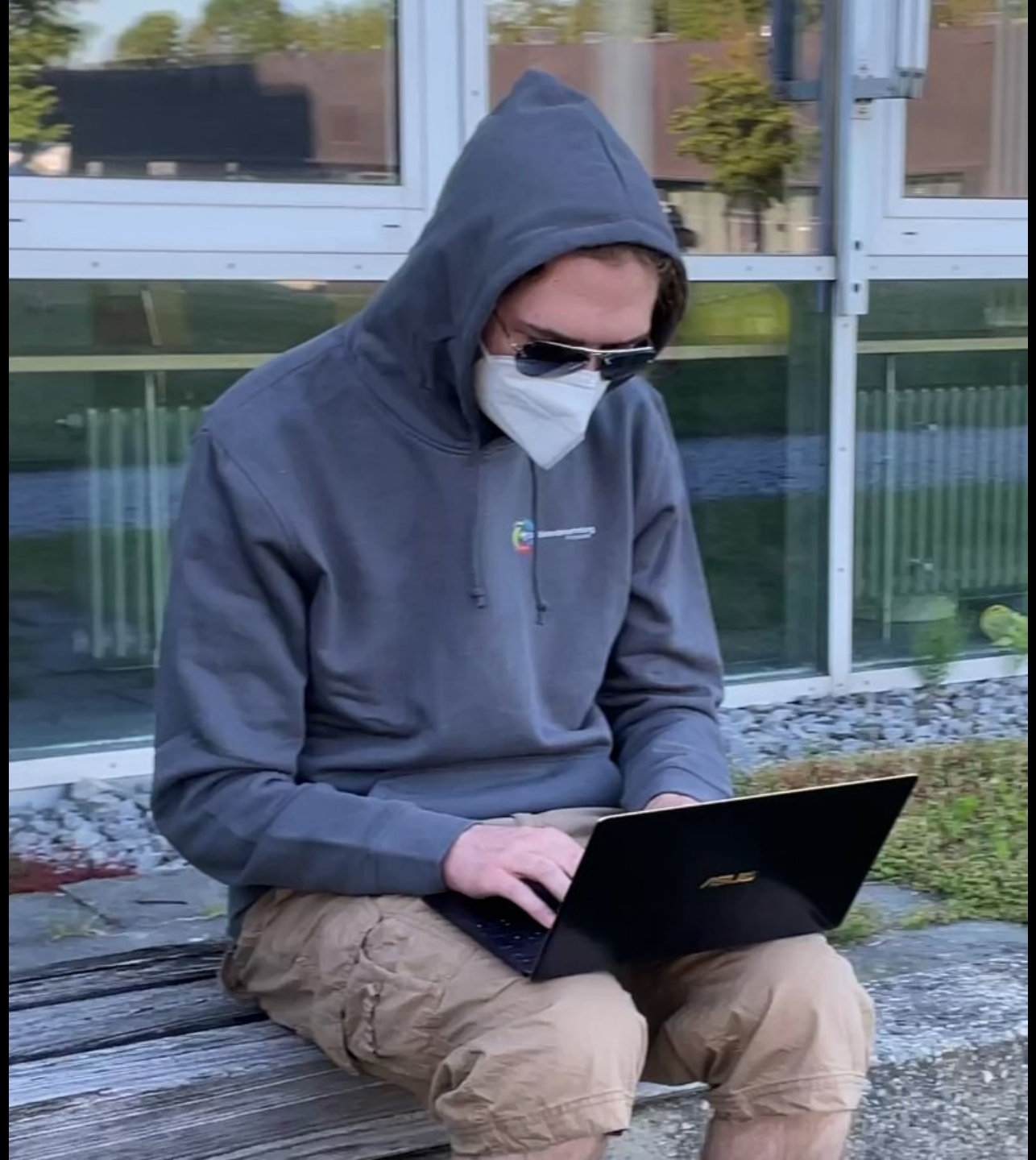
CARISSMA
Institute of Electric,
Connected and Secure Mobility

SAFIR HATS3

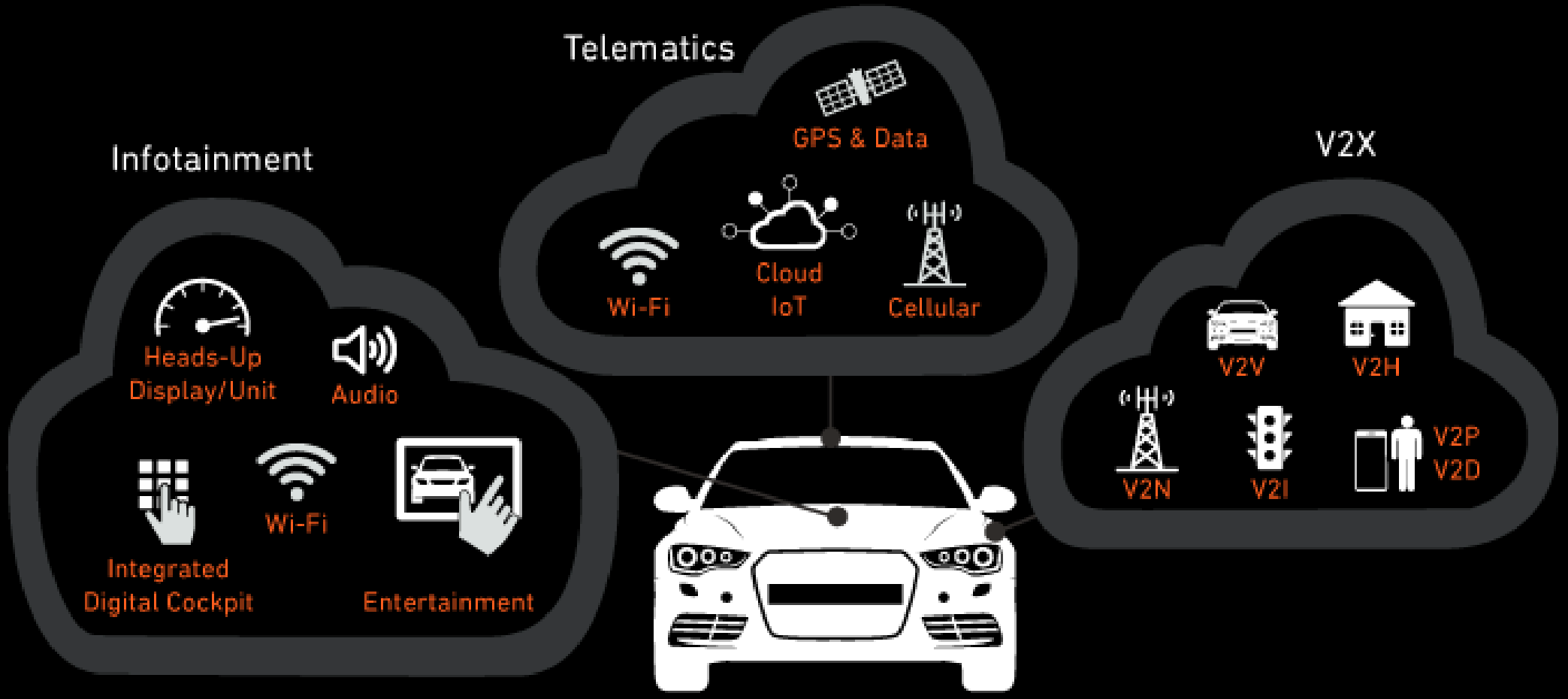
Pentesting mithilfe des HATS3 Security Frameworks

Jakob Löw 30.03.2022

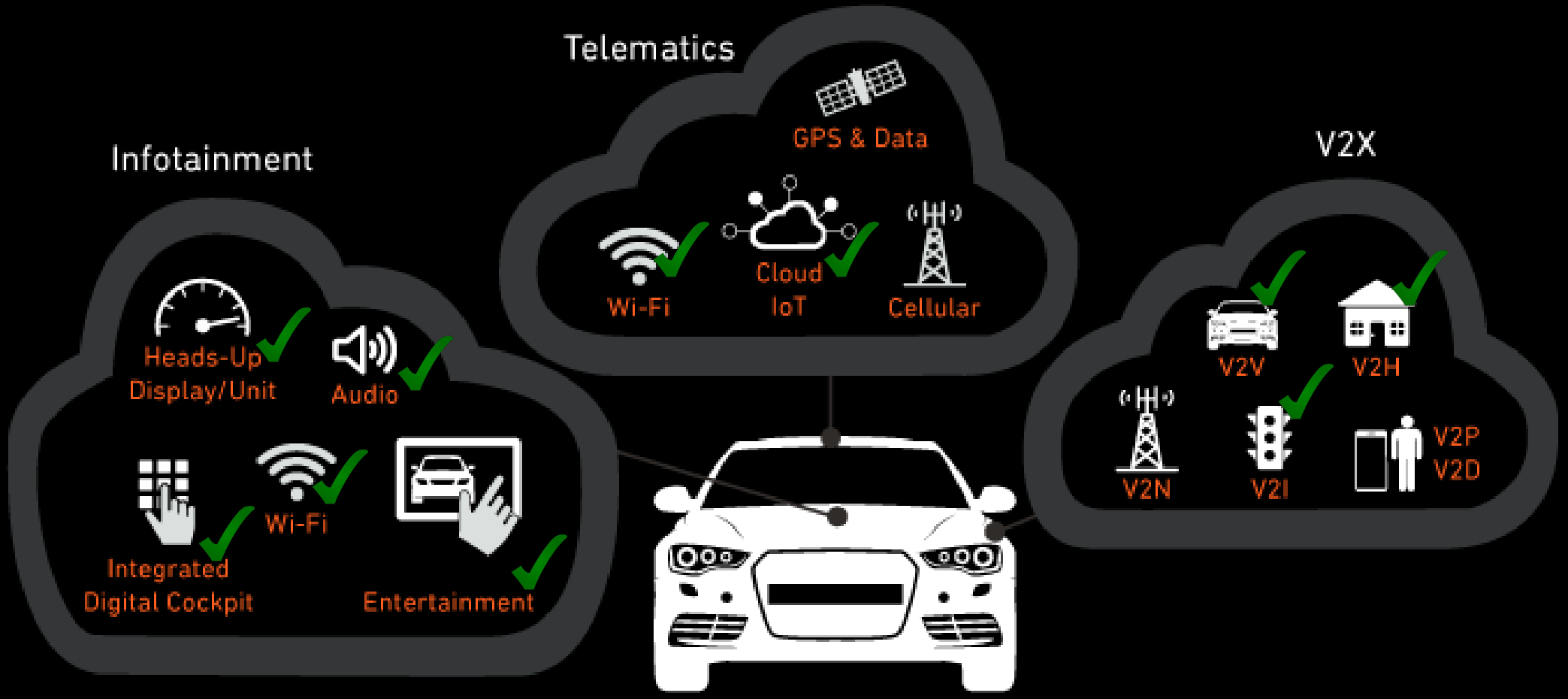
Technische Hochschule Ingolstadt



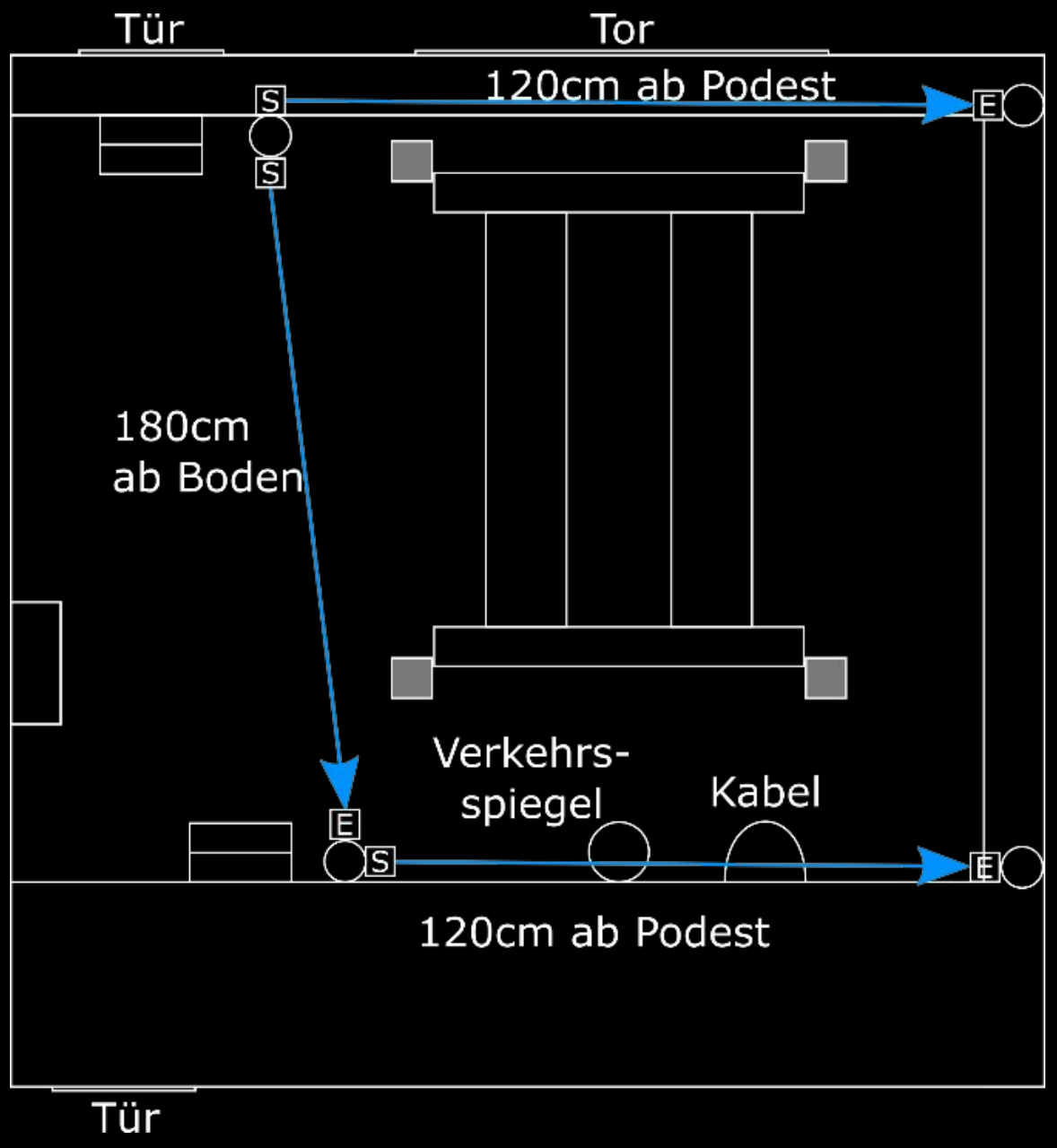
Heterogeneous Connectivity



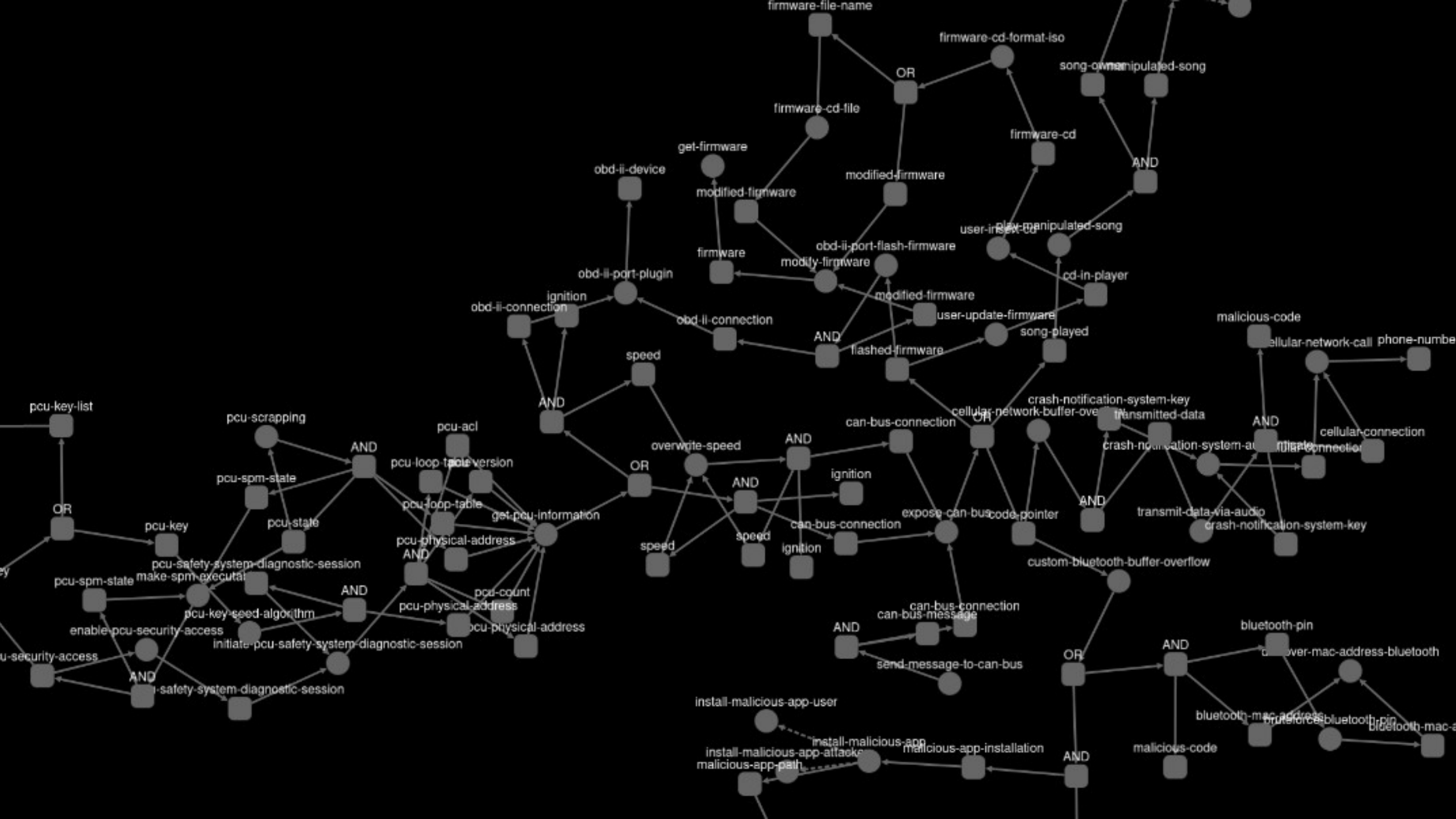
Heterogeneous Connectivity

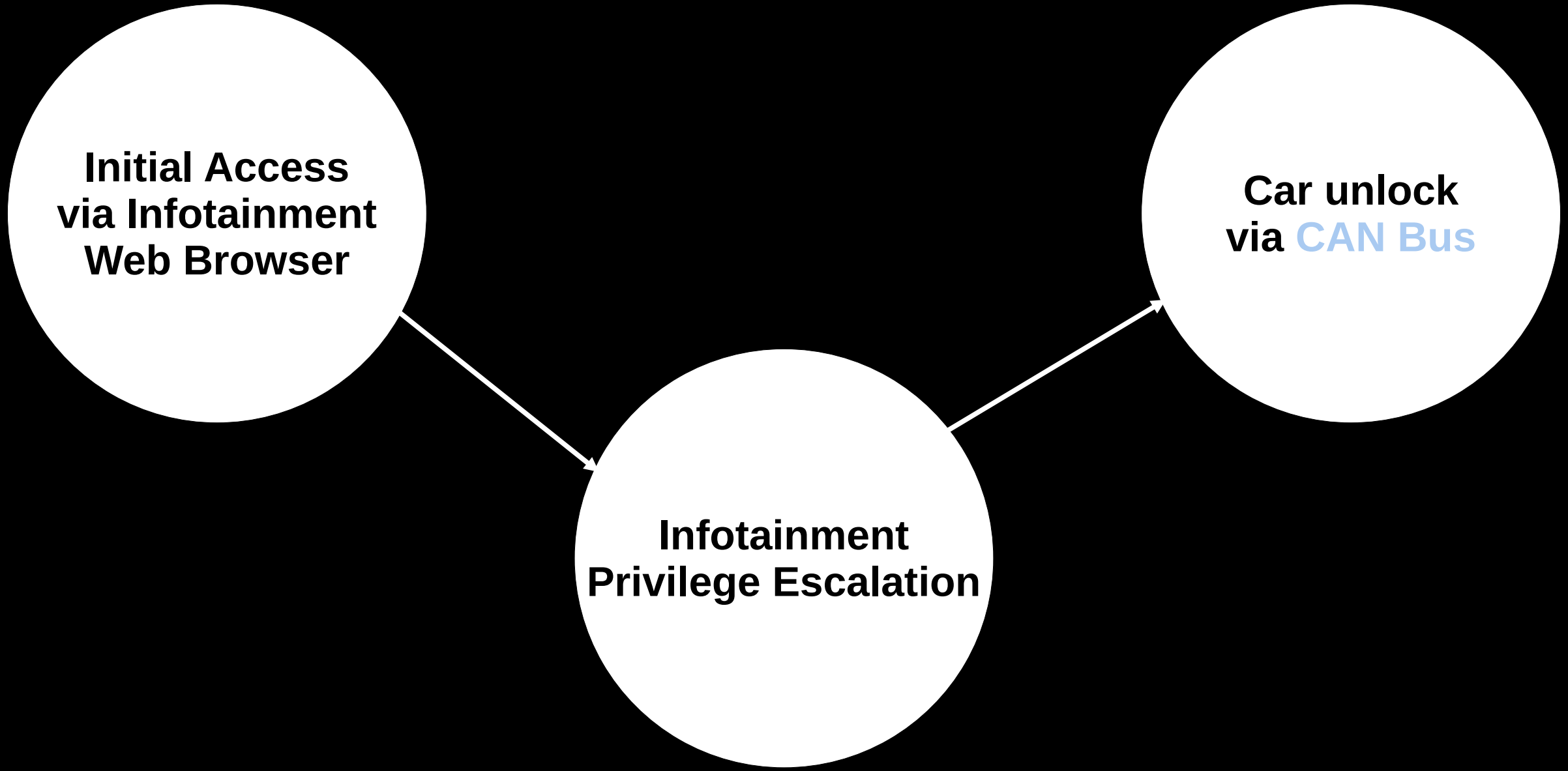


DEUTRONIC
terra
APC


Tür
Tor
120cm ab Podest
S
S
E
180cm
ab Boden
Verkehrs-
spiegel
Kabel
E
S
E
120cm ab Podest
Tür

ABB


firmware-file-name
firmware-cd-format-iso
song-owner-manipulated-song
OR
firmware-cd-file
firmware-cd
get-firmware
obd-ii-device
modified-firmware
modified-firmware
modified-firmware
AND
user-insert-cd
play-manipulated-song
firmware
obd-ii-port-flash-firmware
modify-firmware
obd-ii-port-plugin
cd-in-player
ignition
obd-ii-connection
modified-firmware
obd-ii-connection
user-update-firmware
AND
song-played
flashed-firmware
malicious-code
cellular-network-call
phone-numbe
speed
pcu-key-list
AND
crash-notification-system-key
pcu-scrapping
pcu-acl
can-bus-connection
OR
cellular-network-buffer-ove
transmitted-data
AND
cellular-connection
AND
overwrite-speed
pcu-loop-table-version
crash-notification-system-a
pcu-spm-state
OR
ignition
pcu-loop-table
pcu-key
pcu-state
get-pcu-information
AND
expose-can-bus
code-pointer
AND
transmit-data-via-audio
can-bus-connection
crash-notification-system-key
pcu-physical-address
speed
speed
ignition
pcu-safety-system-diagnostic-session
custom-bluetooth-buffer-overflow
pcu-spm-state
make-spm-executat
AND
pcu-count
pcu-physical-address
can-bus-connection
pcu-key-seed-algorithm
can-bus-message
AND
pcu-physical-address
enable-pcu-security-access
send-message-to-can-bus
initiate-pcu-safety-system-diagnostic-session
bluetooth-pin
AND
OR
over-mac-address-bluetooth
AND
install-malicious-app-user
bluetooth-mac-address
bruteforce-bluetooth-pin
install-malicious-app
malicious-app-installation
malicious-code
malicious-app-path
AND


Initial Access
via Infotainment
Web Browser
Infotainment
Privilege Escalation
Car unlock
via CAN Bus