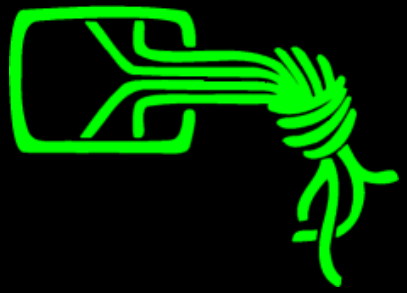


Personal Firewalls

Chaos Seminar
Chaos Computer Club Ulm
http://ulm.ccc.de

Alexander Bernauer
Jonathan Häberle
Ansgar Wiechers

Übersicht

- Grundlagen TCP/IP
- Funktionsweise einer PFW
- Angriffe von außen
- Angriffe von innen
- Ärger mit PFW
- Fazit
- Q&A und Diskussion

Grundlagen

- OSI
- IP
- UDP
- TCP

OSI Modell

Anwendung
Darstellung
Sitzung
Transport
Netzwerk
Sicherung
Bitübertragung

Internet Protocol (IP)

- Jeder Teilnehmer hat eindeutige Adresse
- Netzwerk kennt jede Route
- IPv4: 32 Bit Adressen
- IPv6: 128 Bit Adressen
- Verbindungslos
- Unzuverlässig

User Datagram Protocol (UDP)

- Multiplexer
- 65535 Ports
- Verbindungslos
- Unzuverlässig

Transmission Control Protocol (TCP)

- Multiplexer
- 65535 Ports
- Verbindungsorientiert
- Zuverlässig
- Bidirektionaler Datenstrom

Funktionsweise

- Filtern des Netzwerkverkehrs
- Filtern auf Anwendungsebene
- “Verstecken” des Rechners
- Weitere Zusatzfunktionen:
  - Schutz persönlicher Daten
  - Ad-Blocking
  - ...

Funktionsweise

- Kein Austausch der winsock.dll
- Kerneltreiber
- Dienst
- Benutzerschnittstelle (GUI)

Funktionsweise

Name	Schlüssel	Werte	Ordner	Dateien	Teiber	Dienste
Norman 1.3	16	41	9	64	1	1
Outpost 1.0.187	90	258	17	77	1+n	1
ZoneAlarm 5.1 Pro	163	434	8	72	2	1
Sygate 5.5	167	475	8	53	6	1
Kerio 4.1.2	478	692	9	63	1	1
Tiny 6.0.140	1630	1970	16	357	8	5
Norton 2005	3404	5340	23	330	8	8

Funktionen

- Vertrauliche Informationen blockieren
- Firewall reaktivieren
- Computer verbergen
- Eingehenden Datenverkehr abwehren
- Internetzugriff durch Programme verhindern
- Ad-Blocker
- LiveUpdate

Angriffe von außen

- Angriffe auf Dienste
- Angriffe auf PFW
- Alternativen zu PFW

Angriffe auf Dienste

- Dienst soll erreichbar sein
  - Dienst ist Angriffsziel
  - kein Schutz durch PFW möglich
- Dienst soll nicht erreichbar sein
  - PFW ist Angriffsziel
    - Protokollverletzung
    - Buffer Overflow
    - Self DoS

Angriffe auf Dienste

- Witty-Wurm
- ISS BlackICE 3.6
- Stack-Overflow im Protocol-Analyzer
- Verwundbarkeit besteht nur, wenn der Rechner “geschützt” ist ;-)

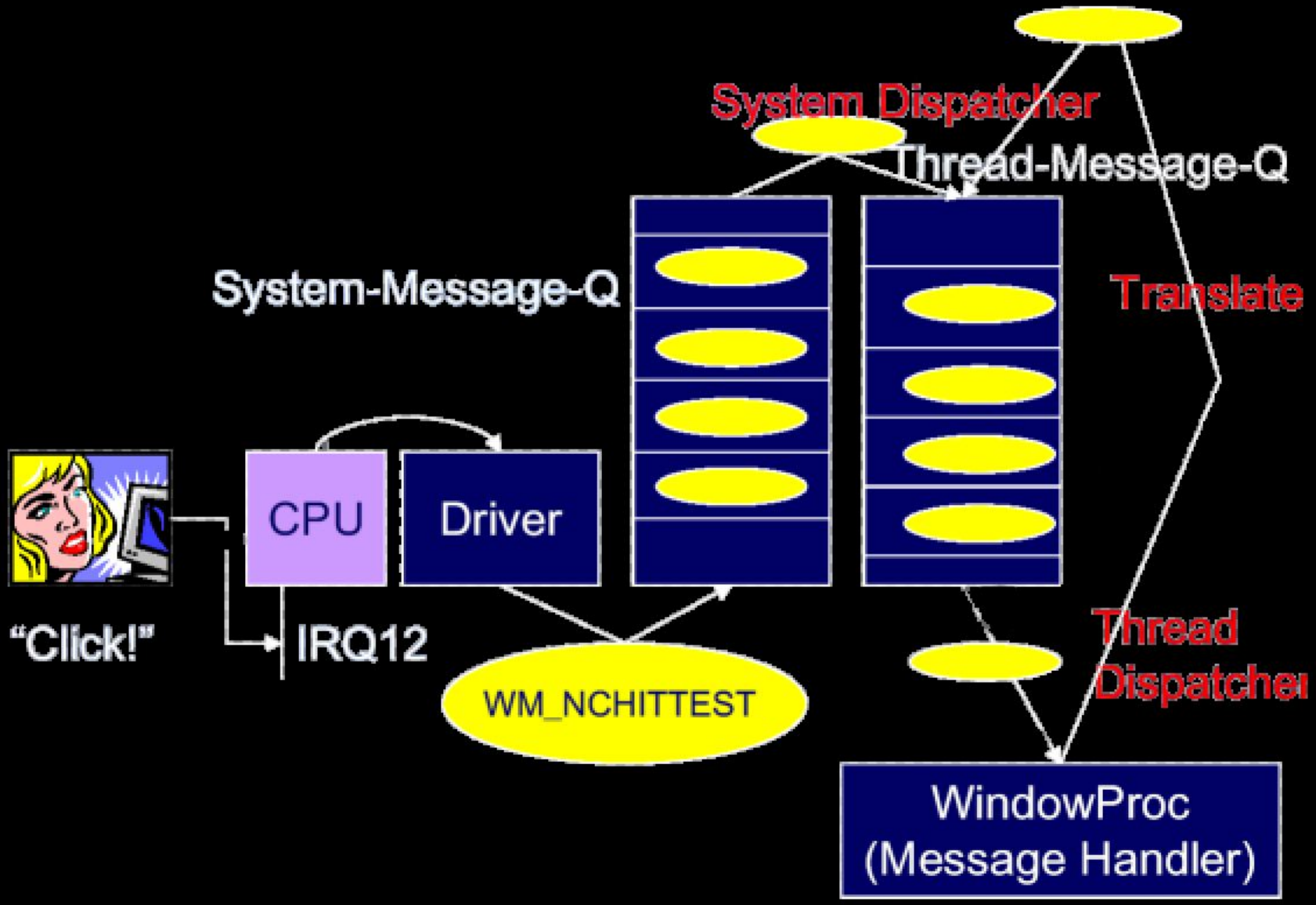
Funktionen

- Vertrauliche Informationen blockieren
- Firewall reaktivieren
- Computer verbergen
- Eingehenden Datenverkehr abwehren X
- Internetzugriff durch Programme verhindern
- Ad-Blocker
- LiveUpdate

Angriffe von innen
(ohne Adminrechte)

- Exkurs: Windows Nachrichten System
- Leak Test
- Privilege Escalation

Windows-Nachrichtensystem



User Simulation

- PFW fragt Benutzer
- Program sendet Nachrichten an Fenster
  - Sicherheitseinstellungen vornehmen
  - auf OK “klicken” :-)

wwwsh

- Trojanisches Pferd startet IE
- Fernsteuerung über Fensternachrichten
- Information base64 kodiert in URL
- Hinweg: URL ansurfen
- Rückweg:
  - Meta Refresh
  - URL Zeile auslesen

Funktionen

- Vertrauliche Informationen blockieren
- Firewall reaktivieren
- Computer verbergen
- Eingehenden Datenverkehr abwehren X
- Internetzugriff durch Programme verhindern X
- Ad-Blocker
- LiveUpdate

Privilege Escalation

- Programmfehler
- Shatter Attacks

Ausspähen leicht gemacht

- Vertrauliche Daten zentral gespeichert
- Internetverkehr wird gescant
- Datei ist “verschlüsselt”
- Verschlüsselung ist nicht personalisiert ...

Danke, Symantec :-)=)

Funktionen

- Vertrauliche Informationen blockieren X
- Firewall reaktivieren
- Computer verbergen
- Eingehenden Datenverkehr abwehren X
- Internetzugriff durch Programme verhindern X
- Ad-Blocker
- LiveUpdate

Ärger mit PFW

- ICMP Blocking
- Systemresourcen

Funktionen

- Vertrauliche Informationen blockieren X
- Firewall reaktivieren
- Computer verbergen X
- Eingehenden Datenverkehr abwehren X
- Internetzugriff durch Programme verhindern X
- Ad-Blocker
- LiveUpdate

Fazit

- PFW kann ihre Aufgabe nicht erfüllen
- PFW bringt weitere Angriffsvektoren ins System
- PFW verändert Systemverhalten
- PFW bremst System aus

PFW sind als Sicherheitssystem
für Endanwender nicht geeignet

Q&A

Links

http://ulm.ccc.de
http://copton.net/vortraege/pfw
http://www.dingens.org