به نام خداوند بخشنده مهربان

مبانی امنیت شبکه

Fundamentals of Network Security



یاشار ابری

دانشکده مهندسی، دانشگاه تهران

Yasharabri.ut.ac.ir@gmail.com

yasharabri@ut.ac.ir

مقدمه‌ای بر رمزنگاری احراز اصالت‌شده (AEAD)

- **مفهوم رمزنگاری احراز اصالت‌شده (Authenticated Encryption with Associated Data):** در رمزنگاری معمولی، هدف اصلی پنهان‌کردن محتوای پیام از دید افراد غیرمجاز است؛ اما این موضوع به‌تنهایی تضمین نمی‌کند که پیام در مسیر انتقال دستکاری نشده باشد. AEAD روشی است که علاوه بر محرمانگی، صحت و اصالت داده‌ها را نیز بررسی می‌کند.
- **مسئله اصلی در انتقال داده‌های رمزنگاری‌شده:** تصور کنید یک کاربر از طریق اینترنت دستور انتقال وجه به بانک ارسال می‌کند. حتی اگر مهاجم نتواند محتوای پیام را بخواند، ممکن است تلاش کند بخشی از اطلاعات رمزگذاری‌شده را تغییر دهد. بنابراین محرمانه‌بودن پیام لزوماً به معنای دستکاری‌نشدن آن نیست.
- **راه‌حل AEAD:** این روش هنگام رمزگذاری، علاوه بر تولید متن رمز (Ciphertext)، یک مقدار امنیتی به نام برچسب احراز اصالت (Authentication Tag) نیز تولید می‌کند. گیرنده با بررسی این برچسب می‌تواند تشخیص دهد که آیا اطلاعات از زمان ارسال تاکنون تغییر کرده‌اند یا خیر.

امام حسین علیه السلام:
عقل، جز با پیروی از حقّ، کامل نمی‌شود.
أعلام الدین، ص ۲۹۸

مقدمه‌ای بر رمزنگاری احراز اصالت‌شده (AEAD)

- **اهمیت AEAD در سامانه‌های امروزی:** الگوریتم‌هایی مانند AES-GCM و ChaCha۲۰-Poly۱۳۰۵ از روش‌های شناخته‌شده رمزنگاری احراز اصالت‌شده هستند و در پروتکل‌های ارتباطی امن مانند TLS ۱.۳ استفاده می‌شوند.

امام صادق علیه السلام:
کسی که برای دیگران
ارزشی قائل نباشد،
خودبین و خودرأی است.
معاني الأخبار: ج۲،
ص۲۴۴

چرا رمزگذاری ساده به‌تنهایی کافی نیست؟

- **رمزگذاری فقط محرمانگی را تضمین می‌کند:** هدف اصلی رمزگذاری این است که افراد فاقد کلید محرمانه نتوانند محتوای پیام را بخوانند. اما بعضی روش‌های رمزگذاری به مهاجم اجازه می‌دهند بدون دانستن کلید، بخش‌هایی از متن رمز را تغییر دهد.
- **امکان دستکاری بدون دانستن کلید:** در برخی شیوه‌های رمزگذاری، تغییر یک بیت از متن رمز می‌تواند باعث تغییر بیت متناظر در پیام رمزگشایی‌شده شود. بنابراین مهاجم ممکن است بتواند پیام را تغییر دهد، بدون آنکه از کلید محرمانه اطلاع داشته باشد.
- **نبود سازوکار تشخیص دستکاری:** اگر الگوریتم رمزگذاری فاقد سازوکار احراز اصالت باشد، گیرنده ممکن است نتواند تشخیص دهد که پیام دریافتی همان پیام اولیه است یا در مسیر انتقال تغییر کرده است.

امام صادق علیه السلام: نگاه کردن، تیری از تیرهای زهرآلود ابلیس است. هر که برای خداوند عز و جل و نه برای غیر او، چشم خود را فرو بندد خداوند در پی آن ایمانی به او ارزانی دارد که مزه‌اش را بچشد.
کتاب من لا یحضره الفقیه: ج۴ ، ص۱۸ ، ح۴۹۶۹

چرا رمزگذاری ساده به‌تنهایی کافی نیست؟

- **تفاوت محرمانگی و جامعیت:** محرمانگی (Confidentiality) یعنی افراد غیرمجاز نتوانند محتوای پیام را بخوانند؛ جامعیت (Integrity) یعنی گیرنده بتواند از تغییرنکردن داده‌ها اطمینان حاصل کند. این دو ویژگی مکمل یکدیگر هستند و برای ارتباطات امن به هر دو نیاز داریم.

پیامبر خدا صلی الله علیه و آله:
ای علی! چهار چیز را پیش از چهار چیز دریاب: جوانی‌ات را پیش از پیری؛ وسلامتی‌ات را پیش از بیماری؛ و ثروتت را پیش از فقر و زندگی‌ات را پیش از مرگ.
الفقیه: ج ۴ ، ص ۳۵۷ ، ح۵۷۶۲

مهاجم چگونه می‌تواند متن رمز را دستکاری کند؟

- **سناریوی مثال:** فرض کنید علی از شرکت خود درخواست می‌کند مبلغ ۱۰۰ هزار تومان از حسابش برداشت شود. شرکت برای محافظت از اطلاعات، پیام علی را رمزگذاری می‌کند تا افراد غیرمجاز نتوانند محتوای آن را مشاهده کنند.
- **ارسال پیام رمزگذاری‌شده:** فرض کنیم پیام اصلی علی عدد ۱۰۰ باشد و برای سادگی از یک روش رمزگذاری پیمانه‌ای برای درک آموزشی استفاده کنیم که در آن کلید محرمانه برابر ۳۷ است. رابطه رمزگذاری به شکل زیر خواهد بود:

$$C = (P + K) \bmod ۲۵۶$$

$$P = ۱۰۰$$

$$K = ۳۷$$

$$C = (۱۰۰ + ۳۷) \bmod ۲۵۶$$

$$C = ۱۳۷$$

- بنابراین متن رمز ارسالی برابر ۱۳۷ خواهد بود.

امیرالمومنین علی علیه السلام:
خدا را، خدا را درباره نماز، که بهترین کردار و ستون دین شماست!
گزیده تحف العقول، ح۶۵

مهاجم چگونه می‌تواند متن رمز را دستکاری کند؟

- **دستکاری توسط مهاجم:** مهاجم در مسیر انتقال پیام، متن رمز ۱۳۷ را مشاهده می‌کند. او بدون دانستن کلید محرمانه، مقدار آن را به ۱۴۷ تغییر می‌دهد. هدف مهاجم این است که مبلغ درخواست علی را از ۱۰۰ هزار تومان به ۱۱۰ هزار تومان تغییر دهد.
- **رمزگشایی در شرکت:** شرکت متن رمز دستکاری‌شده را با کلید محرمانه خودش رمزگشایی می‌کند. اگر فقط از رمزگذاری ساده استفاده شده باشد، نتیجه به شکل زیر خواهد بود:

$$P = (C - K) \bmod ۲۵۶$$

$$P = (۱۴۷ - ۳۷) \bmod ۲۵۶$$

$$P = ۱۱۰$$

پیامبر اعظم صلی الله علیه و آله : هرکه همسری اختیار کند، باید او را گرامی بدارد.

مستدرک الوسائل: ج ۱، ص ۴۱۲

مهاجم چگونه می‌تواند متن رمز را دستکاری کند؟

- **نتیجه حمله:** شرکت به‌جای دریافت درخواست برداشت ۱۰۰ هزار تومانی، مقدار ۱۱۰ را دریافت می‌کند؛ درحالی‌که علی هرگز چنین درخواستی ارسال نکرده است. این مثال نشان می‌دهد که رمزگذاری ساده، به‌تنهایی مانع دستکاری اطلاعات نمی‌شود.
- **توجه:** این یک مدل آموزشی ساده برای نمایش آسیب‌پذیری رمزگذاری بدون احراز اصالت است، نه روش رمزگذاری مورد استفاده در سامانه‌های واقعی.

پیامبر خدا صلی الله علیه و آله:
خداوند کار خیری را که به آن شتاب شود دوست دارد.
کافی: ج۲، ص۱۴۲، ح۴

برچسب احراز اصالت چگونه از دستکاری جلوگیری می‌کند؟

- **تولید برچسب توسط فرستنده:** در AEAD، هنگام رمزگذاری پیام علی، علاوه بر تولید متن رمز، یک برچسب احراز اصالت نیز محاسبه می‌شود. برای ادامه مثال، فرض می‌کنیم کلید محرمانه برابر ۳۷ و متن رمز برابر ۱۳۷ است.
- **فرمول آموزشی تولید برچسب:** برای ساده‌سازی، فرض می‌کنیم برچسب با فرمول زیر تولید می‌شود:

$$T = (K \times C) \bmod ۱۰۱$$

$$T = (۳۷ \times ۱۳۷) \bmod ۱۰۱$$

$$T = ۵۰۶۹ \bmod ۱۰۱$$

$$T = ۱۹$$

- **اطلاعات ارسالی علی:** بنابراین شرکت دو مقدار دریافت خواهد کرد: متن رمز برابر ۱۳۷ و برچسب احراز اصالت برابر ۱۹. این برچسب به‌عنوان یک مهر امنیتی برای بررسی صحت اطلاعات استفاده می‌شود.

امام صادق علیه السلام فرمود:
کسی‌که بر این امر بمیرد و منتظر امام (مهدی) علیه‌السلام باشد همانند کسی‌است‌که در خیمه امام قائم علیه‌السلام باشد.
بحارالأنوار، ج۵۲، ص ۱۲۵
.

برچسب احراز اصالت چگونه از دستکاری جلوگیری می‌کند؟

اطلاعات ارسالی	مقدار
متن رمز (Ciphertext)	137
برچسب (Tag)	19

- **اهمیت کلید محرمانه:** برچسب با استفاده از کلید محرمانه تولید می‌شود. مهاجم می‌تواند مقدار متن رمز یا حتی مقدار برچسب را تغییر دهد، اما بدون دانستن کلید نمی‌تواند به‌سادگی برچسب معتبر جدیدی تولید کند.

امام صادق علیه السلام فرمود:
کسی که در انتظار امام دوازدهم علیه السلام است، همانند کسی است که در رکاب رسول خدا صلی الله علیه و آله شمشیرش را برهنه کرده و از او دفاع می کند.
بحارالأنوار، ج۵۲، ص ۱۲۹
.

مهاجم متن رمز را تغییر می‌دهد؛ شرکت چگونه متوجه می‌شود؟

- **دستکاری متن رمز:** مهاجم که می‌خواهد مبلغ درخواست علی را تغییر دهد، مقدار متن رمز را از ۱۳۷ به ۱۴۷ تغییر می‌دهد. اما چون کلید محرمانه را ندارد، برچسب قبلی یعنی ۱۹ را بدون تغییر باقی می‌گذارد.
- **دریافت پیام در شرکت:** شرکت متن رمز دستکاری‌شده ۱۴۷ و برچسب همراه آن ۱۹ را دریافت می‌کند. اکنون شرکت با استفاده از کلید محرمانه خود، برچسب مورد انتظار را برای متن رمز دریافتی محاسبه می‌کند.

امام حسن عسکری علیه السلام:
بهترین برادر تو کسی است که خطایت را فراموش کند و احسان تو را به خود، به یاد آورد.
بحار الأنوار: ج ۷۸ ، ص ۳۷۹

مهاجم متن رمز را تغییر می‌دهد؛ شرکت چگونه متوجه می‌شود؟

- **محاسبه برچسب جدید:** شرکت از همان فرمول آموزشی استفاده می‌کند:

$$T = (K \times C) \bmod ۱۰۱$$

$$T = (۳۷ \times ۱۴۷) \bmod ۱۰۱$$

$$T = ۵۴۳۹ \bmod ۱۰۱$$

$$T = ۸۶$$

- **مقایسه برچسب‌ها:** شرکت متوجه می‌شود برچسب دریافتی ۱۹ است، اما برچسب محاسبه‌شده ۸۶ است. از آنجا که این دو مقدار برابر نیستند، مشخص می‌شود که اطلاعات در مسیر انتقال دستکاری شده‌اند.

پیامبر خدا صلی الله علیه و آله:
رمضان، رمضان نامیده شد؛ زیرا گناهان را می‌سوزاند.
میزان الحکمه، ح ۷۴۴۱

مهاجم متن رمز را تغییر می‌دهد؛ شرکت چگونه متوجه می‌شود؟

نوع برچسب	مقدار
برچسب همراه پیام دریافتی	19
برچسب محاسبه‌شده توسط شرکت	86
نتیجه مقایسه	عدم تطابق

- **پس پیام نامعتبر است و رد می‌شود.**
- **نتیجه امنیتی:** شرکت متوجه می‌شود که پیام دریافتی با پیام اولیه علی مطابقت ندارد؛ بنابراین نباید درخواست برداشت را اجرا کند. در AEAD واقعی نیز در صورت شکست اعتبارسنجی، متن رمزگشایی‌شده نباید به برنامه تحویل داده شود.

امام صادق علیه السلام:
هر که جویای ریاست باشد، نابود شود.
الکافي : ۲/۲۹۷/۲

اگر مهاجم برچسب را هم تغییر دهد چه اتفاقی می‌افتد؟

- **تغییر دادن برچسب نیز امکان‌پذیر است:** مهاجم می‌تواند علاوه بر تغییر متن رمز از ۱۳۷ به ۱۴۷، مقدار برچسب را نیز از ۱۹ به ۸۶ تغییر دهد. بنابراین نمی‌توان گفت مهاجم قادر به تغییر برچسب نیست؛ مسئله اصلی این است که آیا می‌تواند مقدار صحیح و معتبر آن را تولید کند یا خیر.
- **تفاوت تغییر مقدار با تولید برچسب معتبر:** مهاجم ممکن است به‌صورت تصادفی عدد ۸۶ را جایگزین برچسب قبلی کند، اما برای تولید برچسب صحیح باید از کلید محرمانه ۳۷ و تابع احراز اصالت اطلاع داشته باشد. در الگوریتم‌های واقعی، این کار بدون کلید از نظر محاسباتی بسیار دشوار است.

امام علی علیه السلام:
ارزش مرد، به اندازه همّت اوست.
نهج البلاغه، حکمت ۴۷

اگر مهاجم برچسب را هم تغییر دهد چه اتفاقی می‌افتد؟

- **احتمال حدس تصادفی برچسب در AES-GCM:** اگر AES-GCM با برچسب کامل ۱۲۸ بیتی استفاده شود، احتمال موفقیت یک حدس تصادفی مستقل برای تولید برچسب معتبر، در یک تلاش، برابر است با:

$$P = \frac{1}{2^{128}}$$

- یعنی تقریباً یک شانس در:

۳۴۰,۲۸۲,۳۶۶,۹۲۰,۹۳۸,۴۶۳,۴۶۳,۳۷۴,۶۰۷,۴۳۱,۷۶۸,۲۱۱,۴۵۶

امام عسکری علیه السلام: مبادا روزی تضمین شده (که در هرحال به تو می‌رسد) تو را از کار واجب باز دارد.

تحف العقول، ص۴۸۹

اگر مهاجم برچسب را هم تغییر دهد چه اتفاقی می‌افتد؟

- **نتیجه برای شرکت:** اگر مهاجم هر دو مقدار متن رمز و برچسب را تغییر دهد، شرکت برچسب را مجدداً محاسبه و با برچسب دریافتی مقایسه می‌کند. تنها در صورتی پیام را می‌پذیرد که اعتبارسنجی موفق باشد. در غیر این صورت، درخواست علی رد می‌شود.
- **توجه علمی:** احتمال بالا مربوط به حدس تصادفی یک برچسب ۱۲۸ بیتی کامل در یک تلاش، تحت فرض امنیت الگوریتم و رعایت صحیح الزامات آن است. در عمل، تعداد تلاش‌ها، محدودیت نرخ درخواست و استفاده صحیح از نانس نیز اهمیت دارند.

امام کاظم علیه السلام:
هرگاه خواستی از خداوند حاجتی طلب کنی، بگو: خدایا! به حقّ محمّد و علی از تو مسألت می‌کنم؛ زیرا که آن دو را نزد تو منزلتی است.
الدعوات: ص۱۲۷ ، ح۵۱

مقایسه نهایی سناریوی علی در رمزگذاری ساده و AEAD

مرحله	رمزگذاری ساده	AEAD
پیام اولیه علی	100	100
کلید محرمانه	37	37
متن رمز اولیه	137	137
برچسب اولیه	ندارد	19 در مثال آموزشی
متن رمز دستکاری‌شده	147	147
مقدار حاصل از رمزگشایی	110	به برنامه تحویل داده نمی‌شود
نتیجه	احتمال پذیرش پیام تغییریافته	رد پیام به دلیل عدم تطابق برچسب

پیامبر خدا صلی الله علیه و آله:
به یقین خداوند با خشم فاطمه به خشم می‌آید و با خشنودی او خشنود می‌شود.
بحار الأنوار: ج ۴۳ ، ص ۳۲۰

مقایسه نهایی سناریوی علی در رمزگذاری ساده و AEAD

- **نتیجه‌گیری:** در رمزگذاری ساده، مهاجم می‌تواند با دستکاری متن رمز، نتیجه رمزگشایی را تغییر دهد، بدون آنکه لزوماً شناسایی شود. اما در AEAD، برچسب احراز اصالت به شرکت اجازه می‌دهد تغییرات را تشخیص دهد و از اجرای درخواست دستکاری‌شده جلوگیری کند.

امام جواد علیه السلام:
اینگونه مباش که در ظاهر با خدا دوستی کنی و در پنهانی دشمنی!
بحار الانوار: ج۷۸ ، ص۳۶۵

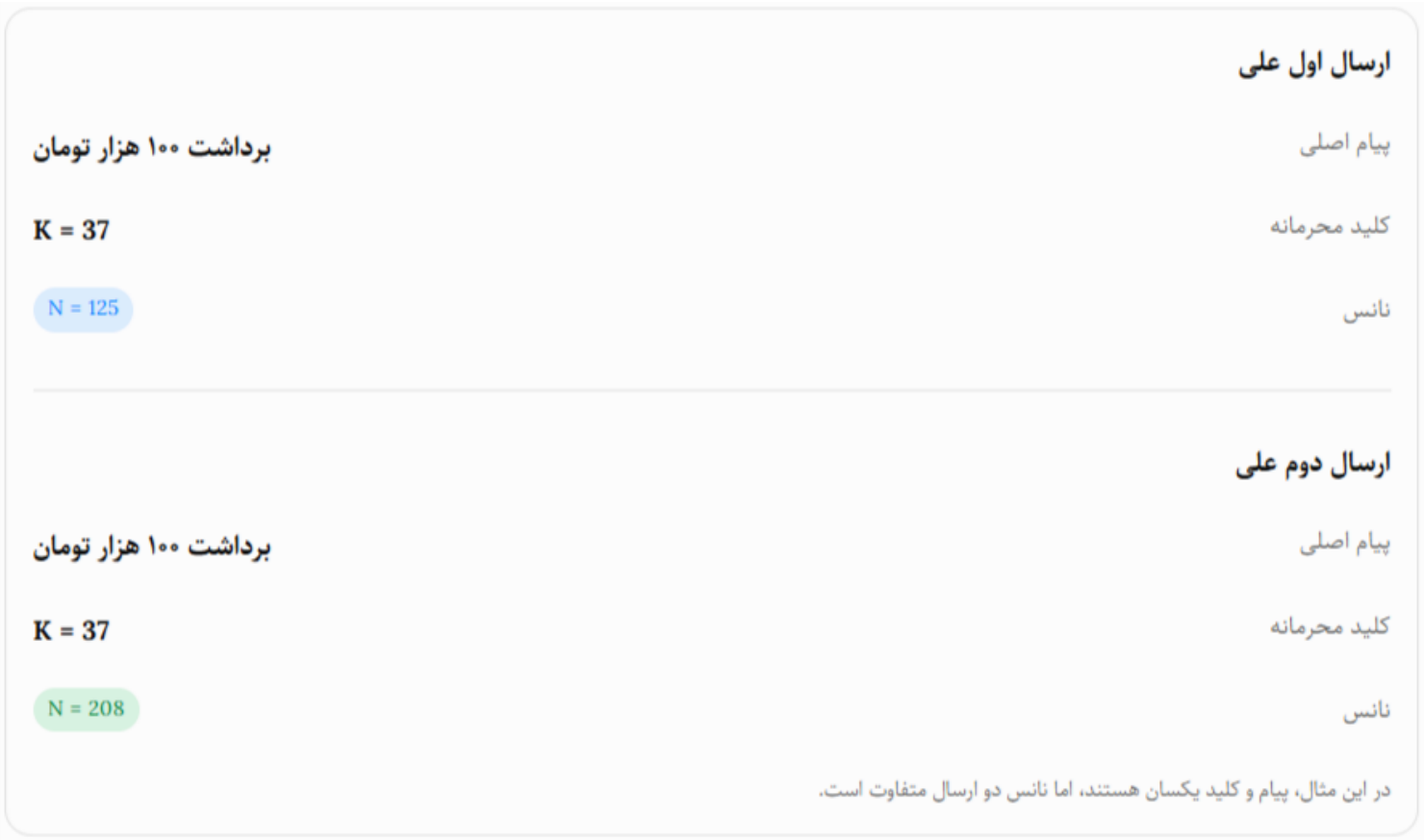
نانس

- نانس (Nonce) مخفف عبارت Number Used Once است؛ یعنی «عددی که فقط یک‌بار استفاده می‌شود».
- در رمزنگاری، نانس یک مقدار ورودی است که همراه با کلید محرمانه در فرایند رمزگذاری استفاده می‌شود تا امنیت ارتباط افزایش یابد. نانس معمولاً محرمانه نیست و می‌تواند همراه پیام برای گیرنده ارسال شود؛ اما نحوه استفاده از آن بسیار مهم است.

امام حسن عسکری علیه السلام:
هرکه زیاد بخوابد، خواب‌های پریشان بیند.
منتخب میزان الحکمه، ص۵۷۴

نانس چه نقشی در مثال علی دارد؟

- فرض کنید علی می‌خواهد از شرکت خود درخواست برداشت ۱۰۰ هزار تومان کند.شرکت و علی یک کلید محرمانه مشترک دارند؛ اما علاوه بر کلید، برای هر پیام یک نانس جدید نیز استفاده می‌شود.مثلاً:



امام زین‌العابدین علیه السلام فرمود:

کسی که در زمان غیبت قائم ما بر ولایت ما استوار باشد، خداوند پاداش هزار شهید از شهدای جنگ بدر و احد را به او خواهد داد.

بحارالأنوار، ج ۵۲، ص ۱۲۵

نانس چه نقشی در مثال علی دارد؟

- **چرا نانس را تغییر می‌دهیم؟** زیرا اگر یک پیام با یک کلید ثابت چندین بار رمزگذاری شود، استفاده تکراری از نانس در الگوریتم‌هایی مانند AES-GCM می‌تواند امنیت را به‌شدت به خطر بیندازد.

امیرالمومنین علی علیه السلام :

نابینایی، آسان‌تر و قابل تحمل‌تر از نداشتن بینش و بصیرت است.

غررالحکم: ج۴، ص۴۱۳

نانس چگونه امنیت را افزایش می‌دهد؟

- برای درک بهتر، فرض کنید علی دو بار دقیقاً یک درخواست یکسان ارسال کند.
- اگر از یک کلید و نانس تکراری استفاده شود، در AES-GCMمتن رمز و برچسب یکسانی برای پیام و داده‌های یکسان تولید می‌شوند.
- اما اگر نانس تغییر کند، خروجی رمزگذاری نیز تغییر خواهد کرد.
- بنابراین نانس کمک می‌کند رمزگذاری مجدد پیام‌های یکسان با یک کلید، خروجی‌های متفاوتی داشته باشد.
- **پس همانطور که از اسم نانس مشخص است نباید تکراری باشد و برای هر درخواست یا تراکنش یا پیام منحصر به فرد باشد.**

امام صادق علیه السلام :
خوشبخت، کسی است
که برای نفس خود خلوت
و فراغتی یابد و به کار
اصلاح آن پردازد.
بحار الأنوار: ج۷۸،
ص۲۰۳، ح۳۵

چرا استفاده مجدد از نانس خطرناک است؟

- این قسمت بسیار مهم است.
- در AES-GCM، اگر یک نانس با یک کلید دوباره استفاده شود، ممکن است اطلاعات امنیتی مهمی افشا شود.
- به‌طور خاص:
  - امکان افشای رابطه میان متن‌های اصلی و متن‌های رمز وجود دارد.
  - امنیت برچسب‌های احراز اصالت ممکن است تضعیف شود.
  - مهاجم ممکن است بتواند حملات جعل پیام را انجام دهد.
  - بنابراین در AES-GCM، استفاده مجدد از نانس با یک کلید یکسان ممنوع است.
- **نکته:** نانس لزوماً نباید تصادفی باشد؛ می‌تواند شمارنده‌ای باشد که برای هر پیام افزایش می‌یابد. مهم این است که تحت یک کلید مشخص، تکرار نشود و سایر الزامات الگوریتم رعایت شوند.

حضرت علی علیه السلام:
خداوند انسانی بهتر از
محمّد صلی الله
علیه و آله نیافریده است.
الکافي: ج۱، ص۴۴۰، ح۲

رمزنگاری برای دستگاه‌های کوچک؛ آشنایی با Ascon

- **یک چالش واقعی:** اینترنت اشیا فقط موبایل و لپ‌تاپ نیست. حسگرهای هوشمند، کارت‌های RFID، تجهیزات پزشکی کاشتنی و گجت‌های کوچک هم اطلاعات حساس ارسال می‌کنند؛ اما پردازنده، حافظه و باتری محدودی دارند. اجرای الگوریتم‌های سنگین‌تر ممکن است برای این دستگاه‌ها پرهزینه باشد.
- **خبر علمی جدید:** استاندارد شدن Ascon در سال ۲۰۲۵. مؤسسه ملی استاندارد و فناوری آمریکا (NIST) در ۱۳ اوت ۲۰۲۵ استاندارد ۲۳۲-۸۰۰SP را منتشر کرد که خانواده Ascon را برای رمزنگاری سبک در دستگاه‌های محدود معرفی می‌کند.
- **Ascon-AEAD۱۲۸:** خویشاوند سبک‌تر از خانواده AEAD. این الگوریتم مانند AES-GCM هم‌زمان محرمانگی و اصالت داده را فراهم می‌کند؛ یعنی هم اطلاعات را رمز می‌کند و هم امکان تشخیص دستکاری را می‌دهد.

امام صادق علیه السلام:
فرزندان خود را احترام کنید و آنها را خوب تربیت کنید تا خداوند شما را بیامرزد.
بحار الأنوار: ج ۱۰۴، ص۹۵

رمزنگاری برای دستگاه‌های کوچک؛ آشنایی با Ascon

- **چرا جالب است؟** تصور کنید یک حسگر کوچک روی بدن بیمار، اطلاعات پزشکی را با باتری محدود ارسال می‌کند. چنین دستگاهی هم به امنیت نیاز دارد و هم باید در مصرف انرژی صرفه‌جویی کند؛ رمزنگاری سبک برای همین موقعیت‌ها طراحی شده است.
- **نکته مهم:** Ascon قرار نیست همیشه جای AES-GCM را بگیرد. انتخاب الگوریتم به سخت‌افزار، نیازهای امنیتی و پیاده‌سازی بستگی دارد. AES-GCM همچنان گزینه‌ای مهم و پرکاربرد است؛ Ascon گزینه‌ای استانداردشده برای محیط‌های محدودتر محسوب می‌شود.
- **منبع:** استاندارد رسمی NIST، سند SP۸۰۰-۲۳۲، منتشرشده در اوت ۲۰۲۵.

امیرالمومنین علی علیه السلام:
کم‌گویی، عیب‌ها را می‌پوشاند و از گناهان می‌کاهد.
شرح غررالحکم: ج ۴، ص ۵۰۵

یک اشتباه کوچک با پیامد بزرگ؛ وقتی نانس تکرار می‌شود!

- **قانون طلایی AES-GCM:** نانس برای هر رمزگذاری باید یکتا باشد. اگر با یک کلید ثابت، دو پیام متفاوت را با یک نانس یکسان رمزگذاری کنیم، ممکن است محرمانگی هر دو پیام آسیب ببیند و حتی سازوکار تشخیص دستکاری نیز تضعیف شود.
- **چرا این اتفاق عجیب است؟** چون ممکن است همه‌چیز ظاهراً درست باشد: کلید محرمانه است، AES قوی است و برچسب احراز اصالت هم تولید شده؛ اما فقط تکرار یک نانس می‌تواند امنیت کلید را به خطر بیندازد.
- **یک تشبیه ساده:** استفاده دوباره از قالب یکسان. فرض کنید دستگاه برای دو پیام متفاوت، با همان کلید و همان نانس، عملاً از جریان رمز یکسانی استفاده کند. در حالت CTR که پایه رمزگذاری GCM است، رابطه‌ای میان متن‌های اصلی و متن‌های رمزشده ایجاد می‌شود که می‌تواند اطلاعاتی درباره پیام‌ها افشا کند.

امیرالمومنین علی علیه السلام فرمود:
منتظر فرج باشید، و از روح خدا مأیوس نشوید، که محبوب‌ترین اعمال در پیشگاه خدا انتظار فرج است.
بحارالأنوار، ج۵۱، ص ۱۲۳

یک اشتباه کوچک با پیامد بزرگ؛ وقتی نانس تکرار می‌شود!

- **راه پیشگیری:** نانس منحصر به فرد و یکتا، نه الزاماً تصادفی. می‌توان از شمارنده یا شماره توالی استفاده کرد؛ نکته اصلی این است که تحت یک کلید مشخص، نانس تکرار نشود. در سیستم‌های چنددستگاهی نیز باید مراقب بود دو دستگاه نانس یکسان تولید نکنند.
- **یک راهکار جالب در طراحی الگوریتم‌ها:** AES-GCM-SIV. این الگوریتم برای کاهش آسیب ناشی از استفاده ناخواسته مجدد از نانس طراحی شده است. البته این ویژگی به معنی بی‌خطر بودن تکرار نانس یا بی‌نیازی از رعایت دستورالعمل‌ها نیست.
- **پیام نهایی:** الگوریتم قوی، پیاده‌سازی درست می‌خواهد. امنیت فقط به انتخاب AES وابسته نیست؛ مدیریت کلید، یکتایی نانس و نحوه استفاده از الگوریتم هم به همان اندازه مهم‌اند.
- **منابع:** ۵۱۱۶RFC درباره پیامدهای تکرار نانس در GCM؛ ۹۷۷۱RFC درباره ویژگی‌های الگوریتم‌های AEAD و مقاومت در برابر سوءاستفاده از نانس.

امیرالمومنین علی علیه السلام: بخیل‌ترین مردم کسی است که مال خویش را از خود دریغ دارد و برای وارثانش بگذارد.
غرر الحکم، ح۳۲۵۳

حضرت علی علیه السلام:

آنچه برای خود نمی‌پسندی، برای دیگران هم نپسند.

وَ اکرَه لَهُ ما تَکرَهُ لِنَفسِک

نامه ۳۱ نهج البلاغه

(نامه امیرالمومنین علی علیه السلام به امام حسن علیه السلام)



دانشگاه تهران
دانشکده مهندسی کامپیوتر

با تشکر از حسن توجه شما