OT-Hacking: Industrieroboter als Sicherheitsrisiko

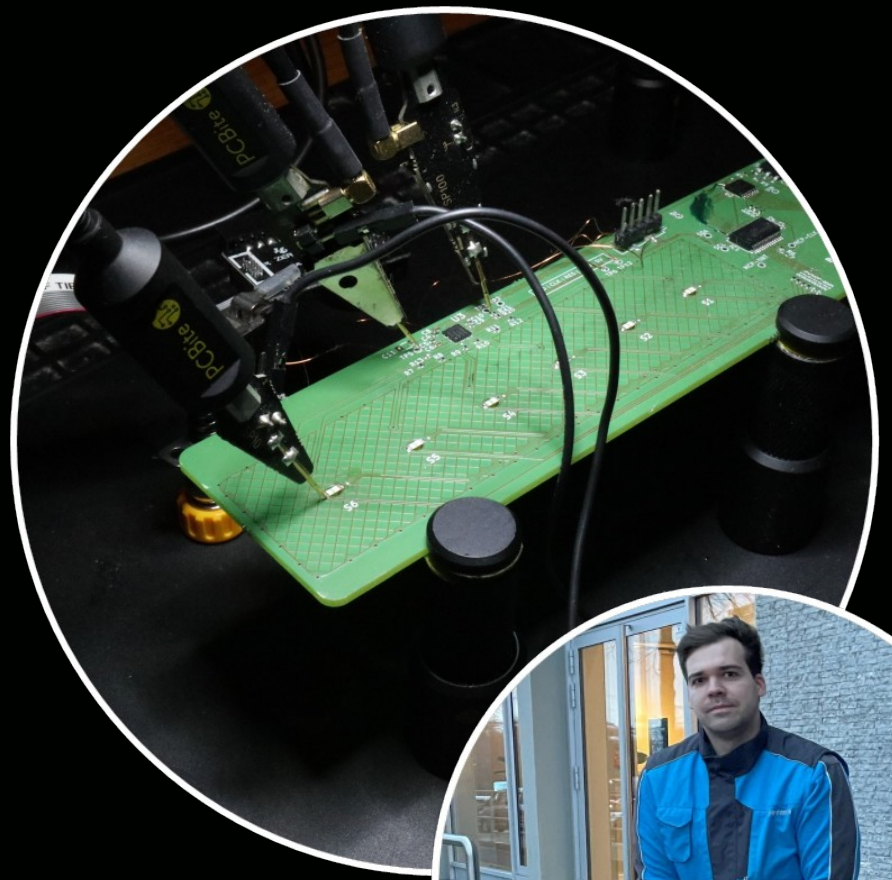
Arne Loose

fernao security force

WHOAMI

Arne Loose

Senior Security Consultant



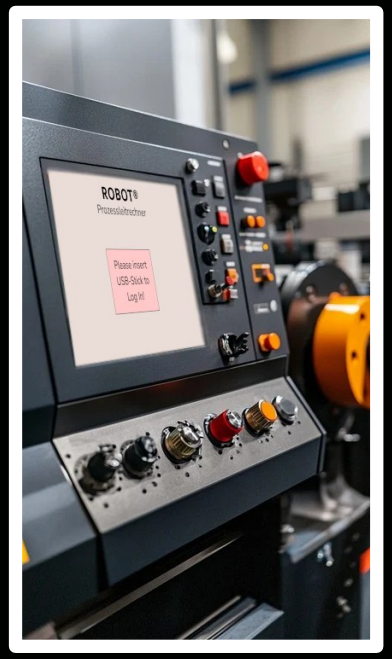
- Embedded
- Automotive
- OT
- Physical Security

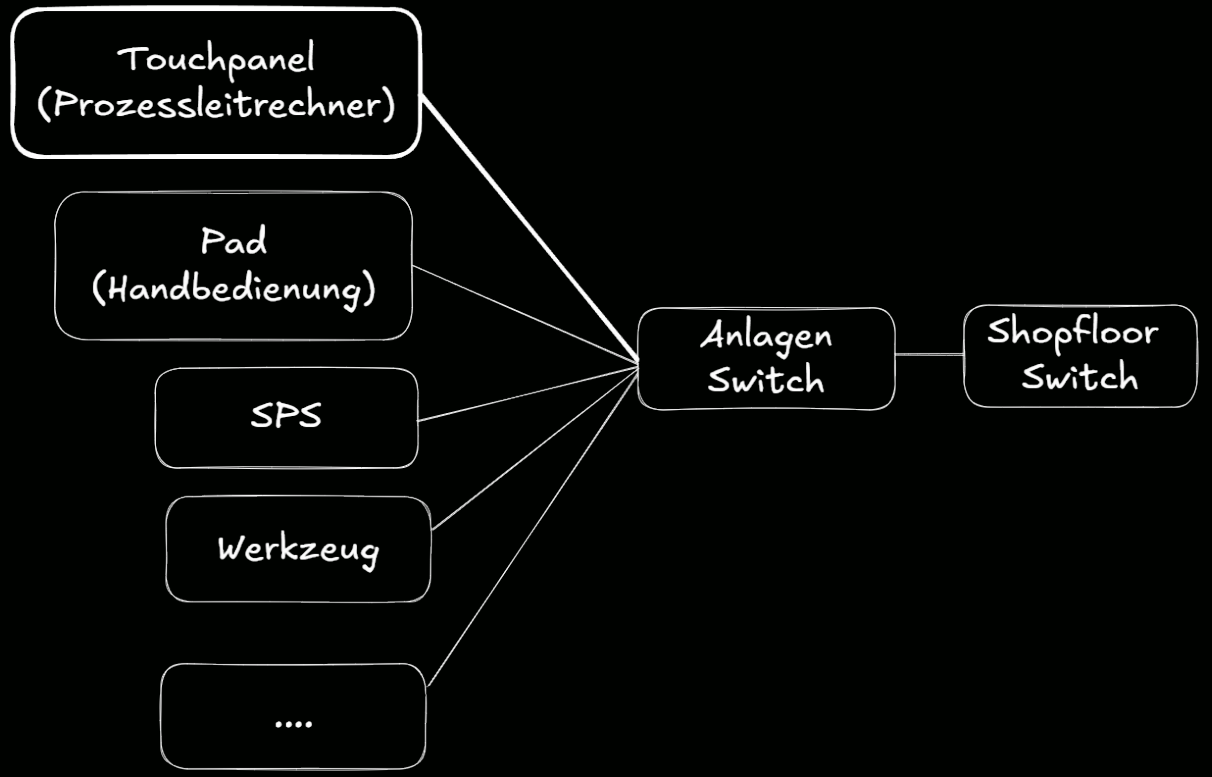
linkedin.com/in/arne-loose

CASE STUDY: Industrieroboter

Ausgangslage: Architektur

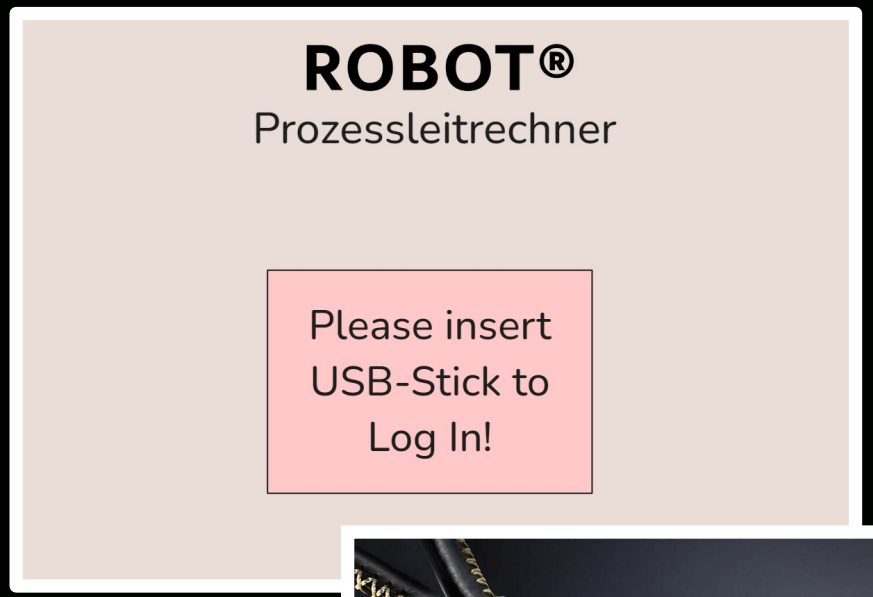
- Ca. **300 Roboter** auf mehrere Werke verteilt
- **Acht „Rechner“** an Anlagen Switch
- Zentrales System: **Prozessleitrechner (Windows XP Embedded)**





Ausgangslage: Sicherheitsmechanismen

Prozessleitrechner („Panel“) in **Kiosk-Modus**
- Eine Anwendung im **Fullscreen-Modus**
- Zugriff auf Betriebssystem nur mit Rolle „Admin“



Anmeldung **über USB-Sticks + Passwort**
- **Standardkomponente** des Herstellers
- **Rollenkonzept** (*Bediener*, *Admin*, *Wartung*, …)
- Ca. **1000 USB-Sticks** im Umlauf

Ausgangslage: Risiken & Angreifermodell

- **Datenintegrität:** Veränderung von Parametern der Anlage
- **Vertraulichkeit:** Auslesen von Daten z.B. zu Prototypen
- **Verfügbarkeit:** Ausfall der Anlage
- **Ausweitung auf Firmennetz?**

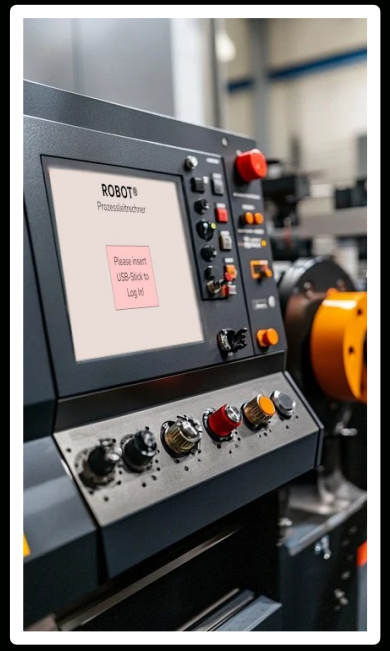
Was kann ein Angreifer mit …

- **physischem Zugang zur Anlage**
- **Zugriff auf USB-Stick**

…

anrichten?

HACK #1: Kiosk Mode



ROBOT®

Prozessleitrechner

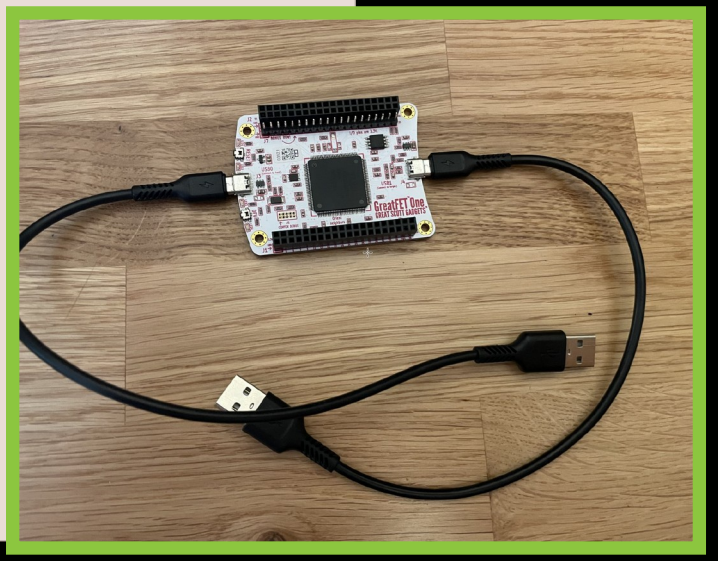
Please insert
USB-Stick to
Log In!

HACK #1: Hacking-Tool „Facedancer“

ROBOT®

Prozessleitrechner

Please insert USB-Stick to Log In!



HACK #1: Kiosk Escape

ROBOT®

Prozessleitrechner

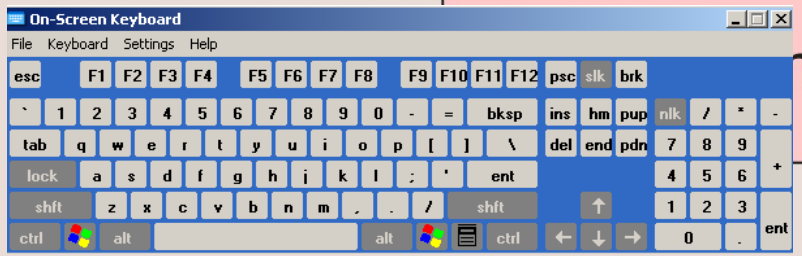
Please insert USB-Stick to Log In!

HACK #1: Kiosk Escape

ROBOT®

Prozessleitrechner

Please insert
USB-Stick to
n!

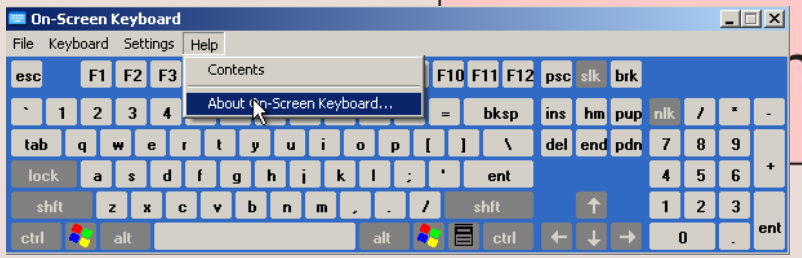


HACK #1: Kiosk Escape

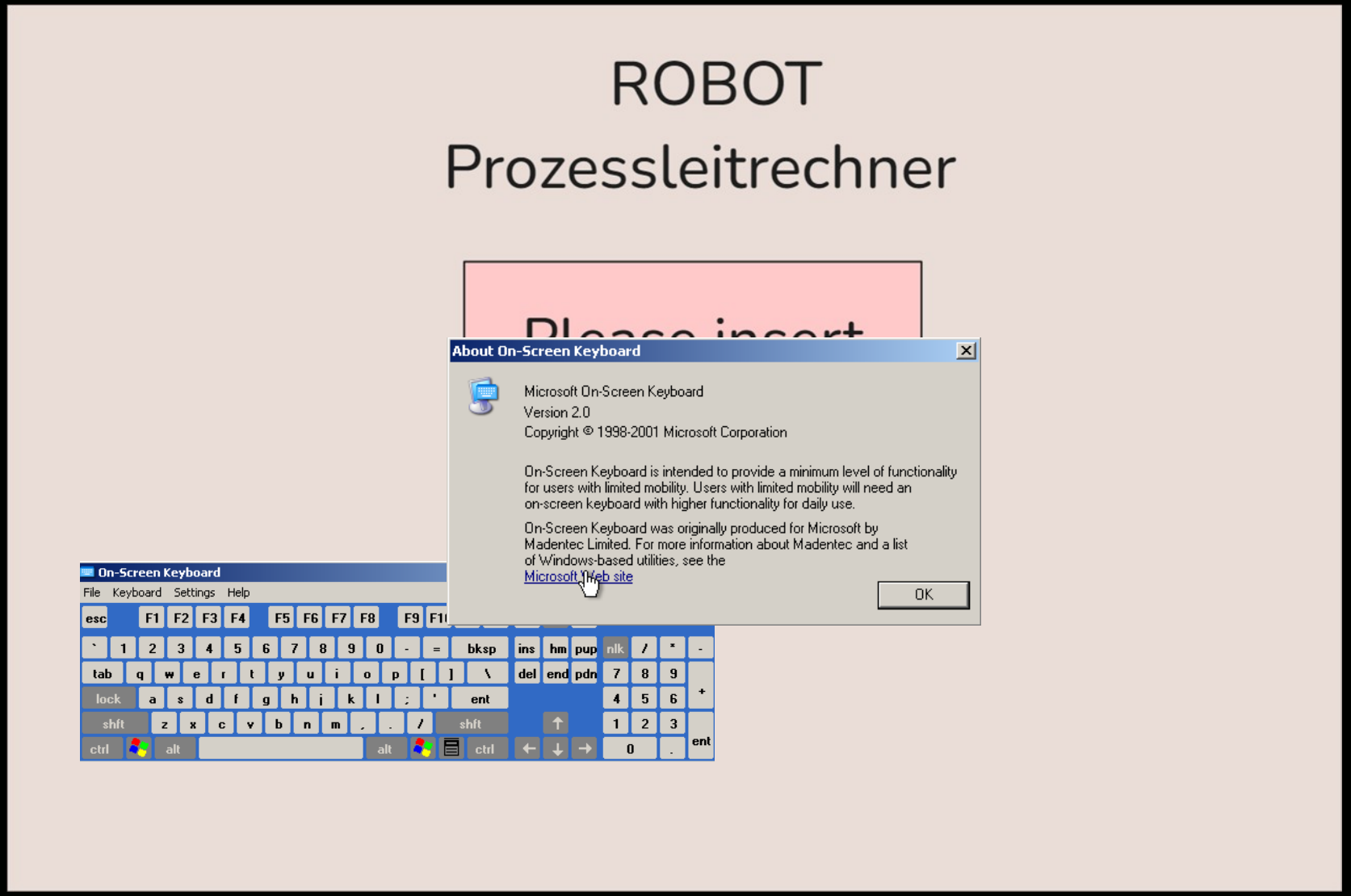
ROBOT®

Prozessleitrechner

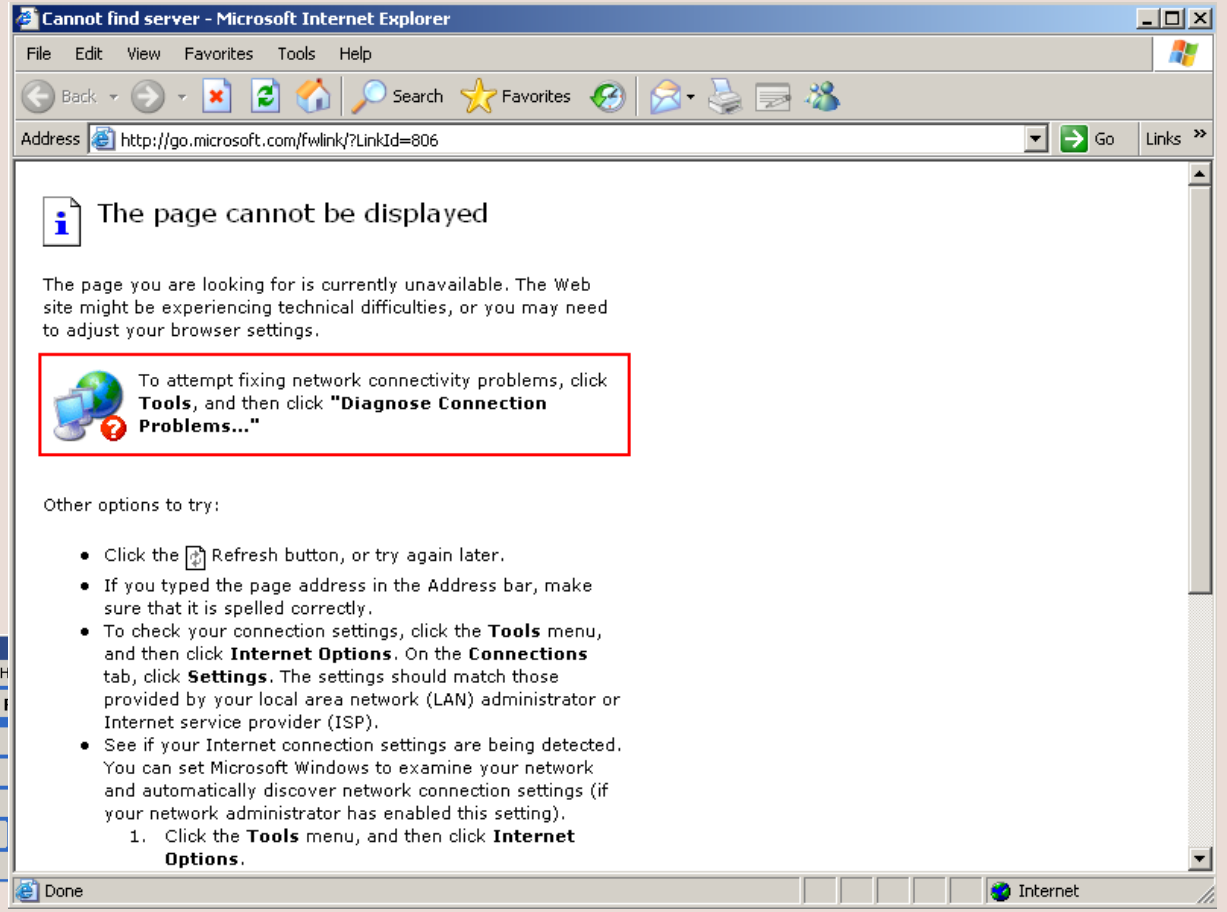
Please insert
USB-Stick to
n!



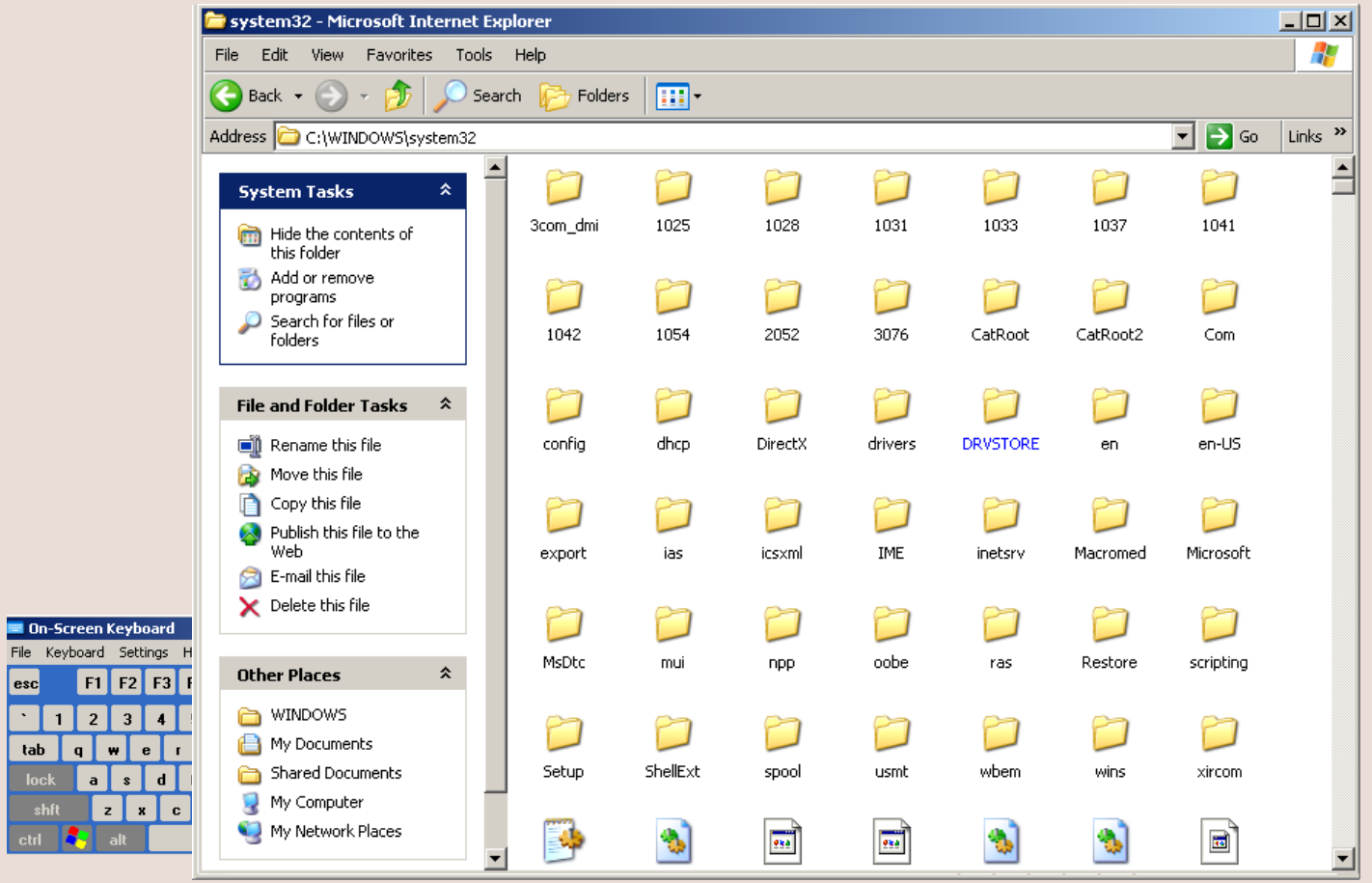
HACK #1: Kiosk Escape



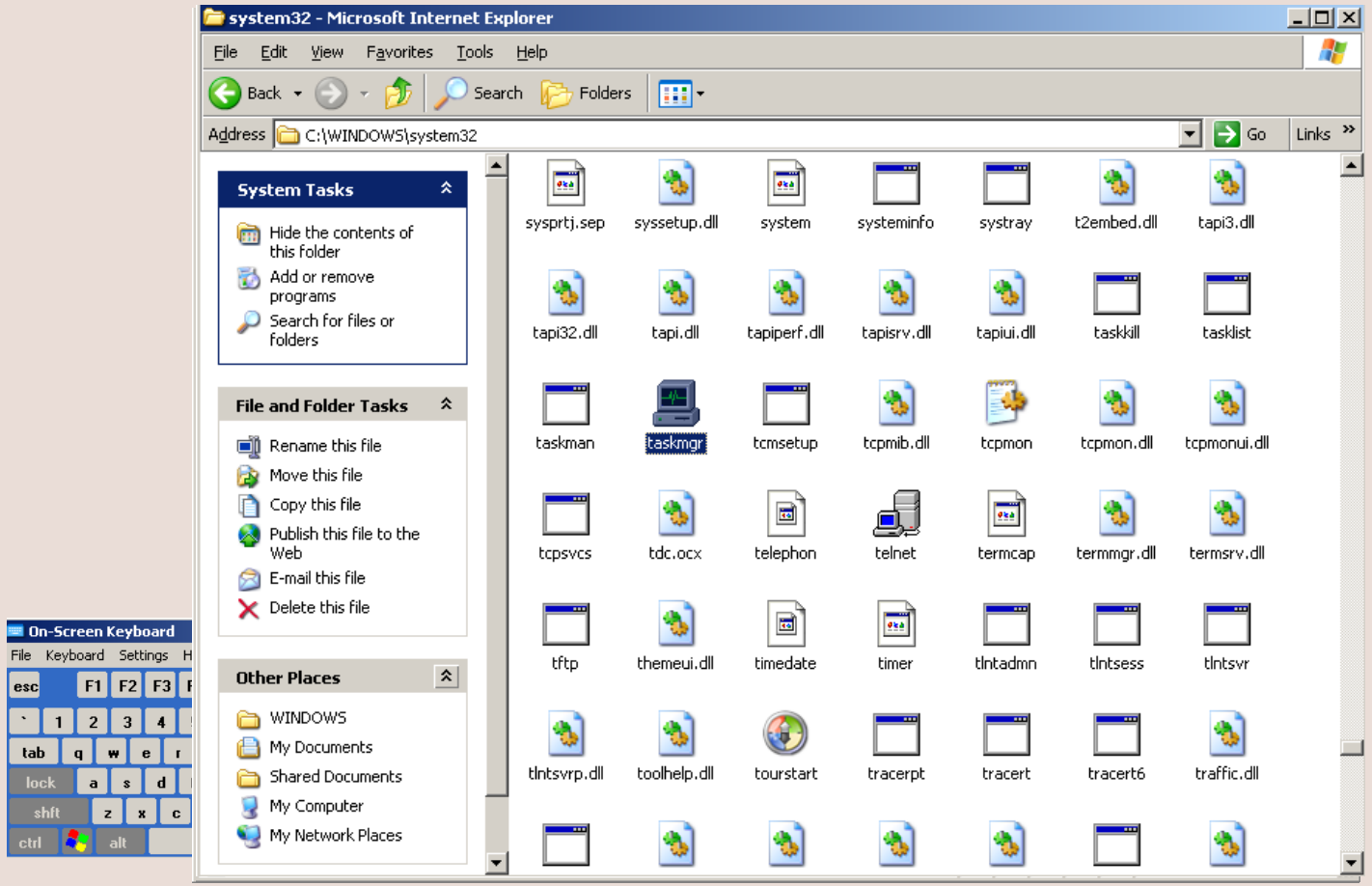
HACK #1: Kiosk Escape



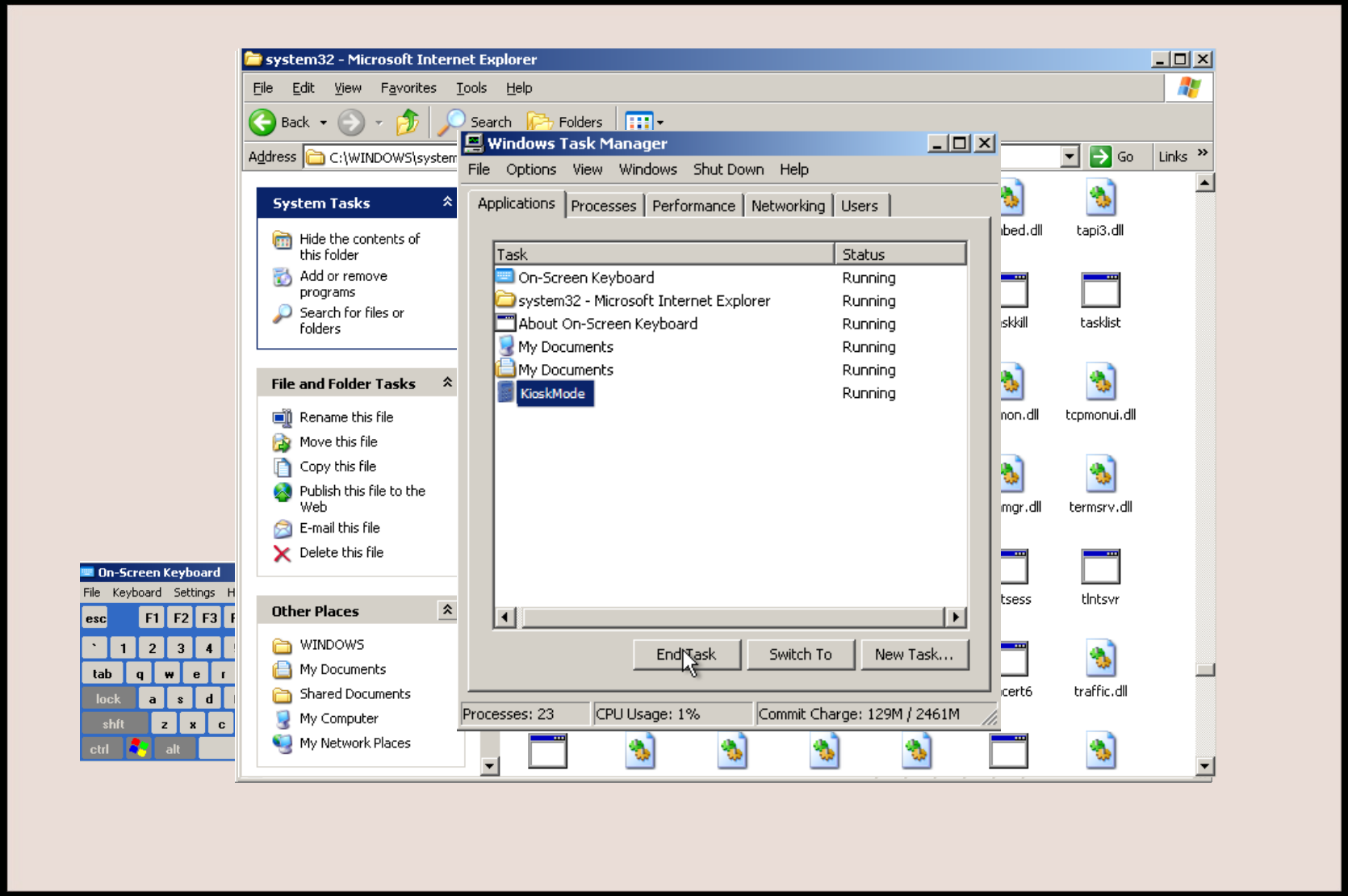
HACK #1: Kiosk Escape



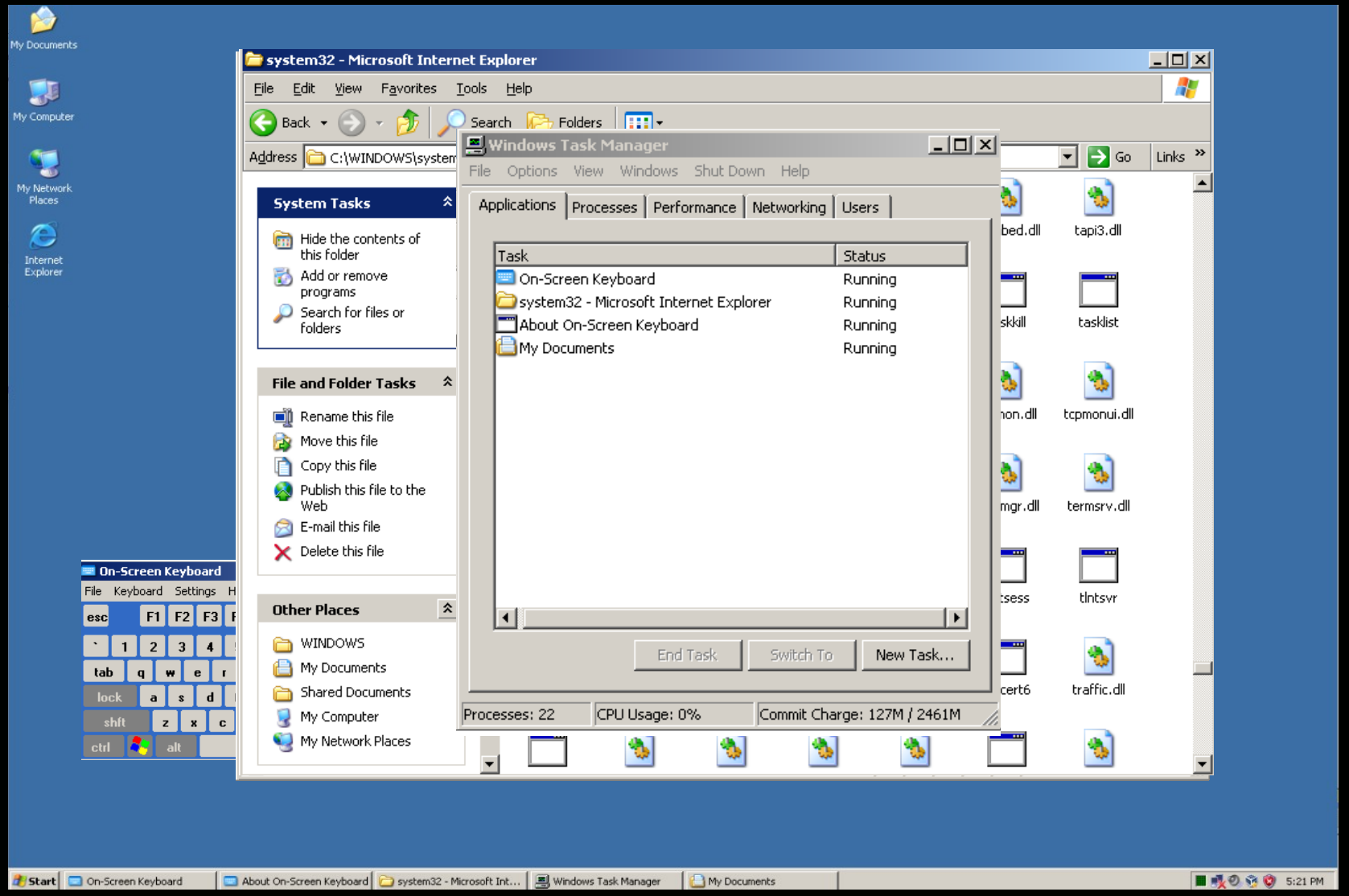
HACK #1: Kiosk Escape



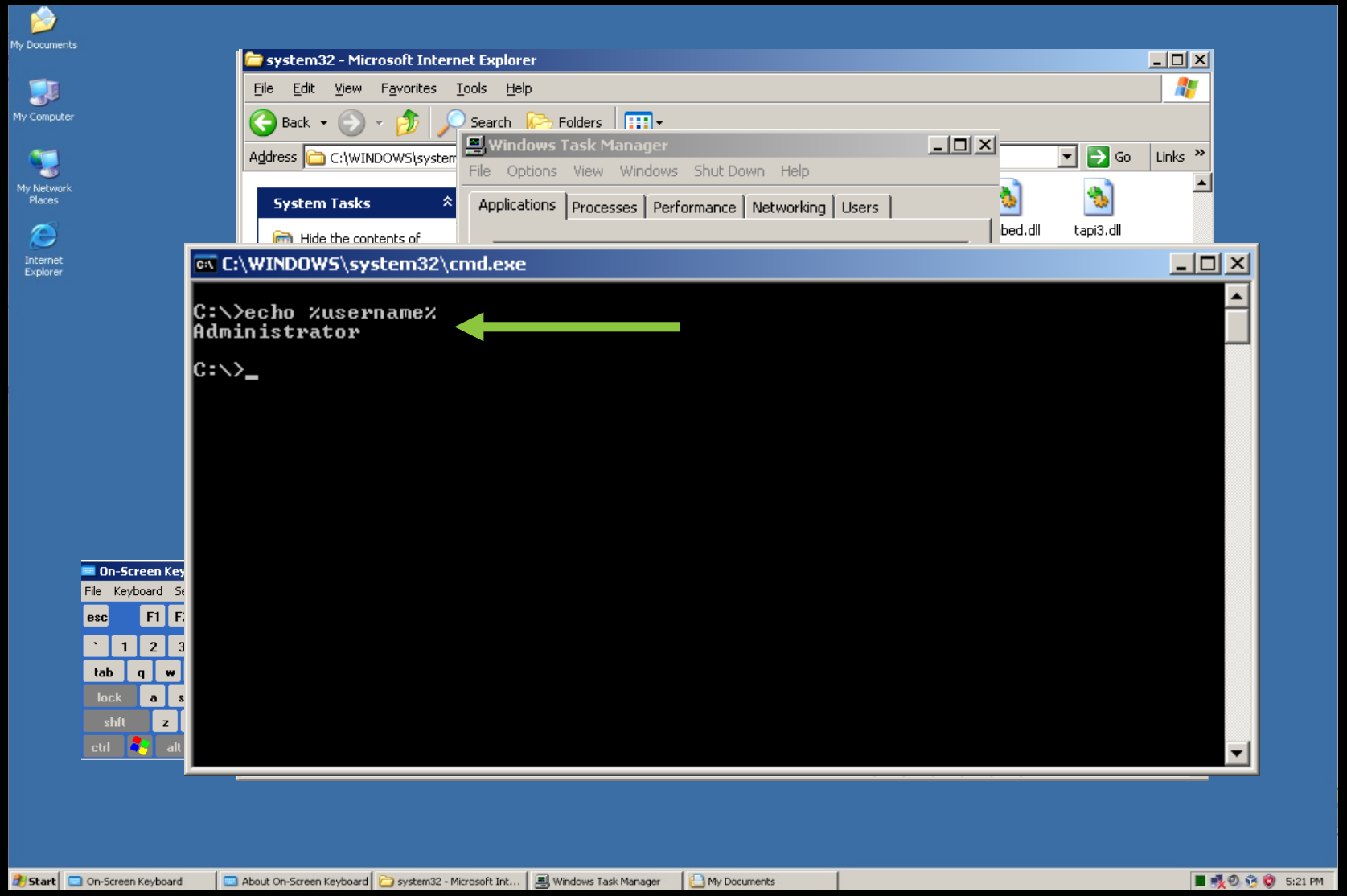
Kiosk Escape



HACK #1: Kiosk Escape



HACK #1: Kiosk Escape



HACK #1: Impact

Zugriff auf System als **lokaler Administrator**

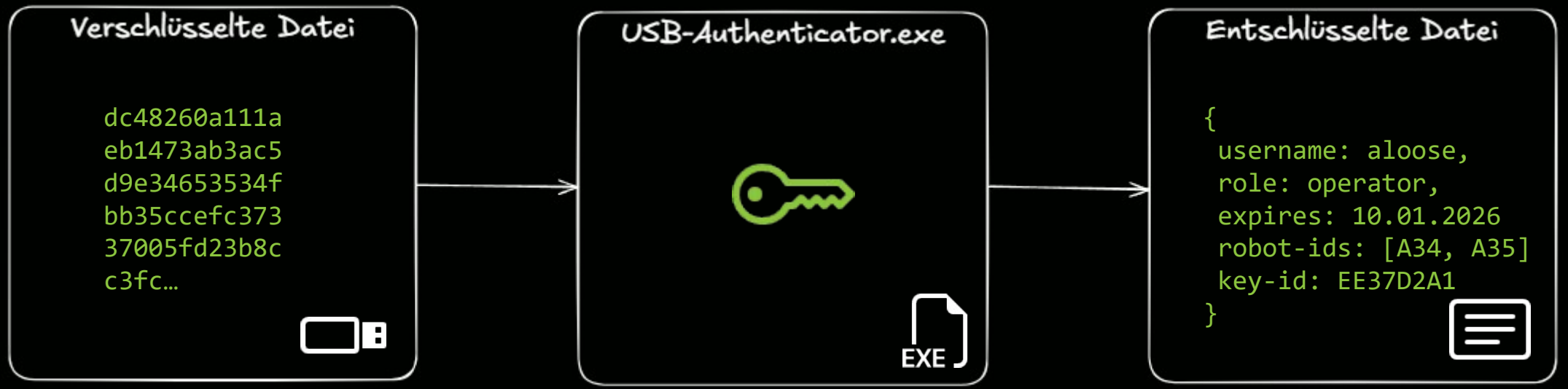
- **Passwort-Hashes der Windows-User**
- **Konfigurationsdateien (MS SQL Passwörter!)**
- **(Hersteller-Software)**

HACK #2: USB Sticks

- Normale **Mass Storage Devices**
- **Verschlüsselte Datei** auf USB Sticks
- Modifikation / „Einfaches Kopieren“ **nicht möglich**

HACK #2: USB Sticks

Vermutung: **Hersteller-Software** entschlüsselt Datei



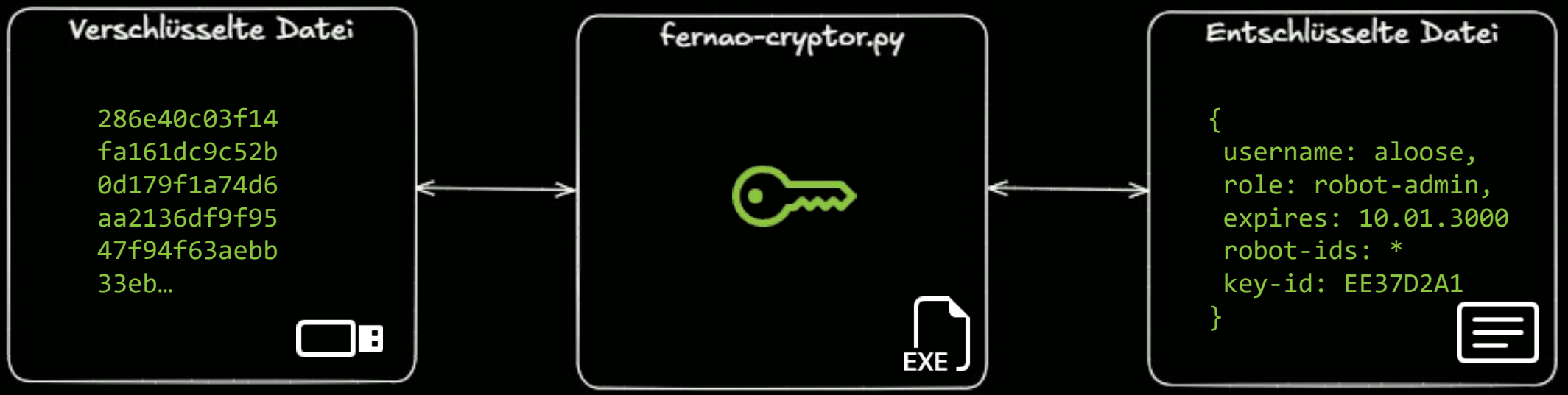
HACK #2: Reverse Engineering

HACK #2: Reverse Engineering

*** Flottenschlüssel** zur Ver-/Entschlüsselung
aller USB-Sticks des Herstellers

HACK #2: USB Sticks

Ausnutzung des extrahierten Schlüsselmatierals



HACK #2: Impact

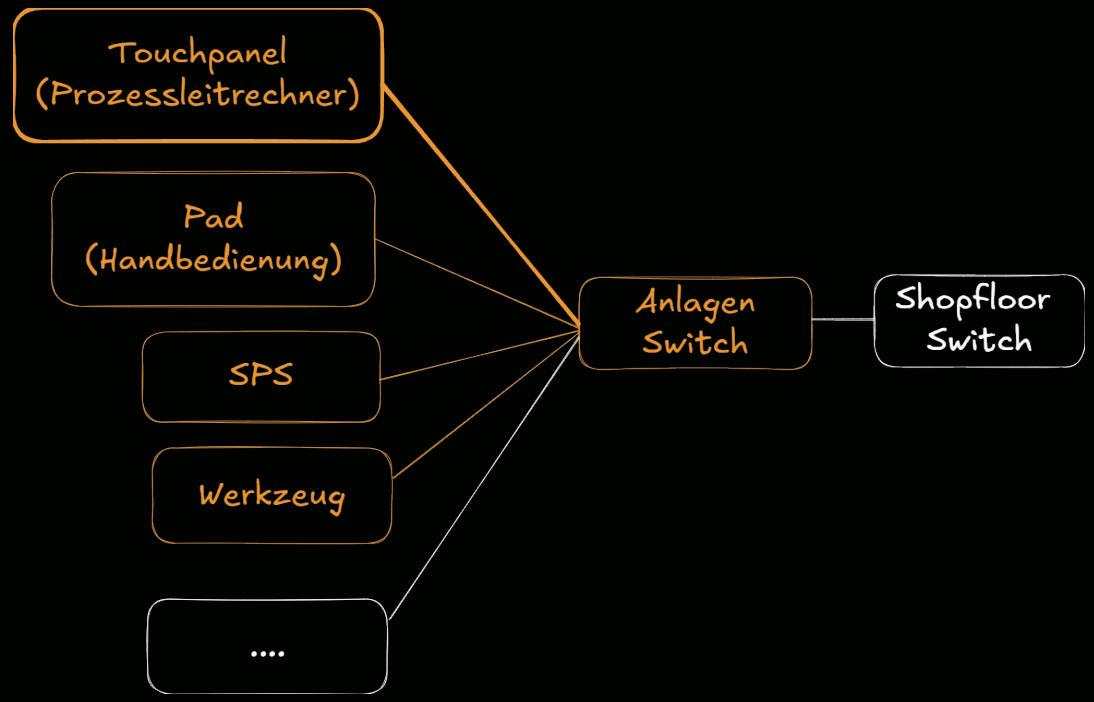
- **Entschlüsselung** von USB-Sticks
- Erstellung von USB-Sticks mit **beliebigen Rollen**
- **Hardcodierte Rollen** durch Hersteller
- **Betroffen: Sämtliche Roboter des Herstellers** (… die Anmeldung via USB nutzen)

Summary

Insgesamt **14**, teils schwerwiegende Befunde

- Zugriff auf Prozessleitrechner als „**Lokaler Administrator**“
- Extraktion von **Passwort-Hashes** (Ausweitung in Firmennetz!)
- Extrahieren von **Klartext-Passwörter** aus Konfigurationsdateien (Ausweitung in Firmennetz!)
- Erstellung von **USB-Sticks mit beliebigen Rollen**

- **Kompromittierung von vier weiteren Systemen**



Portfolio

Security Assessments

- Pentests & Security Audits
  - Web- / Mobile Apps
  - Embedded / Automotive
  - OT
- TIBER DE & Red Teaming
- Social Engineering

Security Compliance

- ISMS-Implementierung (ISO 27001 & VDA TISAX)
- DORA, NIS2
- BaFIN VAIT, BAIT

Security Consulting

- Awareness
- Sicherheitskonzept
- Security Strategie

OT-Hacking: Industrieroboter als Sicherheitsrisiko

fernao

Q & A

Arne Loose
Senior Security Consultant

linkedin.com/in/arne-loose