Date: ۱۴۰۰ / ۷ / ۱۱ راشین احسانی ۹۷۵۲۱۰۱۸ Subject: یادداشت کلاسی

★ انواع نشان گذاری { Visible / Invisible
شکننده / غیر شکننده

★ مثال ← آرم شبکه بالای صفحه ← برای جلوگیری از کپی کردن
↳ Visible

★ استادر از هنری ← بدون خراب شدن اثر (مخفی)
↳ امضا کردن پشت اثر هنری
↳ Invisible

★ شکننده / غیر شکننده
شکننده
↳ تغییر عکس باعث از بین رفتن نشان گذاری میشود
از بین نرود ↳ غیر شکننده
غیر شکننده

مثال ← فیلم ← انجام تغییرات ← واترمارک مقاوم در برابر تغییرات

★ الگوریتم نشان گذاری نوع آن را مشخص می کند ← وابسته به کاربرد

Date: / / Subject:

* حملات

- انواع
  - فعال ← active
  - غیرفعال ← passive

آلیس و باب ← مجاز

باب ↔ کانال ↔ آلیس

ایو

ایو ← attacker

passive

هدف ۱ ← فقط استراق سمع ← قصد دیگری ندارد ← نشود

هدف ۲ ← علاوه بر نشود، تغییر پیام ← active

* Phishing

- ترغیب کاربران به افشای رمز
- مثل ایمیل تغییر رمز

↓

درخواست مسابقه برنده شدید

↓

احراز اصالت مورد هدف قرار می‌گیرد ← سایت فیک

- جلوگیری از این حمله ← احراز اصالت (Authentication)

* Phishing ← از نوع فعال (active)

نه چون فقط نشود، می‌کند

Date: / /

Subject:

* حمله تغییر پیام

↗ باب متوجه این تغییر نمی‌شود

↳ تغییر مقدار چک از ۱ بیلیون به ۲ بیلیون

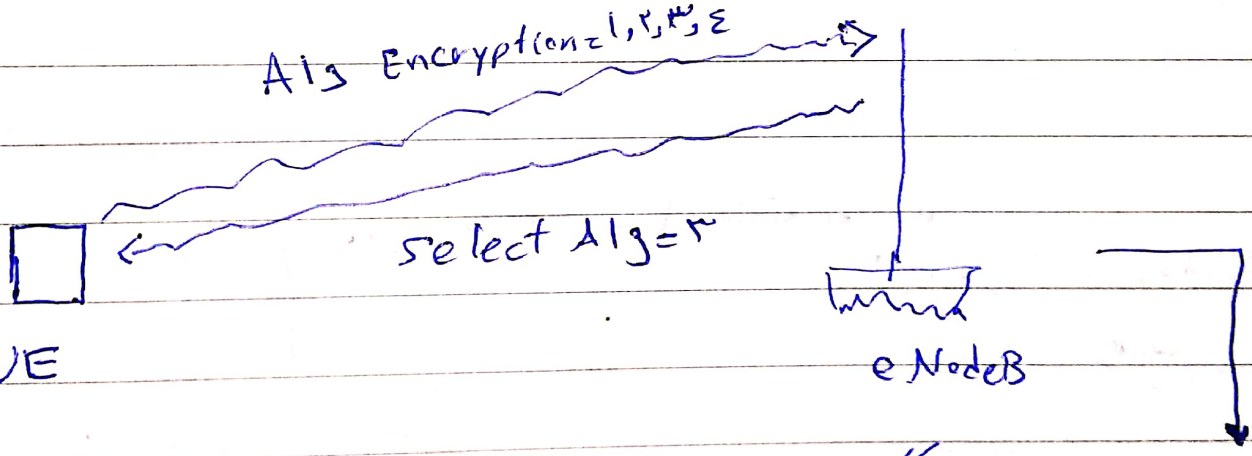
جلوگیری؟ ← استفاده از تابع چکیده ساز ← Hash Function

مثال ← دانلود فایروفاکس از سایت های نامعتبر

↳ تغییر certificate توسط سایت

↳ راه حل ← checksum

↳ اگر یکسان بود ← فایل درست است



ولی پیام اول هیچ گونه encryption ندارد ← او پیام را تغییر می‌دهد

Alg Enc=0 ← هیچ گونه encryption انتخاب نمی‌شود

↳ plainText → active حمله

Date: / /

Subject:

* حمله به تازگی ← حمله freshness
  ↳ کپی پیام ← دوباره فرستاده شدن

جلوگیری؟ ← Timestamp

↳ مشکل؟ ← همه سیستم‌ها ساعتشان یکی نیست
  ↳ sync

* حل مشکل timestamp ← NTP یا
  ↳ ساعت را sync می‌کنند
  ↳ sync کردن با وجود delay
  دو طرف

* امنیت ← دو نوع
  ↳ بدون شرط ← unconditional
  ↳ محاسباتی
  ↳ در صورت توان محاسباتی زیاد نمی‌توانند سیستم را بشکنند
  ↳ از نظر محاسباتی
  ↳ بسیار پیچیده و طولانی است

* تنها سامانه بدون شرط ← one time pad یا Vernam