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

۶ تولید اعداد شبه‌تصادفی و رمزهای دنباله‌ای

- سرفصل‌های این بخش:
  - چرا تصادفی‌بودن واقعی برای رمزنگاری حیاتی است
  - افول RC۴ و علت آن
  - به‌روزرسانی: ChaCha-۲۰-Poly۱۳۰۵

اصول تولید اعداد تصادفی و شبه‌تصادفی

- **تصادفی واقعی در برابر شبه‌تصادفی:** اعداد تصادفی واقعی از پدیده‌های فیزیکی (نویز حرارتی، زمان‌بندی کلیک ماوس) به‌دست می‌آیند؛ اعداد شبه‌تصادفی توسط یک الگوریتم قطعی از یک مقدار اولیه (seed) تولید می‌شوند و اگر seed لو برود، کل دنباله قابل پیش‌بینی است.
- **چرا کیفیت آماری کافی نیست:** برای رمزنگاری، دنباله باید علاوه بر گذر از آزمون‌های آماری، از نظر رمزنگاری غیرقابل‌پیش‌بینی نیز باشد (CSPRNG)؛ یعنی حتی با دیدن بخشی از خروجی نتوان بیت بعدی را حدس زد.
- **درس عبرت: درِ پشتی Dual EC DRBG:** این مولد اعداد شبه‌تصادفی که NIST در دهه ۲۰۰۰ استاندارد کرده بود، بعدها مشخص شد دارای یک ضعف ریاضی است که به یک نهاد خاص امکان پیش‌بینی خروجی را می‌داد؛ این ماجرا اهمیت شفافیت در طراحی PRNG را نشان داد.

حضرت امام حسن بن علی مجتبی علیه‌السلام: هیچ قومی را بدرفتارتر از شما به یاد ندارم. پیکر رسول خدا صلی‌الله‌علیه‌وآله را در مقابل ما رها کردید و امر خلافت را میان خودتان تقسیم کردید.

الاحتجاج، جلد یک، صفحه ۲۰۲

رمزهای دنباله‌ای: از RC۴ تا ChaCha۲۰

- **منطق رمز دنباله‌ای:** به‌جای رمزکردن یک بلوک کامل، یک دنباله کلید شبه‌تصادفی تولید و با متن ساده بایت به بایت XOR می‌شود؛ سرعت بالا و سادگی پیاده‌سازی، مزیت اصلی آن است.
- **RC۴ و علت افول آن:** RC۴ که توسط ران ریوست طراحی شد به دلیل سادگی و سرعت در WEP و TLS اولیه محبوب بود، اما پژوهشگران سوگیری‌های آماری در خروجی اولیه آن یافتند که امکان بازیابی اطلاعات را فراهم می‌کرد؛ به همین دلیل مرورگرهای اصلی طی سال‌های ۲۰۱۵ تا ۲۰۱۶ پشتیبانی از RC۴ را به‌طور کامل حذف کردند.
- **جایگزین مدرن: ChaCha۲۰-Poly۱۳۰۵:** دنیل برنشتاین ChaCha۲۰ را با ساختاری متفاوت (بر پایه توابع جمع، چرخش و XOR) طراحی کرد که هم در نرم‌افزار سریع‌تر از AES بدون شتاب‌دهنده سخت‌افزاری است و هم تحلیل رمز قوی‌تری دارد؛ این الگوریتم همراه با Poly۱۳۰۵ (برای احراز اصالت) امروزه در TLS ۱.۳ و در اکثر برنامه‌های موبایل و پروتکل‌های پیام‌رسان امن استفاده می‌شود.

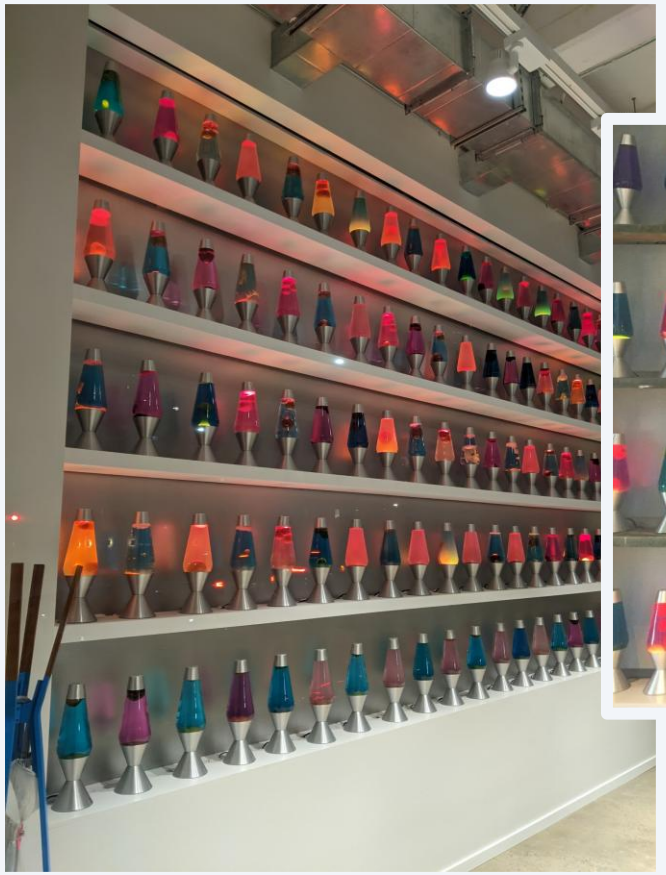
حضرت امام حسن بن علی عسکری علیه‌السلام: چقدر زشت است که انسان مؤمن دلبستگی و خواسته‌ای داشته باشد که او را به خاری بکشد. تحف العقول، صفحه ۴۸۹.

استفاده از نویز فیزیکی در تولید اعداد تصادفی واقعی

- **مفهوم:** استفاده از پدیده‌های فیزیکی غیرقابل‌پیش‌بینی (مانند نوسانات نوری و تغییرات دما در لامپ‌های گدازه‌ای) برای تولید بذر (Seed) جهت تولید اعداد تصادفی واقعی؛ این روش برخلاف الگوریتم‌های ریاضی، فاقد هرگونه الگوی قابل پیش‌بینی است.
- **ارتباط با امنیت دیجیتال:** برای جلوگیری از آسیب‌پذیری‌هایی مشابه با Dual EC DRBG، سیستم‌های امنیتی به جای اتکا صرف بر الگوریتم‌های شبه‌تصادفی (PRNG)، از منابع آنتروپی فیزیکی (Physical Entropy) استفاده می‌کنند تا حتی با داشتن مدل ریاضی، پیش‌بینی خروجی‌های بعدی غیرممکن باشد.
- **نکته کلیدی:** در این رویکرد، حتی ورودی‌های ساده یا تصاویر یکدست نیز با ترکیب با نویزهای محیطی، باعث افزایش آنتروپی و تقویت امنیت کلیدهای رمزنگاری می‌شوند.

حضرت خاتم الأنبیا محمد مصطفی صلی الله علیه و آله و سلم: ایستادگی و استواری دین اسلام تنها به شمشیر علی بن ابی طالب علیه السلام و ثروت خدیجه کبری سلام الله علیها بود. شجره طوبی، جلد ۲، صفحه ۲۳۳

دیوار لامپ گدازه‌ای Cloudflare، استفاده از تصاویر برای امنیت دیجیتال





حضرت امام جعفر بن محمد صادق علیه‌السلام: چهار چیز است که اندک آن هم بسیار است: آتش، دشمنی، فقر و بیماری.

اعیان الشیعه، جلد ۱، صفحه ۶۷۴

دیوار لامپ گدازه‌ای Cloudflare، استفاده از تصاویر برای امنیت دیجیتال

- این تصویر نمایانگر دیوار لامپ‌های گدازه‌ای شرکت کلودفلر است که به منظور تولید داده‌های تصادفی برای رمزنگاری امن به کار گرفته شده است.
- عبور افراد نیز به تولید تصاویر تصادفی کمک می‌کند و الگوریتم داخل سرور تصادفی‌تر می‌کند حتی اگر تصاویر تمام سیاه باشد.
- نکته قابل توجه آن است که در حوزه امنیت دیجیتال، حتی عناصری که به ظاهر ارتباطی با این زمینه ندارند، نظیر تصاویر لامپ‌های گدازه‌ای، می‌توانند به عنوان ابزاری خلاقانه و مؤثر در تقویت حفاظت از داده‌ها ایفای نقش نمایند.

حضرت رسول الله، خاتم الانبیا، محمد مصطفی (صلی الله علیه و آله و سلم):
«مومن حقیقی کسی است که فقیر را در مال خود شریک گرداند و با مردم به انصاف رفتار کند.»
اصول کافی، جلد ۲، صفحه ۱۴۷