Setec Astronomy: An Overview of Hardware-Based Covert Channels

Joe Grand aka Kingpin, Grand Idea Studio

Covert Channels

- Hidden methods to intentionally exfiltrate/transfer data from a normally functioning system
  - First mentioned in 1973
  - Non-conventional, out-of-band techniques
- Can exist in any layer of a compromised system
  - Hardware, peripherals, application, operating system, network stack/protocols, etc.
  - Difficult to detect without knowledge of method & expected results

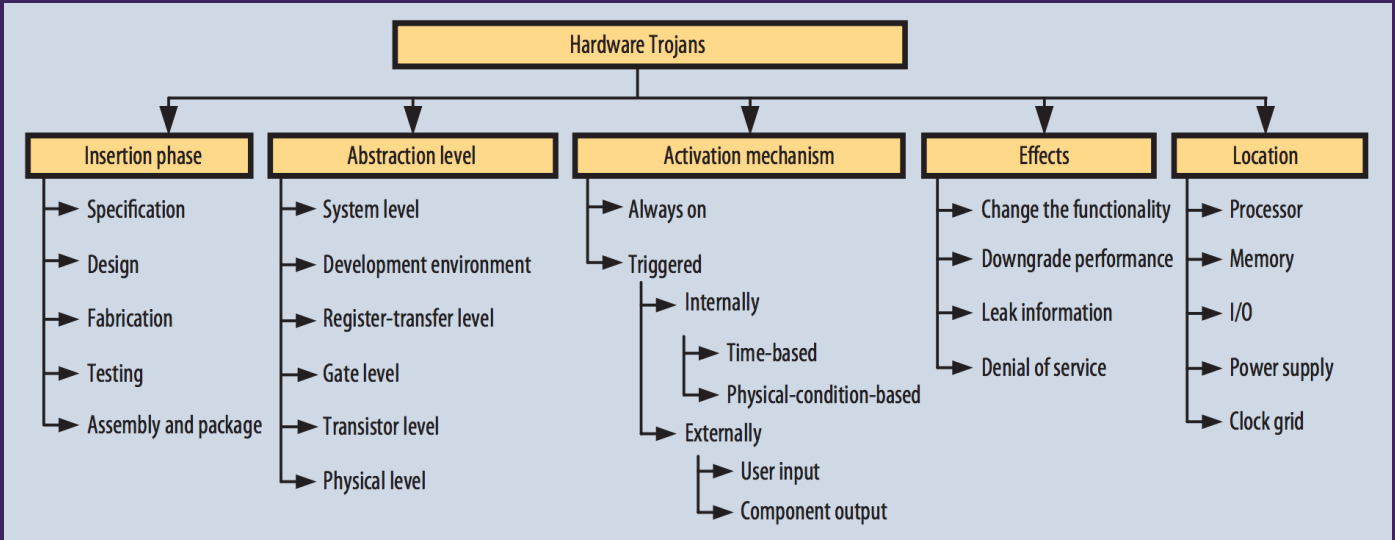
Covert Channels

GRAND IDEA STUDIO ROADSEC

- Requires collusion between transmitter & receiver
  - Software pre-loaded onto target
  - Hardware modification of target not usually needed
- Must be implanted onto target before use
  - Malicious insiders
  - Social engineering
  - Sneakernet (Physical/removable media)
  - Network
  - Hardware espionage

Hardware Espionage

- Embedding malicious code/functionality during product lifecycle
  - Design, fabrication, distribution, storage, integration, in-the-field



Trustworthy Hardware - Identifying and Classifying Hardware Trojans, R. Karri, et al., IEEE 2010

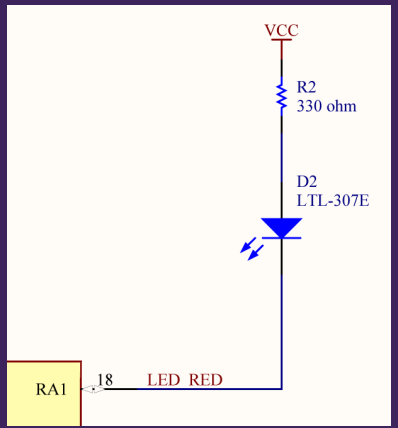
Hardware-Based Channels

GRAND IDEA STUDIO ROADSEC

- Optical
- Electromagnetic/RF
- Electric
- Magnetic
- Thermal
- Acoustic

Optical

- Using LEDs to exfiltrate/send data
  - Redirect data output to LED, discretely control from SW/FW
  - Modulation faster than the human eye can detect
- Requires optical receiver to convert light into voltage or camera system to determine changes in light



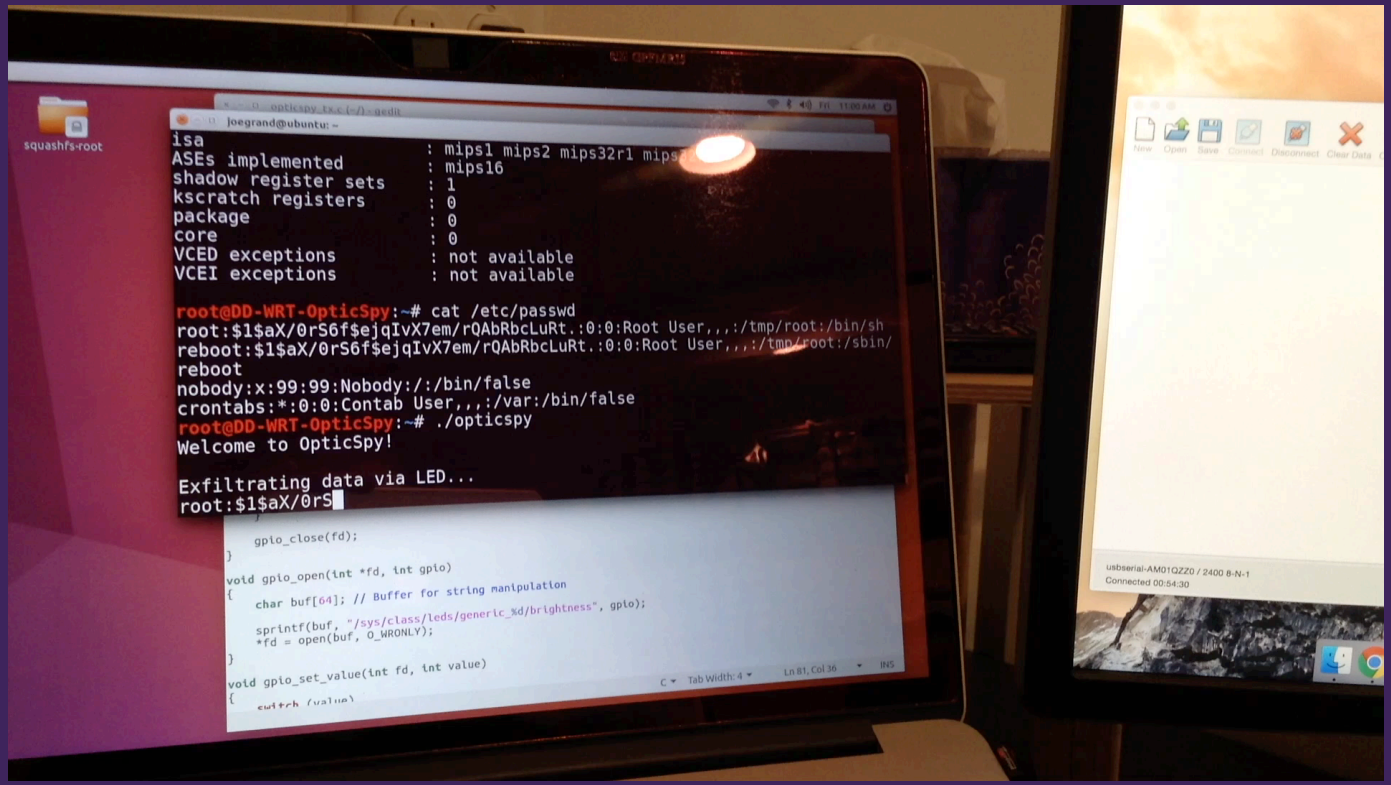
Optical

- Information Leakage from Optical Emanations
- Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks
- Extended Functionality Attacks on IoT Devices: The Case of Smart Lights
- aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared

Optical

- LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED
- xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs
- VisiSploit: An Optical Covert-Channel to Leak Data through an Air-Gap
- BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness

Optical Demonstration

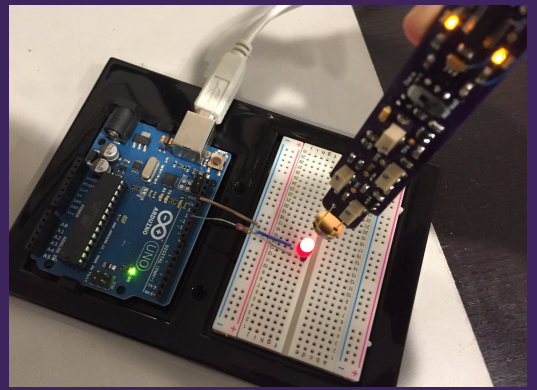


Optical DIY

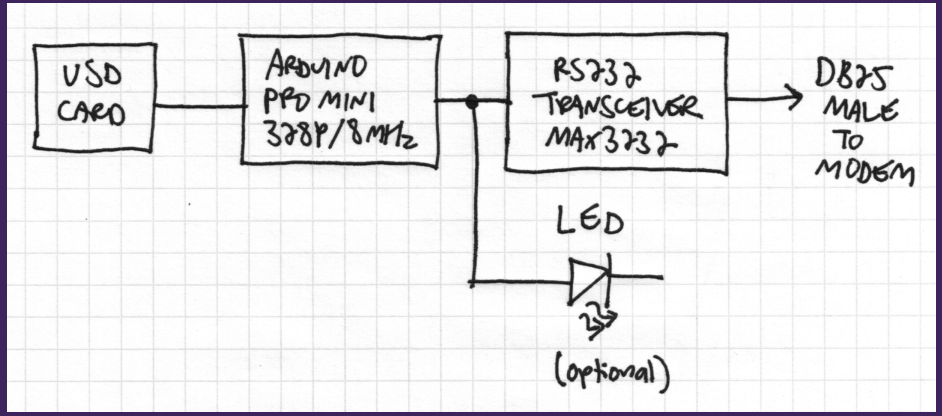
- Arduino + LED (or Laz0r!@)
  - Printable ASCII data via standard UART

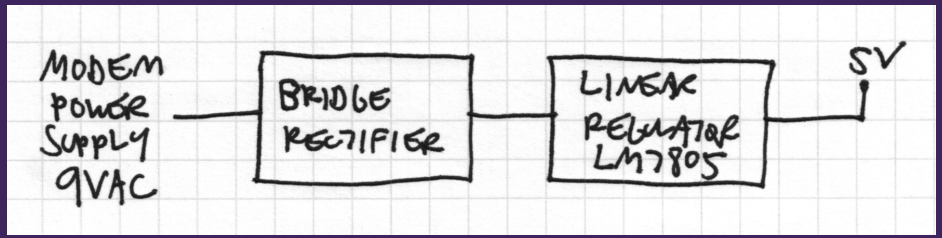
```
// Set up a new serial port
SoftwareSerial opticSerial =  SoftwareSerial(rxPin, txPin);

opticSerial.print(msg_covert); // Transmit secret message through the LED
opticSerial.flush();           // Wait for all bytes to be transmitted
```

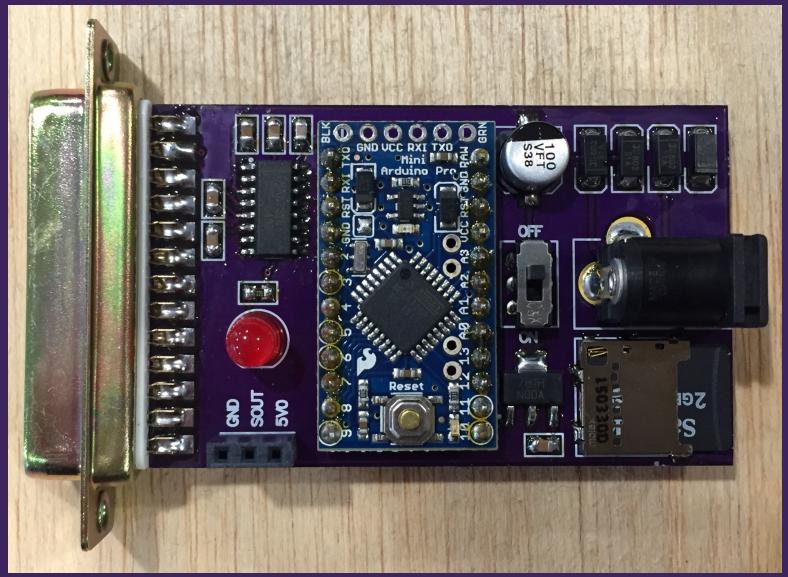
- OpticSpy receiver
  - Open source tool for optoelectronic experiments
  - Hand solderable, off-the-shelf components
  - www.grandideastudio.com/portfolio/opticspy/



Optical DIY

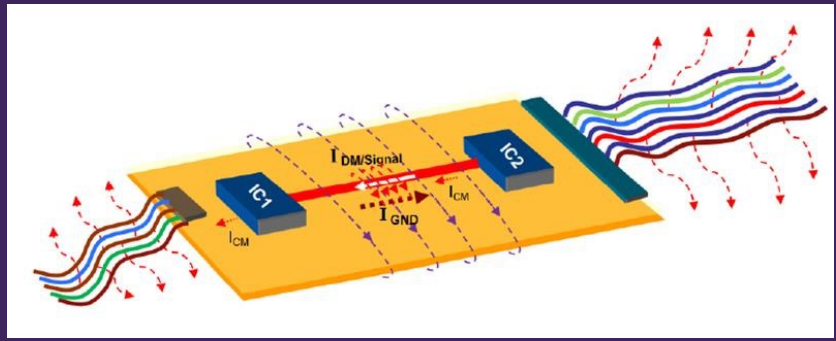

USD CARD
ARDUINO PRO MINI 328P/8MHz
RS232 TRANSCEIVER MAX3232
DB25 MALE TO MODEM
LED
(optional)


MODEM POWER SUPPLY 9VAC
BRIDGE RECTIFIER
LINEAR REGULATOR LM7805
5V


OFF
Reset
GND
SOUT
5V0

Electromagnetic / RF

- Leakage due to changes in electrical signal current
  - Conducted emissions (EM) are a natural byproduct of active circuit operation
  - Dependent on signal current and how signal changes over time
  - If current can be controlled, EM emissions can be controlled (frequency/amplitude)



New Electronics: EMC basics and practical PCB design tips

Electromagnetic / RF

- Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations
- Exfiltrating Reconnaissance Data from Air-Gapped ICS/SCADA Networks
- Emanate Like a Boss: Generalized Covert Data Exfiltration with Funtenna
- Revolting Radios, System Bus Radio, osmo-fl2k, Serial Port SDR

Electromagnetic / RF

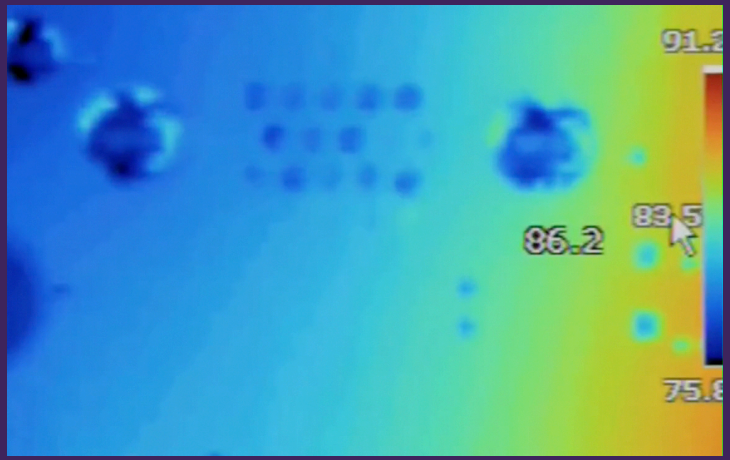
- AirHopper: Bridging the air-gap between isolated networks and mobile phones using RF
- GSMem: Data exfiltration from air-gapped computers over GSM frequencies
- USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB
- A Ghost in your Transmitter: Analyzing polyglot signals for physical layer covert channels detection

Electric / Magnetic

- PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines
- ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields
- MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields

Thermal

- Changes in thermal/temperature properties of a component, system, or environment
  - Increase processing power, control fan/cooling, HVAC/ environmental conditions, affect timing critical functions



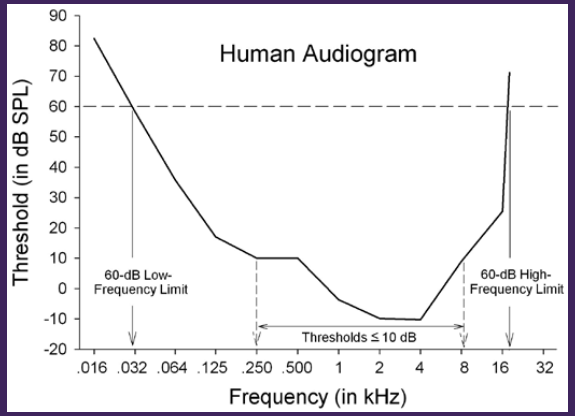
Demonstration of Hardware Trojans (DEFCON 16)

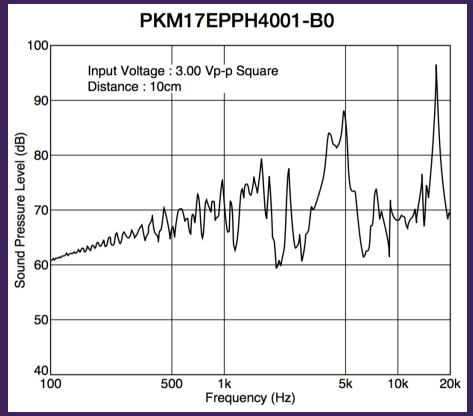
Thermal

- BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations
- HVACKer: Bridging the Air-Gap by Manipulating the Environment Temperature
- Thermal Covert Channel in Bluetooth Low Energy Networks

Acoustic

- Audio generated from speakers, electronic components, or peripherals inside the system
  - Undetectable by normal human hearing
  - Ultrasound, mechanical noise, board/component vibration





The Primate Peripheral Auditory System and the Evolution of Primate Hearing

Acoustic

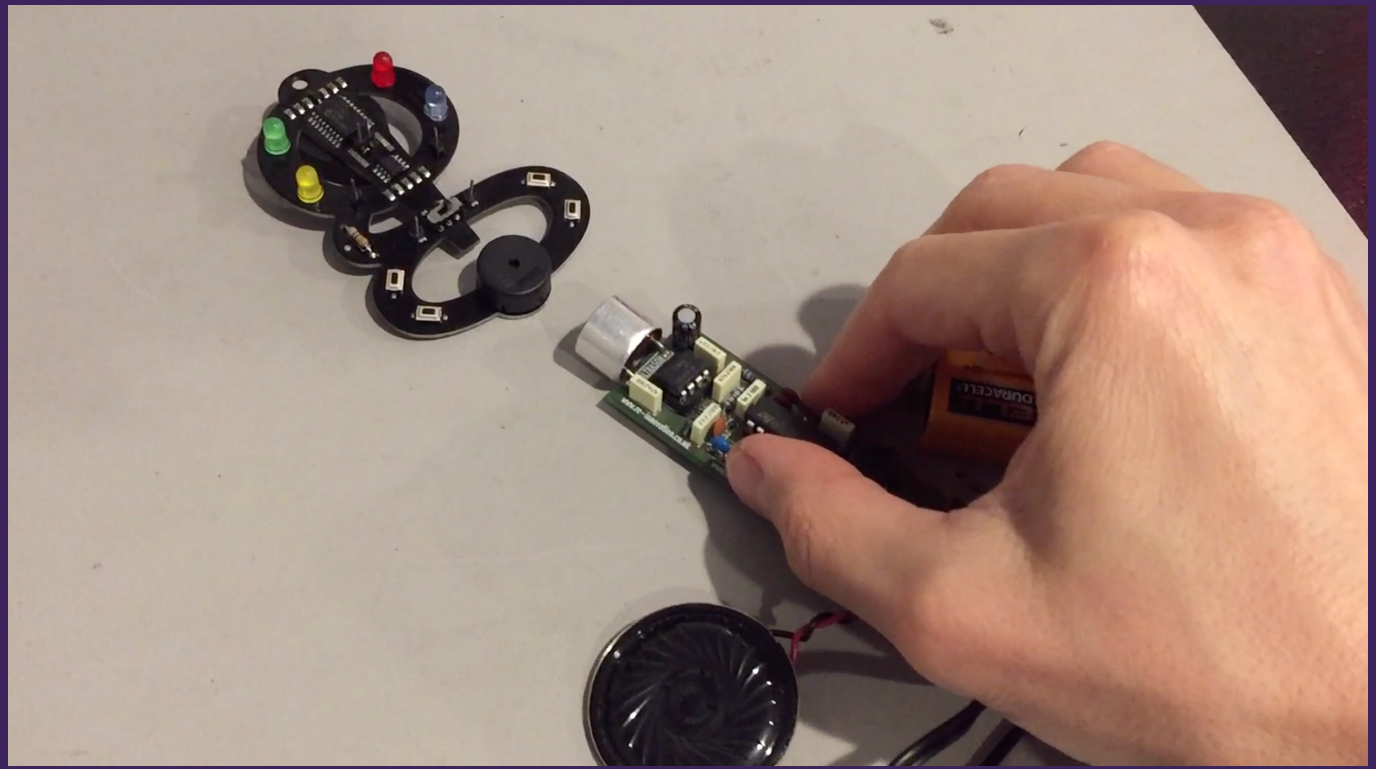
- Passive and Active Leakage of Secret Data from Non Networked Computer
- Secure communications below the hearing threshold: Improved approaches for auditive steganography
- Privacy and Security Aspects of the Ultrasound Ecosystem
- Inaudible Sound as a Covert Channel in Mobile Devices
- BadBIOS
- radBIOS: Wireless Networking with Audio

Acoustic

- See no evil, hear no evil: Hacking invisibly & silently with light & sound
- MOSQUITO: Covert Ultrasonic Transmission via Speaker-to-Speaker Communication
- POWER-SUPPLaY: Leaking Data from Air-Gapped Systems by Turning the Power-Supplies Into Speakers
- On Covert Acoustical Mesh Networks in Air
- DiskFiltration: Acoustic Data Exfiltration from via Covert Hard-Drive Noise

Ultrasonic Demonstration

GRAND IDEA STUDIO ROADSEC

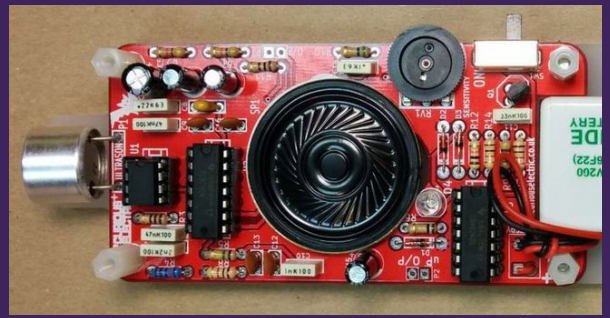


Ultrasonic DIY

- Arduino + passive piezoelectric sounder

```
// Set up output pin
pinMode(audioPin, OUTPUT);
Timer1.initialize(40);  // Period in uS (= 25kHz)

Timer1.pwm(audioPin, 512); // PWM @ 50% duty cycle
```

- Bat Listener Kit receiver
  - Frequency down-converter into audible range
  - github.com/curiouselectric/batlistener/



???

GRAND IDEA STUDIO

ROADSEC


ROADSEC
Obrigado!
www.grandideastudio.com/contact/
@joegrand (Twitter)
MAIS UM EVENTO:
Flipside
SECURITY BEYOND TECHNOLOGY
REALIZAÇÃO:
Green Helmet