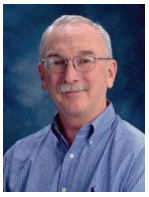
Security

CSCI 334
Stephen Freund




http://roseandcrownpa.com/index.html

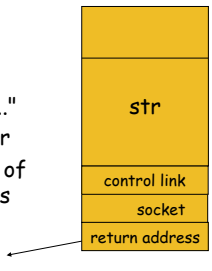
Principles of Security Design

- Least Privilege
  Give each principle the minimum access need to accomplish its task [Saltzer & Schroeder 75]
- Small Trusted Computing Base
  TCB: part of a system that must work to ensure the proper functioning of the whole system.

Stack Smashing

```
void readName(FILE *socket) {
  char str[512];
  fgets(socket, str);
}
```

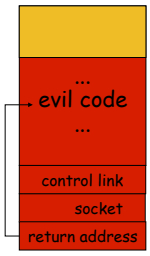
- Send name "asd32423098c0sedh1..."
- Overwrite past end of str
- Replace RA with address of code to perform malicious operation



Stack Smashing

```
void readName(FILE *socket) {
  char str[512];
  fgets(socket, str);
}
```

- Send name "asd32423098c0sedh1..."
- Overwrite past end of str
- Replace RA with address of code to perform malicious operation

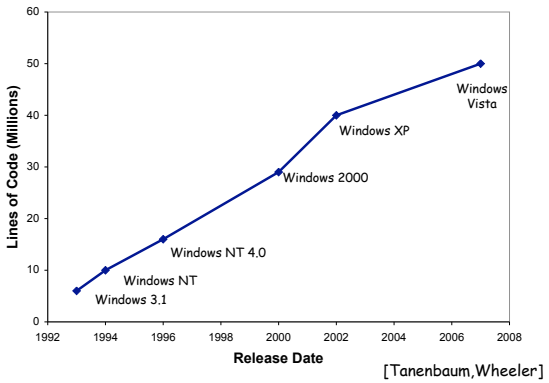


Photoshop Bug (CNet 4/30/2007)

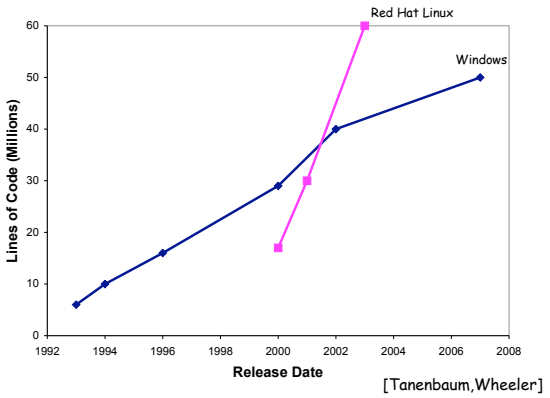
- Security researchers have found a "highly critical" flaw in the portable-network graphics plug-in for the latest version of Adobe Systems' Photoshop Creative Suite.
- The vulnerabilities reported on Monday can be exploited via a boundary error in the PNG.8BI Photoshop format plug-in when processing PNG files. Using a malicious PNG file, attackers can exploit the flaws to launch a *buffer overflow attack* to compromise the user's system...

Context Has Changed

• TCB	Small →	Huge
• Connections	Isolated →	Pervasive Net
• Sys Admins	Skilled →	You and Me
• Vendors	Few →	Many
• Delivery	Physical →	Electronic
• Update freq.	Seldom →	Constant
• Update size	Whole →	Small parts
• Executables	Large Apps →	email, scripts, Active/X, Javascript, plugins,...



[Tanenbaum,Wheeler]



[Tanenbaum,Wheeler]

Recent Attacks

- CERN Vulnerability Notes Database

  http://www.kb.cert.org/vuls/

Bits

Business • Innovation • Technology • Society

May 5, 2010, 1:57 PM

Facebook Security Flaw Publicizes Private Chats

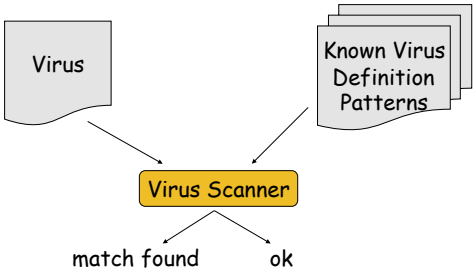
By NICK BILTON

The security flaw allowed users to see active chats and friend requests on a friends pages.

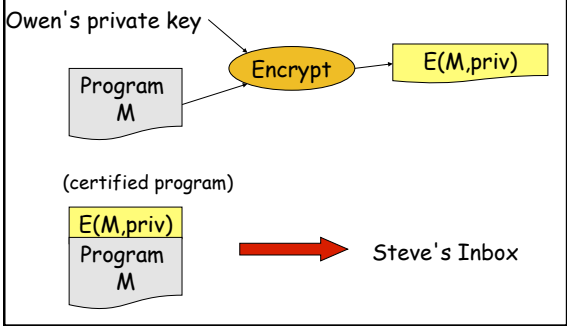
More Technically Savvy Attacks...

- Stuxnet, July 2010
  - Iranian Centrifuges
- "Operation Aurora", 2009 – 2010
  - alleged attack by China against Google, Adobe, Dow Chemical, ...
- South Ossetia War, 2008
  - Georgia systematically hacked news / radio before attacking

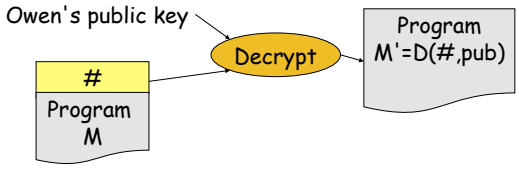
Virus Scanning



Code Signing



Signature Checking



- Does M match M'?
  - yes: Owen signed the code
  - no: Owen did not sign the code