دانشگاه بین المللی امام خمینی قزوین
دانشکدهٔ فنی و مهندسی

مبانی امنیت اطلاعات

(سومین ترم کرونا)

مقدمه

نستوه طاهری جوان
nastooh@aut.ac.ir

معرفی مدرس در ترم و کلاس مجازی!

✓ نستوه طاهری جوان

- لیسانس مهندسی کامپیوتر، نرم افزار
- فوق لیسانس مهندسی کامپیوتر، سخت افزار
- دکترای مهندسی کامپیوتر، شبکه های کامپیوتری
- پسا دکترای مهندسی کامپیوتر، یادگیری ماشین در شبکه های بی سیم

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

- وب سایت شخصی: www.nastooh.com
- صفحه آکادمیک: https://ceit.aut.ac.ir/~nastooh/
- گوگل اسکالر: https://scholar.google.com/citations?user=PmjCrgMAAAAJ
- آدرس ایمیل شخصی: va_nastooh@yahoo.com

بارم بندی

- ✓ امتحان میان ترم
  - ۵ نمره
  - امتحان به صورت Open Book
- ✓ امتحان پایان ترم
  - ۵ نمره
  - امتحان به صورت Open Book
- ✓ تمرین های کلاسی
  - ۵ نمره
  - در طول ترم
- ✓ پروژه پایانی
  - ۵ نمره (بعلاوهٔ نمرهٔ امتیازی)
  - پروژه تحویل **حضوری** دارد.

این بخش بندی ممکن است در طول ترم تغییر کند!

nastooh@aut.ac.ir

منابع

- ✓ منابع اصلی درس
  - کتاب اول: (لینک دانلود مستقیم)

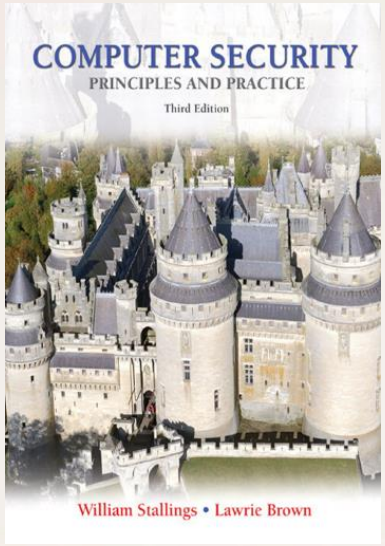
Computer Security, 3th ed., W. Stallings.

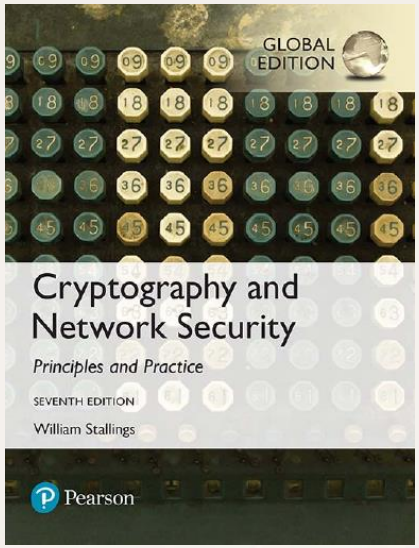
  - کتاب دوم: (لینک دانلود مستقیم)

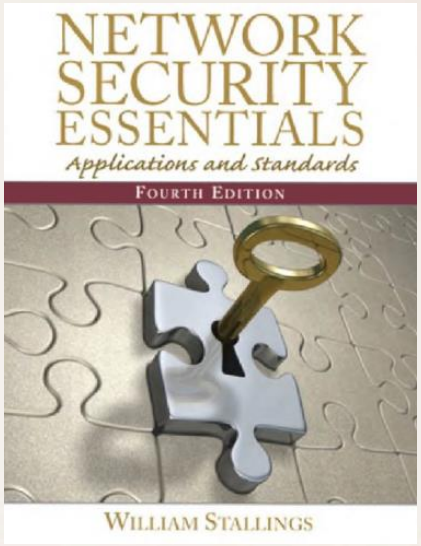
Cryptography and Network Security, 7th ed., W. Stallings.

  - کتاب سوم: (لینک دانلود مستقیم)

Network Security Essentials, 4th ed., W. Stallings.







مباحث درس در یک نگاه

- ✓ امنیت داده
  - مقدمات
  - رمزنگاری
    - متقارن و نامتقارن
  - توابع درهم سازی
    - امضای دیجیتال
  - ساختار PKI
  - احراز هویت
  - رمز ارزها
    - بیت کوین
- ✓ امنیت شبکه
  - IPsec و VPN
  - SSL
  - حملات در شبکه

سر فصل ها از نظر اهمیت و وزن زمانی در طول ترم، لزوماً هم سنگ نیستند!

nastooh@aut.ac.ir

قوانین کلاس

✓ تنها قانون کلاس:

مقیاس زمانی کلیهٔ رویدادهای کلاس به ثانیه است!

- منظور رویدادهایی مانند تحویل تمرین، تحویل پروژه، امتحان میان ترم و امثالهم است.

○ این به این معنی ست: به هیچ وجه رویدادهای کلاس، تمدید نخواهند شد!!!

- حتی برای شما دوست عزیز...

به جز این تنها قانون، هیچ محدودیت و قانونی برای کلاس وجود ندارد.

nastooh@aut.ac.ir

راه های تعامل

- ✓ برای انجام امور کلاس از وبسایت کوئرا استفاده خواهد شد.
  - کلیهٔ اطلاع رسانی ها از طریق این سایت انجام خواهد شد.
  - تحویل تمرین ها از طریق این سایت است.
  - آدرس سایت جهت عضویت: https://quera.ir/
    - از نوع دانشجو اکانت بسازید.
  - لینک ورود به کلاس، پس از ساخت اکانت: (برای کلاس مباحث ویژه ۲، بهمن ۹۹)

    https://quera.ir/overview/add_to_course/course/7617
    - پسورد مورد نیاز برای ملحق شدن به کلاس، در کلاس آنلاین اعلام خواهد شد.
  - لطفا همین امروز ابتدا در این سایت اکانت ایجاد کنید و سپس با کمک لینک فوق به کلاس درس ملحق شوید.
    - در صورتی که موفق به ایجاد اکانت نشدید، لطفا از طریق ایمیل با مدرس در ارتباط باشید. *nastooh@aut.ac.ir* یا *va_nastooh@yahoo.com*

تعریف امنیت اطلاعات

- ✓ عموماً تعریف واحدی نمی توان از امنیت اطلاعات ارائه داد.

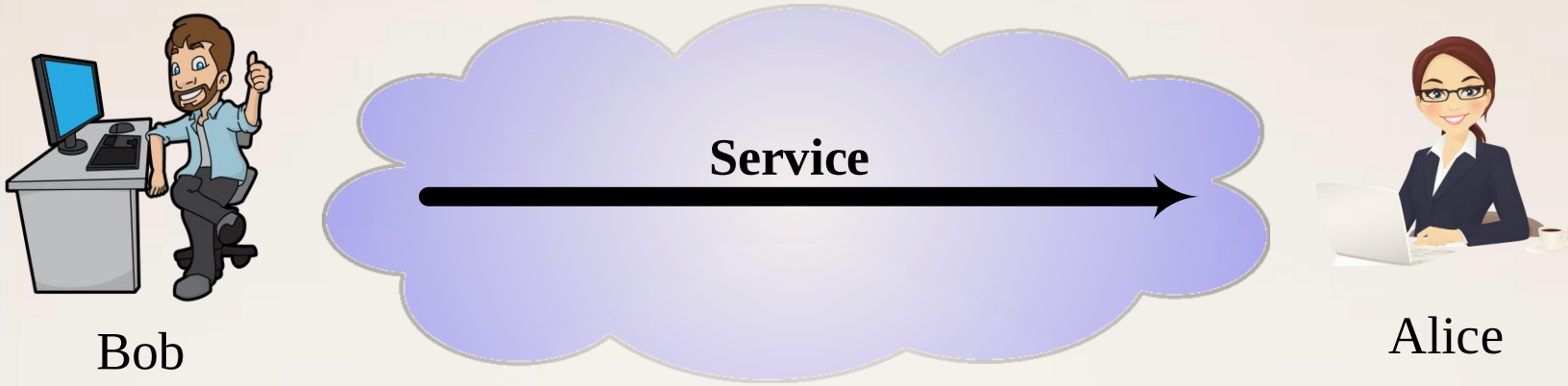
- ✓ یکی از متداول ترین تعاریف:
  - ○ محافظت کردن از اطلاعات در برابر اقدامات غیر مجاز
    - هنگام ذخیره سازی، پردازش یا مبادله...
    - با انواع اقدامات غیر مجاز به مرور آشنا خواهیم شد.

تعاریف کلیدی

- ✓ تهدید (Threat)
  - هر اقدام بالقوه ای که تاثیر نامطلوبی بر روی کارآیی سیستم بگذارد.
- ✓ نقطه ضعف (Vulnerability)
  - هر ویژگی قابل سواستفاده سیستم که به یک تهدید امکان وقوع می دهد.
- ✓ حمله (Attack)
  - عملی که توسط یک نفوذگر زیان رسان انجام می شود و با استفاده از یک نقطه ضعف، به یک تهدید امکان وقوع می دهد.

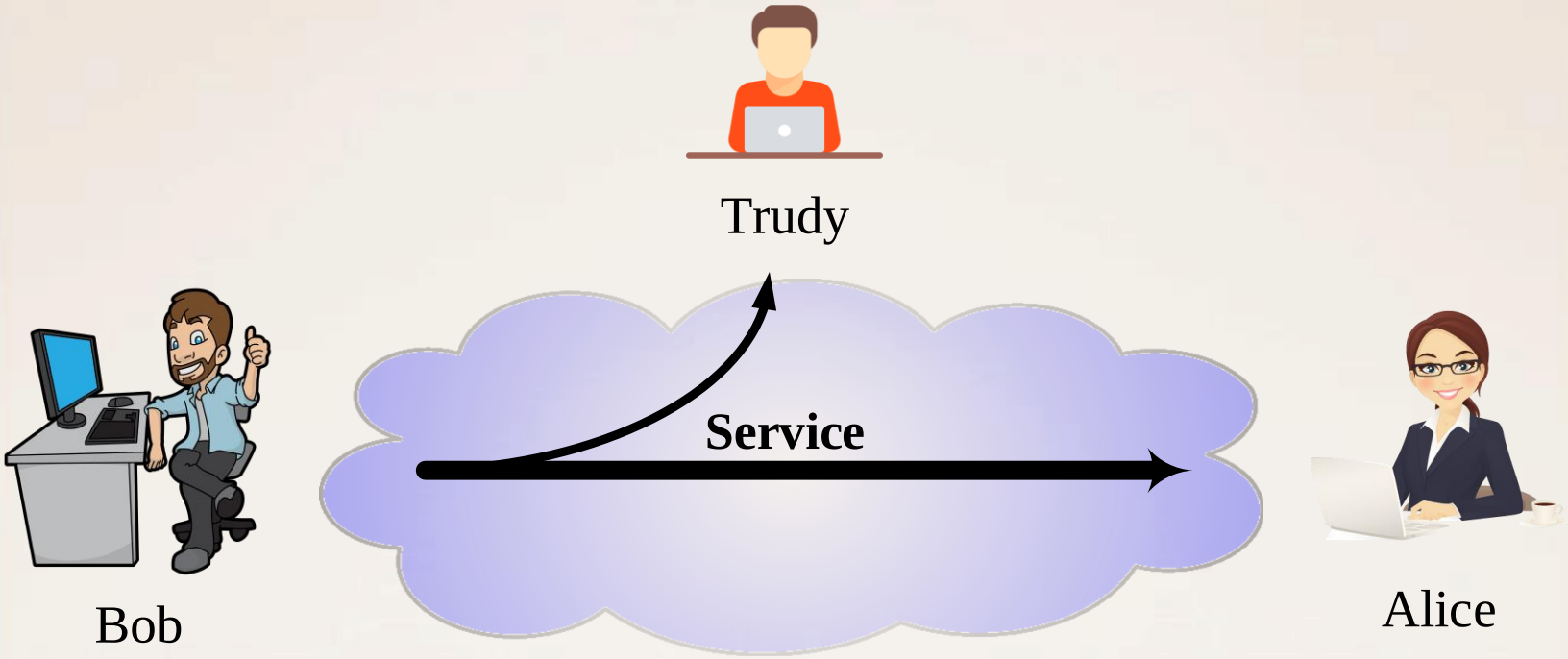
دسته بندی کلی حملات

- فرض: شکل نرمال یک سرویس در سیستم



دسته بندی کلی حملات

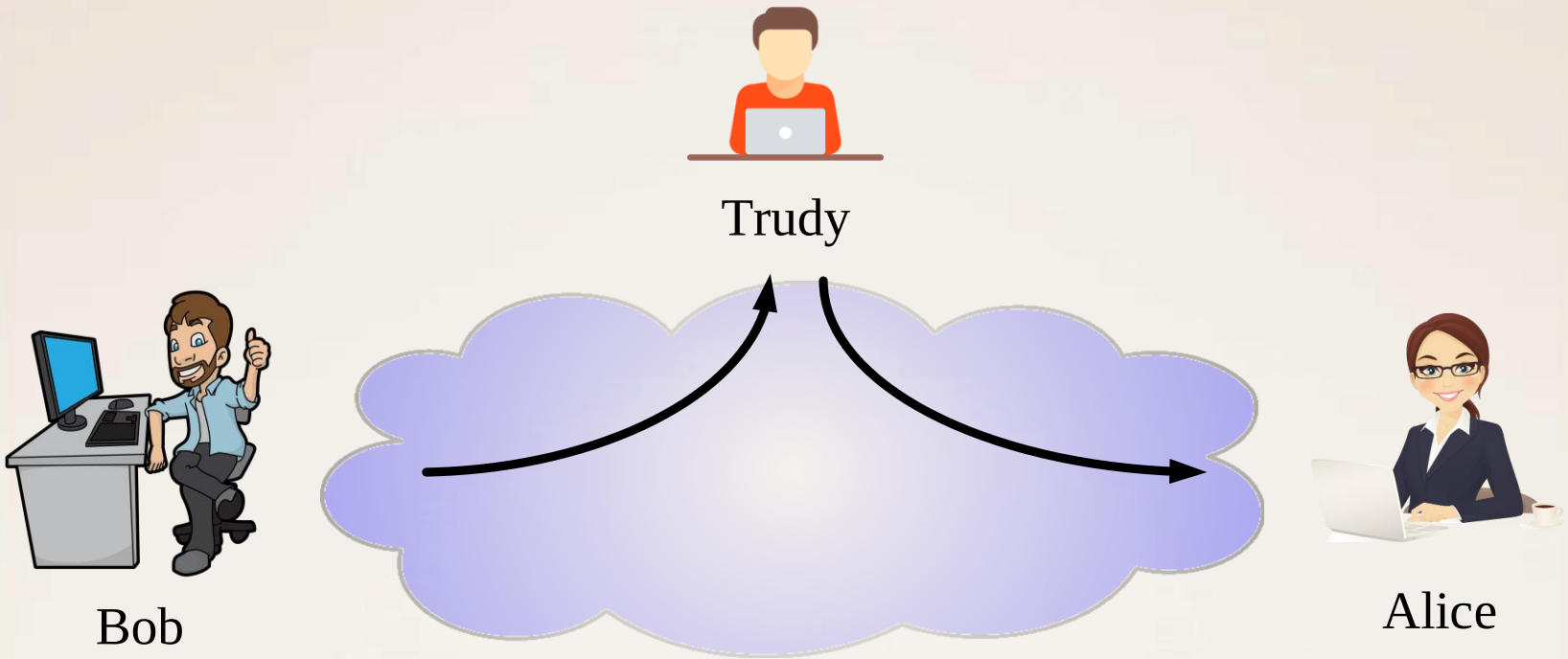
- ✓ حملهٔ نوع اول: Interception



nastooh@aut.ac.ir

دسته بندی کلی حملات

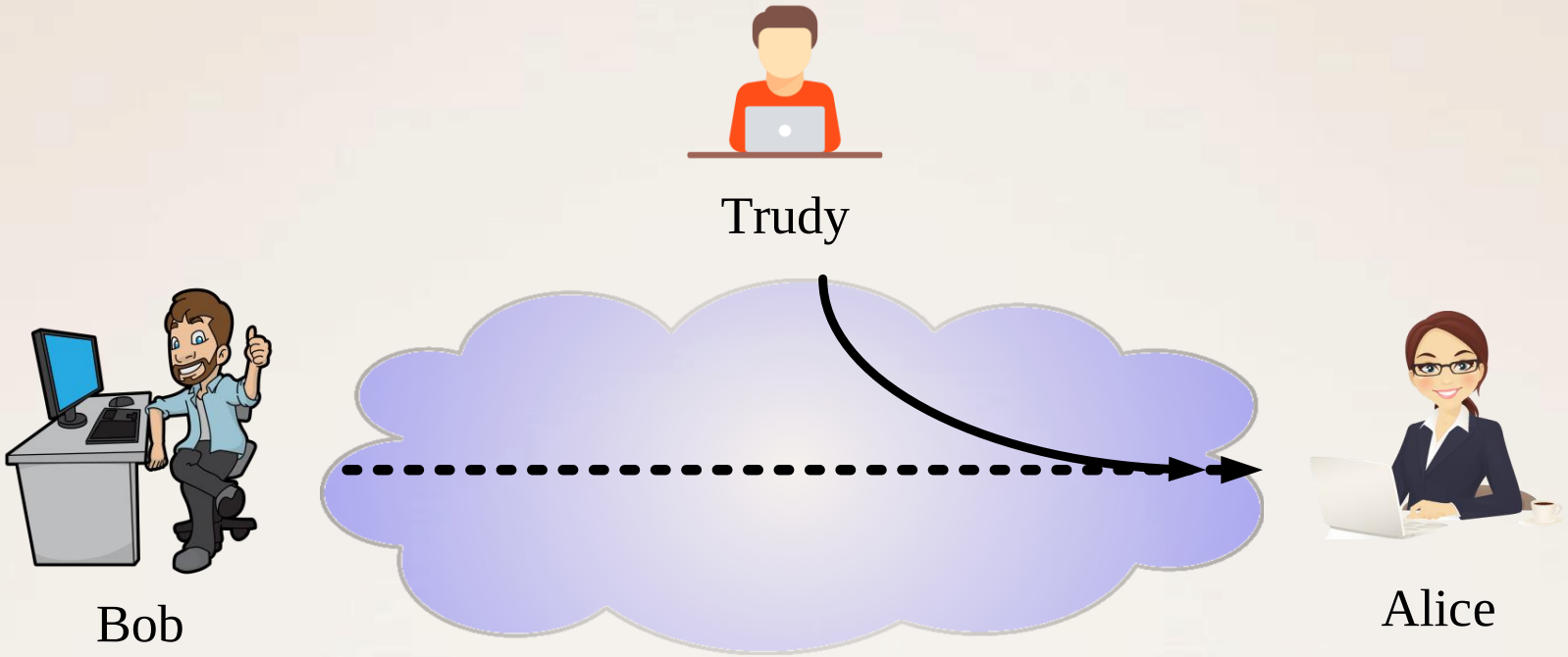
- ✓ حملهٔ نوع دوم: Modification



nastooh@aut.ac.ir

دسته بندی کلی حملات

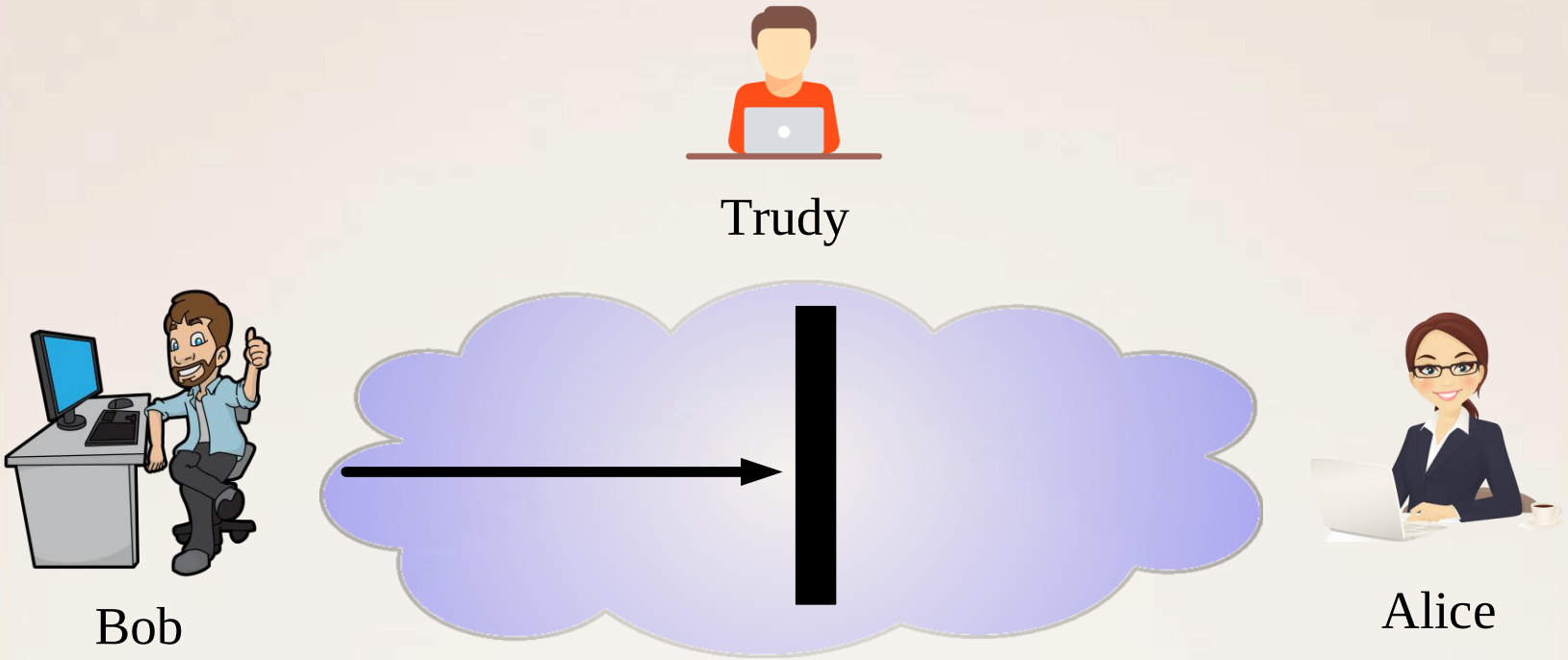
- ✓ حملهٔ نوع سوم: Fabrication



nastooh@aut.ac.ir

دسته بندی کلی حملات

- ✓ حملهٔ نوع چهارم: Interruption



nastooh@aut.ac.ir

مروری بر سرویس های امنیتی

- ✓ Authentication
- ✓ Access Control
- ✓ Confidentiality
- ✓ Integrity
- ✓ Non-Repudiation
- ✓ ...

nastooh@aut.ac.ir

رتبه بندی تهدید ها

- ✓ بحث آزاد دربارهٔ لزوم رتبه بندی تهدید ها

رتبه بندی تهدید ها

- یکی از روش های مرسوم، استفاده از پارامترهای DREAD
  - نمره دادن به پارامترهای زیر به ازای تهدیدها

- Damage Potential
- Re-productibility
- Exploitability
- Affected users
- Discoverability

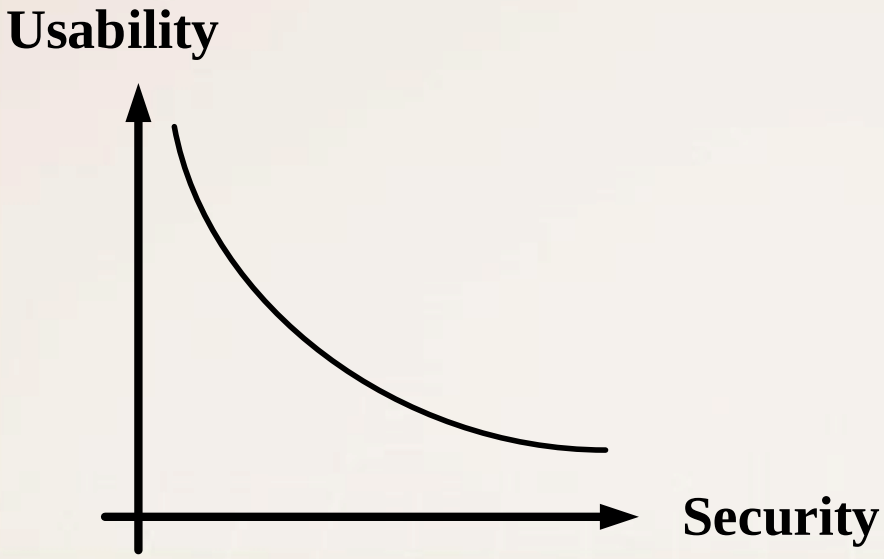
دسته بندی نفوذگران

- ✓ دیدگاه اول:
  - Hacker
  - Cracker
- ✓ دیدگاه دوم:
  - White hat hacker
  - Black hat hacker
  - Gray hat Hacker
- ✓ دیدگاه سوم: از نظر سطح مهارت

nastooh@aut.ac.ir

مقابله با تهدید ها

- در حالت کلی دو روش برای مقابله با تهدیدها وجود دارد:
  - Safeguard
  - Countermeasure



nastooh@aut.ac.ir

مقابله با تهدید ها

✓ تعدادی از اقدامات جهت مقابله با تهدیدها در شبکه:

1. Auditing and Intrusion Detection
2. Encryption
3. Identification & Authentication
4. Access Control
5. ....(شما مثال بزنید)

معرفی IDS

- ابزاری برای تحلیل ترافیک و تشخیص بدرفتاری
- رویکردهای IDS
  - مدلسازی رفتارهای صحیح
  - مدلسازی رفتارهای غیر مجاز
- تفاوت IDS و IPS
- خطاهای تشخیص
  - False Negative
  - False Positive
- تفاوت های NIDS و HIDS در شبکه

معرفی Firewall

- ✓ محل ایست بازرسی بسته ها
- ✓ اعمال پس از بررسی بسته ها
  - Accept mode
  - Block mode
  - Response mode
- ✓ پیکربندی دیواره های آتش
- ✓ انواع دیواره های آتش
  - Traditional
  - State-full
  - Proxy-based

منابع

[1] William Stallings, “Computer Security,” 3th ed. (Download Link)

[2] William Stallings, “Cryptography and Network Security,” 7th ed. (Download Link)

[3] William Stallings, “Network Security Essentials,” 4nd ed. (Download Link)

پایان

nastooh@aut.ac.ir