

مقدمه

محتویات درس

- مقدمه ای بر امنیت کامپیوتر و شبکه
- پروژه های عملی
 - تولید حملات
 - مقابله با حملات
- بررسی امنیت در لایه های مختلف
 - امنیت کاربرد
 - امنیت سیستم عامل
 - امنیت وب
 - امنیت شبکه

اطلاعات کلی

- پیشنیازها
 - شبکه های کامپیوتری
 - سیستم عامل لینوکس
 - زبان برنامه نویسی C++ و Perl
- ارزیابی
 - امتحان ۱۰ نمره
 - تکالیف ۲ نمره
 - پروژه ۸ نمره

فهرست مطالب

- مقدمه ای بر رمزنگاری

منابع

- Charles P. Pfleeger, “**Security in Computing**”, Fourth Edition.
- Kaufman, Perlman, and Speciner, “**Network Security: Private Communication in a Public World**”, Second Edition.
- [Avi KaK] ECE 404 - **Introduction to Computer Security**, Purdue University

امنیت چیست؟

- سیستم درست

- ورودی خوب و درست ← خروجی خوب

- امنیت

- ورودی بد توسط حمله کننده ← عدم خرابی سیستم

امنیت چیست؟

- سیستم خوب

- امکانات بیشتر خوب است

- امنیت

- امکانات بیشتر در دسر است

خصوصیات امنیت

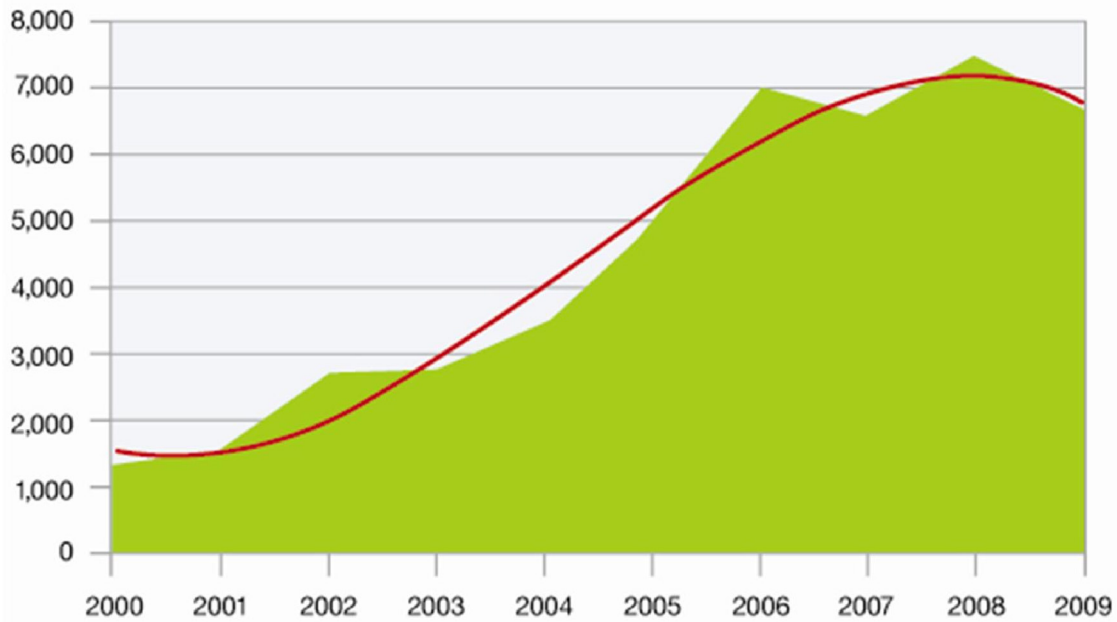
- محرمانگی (Confidentiality)
 - اطلاعات فقط توسط افرادی که تأیید صلاحیت شده اند، قابل دیدن باشد.
- صحت (Integrity)
 - داده نباید به صورت تصادفی یا عمدی تغییر، نابود و یا گم شود.
- دسترس پذیری (Availability)
 - سیستم باید قادر باشد سرویس های مورد نظر را هنگام درخواست کاربر ارائه دهد.

اصطلاحات امنیتی

- آسیب پذیری (Vulnerability)
- یک خطا یا نقص در طراحی، پیاده سازی یا عملیات سیستم
- حمله (Attack)
- بهره برداری از آسیب پذیری های یک سیستم
- تهدید (Threat)
- فردی بدخواه که انگیزه و توانایی حمله داشته باشد
- تایید هویت (Authentication)
- اجازه (Authorization)

روند پیدایش آسیب پذیری ها

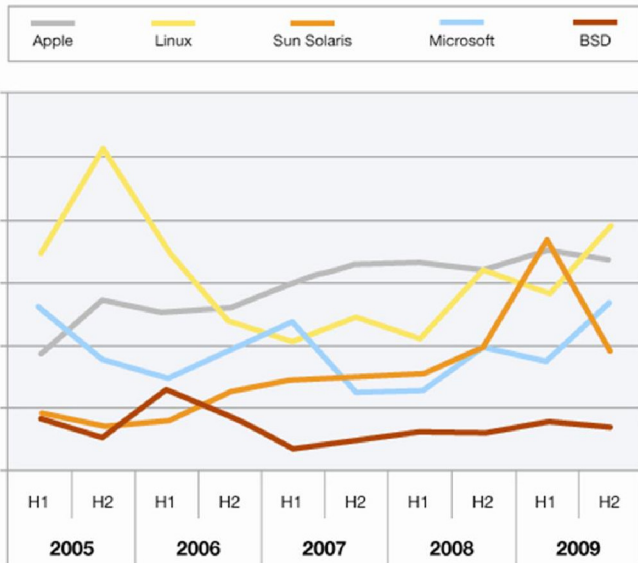
Vulnerability Disclosures
2000-2009



Source: IBM X-Force®

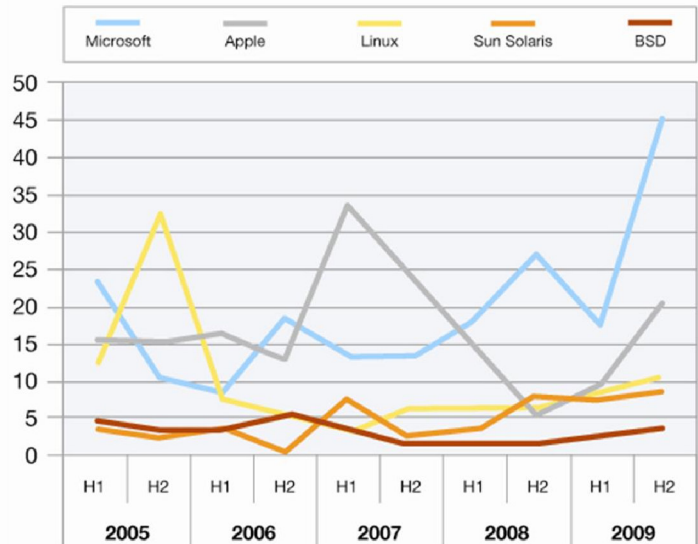
آسیب پذیری های سیستم عامل

Vulnerability Disclosures Affecting Operating Systems
2005-2009



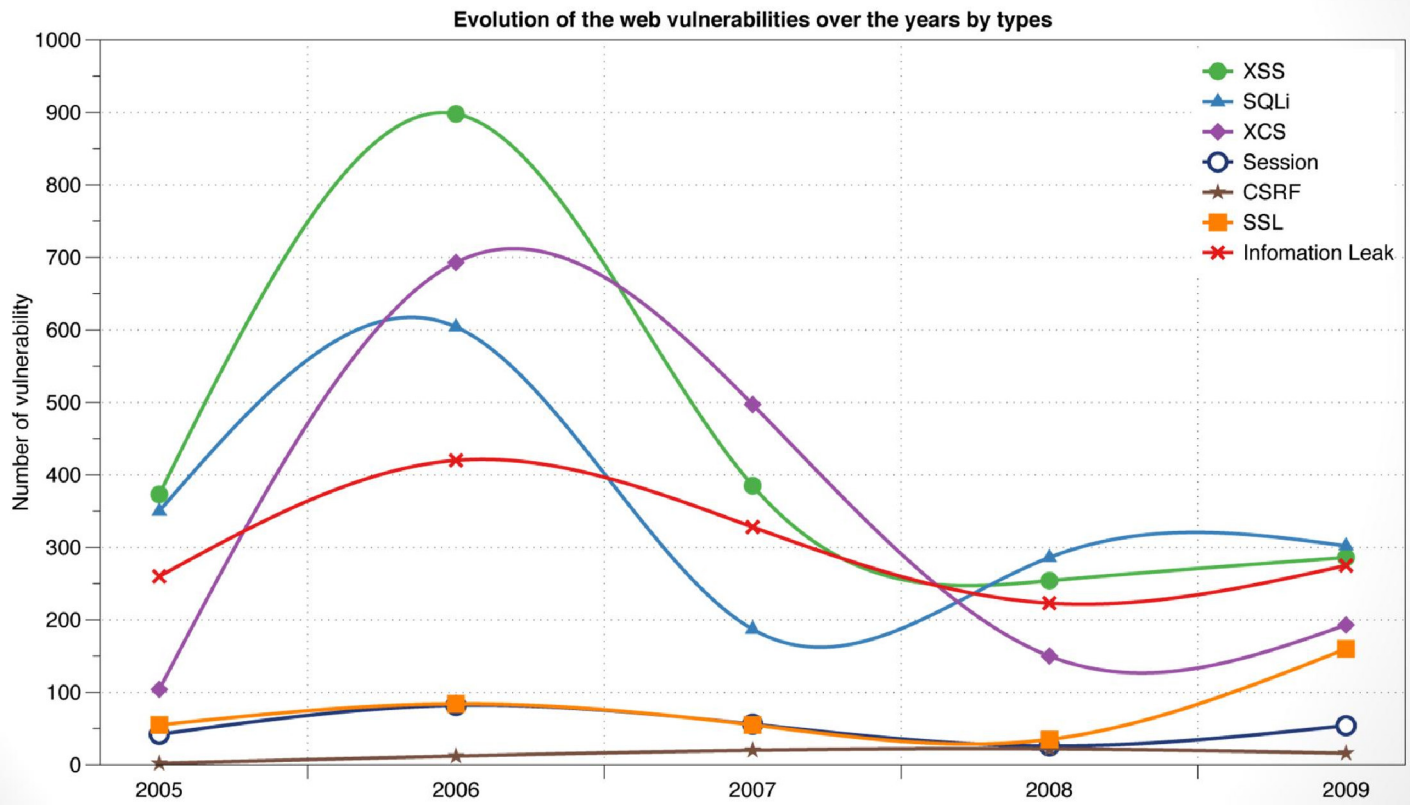
Source: IBM X-Force®

Critical and High Vulnerability Disclosures
Affecting Operating Systems
2005-2009

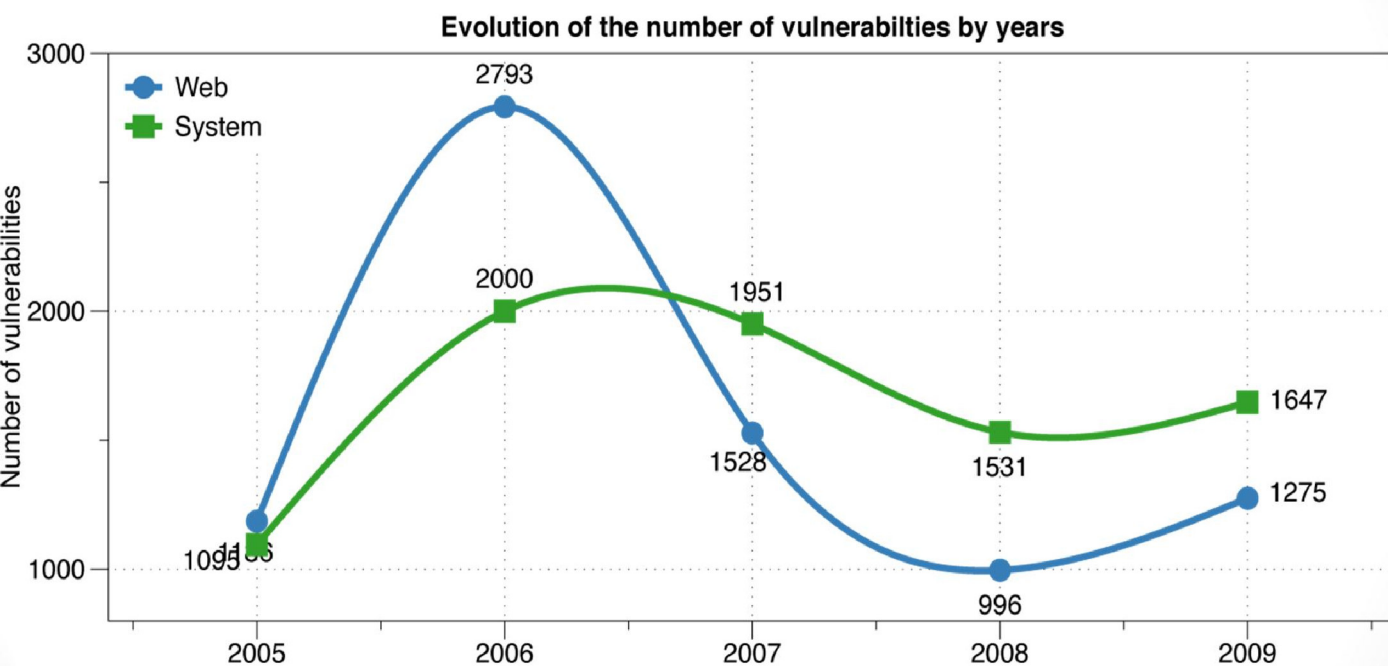


Source: IBM X-Force®

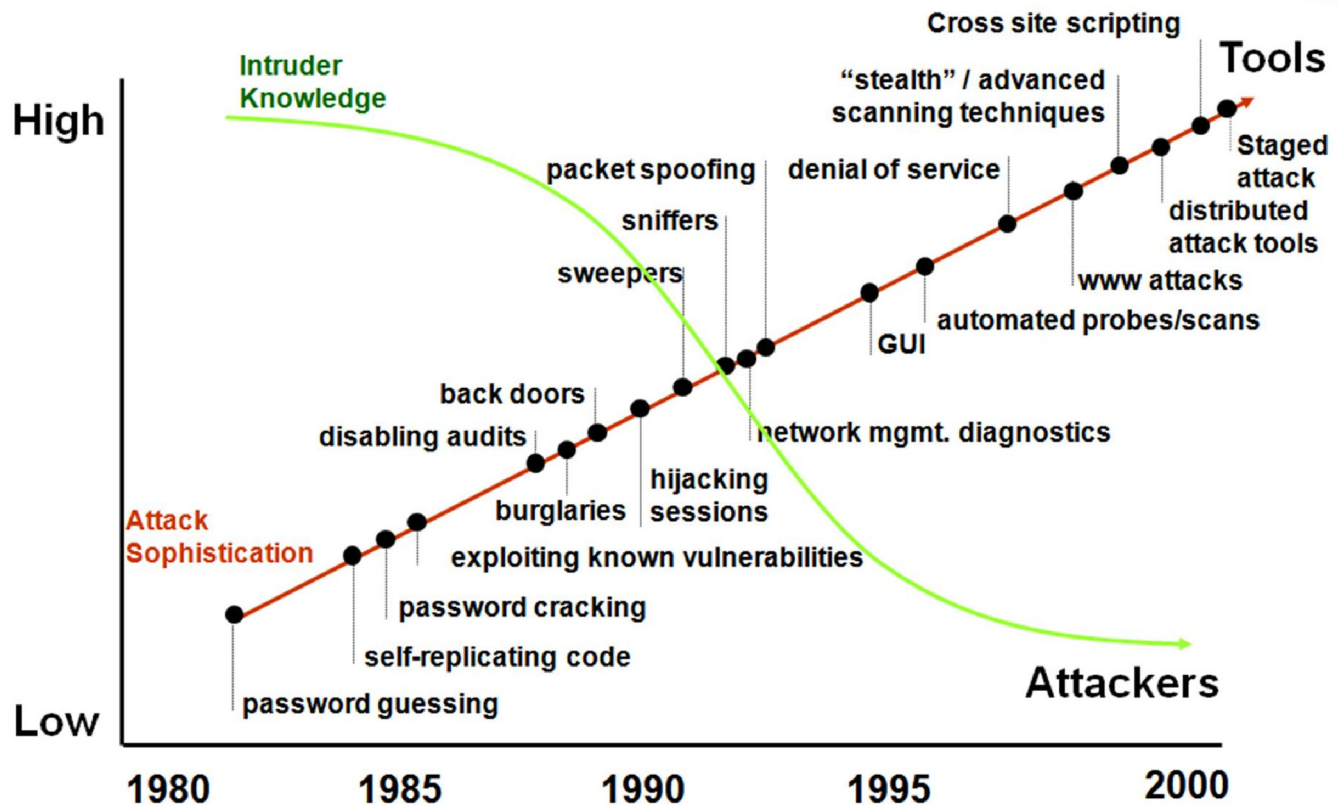
آسیب پذیری های وب



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 هاست
 - نرم افزار
 - سیستم عامل
- آسیب پذیری های شبکه
 - لایه لینک: ARP Spoofing
 - لایه شبکه: IP Forgery
 - لایه انتقال: حدس زدن TCP Sequence-Number
 - لایه کاربرد: کرم های اینترنتی

لایه لینک: ARP Spoofing

- پروتکل ARP برای پیدا کردن آدرس Ethernet یک آدرس IP استفاده می شود.
- ماشین حمله کننده می تواند به درخواست های ARP پاسخ دهد و بسته های 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 می شوند:
 - Initial Sequence Number (ISN)
 - در بعضی از پیاده سازی های TCP، ISN بعد از هر اتصال به اندازه k واحد افزایش می یابد.

$C \rightarrow S: SYN(ISN_C)$

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

$C \rightarrow S: ACK(ISN_S)$

$C \rightarrow S: data$

حَدَس زدن TCP Sequence-Number

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

$X \rightarrow S: SYN(ISN_X)$

- سپس X هویت T را جعل می کند $S \rightarrow X: SYN(ISN_S), ACK(ISN_X)$

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

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

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

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

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 شبکه 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 کارت های 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 آن ها
- شناسایی کردن (Detect)
- مدارا کردن (Tolerate)
- تا جای ممکن اثر حمله را کم کردن
- باز یافتن (Recover)

تأمین امنیت

- امنیت هاست
- راحت تر قابل کنترل است
- مدل های خوبی برای تأیید هویت و اجازه طراحی و پیاده سازی شده است
- امنیت شبکه
- همه می توانند به شبکه متصل باشند
- نحوه اتصال ماشین ها به شبکه قابل کنترل نیست

تأمین امنیت شبکه

- جایگزینی ساختارهای آسیب پذیر
- استفاده از رمزنگاری به جای تأیید هویت مبتنی بر آدرس
- استفاده از فایروال برای ایجاد محدودیت در دسترسی به سرویس های مهم
- بررسی شیوه مند و پی در پی برای جلوگیری از حملات
- مانیتورینگ شبکه برای شناسایی ARP Spoofing
- پایش شبکه