Prison Break

breaking out of kiosk mode environments

PRESENTED BY:

Gerhard “IKARUS” Klostermerier

@iiiikarus · www.icaria.de · contact@icaria.de

Me

- Gerhard / IKARUS
- Pentester, hacker, researcher, IT/HW/RF security enthusiast
- Especially interested in hardware hacking and wireless systems
- Maybe you know me from MIFARE Classic Tool

Agenda

- What is a kiosk mode environment?
- What is this talk about and what not?
- What interfaces / attack vectors do we have?
- Tips, tricks, stories and demos for kiosk mode breakouts
- Lessons learned
- Q&A + tell your stories, tips and tricks

What is a kiosk mode environment?

“A kiosk mode environment is a system setup where a device or application is locked down to only allow specific functionality, preventing users from accessing anything outside of the intended purpose.“

- The interface is streamlined and restricted
- Users can't access system settings or other applications
- It often runs a single application, like a web browser
- Security measures prevent unauthorized modifications

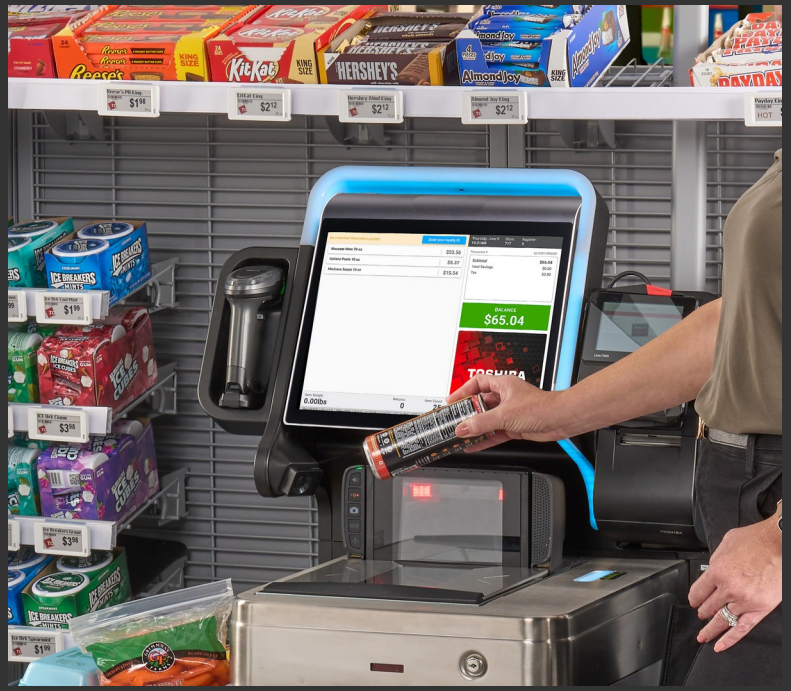
What is a kiosk mode environment?

https://besucherverwaltung.com/kiosk-terminals

What is a kiosk mode environment?

https://besucherverwaltung.com/kiosk-terminalshttps://24x7mag.com/standards/safety/cybersecurity/fda-mitre-offer-cybersecurity-guide-for-legacy-medical-devices/

What is a kiosk mode environment?



https://financialit.net/news/payments/computop-equips-cewe-photo-stations-payment-function
https://commerce.toshiba.com/wps/portal/marketing/Home/tgcs/home/?urile=wcm%3apath%3a%2Fen-us%2Fhome%2Fhardware%2Fself-checkout

What is a kiosk mode environment?

Examples:

- ATM
- Visitor registration
- Self-service order terminal
- Ticket system for public transport
- Info terminal in a museum

What is this talk about?

- What is it about
  - A collection of tips & tricks about kiosk mode breakouts
  - Main focus on devices
  - Stories and lessons learned from analyzing systems
- What is it NOT about
  - Privilege escalation attacks (out of scope)
  - (Pictures of systems I have tested for a customer)

What is this talk about?

Not about Prison Break mems. Sorry, did not watch the show 😬

Previous work

There has been great research in the past e.g.:

- Paul Craig (DEF CON talks, tools)
- Swissky & community (cheatsheet)
- Syed M. Huda (cheatsheet)
- Shain Lakin (collection of useful breakout links)
- Many more...

What interfaces / attack vectors do we have?

- What can we do with the device/terminal?
- What do we know about the platform?
  (Windows/Linux/Android/etc. system, used software)
- What input methods do we have? (touch, keyboard, barcode reader)
- What interfaces do we have? (USB, Ethernet, Wi-Fi, Bluetooth)
- What else can we access? (easy to open, power cord)

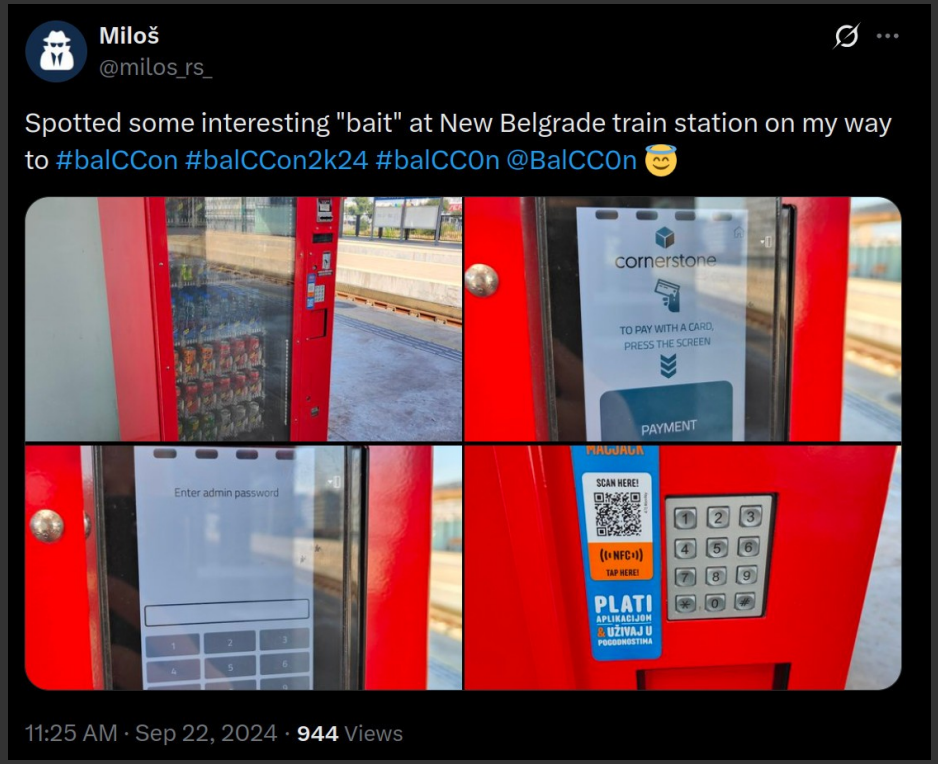
Tips & tricks

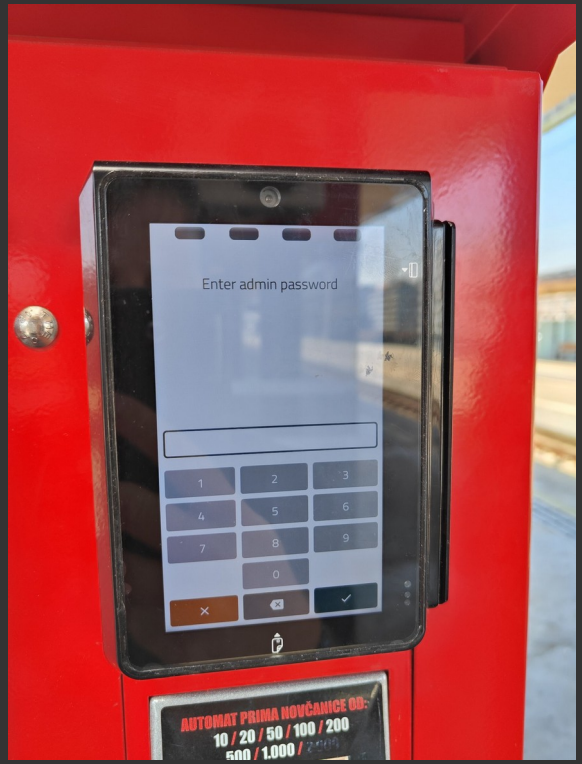
- Kiosk application
- Touchscreen/mouse
- Keyboard
- (Re-)booting & Login screen
- Crashing
- USB
- Network (Ethernet/Wi-Fi)
- Android
- Other

Kiosk application

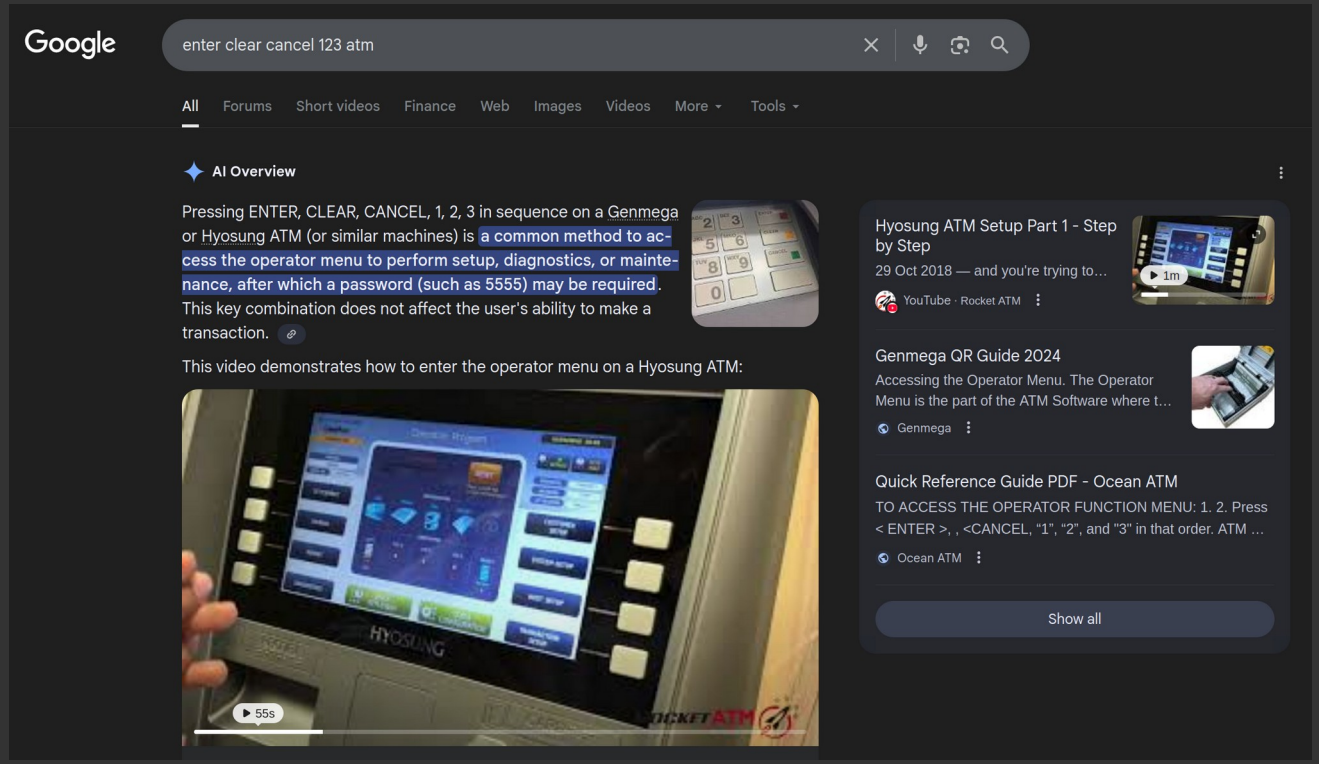
- Most kiosk application have a designed breakout mechanism
- Some require authentication (e.g. PIN)
- Sometimes they are just hidden
- Press/long press/repeatably press on “static” content (logos, clock, version number, etc.)
- Look for known breakout options & default PINs/passwords

Kiosk application





Kiosk application



Kiosk application

General things to look out for:

- Links
- Open/save/download options
- Embedded elements (e.g. browser, PDF viewer, etc.)
- (Sometimes: print options)

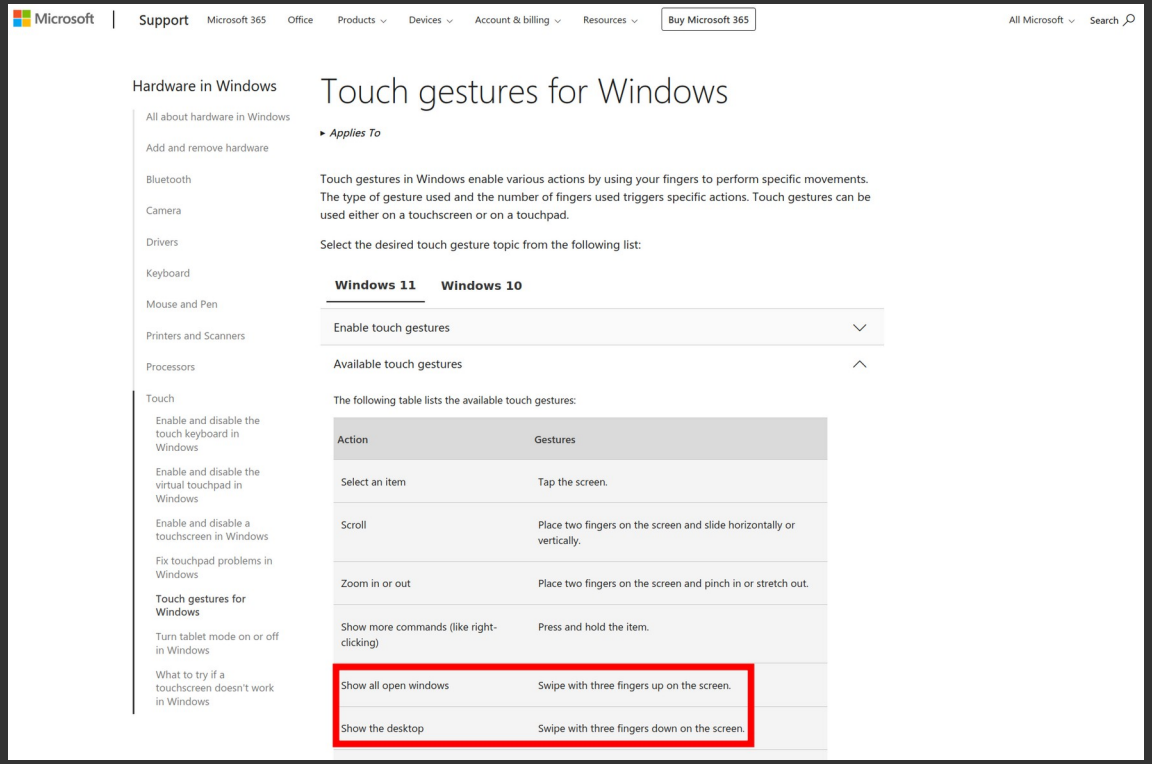
Kiosk application

Demo
breakout from edge with “PDF → open”

Touchscreen / Mouse

- Things to look out for:
  - Long touch/right click (context menus)
  - Drag and drop
  - Screen corners and edges
  - Gestures

Touchscreen / Mouse



https://support.microsoft.com/en-us/windows/touch-gestures-for-windows-a9d28305-4818-a5df-4e2b-e5590f850741

Touchscreen / Mouse

Demo
gesture breakout on ticket system

Keyboard

- Maybe the terminal has one build into it (likely to not have “all” keys)
- Maybe you can plug in your own keyboard via USB
- There are a LOT of keys and keyboard shortcuts which may help with breaking out
- Some examples: Ctrl+Alt+Del, Ctrl+Shift+Esc, Win+X, Win+R, Win+E, Alt+Tab, Alt+Esc, Win+Tab, Win+D
- Watch out for stateful/custom keyboard shortcuts (first X then Y)

Keyboard

Demo
lesser known keyboard shortcuts
(Shift x5, Shift+Alt+Print)

(Re-)booting & Login screen

- Might give you access to system options (BIOS/UEFI)
  - Time, boot order, build-in EFI shell
- Might allow you to boot from a different medium
- There might be timeframes where you can access other programs
- Might allow you to access Windows repair & boot options

(Re-)booting & Login screen

Demo
deactivated sticky keys

(Re-)booting & Login screen

Demo
from login screen to cmd

Crashing

- Overexerted applications might crash or Windows might offer to kill the not responding application (e.g. rapidly change languages)
- It might be to trigger a resource exhaustion via e.g. the network interface (SYN flooding, TLS (re)negotiation, etc.)
- Slow external resources (e.g. emulated USB flash drive) might cause the UI to hang (kill not responding application)
- Blue screen error might give access to Windows repair & boot options

Crashing

Demo
leftover cmd.exe running a program

USB

- Obvious: try if a USB keyboard works
- USB flash drive with “dirty bit” → might trigger repair popup
- BitLocker to Go encrypted drives might trigger a popup
- Devices might trigger a “co-driver installation” popup
- If flash drives are forbidden, MTP devices (Android phone) might work
- If the keyboard protocol is forbidden, a (emulated) mouse with a full keyboard might work

Demo
co-driver install on Windows

Network (Ethernet/Wi-Fi)

- Sorry, no ready-to-use tips & tricks here (yet?)
- There might be services running that help with breaking out (RDP, SMB, etc.)
- Do a portscan and work from there

Android

Look out for

- Android Debug Bridge (adb)
  - Check network and USB
  - Also check when running in safeboot or fastboot
- Recovery mode & bootloader (side loading apps)
- Attach a keyboard and check typical keys & shortcuts
- Check other interfaces (e.g. NFC, camera with QR code reader, etc.)

Other

- (Android) devices with NFC
  - Might support NDEF data format and act on it
- Bluetooth enabled devices
  - Force-pairing might work (CVE-2023-45866, great on “older” Android/Linux)
  - Pairing a BT keyboard might work/help

Other

- Barcode/QR code reader
  - Often emulate a HID device (USB keyboard)
  - Sometimes can be programmed to support keyboard shortcuts
  - Sometimes can be programmed though barcodes
- URI handlers
  - Especially great if you can surf to a attacker controlled website

Other

Demo
Android and NDEF NFC tags

Other

Demo
URI handlers

Let’s recap

- There are endless ways to break out!
- There is no “one way to rule them all”
- Possibilities to break out are mostly tied to available inputs, interfaces and how the system can be accessed

Lessons learned – “Blue Team”

- Don’t build your kiosk mode terminal on a full-featured platform by removing features (e.g. “normal” Windows 10).
- Build you platform with only the features needed for operation (e.g. Yocto Linux, no Xserver, no desktop, no additional drivers, etc.)
- All input is evil! Validate everything & build/use robust system
- Hiding functions is not security; use strong authentication for admin
- Don’t reinvent the wheel, use well known features/software

Lessons learned – “Red Team”

- Check what interfaces/attack vectors are available
- Be creative
- Be persistent
- Do your research

Kiosk mode breakout: tips & tricks

https://github.com/ikarus23/kiosk-mode-breakout

Contributions Welcome!

Questions?

Share your stories, tips & tricks!

CONTACT:
𝕏 @iiiikarus · @iiiikarus@infosec.exchange · www.icaria.de · contact@icaria.de

Creative Commons Attribution-ShareAlike 4.0 International License, https://creativecommons.org/licenses/by-sa/4.0/