دانشگاه شهید بهشتی
دانشکده‌ی مهندسی و علوم کامپیوتر

مقدمه

امنیت شبکه‌های کامپیوتری

دکتر مقصود عباسپور

محتویات درس

- مقدمه‌ای بر امنیت کامپیوتر و شبکه
- پروژه‌های عملی
  - تولید حملات
  - مقابله با حملات
- بررسی امنیت در لایه‌های مختلف
  - امنیت کاربرد
  - امنیت سیستم عامل
  - امنیت وب
  - امنیت شبکه

اطلاعات کلی

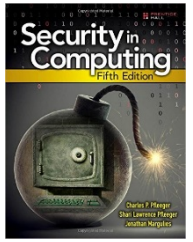
- **پیشنیازها :**
  - شبکه های کامپیوتری
  - سیستم عامل لینوکس
  - زبان برنامه نویسی C/C++
- **ارزیابی :**
  - امتحان ۱۰-۱۲ نمره
  - تکالیف ۲ نمره
  - پروژه ۸-۶ نمره
- **کمک استاد**

فهرست مطالب

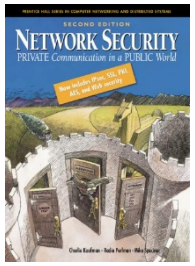
- ✓ مقدمه‌ای بر رمزنگاری
- ✓ امنیت نرم افزار
- ✓ Sandboxing
- ✓ آسیب پذیری‌های شبکه
- ✓ Secure Sockets Layer (SSL)
- ✓ امنیت IP (IPsec)
- ✓ Firewall
- ✓ Intrusion Detection Systems (IDS)
- ✓ همبستگی هشدارها (Alert Correlation)
- ✓ غیر فعال نمودن سرویس (Denial of Service)

منابع درس امنیت شبکه های کامپیوتری

- Charles P. Pfleeger, "**Security in Computing**", Fourth Edition.



- Kaufman, Perlman and Speciner, "**Network Security: Private Communication in a Public World**", Second Edition.

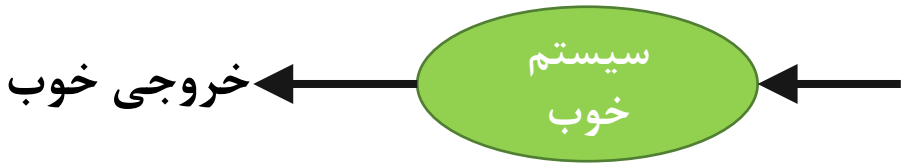


- Avinash Kak, ECE 404 - **Introduction to Computer Security**, Purdue University

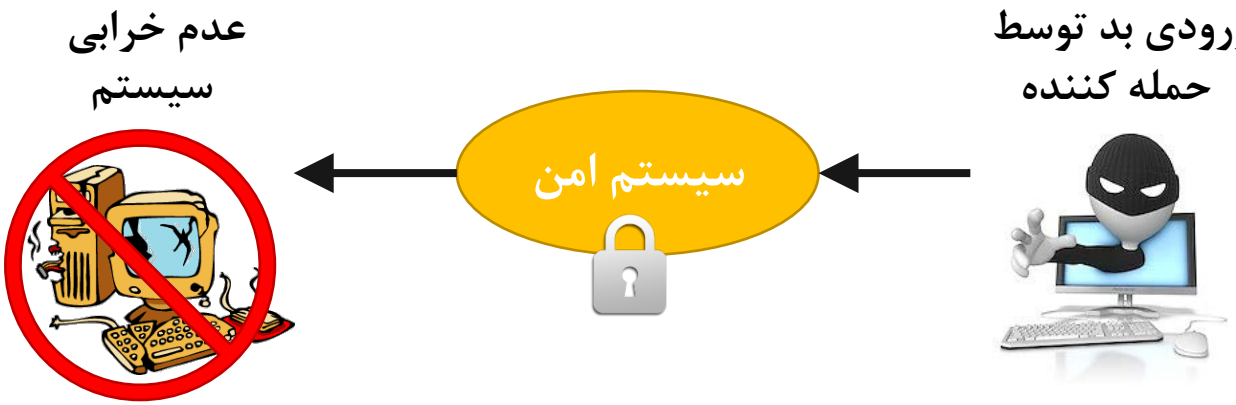
- Papers

امنیت چیست؟

سیستم درست :



امنیت :



- **سیستم خوب**
  امکانات بیشتر خوب است!
- **امنیت**
  امکانات بیشتر دردسر است!

خصوصیات امنیت

- **محرمانگی (Confidentiality)**

اطلاعات فقط توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد.

- **صحت (Integrity)**

داده نباید به صورت تصادفی یا عمدی تغییر، نابود و یا گم شود.

- **دسترس پذیری (Availability)**

سیستم باید قادر باشد سرویس‌های مورد نظر را هنگام درخواست کاربر ارئه دهد.

اصطلاحات امنیتی

- ✓ **آسیب پذیری (Vulnerability) :**
  یک خطا یا نقص در *طراحی*، *پیاده سازی* یا *عملیات* سیستم.

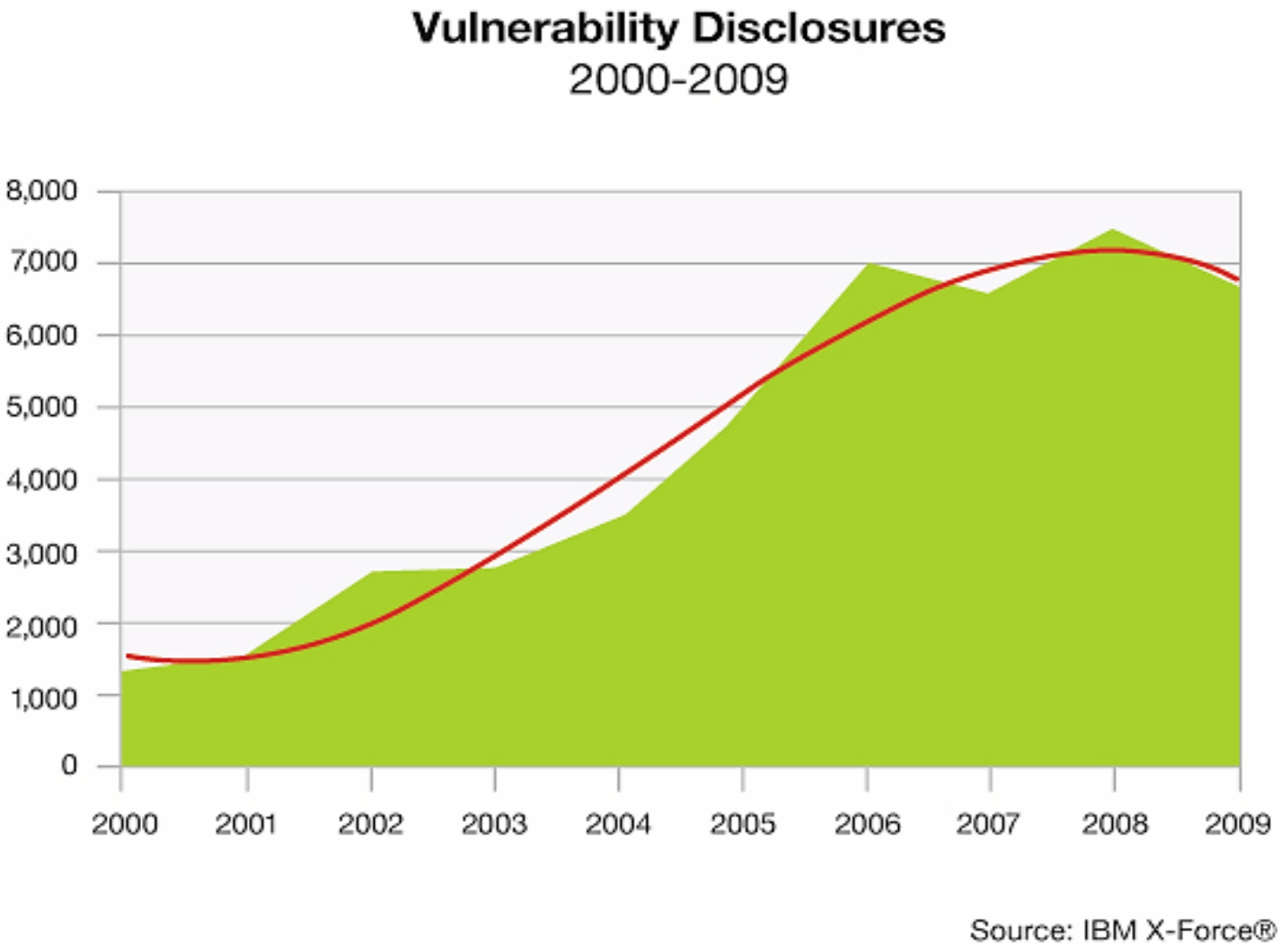
- ✓ **حمله (Attack) :**
  بهره برداری از آسیب پذیری‌های یک سیستم.

- ✓ **تهدید (Threat) :**
  فردی بدخواه که انگیزه و توانایی حمله داشته باشد.

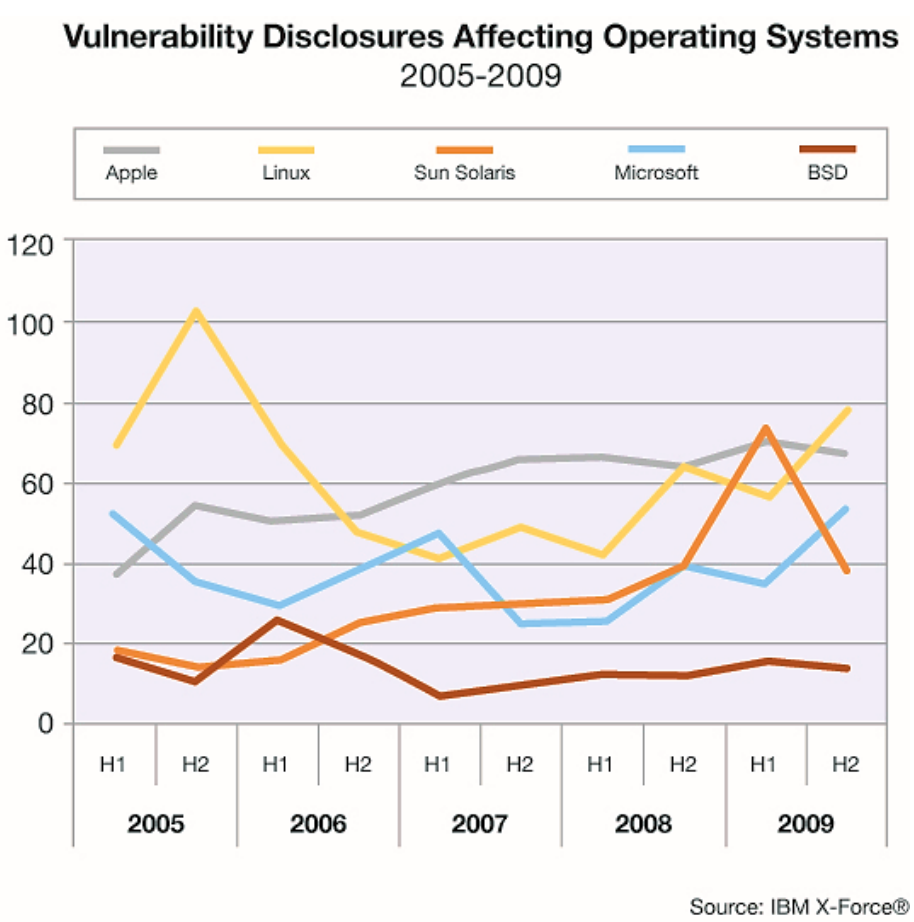
- ✓ **تایید هویت (Authentication)**

- ✓ **اجازه (Authorization)**

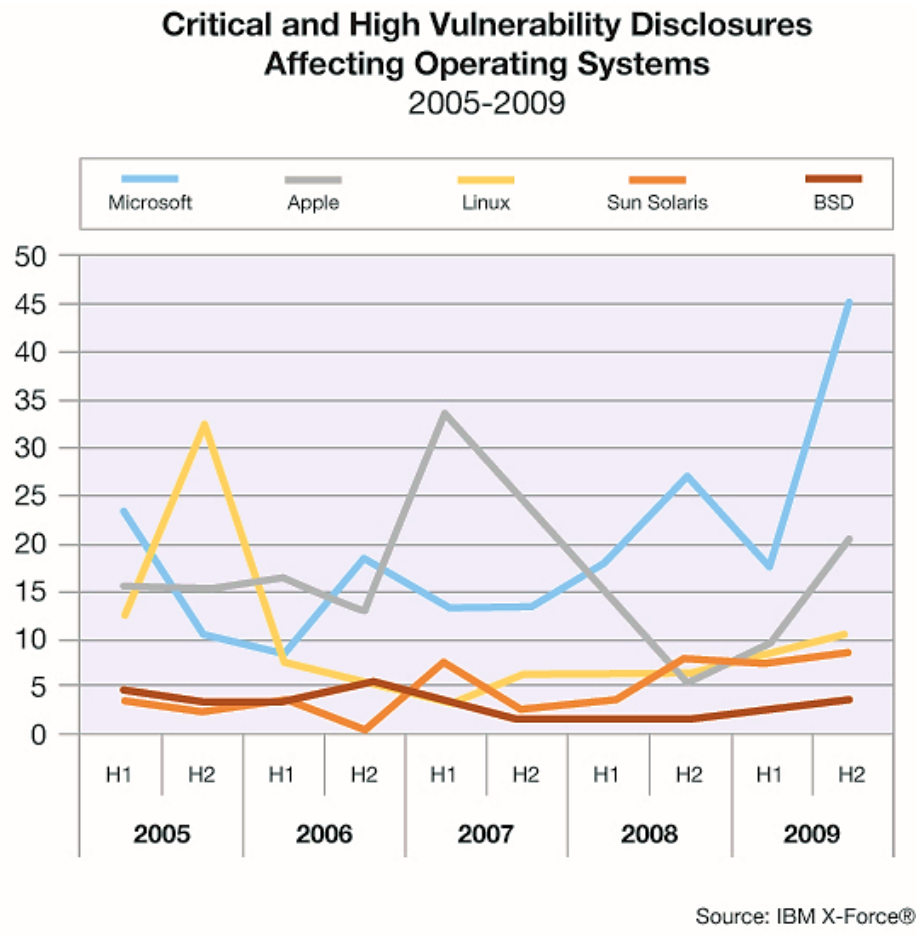
روند پیدایش آسیب پذیری ها



آسیب پذیری های سیستم عامل

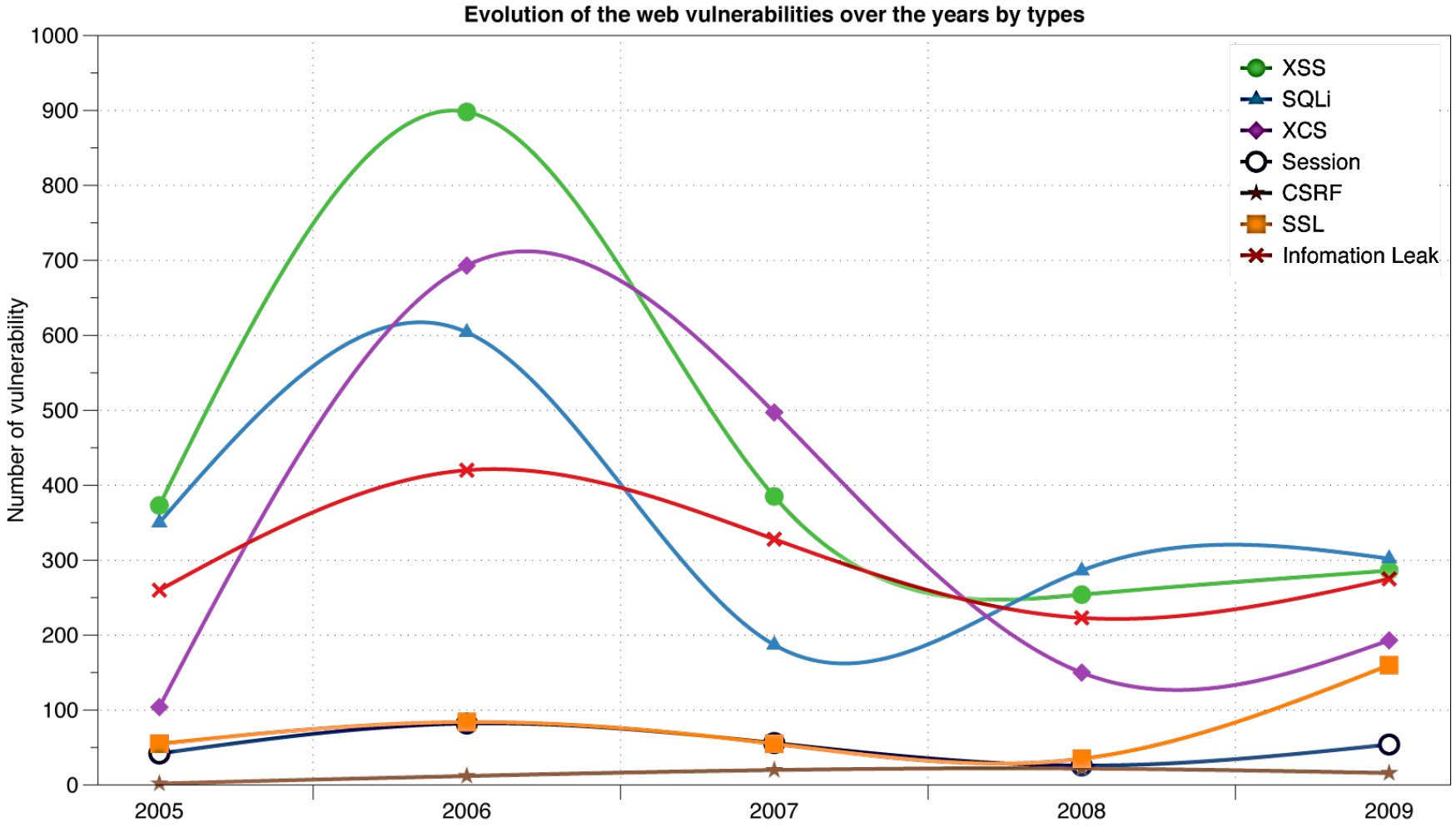


Source: IBM X-Force®

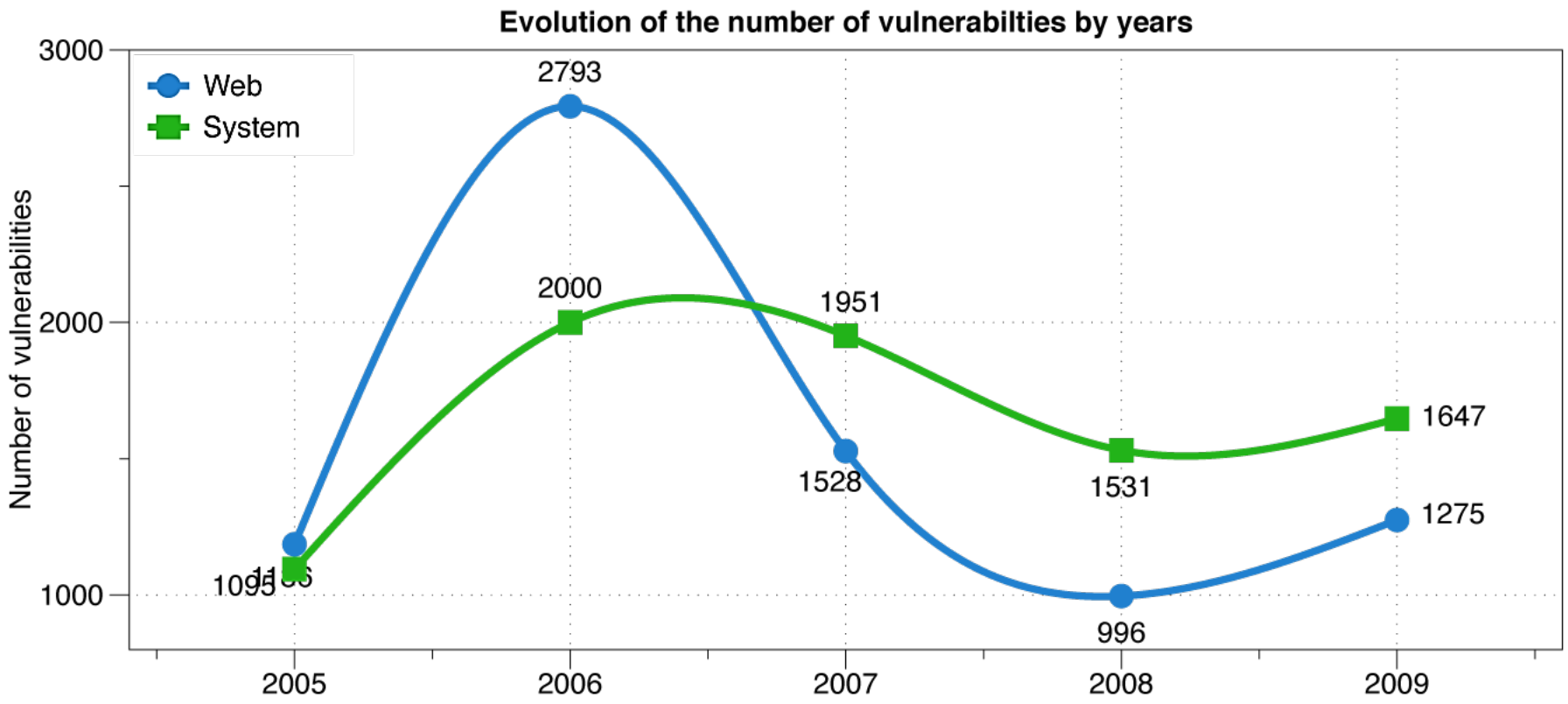


Source: IBM X-Force®

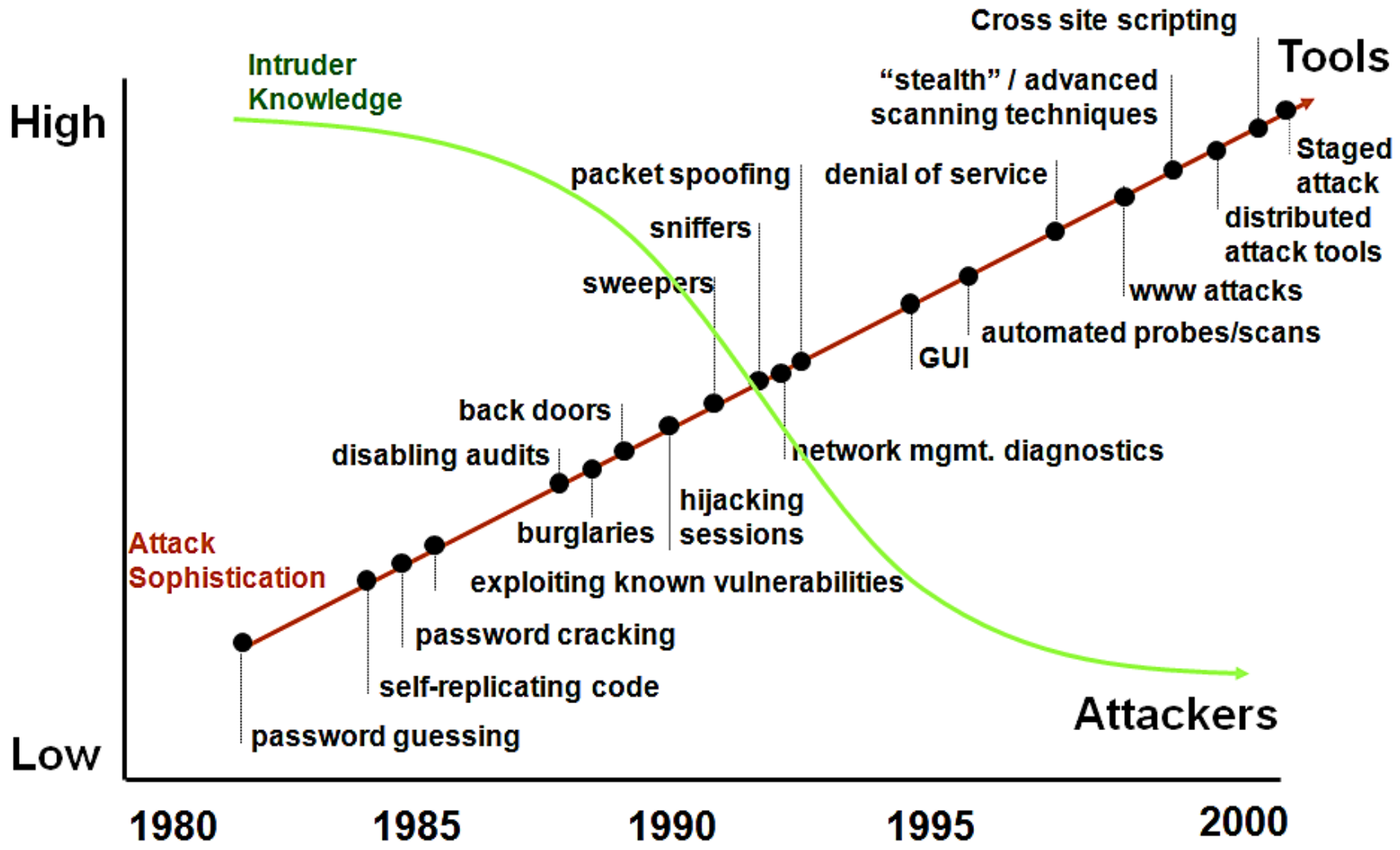
آسیب پذیری های وب



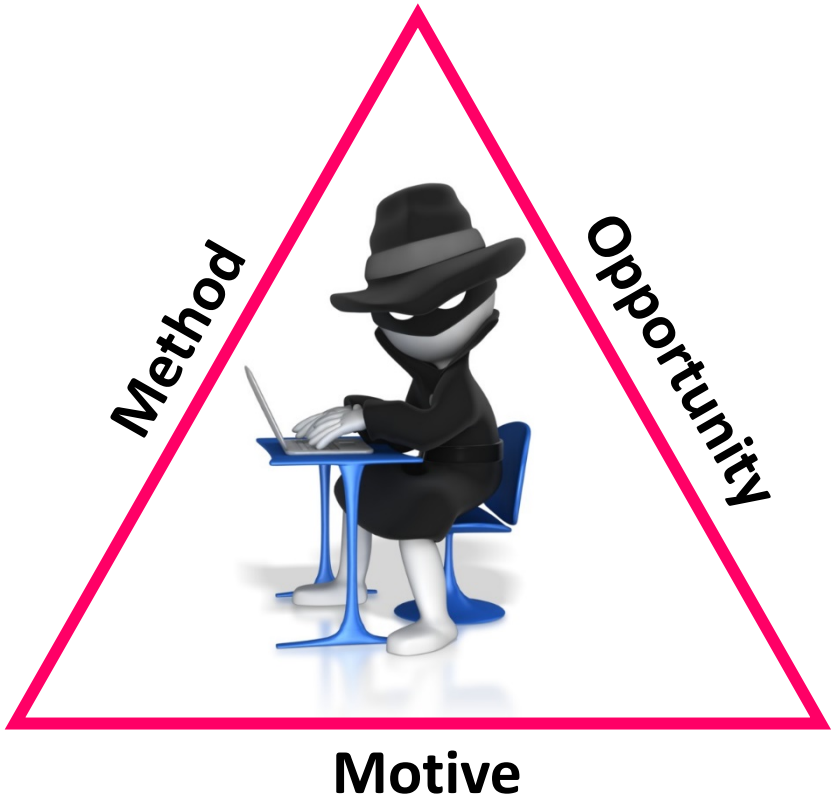
آسیب پذیری های وب و سیستم



دانش حمله کننده ها در مقایسه با ابزارها



مفهوم MOM در حملات



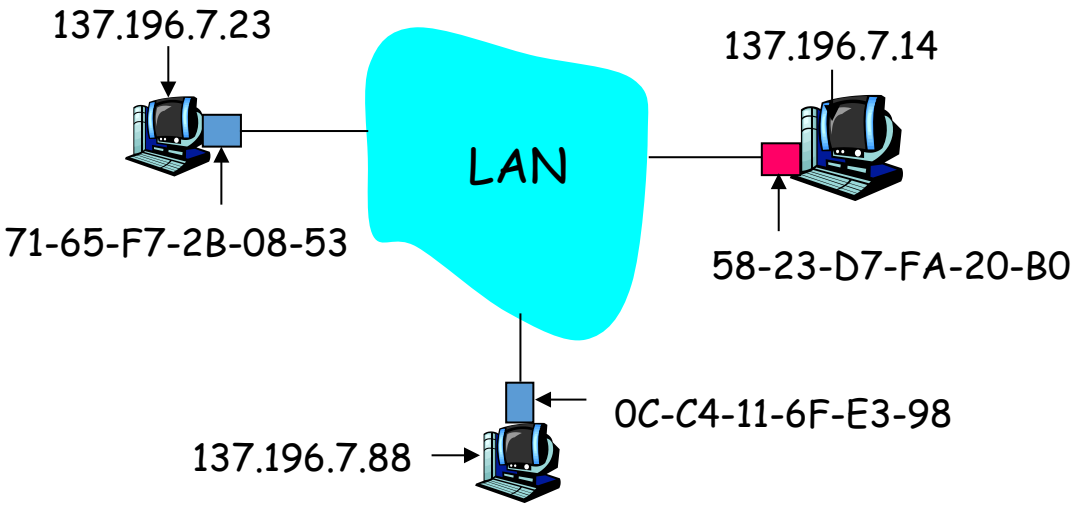
- روش (Method)
  - مهارت
  - دانش
  - ابزار
- فرصت (Opportunity)
  - زمان
  - دسترسی
- انگیزه (Motive)
  - سرگرمی : خرابکاری
  - منفعت : سازماندهی شده
  - جاسوسی

انواع آسیب پذیری ها

- آسیب پذیری های **Host** :
  - نرم‌افزار
  - سیستم عامل
- آسیب پذیری های **Network** :
  - **لایه لینک** : ARP Spoofing
  - **لایه شبکه** : IP Forgery
  - **لایه انتقال** : حدس زدن TCP Sequence-Number
  - **لایه کاربرد** : کرم‌های اینترنتی

لایه لینک : ARP Spoofing

- Address Resolution Protocol
- پروتکل ARP برای پیدا کردن آدرس Ethernet یک آدرس IP استفاده می‌شود.
- ماشین حمله کننده می‌تواند به درخواست‌های ARP پاسخ دهد و بسته‌های ماشین قربانی را به سمت خود منحرف کند.



لایه انتقال : TCP 3-Way Handshake

- برای برقراری اتصال بین کلاینت C و سرور S بسته های زیر رد و بدل می‌شوند :
  - Initial Sequence Number (ISN)
  - در بعضی از پیاده‌سازی‌های TCP، ISN بعد از هر اتصال به اندازه $\boldsymbol{k}$ واحد افزایش می‌یابد.

$$C \rightarrow S: \ SYN(ISN_C)$$

$$S \rightarrow C: \ SYN(ISN_S), ACK(ISN_C)$$

$$C \rightarrow S: \ ACK(ISN_S)$$

$$C \rightarrow S: \ data$$

حدس زدن TCP Sequence-Number

- X برای یاد گرفتن ISN_S یک اتصال برقرار می کند :

$$X \rightarrow S: \quad SYN(ISN_X)$$

$$S \rightarrow X: \quad SYN(ISN_S), ACK(ISN_X)$$

- سپس X هویت T را **جعل** می کند :

$$X \rightarrow S: \quad SYN(ISN_X), SRC = T$$

$$S \rightarrow T: \quad SYN(ISN_S + k), ACK(ISN_X)$$

$$X \rightarrow S: \quad ACK(ISN_S + k), SRC = T$$

$$X \rightarrow S: \quad ACK(ISN_S + k), SRC = T, nasty\ data$$

دسته بندی کلی حملات

- **قطع ارتباط (Interruption)**
  - عدم دسترس پذیری
- **سرقت اطلاعات (Interception)**
  - عدم محرمانگی
- **تغییر اطلاعات (Modification)**
  - عدم صحت
- **جعل اطلاعات (Fabrication)**
  - عدم اعتبار
- **رد درخواست (Denial of Service)**
  - عدم دسترس پذیری

نمونه ای از حملات

- **اسکن کردن شبکه**
  - شناسایی ساختار شبکه سازمان

- **مصرف پهنای باند**
  - Denial of Service (DoS)
  - استفاده از پهنای باند سازمان برای حمله به یک شبکه‌ی دیگر
  - Reflector Attack

- **سوء استفاده**
  - استفاده از کامپیوترهای یک سازمان برای کارهای بدخواهانه

نمونه ای از حملات

- **استراق سمع (Eavesdropping)**
  - برنامه های استنشاق اطلاعات (Sniffer)
  - استنشاق کارت‌های اعتباری
- **مهندسی اجتماعی**
  - تحریک مدیران فنی سیستم و اخذ اطلاعات

روش های دفاعی

- **ممانعت کردن (Prevent)**
- **باز داشتن (Deter)**

تا جای ممکن سخت کردن وقوع حمله.

- **منحرف کردن (Deflect)**

ایجاد اهداف ساختگی برای منحرف کردن حمله به سمت آن‌ها.

- **شناسایی کردن (Detect)**
- **مدارا کردن (Tolerate)**

تا جای ممکن اثر حمله را کم کردن.

- **باز یافتن (Recover)**

تأمین امنیت

o امنیت Host

- راحت‌تر قابل کنترل است.
- مدل‌های خوبی برای تأیید هویت و اجازه طراحی و پیاده‌سازی شده است.

o امنیت Network

- همه می‌توانند به شبکه متصل باشند.
- نحوه اتصال ماشین‌ها به شبکه قابل کنترل نیست.

تأمین امنیت شبکه

- **جایگزینی ساختارهای آسیب پذیر**
  - استفاده از رمزنگاری به جای تأیید هویت مبتنی بر آدرس
- **استفاده از Firewall برای ایجاد محدودیت در دسترسی به سرویس‌های مهم**
- **بررسی شیوه‌مند و پی در پی برای جلوگیری از حملات**
  - مانیتورینگ شبکه برای شناسایی ARP Spoofing
- **پایش شبکه**

پایان مقدمه