

Malicious Mobile Code

SGRP

13. Sept. 2002

„In god we trust, all other we monitor“
[NSA, 2002] National Security Agency)

Compass Security Network Computing

<http://www.csnc.ch/>

Professional Ethical Hacking

Ivan Buetler. Dipl. El. Ing. HTL, STV
ivan.buetler@csnc.ch

Compass Security Services

- Security Assessments
 - Penetration Tests
 - Security Reviews
- Security Training
 - Internet Security Lab
 - Application Security Lab

Imagine ...

... you would have the job

... to compromise a choosen target?

... and to compromize obligation of secrecy
and privacy

The most promising hacking technique

Malicious Mobile Code

Trojan

Virus

Backdoor

Active Scripting

White-collar Crime

Wirtschaftskriminalität

How would you do that?

How do you proceed?

Anti-Virus will deny my Trojan?

Content Filters will stop my EXE Trojan?

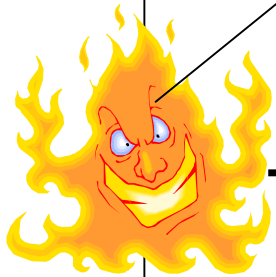
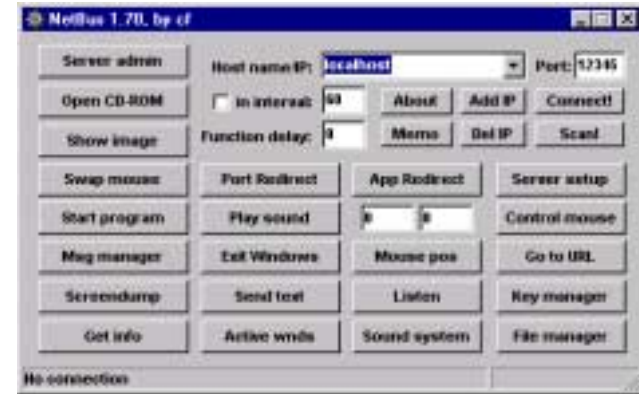
Firewalls will block my Internet attack?

Is Computer Forensic able to trace my activities?

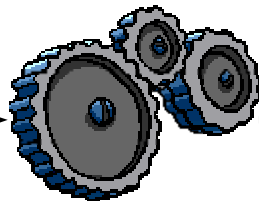
Anti-Virus will deny my Trojan?

-> Demo

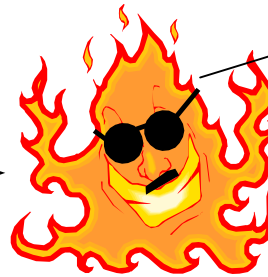
■ Virus Obfuscating



Known Virus



Changing the patterns

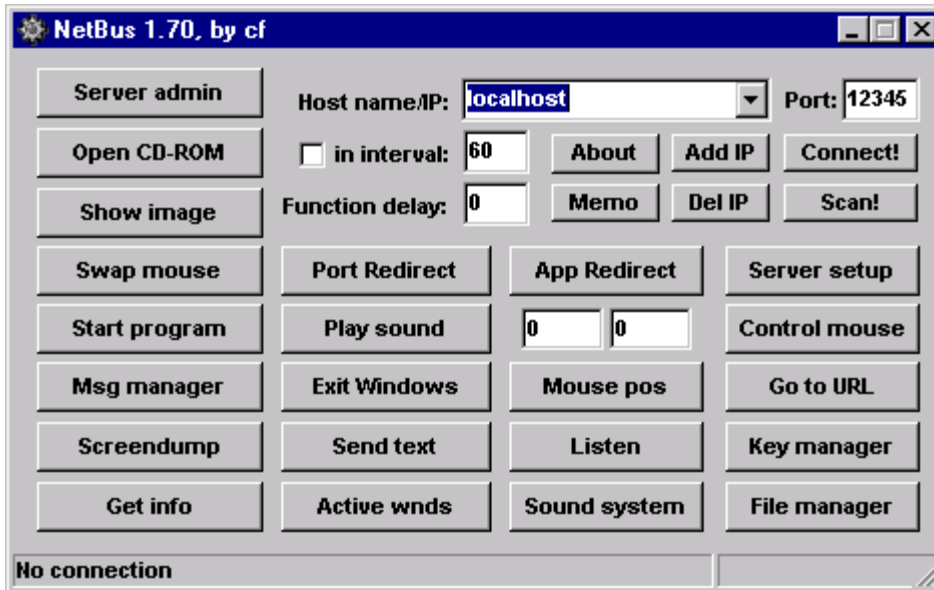
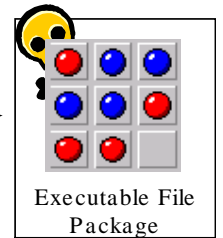
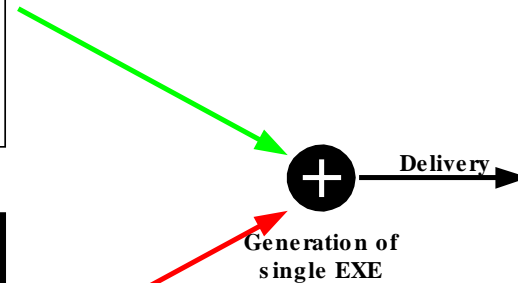
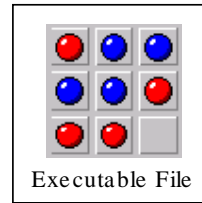


New Virus!

Antivirus software protects the internet from virus attacks in the large.

It does not help you, if someone decides to attack your company with this technique.

■ Virus Hiding Technique



Content Filters will stop my EXE Trojan?

-> Demo

- Bypass Content Filter

"Content-Type: application/binary; name=gobo.exe\n"

"Content-Disposition: attachment; filename=\"gogo.exe\"\n"

"Content-Type: application/binary; name=\"\"gobo.exe\n"

"Content-Disposition: attachment; filename=\"gogo.exe\"\n"

"Content-Type: text/html; charset=utf-7; name=\"gobo.exe\"\n"

"Content-Disposition: attachment; filename=\"gogo.exe\"\n"

"Content-Length: 0\n"

- Bypass SMTP Content Filter (12. Sept. 2002)

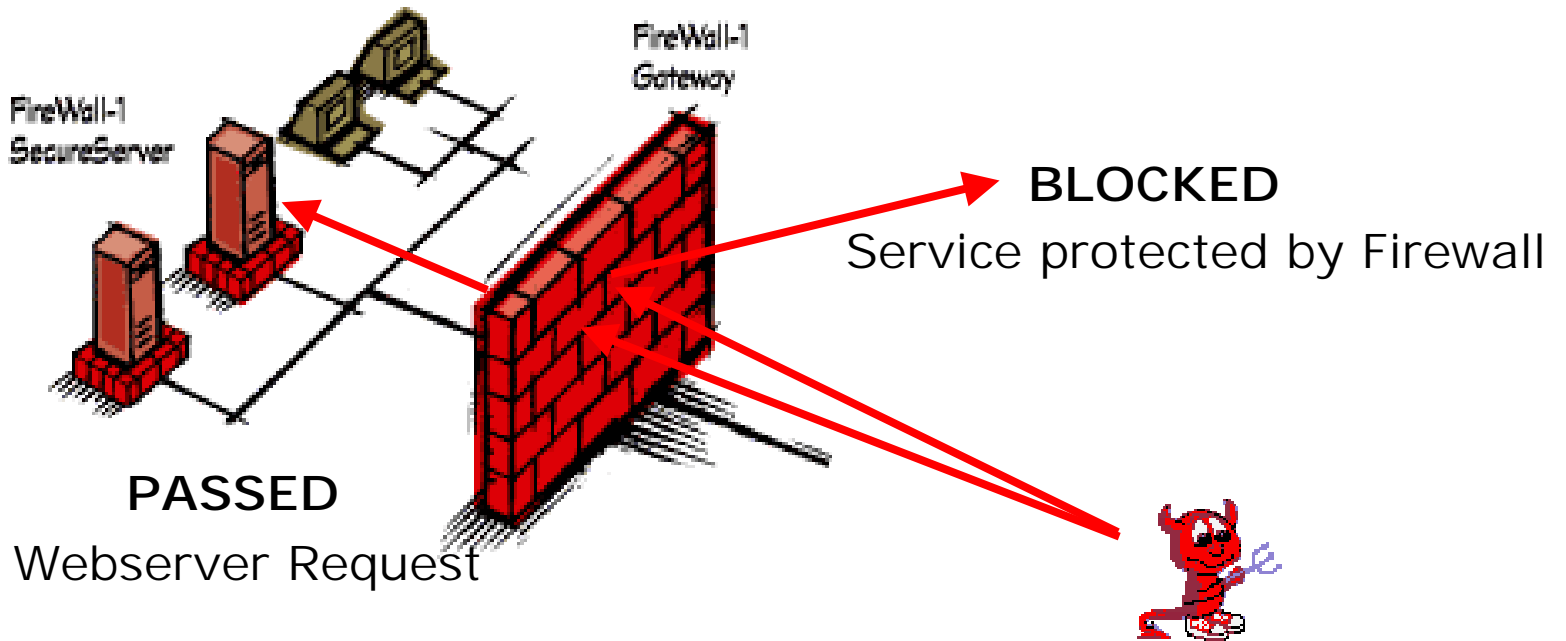
<http://www.securiteam.com/securitynews/5YP0A0K8CM.html>

The feature called "Message Fragmentation and Reassembly" (RFC2046, section 5.2.2.1) allows anyone to bypass most of the security restrictions imposed on email messages, due to the fact that messages are spliced into smaller segments that will not be detected by virus scanners or other content testing mechanisms.

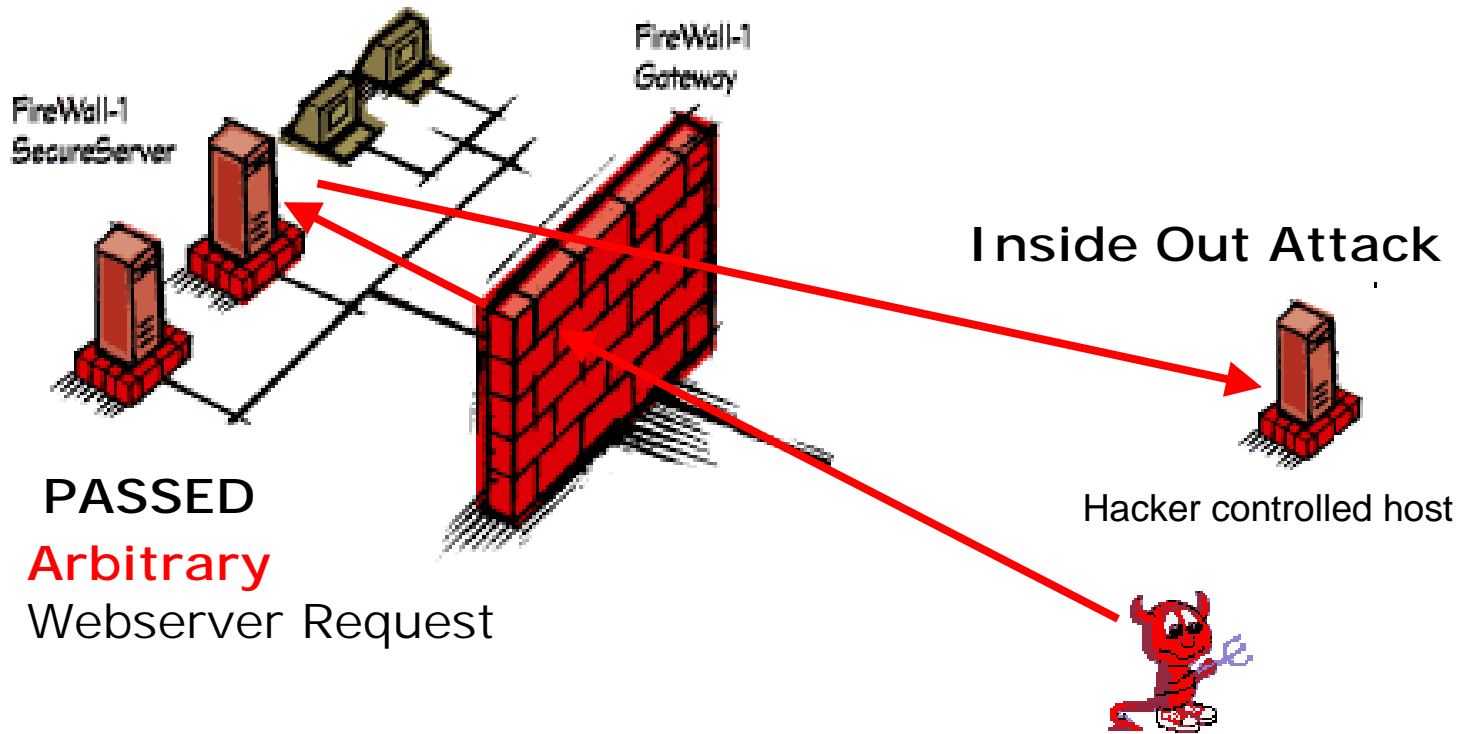
Firewalls will block my Internet attack?

-> Demo

■ Webservice Protection



■ Inside Out



- BufferOverflow PGP (8.Sept. 2002)

Vulnerable systems:

- * PGP Corporate Desktop version 7.1.1

A malicious attacker could create a filename containing:

<196 bytes><eip><9 bytes><readable address><29 bytes>

The encrypted archive could then be sent to the target user; potentially via a Microsoft Outlook attachment. The email attachment could have a filename such as "foryoureyesonly.pgp" or "confidential.pgp". When the unsuspecting user decrypts the archive (either via autodecrypt or manual), the overflow will occur if the file within the archive has a long filename.

In some cases, the attacker may also obtain the pass phrase of the target user. PGP crashes immediately after the decryption of the malicious file and before the memory containing the pass phrase is overwritten.

- Buffer Overflow Apple QuickTime (13.Sept. 2002)

Vendor Response:

Apple was notified of this issue by @stake on May 13, 2002.

Apple has resolved this issue within QuickTime 6 which can be downloaded from <http://www.apple.com/quicktime/>.

Vulnerable systems:

- * Apple QuickTime ActiveX version 5.0.2

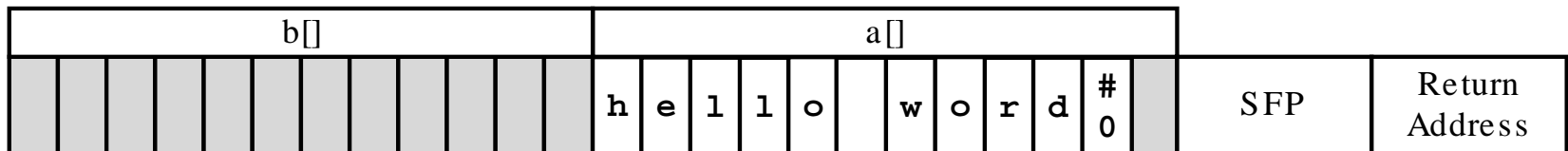
Apple QuickTime is a known media player. There is a buffer overrun caused by the way that the QuickTime ActiveX component handles the "pluginspage" field when parsed from a **malicious remote or local HTML page**. This can allow the execution of arbitrary computer code

- Normal writing to a buffer

```
int main(int argc, char* argv[])
{
    char a[12];
    char b[12];

    strcpy(a, "hello world");
    strcpy(b, "12345678901234");
    cout << "a=" << a;
}
```

Allocated Memory

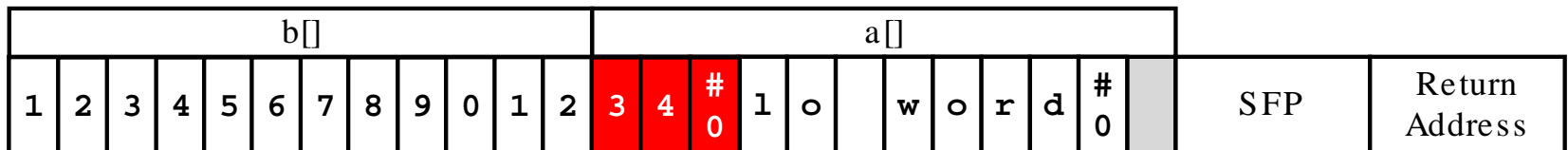


- Writing over the end of the buffer (overflow)

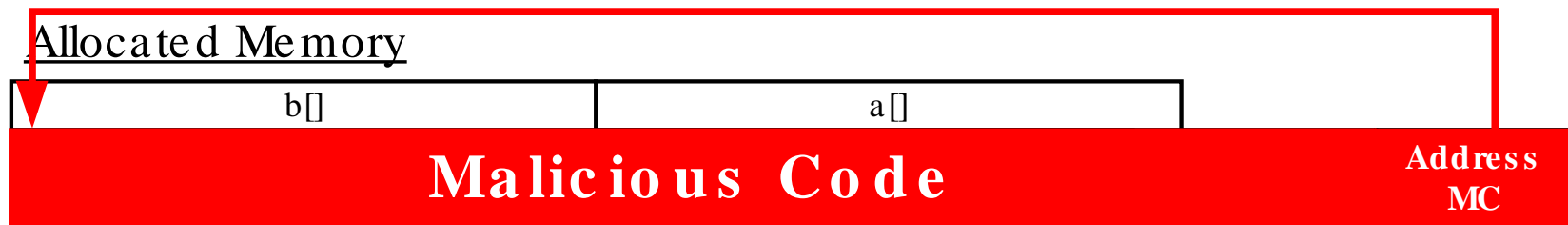
```
int main(int argc, char* argv[])
{
    char a[12];
    char b[12];

    strcpy(a, "hello world");
    strcpy(b, "12345678901234");
    cout << "a=" << a;
}
```

Allocated Memory

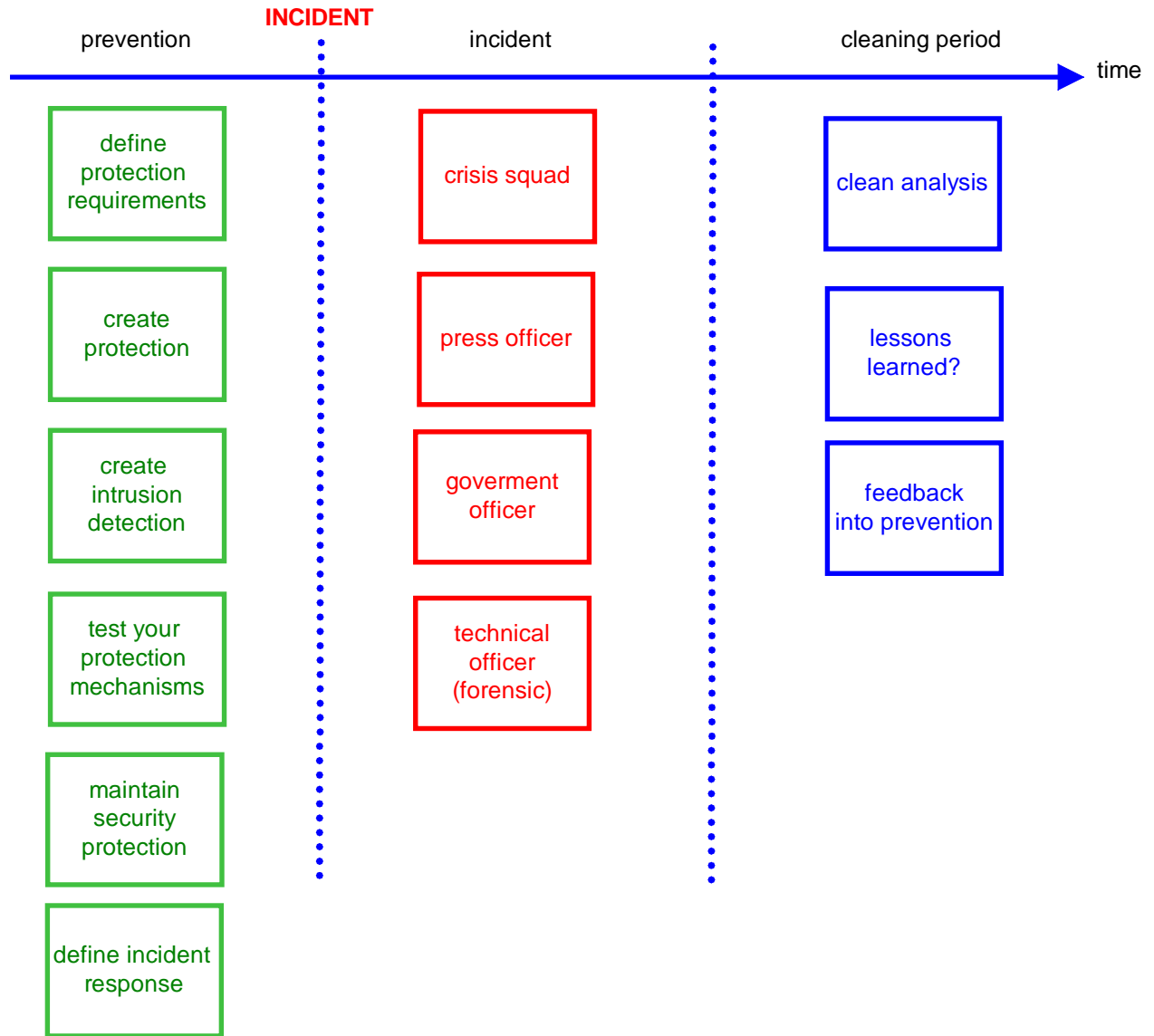
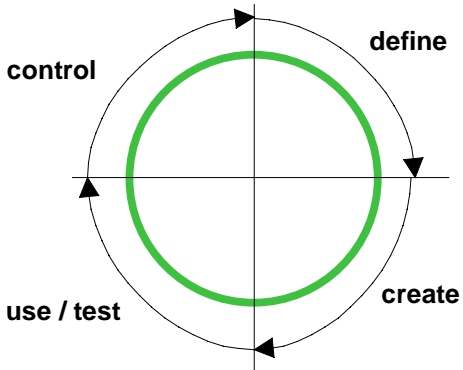


- Writing over the end of the buffer into the Return Address allows execution of arbitrary code. (Note that this technique bypasses authentication and access control!)
- What to do in short: Write malicious code to buffer b[], but overwrite SFP and Return address. **Return Address points finally to the beginning of the malicious code!**



Is Computer Forensic able to trace my activities?

**Let'z wait for
„Forensic im IT Umfeld“**





Compass Security AG
Glärnischstrasse 7
Postfach 1671
8640 Rapperswil

info@csnc.ch

<http://www.csnc.ch/>

Tel: 055 214 41 60

Fax: 055 214 41 61