امنیت شبکه

محمدمهدی فرح بخش

۱۸ خرداد ۱۴۰۳

به نام خداوند بخشنده مهربان

۱.۰ فصل ۶: کد های تصدیق صحت پیام

- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- عملکرد ها برای تصدیق صحت پیام:
  - یک تابع تولید کننده ← عامل تصدیق پیام
  - یک تابع وارسی ← چک کردن عامل تصدیق پیام
- از الگوریتم های رمزنگاری برای تصدیق صحت پیام می شه استفاده کرد اما:
  - کارایی پایین
  - بررسی مفهوم بودن محتوی همواره آسان نیست
    - نیاز به قالب استاندارد
    - نیاز به افزونگی
    - دوشواری خودکار سازی فرآیند تولید و وارسی
- هدف رمزنگاری ← محرمانگیست نه صحت
- کدهای تشخیص خطا:
  - Parity (CRC-1 bit)
    - تعداد ۱ ها فرد بود یک دونه ۱ اضافه می کنه
  - CRC-32 bit
    - قطعات ۳۲ بیتی رو جمع می کنه
- کد تشخیص کلید ندارد ← برای تشخیص نویز (غیر عمدی و غیر هوشمند) ه حمله دشمن (عمدی و هوشمند) برخلاف امضاء دو طرف قادر به ایجاد MAC هستند.
- ایراد اصلی MAC ← کارایی پایین
- ویژگی توابع درهم ساز:
  ۱. تابع یکطرفه
  ۲. طول ورودی دلخواه
  ۳. طول خروجی ثابی
  ۴. کلید در کار نیست ← برخلاف رمزنگاری و MAC
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
  - OW
  - ۲PR
  - CR
- با تست

$$1.25 \times 2^{\frac{n}{2}}$$

← احتمال 50% یک تصادم پیدا می شود.

  - n: طول خروجی
- تابع f حتما CR باشد.

- با داشتن $H(x)$ برای x های نا معلوم به طول L

$$H(x||pad(x)||L||y)$$

  - y: دلخواه
  - راه حل:
    * طول پیام قطعه اول ؟؟؟؟
    * قطعه آخر با تابع H متفاوت

- تشابه و تفاوت MAC و Hash :
  - هر دو چکیده ساز
  - کلید:
    * hash کلید ندارد $\leftarrow H(x) = y$
    * MAC کلید دارد $\leftarrow MAC(x, Key) = y$
- MD۵: حمله روز تولد $\leftarrow 2^{64}$ گام $\leftarrow$ نا امن
- SHA: حمله روز تولد $\leftarrow 2^{80} \leftarrow 2^{60.3}$
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.

۱.۱.۰ سوال

۱. آیا همیشه محرمانگی مهم است؟

۲. عملکرد های تصدیق صحت پیام کدوما هستن؟

۳. از الگوریتم های رمزنگاری میشه استفاده کرد برای تصدیق صحت پیام؟

۴. هدف رمزنگاری چیست؟

۵. کدهای تشخیص خطا چیا هستن؟

۶. خطای بیرونی و خطای درونی؟؟

۷. کد تشخیص خطا امنه؟ چرا؟ مثال؟

۸. کد های تصدیق صحت پیام

۹. توضیح MAC ؟

۱۰. توضیح CBC-MAC ؟ حمله؟ راه حل؟ حمله؟ راه حل؟

۱۱. تفاوت MAC با رمزنگاری؟

۱۲. آیا MAC غیرقابل امضا است؟

۱۳. روش های ترکیب MAC با رمزنگاری؟

۱۴. ایراد اصلی ؟MAC

۱۵. ویژگی توابقع درهم ساز؟

۱۶. امنیت توابع درهم ساز چگونه تامین میشود؟

۱۷. حمله آزمون جامع به ؟Hash

۱۸. مرکل دمگارد ؟MD

۱۹. تشابه و تفاوت MAC و ؟Hash

۲۰. MD۵ چیه؟حمله؟

۲۱. SHA جیه؟حمله روز تولد؟

۲۲. SHA-۲ چیه؟

۲۳. HMAC چیه؟اهداف؟

۲۴. مقاوم در برابر یافتن پیش نگاره اول چیه؟

۲۵. مقاوم در برابر یافتن پیش نگاره دوم چیه؟

۲۶. کدام یک پیشنگاره اول یا پیشنگاره دوم از ویژگی مقاوم در برابر تصادم نتیجه می شود؟ چرا؟

۲۷. اگر تابع ویژگی « پیش نگاره دوم را داشته باشد مقاومت در برابر یافتن پیشنگاره اول را نیز دارد؟ دلیل؟