

Security

CSCI 334
Stephen Freund



Principles of Security Design

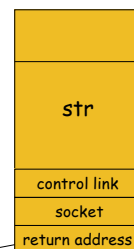
- Least Privilege
Give each principle the minimum access need to accomplish its task [Saltzer & Schroeder 75]
- Small Trusted Computing Base
TCB: part of a system that must work to ensure the proper functioning of the whole system.



Stack Smashing

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

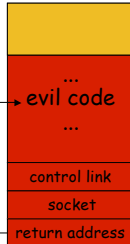
- Send name
"asd32423098c0sedh1..."
- Overwrite past end of str
- Replace RA with address of code to perform malicious operation



Stack Smashing

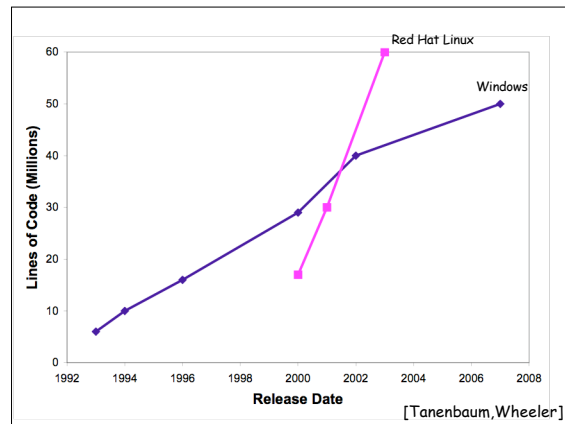
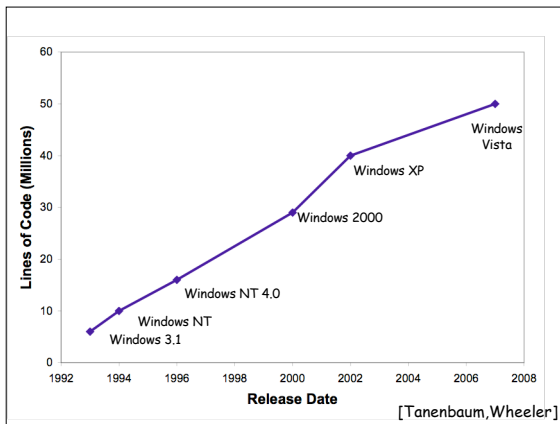
```
void readName(FILE *socket) {
    char str[512];
    fgets(socket, str);
}
```

- 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...



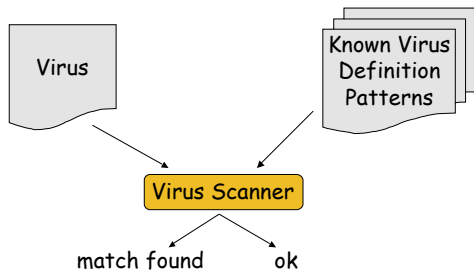
Context Has Changed

- | | | | |
|----------------|------------|---|--|
| • 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, ... |

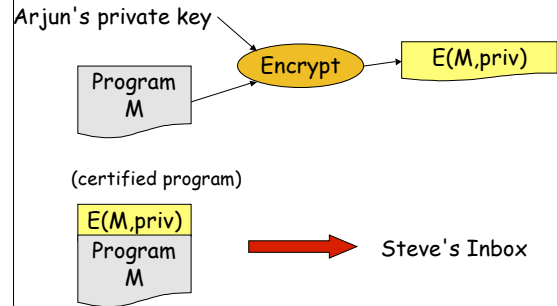
Williams Anti-Virus Center

- WMF vulnerability
- AIM viruses
- Esbot and Zotob viruses
 - Windows Plug&Play
- Troj/BagleDI-M
 - email attachment
- MyDoom-O, Korgo, MyDoom.N, Bagle.AQ, Sasser, ...
 - email attachments...
- GAOBOT / AGOBOT / POLYBOT
 - weak passwords
- ...

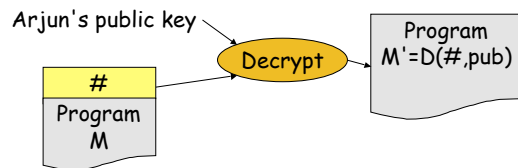
Virus Scanning



Code Signing



Signature Checking



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