Hacking

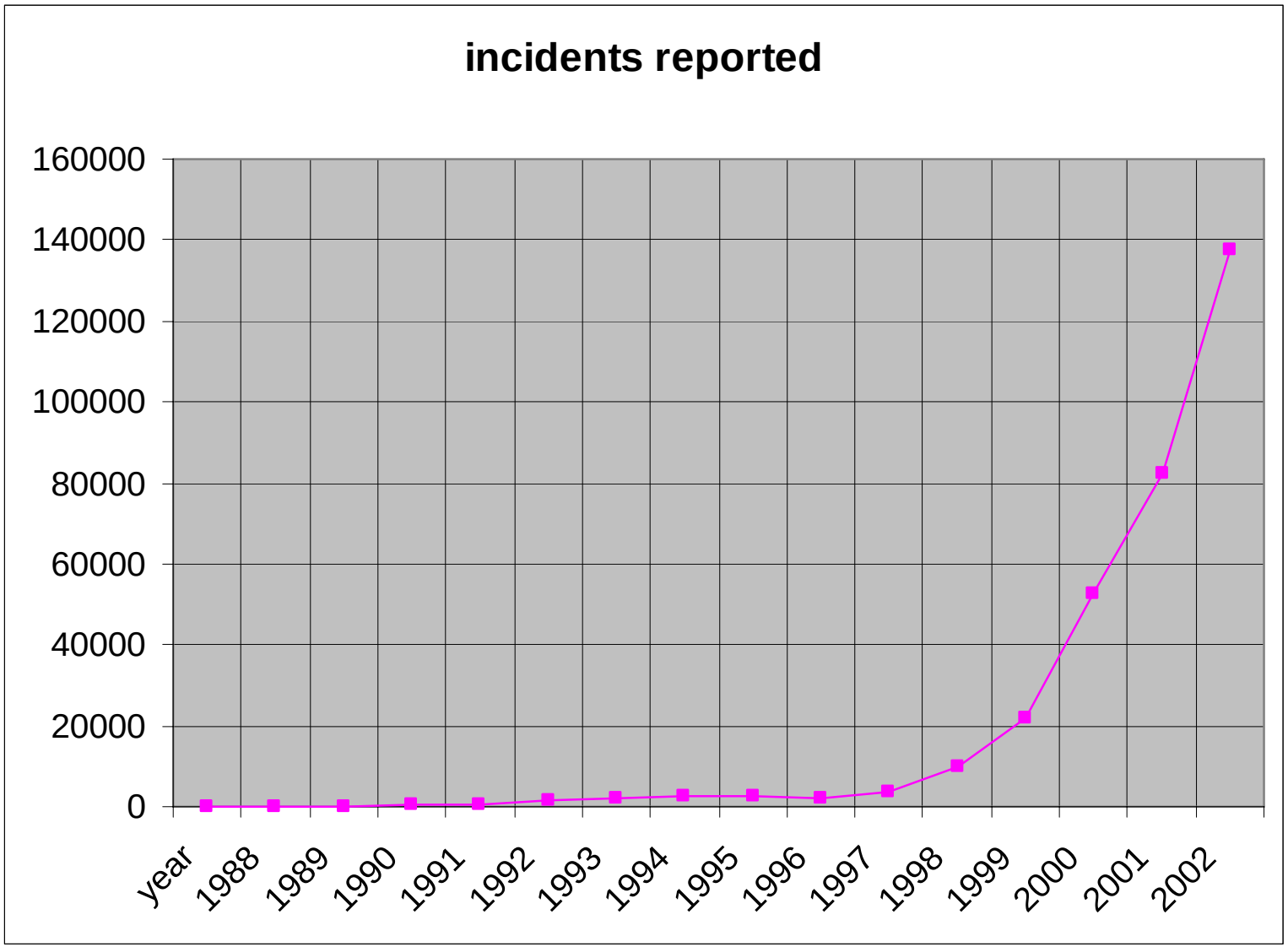
InfoPoint 07.12.2005

Jörg Wüthrich

Inhalte

- Rund um das Thema Hacking
- Angriffs-Techniken
  - Session Handling
    - Cross Site Scripting (XSS)
  - SQL-Injection
  - Buffer Overflow

Anzahl Vorfälle

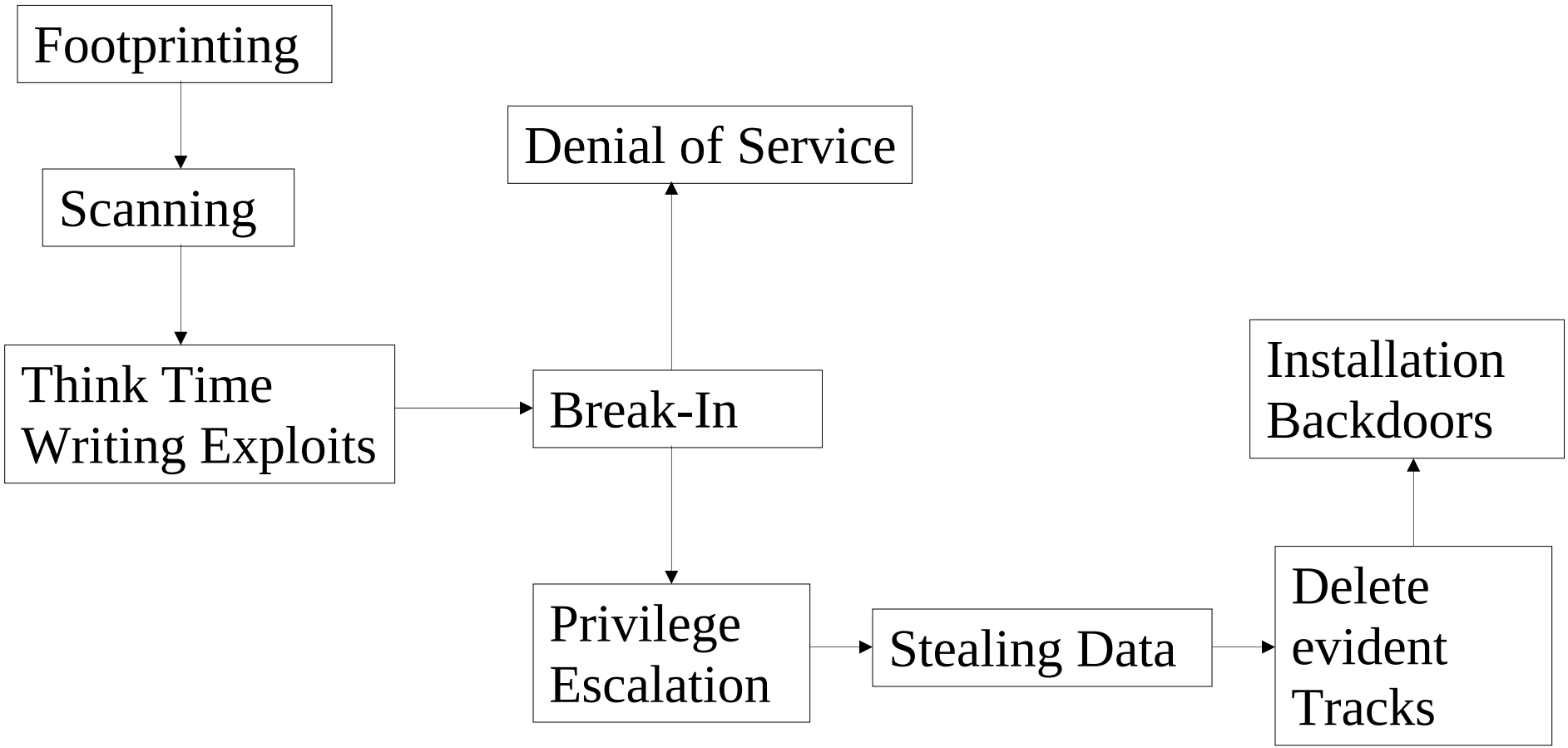


Quelle:
www.cert.org/stats/#incidents

year	incidents
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	52658
2002	82094
2003	137529

„Standard“-Vorgehen eines Hackers

Quelle: "Hacking exposed"



Inhalte

- Rund um das Thema Hacking
- Angriffs-Techniken
  - Session Handling
    - Cross Site Scripting (XSS)
  - SQL-Injection
  - Buffer Overflow

Session Handling

- Warum Sessions?
  - HTTP-Protokoll ist zustandslos
  - Tracking von benutzer-spezifischen Zuständen auf dem Server über mehrere Requests hinweg

Session Handling

- Session Identifikatoren
  - Cookies
  - versteckte Felder in Html-Formularen
  - URL-Parameter (http://www.foo.com/app?id=xx)

Session Handling Attacken

- Ziel
  - Übernahme einer fremden Benutzer-Session durch Stehlen, Erraten oder Unterschieben
- Arten
  - Session Hijacking
    - Diebstahl der Session nach Login des Users
  - Session Fixation
    - Angriff bevor sich User eingeloggt hat (Unterschieben)

Session Hijacking

- Abfangen
  - Sniffing (passiv)
  - Cross Site Scripting (XSS – aktiv)
- Erraten
  - Session ID generieren (da vorhersagbar)
- Brute Force
  - mechanisches Durchprobieren von Zeichenfolgen

Session Fixation

Quelle: http://www.csnc.ch/

- Fixation
  - Vorgängiges Festlegen der Session ID
- Voraussetzungen
  - Session über URL Parameter codiert
  - oder serverseitige Bugs, damit Cookie manipuliert werden kann
  - Benutzer nimmt den per E-Mail verschickten Köder an (Social Engineering)

Gegenmassnahmen Session Handling Attacken

- Verwendung von SSL (Sniffing)
- neue Session vergeben nach Login (Sniffing)
- Verwendung von sicheren Cookies (nur bei Verwendung einer SSL-Verbindung schicken; Sniffing)
- echt zufällige Session ID vergeben (Brute Force)

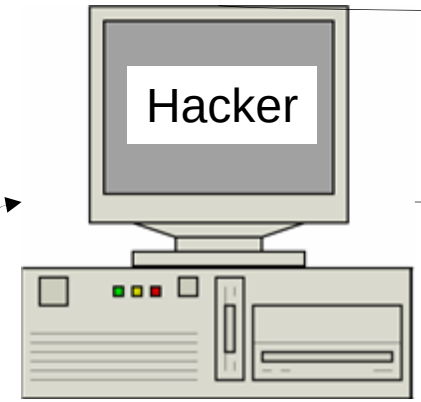
Inhalte

- Rund um das Thema Hacking
- Angriffs-Techniken
  - Session Handling
    - Cross Site Scripting (XSS)
  - SQL-Injection
  - Buffer Overflow

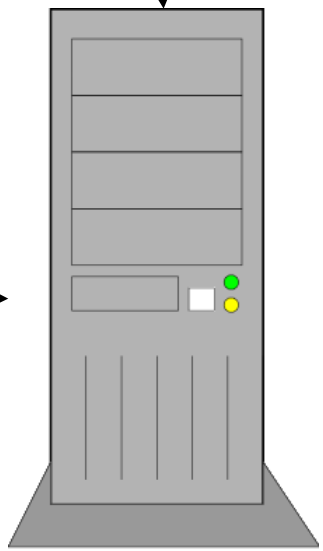
Cross Site Scripting

- Variante, um Session-ID abzufangen
  - z.B. wenn Sniffing nicht möglich (SSL)
- Vorgehen
  - Erzeugen einer Skript-Eingabe, welche auf dem Opfer-Client eine unerwünschte Antwort an den Angreifer auslöst

Cross Site Scripting

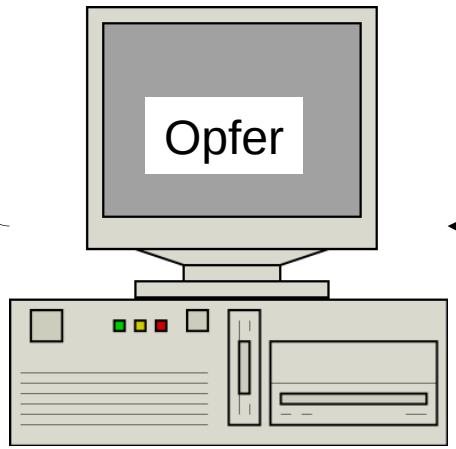


1. Angreifer fügt Skript in Beitrag ein und wartet auf Opfer



4. Angreifer besucht Website und weist sicht mit gestohlenem Cookie aus

3. Skript des Angreifers leitet das Session Cookie weiter



2. Server schickt Website mit Skript und Session-Cookie

Cross Site Scripting

- Demo Cross Site Scripting

Gegenmassnahmen Cross Site Scripting

- Input / Output Filterung (immer beim Server; keine Javascripts im Html-Code)

Inhalte

- Rund um das Thema Hacking
- Angriffs-Techniken
  - Session Handling
    - Cross Site Scripting (XSS)
  - SQL-Injection
  - Buffer Overflow

SQL-Injection

- Übermittlung von Daten an Subsysteme
- Metazeichen-Problem
  - „SELECT * FROM user WHERE name='"
  - + request.getParameter("username") + "'"
  - + and password='"
  - + request.getParameter("password") + "';"
- Absicht Entwickler:
  - SELECT * FROM user WHERE name='smith' AND password='smithpw'

SQL-Injection

- Demo SQL-Injection

Gegenmassnahmen SQL-Injection

- Input Validierung immer serverseitig
- Berechtigungen separieren (versch. User)
- Escape von Metazeichen
- Prepared Statements
  - select * from login where user=?
  - schlecht: “select * from login where user=“ + user;
- Stored Procedures

Encoding "<"

- <
- %3C
- &lt
- <
- &LT
- <
- &#60
- &#060
- &#0060
- &#00060
- &#000060
- &#0000060
- <
- <
- <
- <
- <
- <
- &#x3c
- &#x03c
- &#x003c
- &#x0003c
- &#x00003c
- &#x000003c
- <
- <
- <
- <
- <
- <
- &#X3c
- &#X03c
- &#X003c
- &#X0003c
- &#X00003c
- &#X000003c
- <
- <
- <
- <
- <
- <
- &#x3C
- &#x03C
- &#x003C
- &#x0003C
- &#x00003C
- &#x000003C
- <
- <
- <
- <
- <
- <
- &#X3C
- &#X03C
- &#X003C
- &#X0003C
- &#X00003C
- &#X000003C
- &#X3C
- &#X03C
- &#X003C
- &#X0003C
- &#X00003C
- &#X000003C
- <
- <
- <
- <
- <
- <
- \x3c
- \x3C
- \u003c
- \u003C

Inhalte

- Rund um das Thema Hacking
- Angriffs-Techniken
  - Session Handling
    - Cross Site Scripting (XSS)
  - SQL-Injection
  - Buffer Overflow

Buffer overflow

vulnerable.c:

```
void fn(char* a) {
  char buf[100];
  strcpy(buf, a);
}

main (int argc, char* argv[]) {
  fn(argv[1]);
  printf("the end\n");
}

------

>> vulnerable AAAAAAAAAAAAAA
```

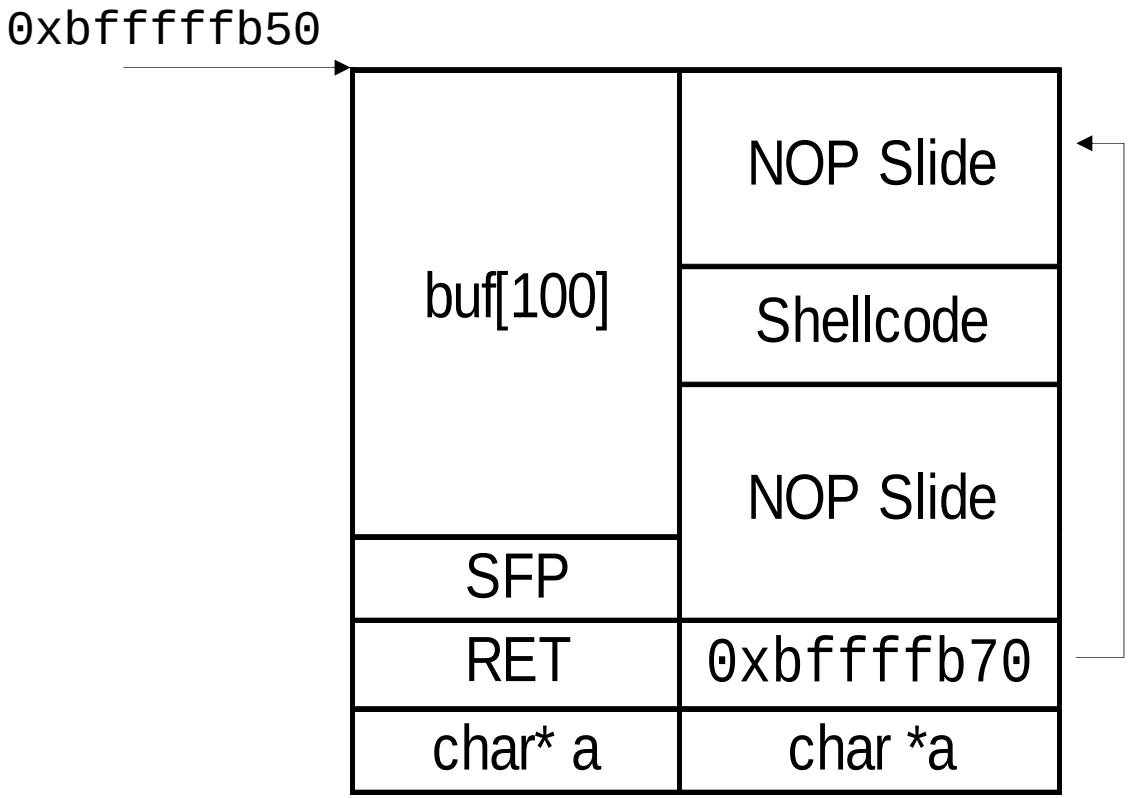
Abbildung "fn" auf dem Stack:

buf[100]	AAAAAAAAAA AAAAA#0…
SFP	0x…
RET	0x…
char* a	char* a

Buffer overflow

- Ziele
  - Kontrolle über Instruction Pointer erlangen
  - Instruction Pointer auf Angreifer-kontrollierten Speicherbereich zeigen lassen

Abbildung mit Buffer overflow:



Gegenmassnahmen Buffer overflow Attacken

- Prüfen, ob Zielspeicher Platz für Source-String hat (z.B. strncpy(buf, param, sizeof(buf))
- wenn möglich Sprachen verwenden, welche automatische Bereichsüberprüfungen durchführen (Perl, Python, Java, …)
- patchen, patchen, patchen

Referenzen

- http://www.owasp.org/ - **O**pen **W**eb **A**pplication **S**ecurity **P**roject
  - WebGoat: Lehr-Applikation zum Verstehen und Ausprobieren von Sicherheitslücken
- http://www.cert.org/ - Carnegie Mellon University's **C**omputer **E**mergenc**y** **R**esponse **T**eam
- http://www.oxid.it/ - Hacker Tool "Cain & Abel" (wäre „ungünstig“, wenn dieses auf einem Geschäfts-PC gefunden würde)
- http://www.csnc.ch/ - Firma, welche auf Security Assessments und forensische Untersuchungen spezialisiert ist -> diverse Papers mit leicht verständlichen Erklärungen
- http://www.hackingexposed.com/ - Companion Website zu einem Buch rund ums Hacking
- http://www.heise.de/security/artikel/37958 - Buffer overflow (in Deutsch)
- http://www.sans.org/rr/whitepapers/securecode/386.php - Buffer overflow (detailliert in Englisch)
- Sicherheitsrisiko Web-Anwendung – Wie Webprogrammierer Sicherheitslücken erkennen und vermeiden; ISBN 3-89846-259-3
- The art of intrusion – von Kevin Mitnick; weltweit bekannter ehemaliger Hacker spezialisiert auf Social Engineering; ISBN 0-76456-959-7