نیاز به ذخیره کلید(های) استفاده‌شده در اصالت‌سنجی کارساز دارند (یا اگر اصالت‌سنجی متقابل با کارساز استفاده می‌شود) و کارخواه‌ها ممکن است وضعیت امنیتی پیش فرض سبک‌تری را نسبت به کارسازی که در یک مرکز داده به خوبی مدیریت‌شده است، داشته باشند. هنگام استفاده از PSK، ممکن است نیاز باشد ذخیره‌سازی کلید قوی‌تر شود.
- مخاطرات مرتبط با تکیه بر منبع اصالت‌سنجی را درک کند - زمانی که اصالت‌سنجی توسط دانش کلید به تنهایی به دست می‌آید، واپایش‌های جبران افزودهی ممکن است مورد نیاز باشد. به عنوان مثال، موردی که PSK کارساز به خطر افتاده است را در نظر بگیرید: مهاجم می‌تواند تقلیدی جعلی از آن کارساز را راه‌اندازی کند و کارخواه‌ها را به سمت آن بفرستد (شاید با بهره برداری مبتنی بر سامانه نام دامنه (DNS)[1]) و از کارساز واقعی غیر قابل تشخیص باشد. برای جبران ضعف اصالت‌سنجی منبع، ممکن است لازم باشد در یک محیط خاص، محیط شبکه به دقت جدا شود و واپایش‌های دسترسی سختی به منظور محدود کردن قابلیت مهاجم برای ایجاد کارساز سرکش در دامنه ارتباطات کارخواه‌ها به کار گرفته شود.

1 - Domain Name System

کتاب‌نامه

[1] ISO/IEC 9594-8:2008, Information technology — Open Systems Interconnection — The Directory:Public-key and attribute certificate frameworks

[2] ISO/IEC 9797-2:2011, Information technology — Security techniques — Message AuthenticationCodes (MACs) — Part 2: Mechanisms using a dedicated hash-function

[3] ISO/IEC 11770-5:2011, Information technology — Security techniques — Key management —Part 5: Group key management

[4] ISO/IEC 17826:2012, Information technology — Cloud Data Management Interface (CDMI)

[5] IETF RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, November 1996

[6] IETF RFC 2246, The TLS Protocol Version 1.0, January 1999

[7] IETF RFC 4279, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), December 2005

[8] IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[9] IETF RFC 5116, An Interface and Algorithms for Authenticated Encryption, January 2008

[10] IETF RFC 5288, AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008

[11] IETF RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

[12] IETF RFC 5487, Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode, IETF, March 2009

[13] IETF RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions, January 2011

[14] IETF RFC 6101, The Secure Sockets Layer (SSL) Protocol Version 3.0, August 2011

[15] IETF RFC 6176, Prohibiting Secure Sockets Layer (SSL) Version 2.0, March 2011

[16] IETF RFC 6460, Suite B Profile for Transport Layer Security (TLS), IETF, January 2012

[17] IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,June 2013

[18] PKCS#12 Personal Information Exchange Syntax Standard

[19] Storage Networking Industry Association (SNIA). Storage Management Initiative –Specification (SMI-S), Version 1.6.1, Architecture Book, http://www.snia.org/tech_activities/standards/curr_standards/smi

[20] Practical Padding Oracle Attacks, Juliano Rizzo, Thai Duong, May 25, 2010, USENIX WOOT 2010,https://www.usenix.org/legacy/event/woot10/tech/full_papers/Rizzo.pdf