تاریخ دریافت مقاله: ۱۳۹۲/۶/۲۵
تاریخ پذیرش مقاله: ۱۳۹۲/۱۰/۱۵

ارائه الگوی الگوریتم رمزنگاری و احراز اصالت در سامانه‌های دورسنجی نظامی

امیرمهدی سازدار[۱]
منصور نجاتی جهرمی[۲]
جلال راعی[۳]
افشین احمدلو[۴]

چکیده:

ارسال و دریافت ایمن داده‌ها و حصول اطمینان از وجود فرستنده و گیرنده‌ی خاص از جمله موضوعاتی است که در ارتباطات دیجیتال و به خصوص در سامانه‌های دورسنجی، مورد توجه قرار گرفته است. روش‌های اعمال شده برای رمزنگاری و احراز اصالت از کاربردی‌ترین مولفه‌های تبادل داده‌های دورسنجی و فرمان از راه دور است. این مقوله در ارتباطات نظامی و دفاعی بسیار حساس‌تر و مخاطره انگیزتر است. در این مقاله ابتدا به معرفی روش‌های رمزنگاری و احرازاصالت پیام‌ها در سنجش و فرمان از را دور در حوزه‌ی استاندارد CCSDS[۵] پرداخته و در نهایت الگوی جدیدی با رویکرد ترکیبی و امکان کاربرد همزمان رمزنگاری و احرازهویت برای سامانه‌های نظامی ارائه می‌شود. بیان این مطالب کاربرد رمزنگاری و احراز اصالت پیام، در عرصهٔ سنجش و فرمان از راه دور در سازمان‌های نظامی و دفاعی را تبیین خواهد نمود.

کلمات کلیدی:

سنجش از راه دور، رمزنگاری، احراز اصالت، سامانه داده فضایی، استانداردهای ارتباط ماهواره‌ای

۱- کارشناس ارشد برق، مخابرات گرایش رمز، دانشگاه علوم و فنون هوایی شهید ستاری، Sazdar@gmail.com
۲ - استادیار مخابرات، مرکز تحقیقات و جهاد دانشگاه هوایی شهید ستاری،
۳ - مدرس دانشگاه علوم و فنون هوایی شهید ستاری
۴ - مدرس دانشگاه علوم و فنون هوایی شهید ستاری

5 - Consultative Committee Space Data System

مقدمه

در سامانه‌های دفاعی، امنیتی و نظامی اطمینان از عدم افشای اطلاعات توسط فرایندها یا عوامل غیر مجاز از مصادیق بارز محرمانگی است، که در سامانه‌های مخابراتی با روش‌های رمزنگاری و احرازاصالت بدست می‌آید. نوع روش رمزنگاری وابسته به نوع ماموریت سامانه دورسنجی و میزان امنیت مورد نیاز و با توجه به تحلیل آسیب پذیری هر سامانه متفاوت است و مهمترین هدف آن، ممانعت از افشای اطلاعات توسط عوامل غیر مجاز و از دست رفتن اهداف عملیاتی است. در سامانه‌های ارتباطی محرمانگی توسط دو سازوکار اساسی یعنی انتقال اطلاعات از طریق کانال امن و رمزنگاری بوجود می‌آید. در ارتباطات ماهواره‌ای و مخابراتی نظیر دورسنجی و فرمان از راه دور، به علت عدم امکان وجود کانال امن، امنیت اطلاعات با رمزنگاری تامین می‌شود و باعث اطمینان از عدم افشای اطلاعات در طول مسیر انتقال از فضاپیما به سمت زمین یا بالعکس و همچنین بین ایستگاه‌های فضایی می‌شود. برای نیل به این اهداف، الگوریتم‌های رمزنگاری صرفنظر از اینکه کجا و چگونه سرویس‌های محرمانگی را پیاده‌سازی می‌نمایند، اساس و پایه امنیت هستند. در این راستا مدل استاندارد CCSDS روش‌های مدون و جامعی را به منظور یکسان‌سازی و یکپارچگی فعالیت‌های ارتباط فضایی و جلوگیری از تلاش‌های موازی مطرح نموده است.

رمزنگاری در ساختار CCSDS

سامانه‌های دورسنجی از ماموریت‌های متفاوتی پشتیبانی می‌کنند و گاهی برای این ماموریت‌های متفاوت، از فرکانس‌های رادیویی مشابه و کانال‌های ارتباطی یکسان استفاده می‌شود. هر جزء از این مجموعه محرمانگی خاص خود را دارند و به فرامین خود اجازه دسترسی و درهم آمیختن با سایر دستورات و سَنجه‌ها را نمی‌دهند.

استاندارد CCSDS نیز مشابه سایر ارتباطات شبکه‌ای، از مدل لایه‌ای (مشابه OSI[1]) تبعیت می‌کند و با عبور ریزبسته‌های۲-[2] اطلاعاتی از هر لایه و اعمال تنظیمات خاص هر لایه بر روی ریزبسته‌ها الگوریتم‌های محرمانگی اعمال می‌شوند.

البته تاکنون هیچ روش نهایی و تضمین کننده‌ای برای انتخاب الگوریتم و محل لایهٔ مورد نظر بیان نشده‌است (CCSDS 350.0-G-2, 2006). رمزنگاری می‌تواند در لایه‌های متفاوتی از

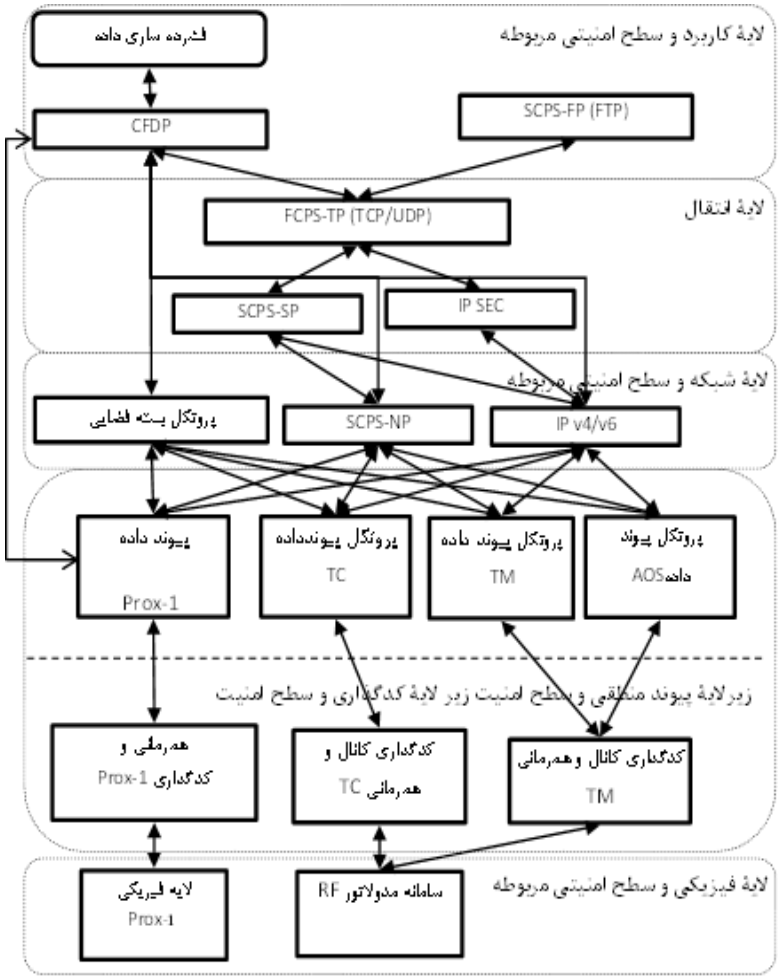
1- Open System Interconnection
2-Packets

استاندارد CCSDS مانند لایهٔ کاربرد (نظیر TLS/SSL[1] (Dierks and Rescorla, 2006)) یا روی لایهٔ شبکه در SCPS-SP[2] (CCSDS 713.5-B-1, 1999) و IPSec[3] (Kent and Seo, RFC 4301, 2005) و (Kent, RFC 4303, 2005). و یا در لایهٔ پیوند و حتی در لایهٔ فیزیکی مانند رمزنگاری یکجا[4] و یا امنیت انتقال[5] بکار رود.

در مورد رمزنگاری یکجا ذکر این نکته لازم است که، این روش در لایهٔ فیزیکی پیاده‌سازی می‌شود و محرمانگی را برای تمام ساختارهای داده ارتباطی و کلیهٔ فیلدهای ریزبسته فراهم می‌کند. این روش حداکثر محرمانگی را در ارتباطات نقطه به نقطه[6] پوشش می‌دهد و نام دیگر آن رمزنگاری پیوند[7] است. در امنیت انتقال برای مقابله با عمل تولید پارازیت و اختلال در سامانه[8] روش‌هایی نظیر گسترش طیف[9] با بکارگیری ترتیب مستقیم[10] و یا پرش فرکانسی[11] بکار می‌رود که این روش‌ها به نام امنیت انتقال یا TRANSEC مشهور هستند.

البته برای افزایش امنیت می‌توان بصورت همزمان در چندین لایه از الگوریتم‌های رمزنگاری استفاده کرد. درشکل (۱) ترکیب برخی پروتکل‌های مختلف ارتباطی در سامانهٔ دورسنجی و مدل لایه‌ای CCSDS و تنظیمات امنیتی مربوطه نشان داده شده است (CCSDS 130.0-G-2, 2007). در شکل(۱) چهار سطح امنیتی روی لایهٔ فیزیکی، لایهٔ پیوند داده، لایهٔ شبکه و لایهٔ کاربرد مشاهده می‌شود. البته در صورت نیاز می‌توان روی سایر لایه‌ها نظیر لایهٔ انتقال نیز تنظیمات امنیتی را اعمال کرد است (CCSDS 130.0-G-2, 2007). کاربرد هر یک از روش‌های متنوع رمزنگاری در سامانه، با توجه به هزینه‌های راه‌اندازی بر اساس نیاز ماموریت و تحلیل عوامل خطر پذیری متفاوت است.

1- Transport Layer Security And Secure Socket Layer
2- 4Space Communications Protocol Specification - Security Protocol
3- Internet Protocol Security
4- Bulk Encryption
5- Transmission Security
6- Point to Point
7- Link Encryption
8- Jamming
9- Spread Spectrum
10- Direct Sequence
11- Frequency Hopping



شکل(۱) : پروتکل‌های‌ماموریت‌های CCSDS **و تنظیمات‌امنیتی‌لایه‌ها**

در جدول(۱) الگوریتم‌های معمول که در استاندارد CCSDS برای رمزنگاری استفاده می‌شوند به همراه برخی از خصوصیات آنها آمده است (CCSDS 350.2-G-0, 2007).

جدول(۱) الگوریتم‌های معمول رمزنگاری در CCSDS

ردیف	الگوریتم	طول بلوک (بیت)	نوع	طول کلید (بیت)	تعداد رُند	ساختار

۱	DES	۶۴	متقارن	۵۶	۱۶	FN [۱] متوازن
۲	Triple DES (3DES)	۶۴	متقارن	۵۶، ۱۱۲، ۱۶۸	۴۸	FN
۳	Rijndael (AES)	۱۲۸	متقارن	۱۲۸، ۱۹۲، ۲۵۶	۱۰، ۱۲، ۱۴	SPN [۲]
۴	Serpent	۱۲۸	متقارن	۱۲۸، ۱۹۲، ۲۵۶	۳۲	SPN
۵	Twofish	۱۲۸	متقارن	۱۲۸، ۱۹۲، ۲۵۶	۱۶	FN
۶	Blowfish	۶۴	متقارن	۴۴۸ ،۲۵۶	۱۶	FN
۷	RC6	۱۲۸	متقارن	۱۲۸، ۱۹۲، ۲۵۶	۲۰	FN
۸	TEA [3]	۶۴	متقارن	۱۲۸	۳۲	FN
۹	XTEA [4]	۶۴	متقارن	۱۲۸	۶۴	FN
۱۰	IDEA [5]	۶۴	متقارن	۱۲۸	۸/۵	SPN
۱۱	MARS	۱۲۸	متقارن	۱۲۸ تا ۱۰۲۴	۳۲	FN
۱۲	Kasumi (A5/3) [6]	۶۴	متقارن	۱۲۸	۸	FN
۱۳	SEED [7]	۱۲۸	متقارن	۱۲۸	۱۶	FN تودرتو
۱۴	RSA	نامعلوم	نامتقارن	۱۰۲۴ تا ۲۰۴۸	-	-
۱۵	الگوریتم‌های مبتنی بر خم بیضوی (ECC) [8]	-	نامتقارن	حداقل ۱۶۰	-	-

الگوریتم‌های رمزنگاری در CCSDS

برای بهینه نمودن ماموریت‌های دورسنجی فضایی، استاندارد CCSDS، الگوریتم AES با حالت شمارنده‌ای را پیشنهاد می‌نماید (FIPS-197, 2001) در استاندارد CCSDS کلیدها با طول ۱۲۸ بیت استفاده می‌شوند، ولی استفاده از کلیدهای با طول بیشتر برای امنیت بهتر نیز توصیه می‌شود (CCSDS 350.0-G-2, 2006).

الگوریتم AES یک الگوریتم متقارن و بلوکی است که روی بلوک‌های ۱۲۸ بیتی اجرا می‌شود در مورد نحوه کاربرد الگوریتم AES، پنج مد زنجیره بلوک رمزی [۱] (CBC)، کتاب کد

1- Feistel Network
2- Substitution Permutation Network
3- Tiny Encryption Algorithm
4- eXtended Tiny Encryption Algorithm
5- International Data Encryption Algorithm
۶- این الگوریتم در سامانه‌های ارتباطات تلفن همراه 3GPP و سامانه‌های UTMS، GSM و GPRS استفاده می‌شود.
۷- این الگوریتم ازسال ۲۰۰۹ توسط مرورگر Mozilla 3.5.4 پشتیبانی شد و هم اکنون در IPSec نیز از این الگوریتم استفاده می‌شود.
8- Elliptic Curve Cryptosystem

الکترونیک[۲] (ECB)، پسخور رمزی[۳] (CFB)، پسخور خروجی[۴] (OFB) و مد شمارنده[۵] (CTR) بیان شده است (Dworkin, NIST 800-38A, 2001). استاندارد CCSDS با تبعیت از توصیه‌نامه IETF[۶] از پروتکل IPSec و مد CTR استفاده می‌نماید (Housley, RFC 3686, 2004). البته با توجه به محدودیت‌های سرعت و پهنای باند در سامانه‌های نظامی و دفاعی استفاده از الگوریتم‌هایی که، با طول کلید کمتر و سرعت بالاتر امنیت مشابه‌ای را تولید می‌کنند، همواره در ارجعیت است. با توجه به سرعت بالا و طول کوتاه کلید در الگوریتم‌های مبتنی برخم بیضوی توصیه می‌شود از این روش‌ها برای رمزنگاری در سامانه‌های نظامی بومی استفاده نمود.

همانگونه که در جدول(۲) ملاحظه می‌کنید، در امنیت مشابه (هر ستون از جدول امنیت مشابه دارد) طول کلید در رمزنگاری متقارن DES فقط نصف طول کلید در الگوریتم‌های مبتنی برخم‌بیضوی است، درحالیکه طول کلید در الگوریتم RSA چندین برابر (تا ۶۰ برابر در آخرین ستون) شده است (استالینگ، ۲۰۰۵ : ۳۱۳).

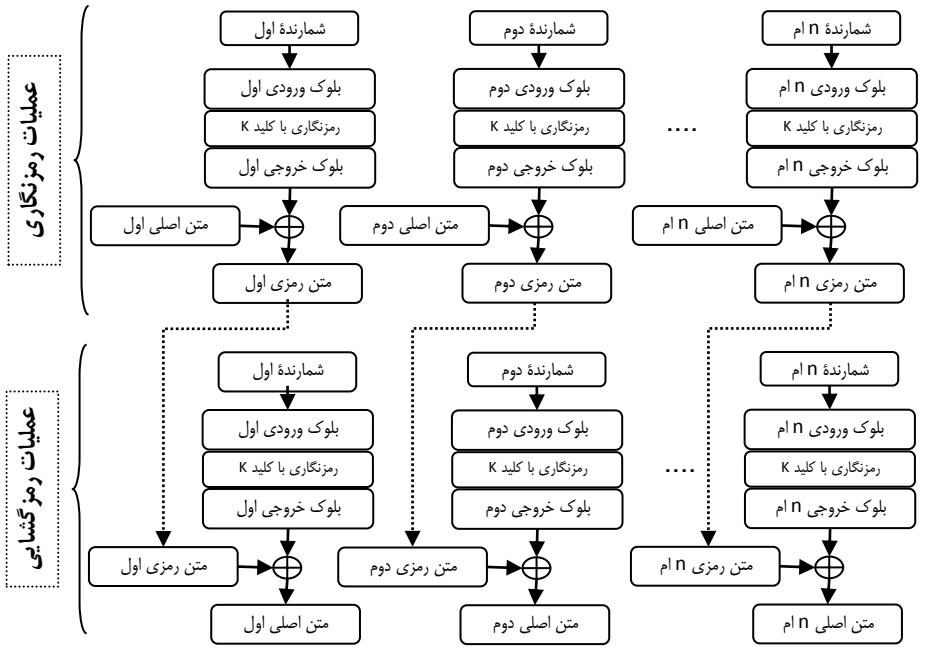
جدول(۲) مقایسه سیستم‌های رمزنگاری از نظر طول کلید

سیستم رمز		طول کلید (bit)					
متقارن (DES)		۵۶	۸۰	۱۱۲	۱۲۸	۱۹۲	۲۵۶
نامتقارن	RSA	۵۱۲	۱۰۲۴	۲۰۴۸	۳۰۷۲	۷۶۸۰	۱۵۳۶۰
	ECC	۱۱۲	۱۶۰	۲۲۴	۲۵۶	۳۸۴	۵۷۲

این امر خود بیانگر توانایی‌های الگوریتم‌های مبتنی بر خم بیضوی است و می‌تواند به عنوان نقطهٔ اتکایی برای استفاده در ارتباطات و تبادل اطلاعات دورسنجی در سامانه‌های نظامی و دفاعی باشد. نکته قابل توجه برای انجمن CCSDS اینست که با توجه به استقلال

1- Cipher Block Chaining Mode
2- Electronic Code Block Mode
3- Cipher Feedback Mode
4- Output Feedback Mode
5- Counter Mode
6- International Engineering Task Force

هر بلوک از سایر بلوکها، حالت شمارنده‌ای می‌تواند به صورت موازی و لوله‌ای[1] نیز انجام شود. همانطور که در شکل(۲) ملاحظه می‌شود، در مد CTR فرایند رمزنگاری به توالی و دریافت خروجی یک بلوک به عنوان ورودی بلوک بعدی متکی نیست، که این امر باعث افزایش سرعت و کارایی الگوریتم می‌شود (CCSDS 353.0-R-1, 2008).



شکل(۲) نحوه اجرای مد شمارشی(CTR)

متناظر با هر کلید داده شده، مقدار اولیه‌ای برای این شمارنده انتخاب می‌شود، که البته مجموعه تصادفی از بیت‌ها می‌تواند برای مقدار دهی اولیه شمارندهٔ مورد نظر مورد استفاده قرار گیرند (FIPS-197, 2001).

احرازاصالت در ساختار CCSDS

احرازاصالت پیام در سامانه‌های نظامی و دفاعی برای جلوگیری از تهدیداتی نظیر جعل و یا انکار سرویس[2] بسیار حائز اهمیت است. الگوریتم‌های پیشنهادی احرازاصالت بر پایه

1- Parallel and Pipeline
1-Denial of Service

تکنولوژی امضای دیجیتال بنا شده است. حداقل دو روش کلی "امضای دیجیتال" و "کدهای احراز اصالت پیام (MAC)[1] " برای پیاده سازی سازوکارهای احراز اصالت و بررسی سندیت وجود دارد. در ادامه به معرفی این روش‌ها پرداخته می‌شود (CCSDS 350.3-G-1, 2008).

امضای دیجیتال

امضای دیجیتال نیازمند رمزنگاری کلید عمومی است و زوج کلید عمومی و خصوصی را بکار می‌برد. فرستنده پیام را با محاسبه خلاصه پیام[2] یا مقدار درهم‌ساز[3] و استفاده از کلید خصوصی خویش به صورت دیجیتال امضا و سپس ارسال می‌نماید. گیرنده با استفاده از کلید عمومی فرستنده، خلاصه پیام را کنترل می‌نماید و اگر این خلاصه پیام صحیح بود پیام از طرف فرستنده صحیح آمده است. سه نوع امضای دیجیتال توسط CCSDS مطرح شده که خصوصیات آنها در جدول (۳) آمده است، در میان این سه روش، روش‌های مبتنی بر خم بیضوی با توجه به طول کوتاه کلید مورد استفاده به مراتب پرکاربردتر و موثرتر از سایر روش‌ها است (CCSDS 350.3-G-1, 2008).

جدول (۳) الگوریتم‌های امضای دیجیتال

نام	نوع	حداقل طول‌کلید (بیت)
امضای دیجیتال استاندارد[4]	امضای دیجیتال مبتنی بر SHA1	۱۰۲۴
امضای دیجیتال مبتنی بر RSA	امضای دیجیتال RSA	۱۰۲۴
امضای دیجیتال مبتنی بر خم بیضوی[5]	امضای دیجیتال مبتنی بر خم بیضوی	۱۶۰

کدهای احرازاصالت پیام (MAC)

علاوه بر امضای دیجیتال برای احرازاصالت از روش دیگری به نام کدهای احرازاصالت پیام نیز استفاده می‌شود. برخلاف امضای دیجیتال MAC از کلید خصوصی اشترکی کمک

2- Message Authentication Code (MAC)
3-Check Sum
4- Hash
5-Digital Signature Standard
1- Elliptic Curve Digital Signature Algorithm (ECDSA)

می‌گیرد و می‌تواند صحّت و سندیت را از طرق مختلف تامین نماید. کدهای احرازاصالت بر دو اصل کلی درهم‌سازی و رمزنگاری استوار هستند (CCSDS 350.3-G-1, 2008)

کدهای احرازاصالت پیام مبتنی بر درهم‌سازی[1]

این کدها از انواع قویتری از الگوریتم‌های درهم‌ساز نظیرMD5، SHAها (در آینده SHA3)، برای تولید یک کلمه کنترل روی داده‌ها و کلید جاسازی شده استفاده می‌کنند. تعداد متنوعی از الگوریتم‌های HMAC وجود دارد که دقیقاً نحوه ترکیب داده و کلید را قبل از درهم‌سازی مشخص کرده‌اند. گیرنده با داشتن کلید خصوصی به کمک اعمال تابع درهم‌ساز مشابه روی داده و باز تولید کلمه کنترل، در صورت مشابه بودن کلمه کنترل تولید شده با کلمه کنترل دریافتی صحّت پیام را تایید می‌نماید. در فضای MAC مبتنی بر درهم‌سازی الگوریتم‌های بسیاری وجود دارد. برجسته‌ترین الگوریتم HMAC مدل استاندارد (RFC2104) IETFکه دارای استاندارد FIPS 198 است. الگوریتم HMAC می‌تواند از الگوریتم‌های درهم‌ساز MD5 یا انواع SHA ها استفاده نماید. علاوه بر این FIPS 198 می‌تواند از سایر الگوریتم‌های درهم‌ساز نظیر RIPEMD-160[2] و Tiger نیز بهره بگیرد. برخی از مشخصات این الگوریتم‌ها در جدول(۴) آمده است (CCSDS 350.3-G-1, 2008).

جدول(۴) کدهای سندیت پیام مبتنی بر درهم سازی

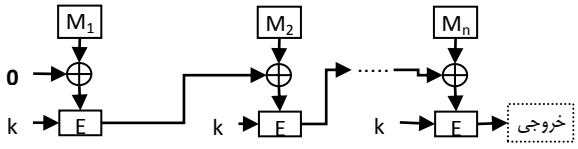
نام الگوریتم	نوع الگوریتم	ویژگیها و مشخصات	خروجی CCSDS (بیت)
SHA1	درهم‌ساز	نسخه‌های متفاوت با خروجی‌های طولانی‌تر SHA256, SHA384 و SHA512	۱۶۰
MD5	درهم‌ساز	از مجموعه SHA2 و در ۴ مرحله (رُند)	۱۲۸
UMAC[3]	MAC درهم‌سازی	طراحی شده بر اساس توابع درهم‌ساز سریعتری چون AES توصیه شده توسط IETF	۹۶ ،۶۴ ،۳۲
RIPEMD-160	درهم‌ساز	بر اساس ارتقای MD4 دارای خروجی‌های ۱۲۸،۲۵۶،۳۲۰ نیز است.	۱۶۰

2 - Hash Base Message Authentication Code (HMAC)
3- RACE Integrity Principals Evaluation Message Digest
1- Universal Message Authentication Code (UMAC)

TIGER	درهم‌ساز	کارایی بهتر در بسترهای ۶۴ بیتی، در ۲۴ رُند اجرا، از مجموعه SHA2 دارای خروجی‌های ۱۲۸،۱۶۰،۱۹۲ بیتی.	۱۹۲
HMAC-SHA1-96	MAC درهم‌سازی	از SHA1 برای درهم‌سازی استفاده و توسط پروتکل‌های IPSec و TLS پشتیبانی می‌شود.	۹۶
HMAC-MD5-96	MAC درهم‌سازی	از MD5 برای درهم‌سازی استفاده و توسط پروتکل‌های IPSec و TLS پشتیبانی می‌شود.	۹۶

کدهای سندیت پیام مبتنی بر رمزنگاری

پرکاربردترین MAC ها عموماً بر اساس ترکیب درهم‌سازی و رمزنگاری است (مد CBC). این نوع MAC یک کلمه کنترل روی داده با کمک الگوریتم درهم‌ساز ایجاد می‌نماید. سپس الگوریتم رمزنگاری از کلید خصوصی برای رمزکردن کلمه کنترل استفاده می‌کند. گیرنده با داشتن کلید خصوصی کلمه کنترل را مجدداً تولید و کلمه کنترل رسیده را رمزگشایی می‌کند. با مقایسه کلمه کنترل تولید شده و رمزگشایی شده، اصالت پیام تایید می‌شود. ساختار انجام این روش در شکل (۳) آمده است.



شکل (۳) ساختار مد CBC

در مد CCM از ترکیب زنجیره بلوک رمزی و مد CTR برای تولید MAC و ایجاد موجودیت مستقل داده که دارای MAC و رمز در کنار هم هستند، بهره می‌گیرند. مد CTR اعمال شده به MAC برای تغییر شکل ورودی طولانی به حالتی ناخوانا به نام متن رمزی است. بنابراین تولید رمزنگاری CCM ، با افزایش اندازه MAC باعث افزایش بازدهی می‌شود. در تایید رمزگشایی[1] حالت رمزگشایی شمارنده‌ای به متن رمزی اعمال می‌شود، تا MAC و متن متناظر آن باز تولید شود. تصدیق موفقیت آمیز با دسترسی به کلید باعث تضمین داده و تصدیق منبع آن می‌شود. مد CCM تنها روی الگوریتم‌های با طول کلید ۱۲۸ بیت یا بیشتر

1- Decryption Verification

کاربرد دارد و با الگوریتم 3DES که از کلیدهای ۶۴ بیتی بهره می‌گیرند سازگاری ندارند. در جدول(۵) مشخصات این کدها به اختصار بیان شده است (CCSDS 350.3-G-1, 2008).

جدول(۵) برخی ازکدهای احرازاصالت پیام براساس رمزنگاری

نام الگوریتم MAC	نوع	مشخصات و ویژگیها	خروجی CCSDS (بیت)
DES-CBC	MAC پنهانی	مبتنی بر الگوریتم DES	۶۴
CMAC	MAC پنهانی	بر اساس رمزنگاری رمزهای بلوکی متقارن	۶۴، ۱۲۸، ۱۹۲، ۲۵۶
CCM	MAC پنهانی	استفاده از CBC با مد CTR رمزنگاری برای پوشش هر دو حالت محرمانگی و احرازاصالت، استفاده از رمزبلوکی با طول کلید حداقل ۱۲۸ بیت	۱۲۸، ۱۹۲، ۲۵۶

ترکیب رمزنگاری و احراز اصالت

روش‌های زیادی از مد CTR برای ایجاد امنیت در هر دو حالت رمزنگاری و احراز اصالت منشعب شدند که به روش‌های رمزنگاری احرازهویت شده[1] (AEAD) مشهور شدند. حالت‌های AEAD شامل مد کتاب کد مبدا[2] (OCB)، شمارنده با CBC-MAC، EAX (که مخفف عبارتی هم نیست)، کارتروگمن به همراه شمارنده[3] (CWC) و مد شمارندهٔ متناهی (GCM)[4] است. مد GCM در شکل(۴) نمایش داده شده است که در آن CCM برای امنیت بیسیم در استاندارد IEEE 802.11i مطرح شده است. حالت‌های مختلف ارائه شده در AEAD به اختصار در جدول(۶) آمده است.

جدول(۶) حالتهای مختلف AEAD

ردیف	مد	ویژگی
۱	OCB	در IEEE 802.11i اختیاری است
۲	CCM	مد اجباری برای امنیت بیسیم در IEEE 802.11i
۳	EAX	جایگزین ساده برای CCM در استاندارد ANSI C12.22
۴	CWC	ترکیبی از مد شمارنده و چند جمله‌ای موثرِ کدِ احرازهویتِ پیامِ کارتروگمن
۵	GCM	براساس ارتقای مد CWC مطابق استاندارد IEEE802.1AE در امنیت اترنت و استاندارد پروتکل‌های IPSec در IETF و TLS/SSL بکار می‌رود.

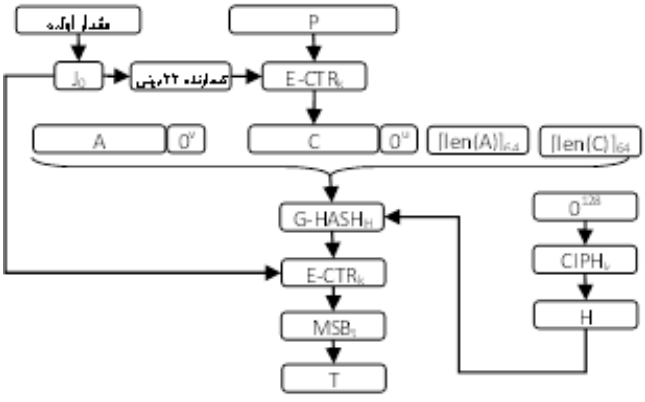
1-Authenticated Encryption with Associated Data (AEAD)
2- Offset Codebook(OCB)
3- Carter-Wegman + Counter (CWC)
4- Galois/Counter Mode

مد CWC از ضرب‌های ۱۲۸ بیتی استفاده می‌کند. مد GCM برخلاف اغلب حالت‌های AEAD، توانایی ایجاد رمزنگاری احرازاصالت شده با سرعت بسیار بالا را در پیاده‌سازی سخت‌افزاری به خوبی برنامه نرم‌افزاری دارد. همچنین می‌تواند موازی و لوله‌ای نیز اجرا شود (Viega and McGrew, RFC 4106, 2005: 5)، که این روش در ارتباطات سریع دورسنجی بسیار سودمند است. برخلاف مد CWC احرازهویت در GCM ها از ضرب در میدان باینری استفاده می‌کنند، که این امر باعث کارایی بسیار بالا در پیاده‌سازی آن‌ها می‌شود. پیشنهاد CCSDS برای رمزنگاری و احرازاصالت مبداء استفاده از مد GCM است (CCSDS 350.0-G-2, 2006).

البته همانطور که واضح است انتخاب الگوریتم مشابه برای رمزنگاری و احرازاصالت پیچیدگی‌های مربوط به پیاده‌سازی را به شدت کاهش می دهد، اما باید با در نظر گرفتن مفروضات امنیتی سامانه، الگوریتمی را انتخاب نمود که نفوذ به آن مشکل و حتی‌الامکان محال باشد. به همین دلیل می‌توان از الگوریتم‌های مطرح مبتنی بر خم بیضوی به دلیل محاسبات ساده و درعین حال امنیت بالای آن بهره گرفت.

مد GCM

این مد براساس ارتقای CWC طراحی و برای بررسی هر دو عامل رمزنگاری و احراز اصالت بکار می‌رود و بر اساس رمزنگاری متقارن و بلوکی کار می‌کند. مد GCM ترکیبی از مد شمارشی رمزنگاری و مد احرازهویت است. این روش بدلیل تولید موازی کلید بسیار سریعتر از مدهای زنجیره‌ای است (Viega and McGrew, RFC 4106, 2005: 5).



شکل(۴) تابع رمزنگاری احرازهویت شده GCM

در شکل(۴) نحوه فعالیت این مد مشاهده می‌شود. در این روش توسط چندجمله‌ای مولد $x^{128}+x^7+x^2+x+1$ عناصر میدان $GF(2^{128})$ تولید می‌شوند. تابع $E\text{-}CTR_k$ تابعی است که ورودی را با کلید k در مد CTR رمز می‌کند و تابع G-HASH بصورت $G\text{-}HASH(H,A,C)=X_{m+n+1}$ تعریف می‌شود که در آن H، تعداد ۱۲۸ بیت صفر رمزشده توسط رمز بلوکی است. A نیز داده‌ای است که فقط احرازهویت می‌شود (نه رمزنگاری) و C متن رمزی است. همچنین m و n به ترتیب تعداد بلوک‌های ۱۲۸ بیتی در A و C هستند (البته بلوک‌های نهایی A و C می‌توانند دقیقاً ۱۲۸ بیتی نباشند) و برای $i=0,\ldots,m+n+1$ متغیر x_i بصورت رابطهٔ (۱) تعریف می‌شود (CCSDS 350.3-G-1, 2008).

$$X_i = \begin{cases} 0 & i = 0 \\ (X_{i-1} \oplus A_i).H & i = 1,\ldots,m-1 \\ (X_{m-1} \oplus (A_m^* \parallel 0^{128-v})).H & i = m \\ (X_{i-1} \oplus C_{i-m}).H & i = m+1,\ldots,m+n+1 \\ (X_{m+n-1} \oplus (C_m^* \parallel 0^{128-u})).H & i = m+n \\ (X_{m+n} \oplus (len(A) \parallel len(c))).H & i = m+n+1 \end{cases} \quad (۱)$$

پیشنهاد انتخاب الگوریتم و لایهٔ رمزنگاری نظامی

همانطور که در بخش ۲ ذکر شد هنوز روش مدون و تضمین کننده‌ای برای انتخاب لایه و الگوریتم رمزنگاری مطرح نشده است، با توجه به طراحی لایه‌ای CCSDS و الگوریتم‌های استاندارد معرفی شدهٔ آن می‌توان بدون ایجاد مشکل در تاکیدات استاندارد امنیت را افزایش داد که در این بخش به ذکر چند پیشنهاد می‌پردازیم.

با وجود لایه‌های متفاوت در CCSDS و امکان استفاده از الگوریتم‌های رمزنگاری و احرازاصالت در هرلایه، می‌توان در هر کدام از آنها عملیات محرمانگی و احراز اصالت را انجام داد. البته باید توجه داشت که در سامانه‌های بلادرنگ[1] و برخط (نظیر سامانه‌های آفندی، پدافندی و کنترل موشک‌ها و تسلیحات در سازمان‌های نظامی و دفاعی) کند شدن سامانه و کاهش کارایی زمانی آن، می‌تواند مشکلاتی را فراهم آورد و حتی خساراتی را به سامانه وارد نماید. در این حالت بسته به نوع ماموریت و تحدیداتی نظیر تحلیل ترافیک، تشخیص نوع اطلاعات و نرم‌افزارهای دورسنج موجود، می‌توان با انتخاب چند لایه‌ی ساده و حتی

1- Real Time

تنها با انتخاب لایه فیزیکی، برای رمزنگاری و احرازهویت، نفوذگران و دشمن را تا زمان محقق شدن اهداف عملیاتی، ناامید نگه داشت. از آنجا که می‌دانیم طول کوتاه کلید در الگوریتم‌هایی نظیر AES و خم‌های بیضوی و وجود امنیت تضمین شده در آنها کار با این الگوریتم‌ها را ساده‌تر نموده است، می‌توان از آن‌ها به عنوان نقطهٔ اتکای این فرایند نام برد و امنیت سامانه را بیشتر نمود. البته می‌توان از ترکیب الگوریتم‌های رمز AES و خم‌های بیضوی و به صورت یک لایه در میان، یا انتخاب برخی لایه‌ها برای عملیات‌های متفاوت و همچنین تکنیک‌هایی نظیر شبکه‌های فیستلی تو در تو (ایدهٔ الگوریتم رمزنگاری SEED) و مد پیشنهادی GCM، امنیت رمز را چندین برابر نمود و ترکیبی از رمز متقارن و نامتقارن در لایه‌های متفاوت تولید، تا از سرعت زیاد الگوریتم‌های متقارن و امنیت بالای رمزهای نامتقارن همزمان بهره گرفت. البته در این حالت ممکن است انتخاب کلیدها و توزیع آنها ظاهراً مشکل به نظر برسد، برای رهایی از این چالش نیز می‌توان از ایده کلیدهای یکبار مصرف[1] (OTP) و مولدهای شبه تصادفی کمک گرفت، تا امنیت کلید نیز به سادگی هرچه بیشتر تضمین نمود.

نتیجه

در سازمان‌های نظامی و دفاعی با توجه به نوع ماموریت سامانه و نیازمندی‌های عملیاتی نظیر سرعت، دقت در محاسبات و تشخیص فرامین و همچنین وجود سامانه‌های هوشمندِ بلادرنگ و برخط ونیز انواع سرویس‌های ذخیره‌سازی و نیاز به امنیت مربوط به هرکدام از این سامانه‌ها، می‌توان از روش‌های ترکیبی مطرح شده بهره گرفت. در اینصورت می‌توان با تحلیل سربار ناشی از انجام الگوریتم‌های رمزنگاری و حساسیت‌های خاص عملیات هوافضایی بین سرعت انجام پردازش‌ها، محرمانگی و میزان امنیت مورد نیاز موازنه برقرار نمود.در مواردی حتی تحلیل ترافیک سامانه نیز به نگرانی‌های مربوطه می‌افزاید و نیاز به رمزنمودن اطلاعاتی چون سرایندهای هر ریزبسته نیز احساس می‌شود، این امر سبب کاهش احتمال نفوذ و خرابکاری در نقاط حساس و گلوگاه‌های سامانه می‌شود. در احرازاصالت و سندیت فرامین و سَنجه‌ها نیز می‌توان از روش‌های مطرح شده بهره گرفت و حتی علاوه بر لایهٔ کاربرد در ارتباطات بین لایه‌های CCSDS نیز از تکنولوژی‌های مربوطه کمک گرفت تا مواردی چون جعل، انکار و تکرار فرامین و سنجه‌ها از لایه‌ای به لایهٔ دیگر

1- One Time Pad

در تقویت‌کننده‌ها، مسیریاب‌ها و ایستگاه‌های فضایی یا زمینی اتفاق نیافتد. البته می‌توان با استفاده از الگوریتم‌های نظیر رمزهای اشتراکی و تشکیل گروه‌های متعدد با سطوح دسترسی متفاوت و تولید ساختارهای دسترسی به کلیدهای رمزنگاری باعث افزایش ضریب امنیت شد.

منابع

- The Application of CCSDS Protocols to Secure Systems. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.
- T. Dierks and E. Rescorla, April 2006, The Transport Layer Security (TLS) Protocol. RFC 4346.Version 1.1. Reston, Virginia: ISOC.
- Space Communications Protocol Specification (SCPS)—Security Protocol (SCPSSP). Recommendation for Space Data System Standards, CCSDS 713.5-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.
- S. Kent and K. Seo , December 2005,. Security Architecture for the Internet Protocol. RFC 4301. Reston, Virginia: ISOC, http://www.ietf.org/rfc/rfc4301.txt
- S. Kent, December 2005, IP Encapsulating Security Payload (ESP). RFC 4303. Reston, Virginia: ISOC.
- Overview of space communications Protocol. Report Concerning Space Data System Standards, CCSDS 130.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, December 2007.
- Encryption Algorithm Trade Survey. Draft Report Concerning Space Data System Standards, CCSDS 350.2-G-0. Draft Green Book. Issue 0. Washington, D.C.: CCSDS, July 2007.
- Advanced Encryption Standard (AES). Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001.
- Morris Dworkin. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. National Institute of Standards and Technology Special Publication 800-38A. Gaithersburg, Maryland: NIST, 2001.
- R. Housley. Using Advanced Encryption Standard (AES) Counter Mode with IPSec Encapsulating Security Payload (ESP). RFC 3686. Reston, Virginia: ISOC, January 2004.
- Symmetric Encryption. Draft Recommended Practice for Space Data System Standards, CCSDS 353.0-R-1. Red Book. Issue 1. Washington, D.C.: CCSDS, October 2008.
- Morris Dworkin. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007.

- J. Viega and D. McGrew. The Use of Galois/Counter Mode (GCM) in IPSec Encapsulating Security Payload (ESP). RFC 4106. Reston, Virginia: ISOC, June 2005. David A. McGrew and John Viega, "The Galois/Counter Mode of Operation (GCM)", page 5, 2005
- Authentication/Integrity Algorithm Issues Survey. Information Report for Space Data System Standards, CCSDS 350.3-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, March 2008.