



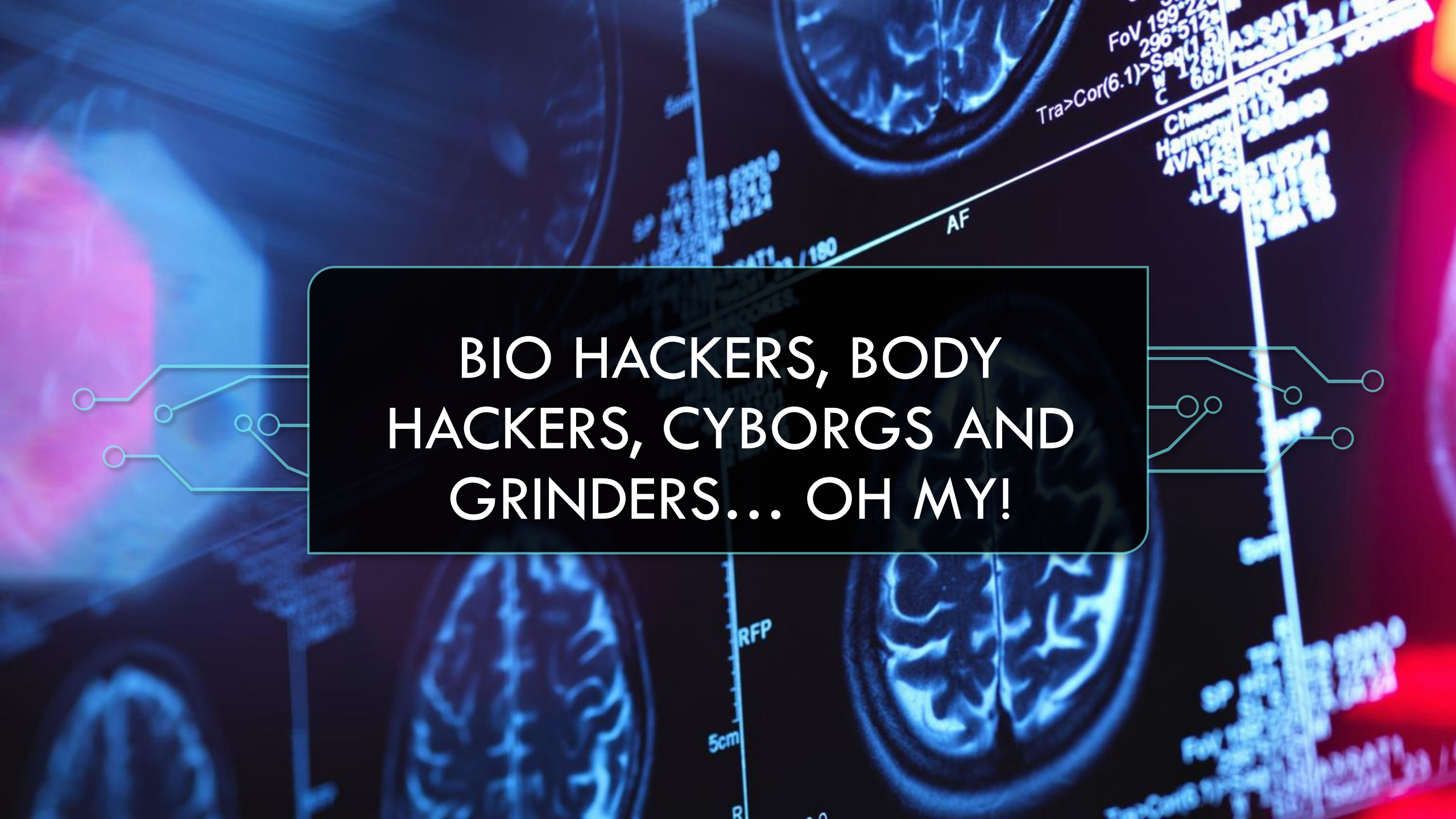
# THE INVISIBLE THREAT – WHERE HUMAN AND TECHNOLOGY MEET

PRESENTER: JASON MOULDER

SR. PENETRATION TESTER - PRATUM

# OVERALL OBJECTIVE

To highlight and understand the possible effects of device implantation in an environment from a Red Team point of view.



The background is a collage of medical and technological imagery. It includes several axial MRI slices of a human brain, showing internal structures like the ventricles and gyri. Overlaid on these are various technical labels and data points in a white, monospaced font, such as 'FoV 199', '296', '512', 'Sag(1.5)', 'Tra>Cor(6.1)', 'W 128', 'C 66', 'Chilom', 'Harmony', '4VA12', 'HFS', '+LPT', 'AF', 'RFP', '5cm', and 'R'. There are also stylized circuit board traces in a light blue/cyan color, with small circles at the end of the lines, extending from the left and right sides towards the central text box. The overall color palette is dominated by deep blues, purples, and a hint of red on the far right edge.

**BIO HACKERS, BODY  
HACKERS, CYBORGS AND  
GRINDERS... OH MY!**

# WHAT DOES ALL THIS MEAN?

- The term 'cyborg' arose as a short form of 'cybernetic organism,' which is an entity made up of both biological and technical elements.
- Grinders largely identify with transhumanist and biopunk ideologies. Transhumanism is the belief that it is both possible and desirable to alter the human condition using technologies.
- Overall desire to expand the boundaries of human perception and even create "new senses".





Technology is a part of us already. While we aren't currently enveloped yet, what is stopping us? Prosthetics have become "smart" and can be controlled by electrical impulses. Is it just an ethical thing?



# CONSPIRACIES OF RFID TRACKING

- I'm going to be tracked... Do you have a cell phone, get online, drive on a tollway?

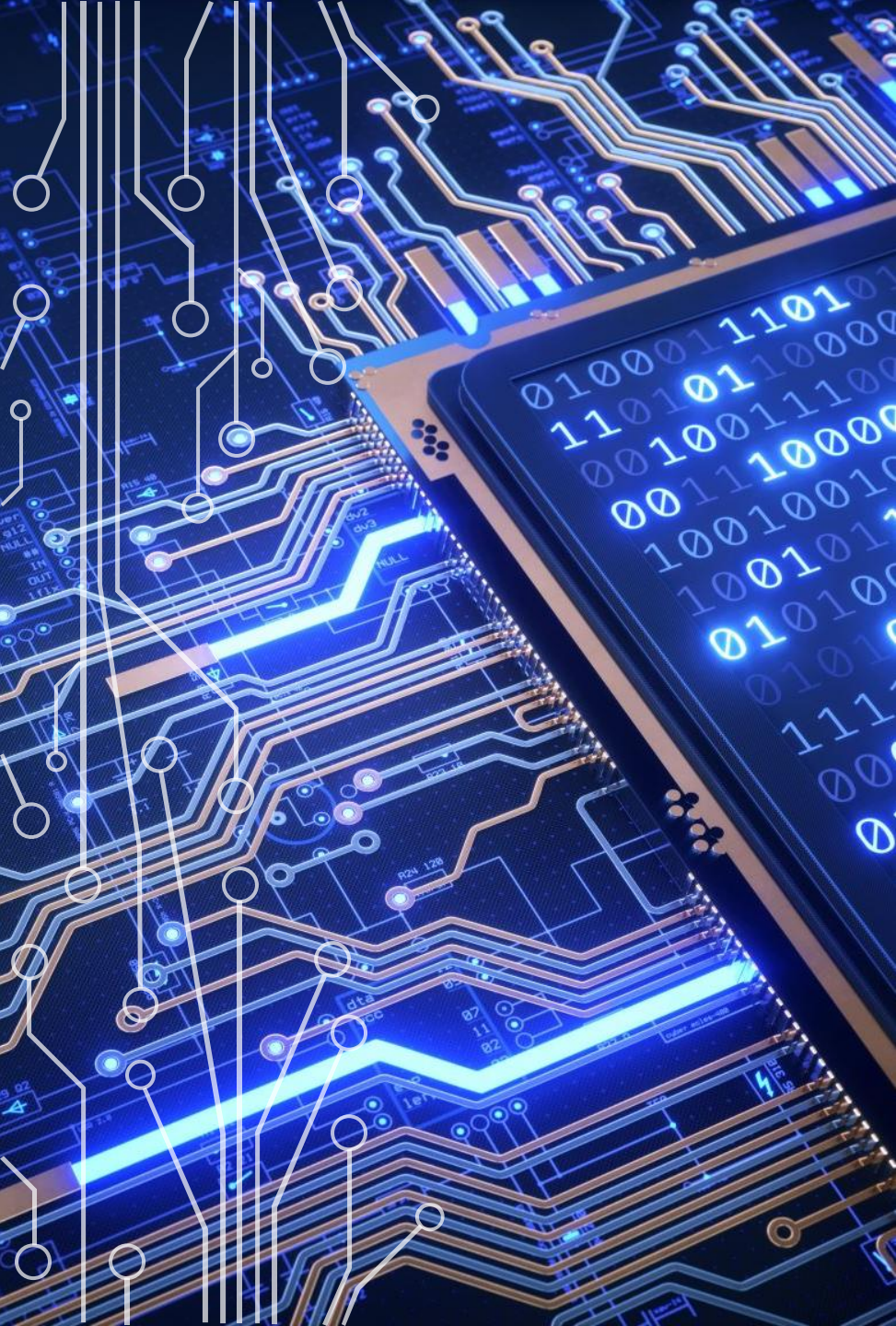
Legitimate uses:

- Children on School Buses
- Residents at Nursing Homes
- Time and Attendance
- Hazardous Worksite Safety

# RED TEAMING AND BIOHACKING

- Red teaming is a concept developed by the military when teams would penetrate friendly lines to expose flaws in their security.
- Often left a calling card or some sort.
- Late adopted in the cyber industry.
- How can you take a punch if you if you never get into the fight? Red Teamers bring that fight to you.





# RFID TAG FREQUENCIES

Two main types-

- Low Freq (LF) — 120kHz — 140kHz —  
Distance: up to 914 mm
- High Freq(HF) — 13.56MHz — Distance: from  
914mm to 3 Meters



# UNDERSTANDING RFID ACCESS SYSTEMS

Who uses them?

- The 'Legacy 125-kilohertz proximity technology' model is still at 70% to 80% of all physical access control for US companies that include
  - Government Establishments (and their contractors)
    - - Medical establishments
    - - Financial Institution
    - - Nuclear Sites
    - - Energy and water supplying establishments
    - - Educational institutions

And most are not encrypted and contain default or weak keys

# COMPONENTS OF AN RFID ACCESS BADGE SYSTEM

**Card:** sends a 26–37-bit number.

**Reader:** Converts the information on the card to the 'Wiegand Protocol' for transmission to the controller.

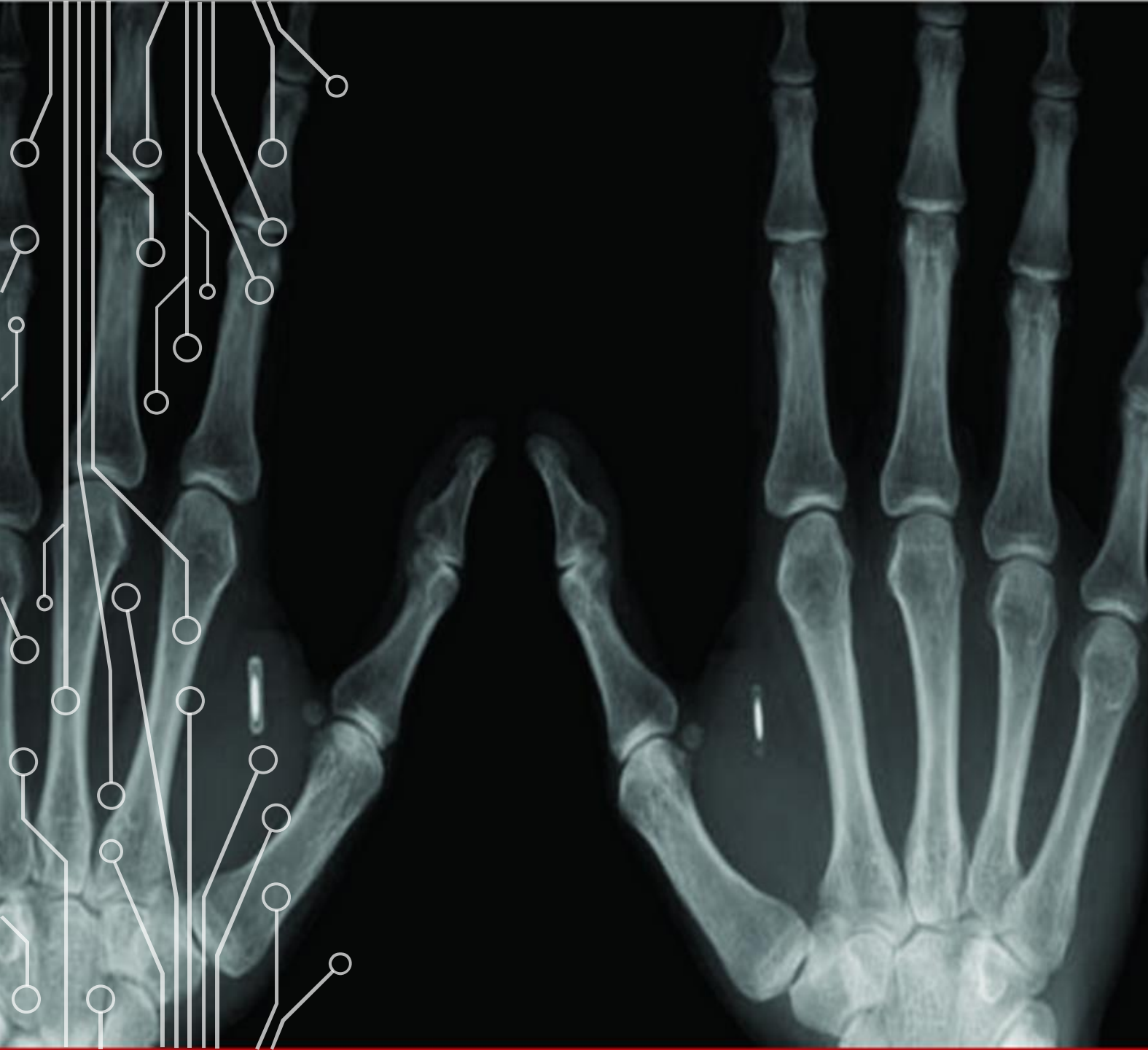
- No access decisions are made by the reader.

**Controller:** Data passed by the card in binary code is decoded.

- Decide whether to grant access.

**Host Computer:** Adds or removes cardholders, access privileges.

- Monitors real-time system events.



# THE CHIPS I HAVE IN ME

- NExT – NTAG216 13.56MHz NFC Type 2 ISO14443A RFID/NExT – T5577 125kHz Chip Emulator
- xM1 – 13.56MHz “Magic” gen1 Mifare 1k Emulator
- xG3 v2 – Injectable, clinically sterile, diametrically magnetized, lifting biomagnet implant
- Spark 2 – 13.56MHz NFC Type 4 ISO14443A RFID



### **NExT Chip Implant**

- The NExT is a 2mm x 14mm cylindrical chip implant. It contains both a 13.56MHz NTAG216 NFC chip and a 125kHz T5577 RFID chip. The NTAG216 NFC chip inside the NExT works with NFC capable smartphones, certain commercial access control systems and door locks, and USB contactless ISO14443A readers. The T5577 RFID chip inside the NExT is a 125kHz emulator that can be programmed to behave like many different types of common 125kHz low frequency chips, including EM41xx, EM4200, HID 1326 ProxCard II, HID 1346 ProxCard III, Indala (and more!) access cards and keyfobs.

### **xM1 Chip Implant**

- The xM1 is a 3mm x 13mm cylindrical chip. It has a gen1 “Magic” Chinese backdoor Mifare 1k Classic emulator chip inside which can be programmed to behave exactly like any Mifare S50 1k Classic chip-based access card or keyfob. While these types of RFID chips are considered “legacy”, there are many systems in use today that still use Mifare S50 1k Classic chips.

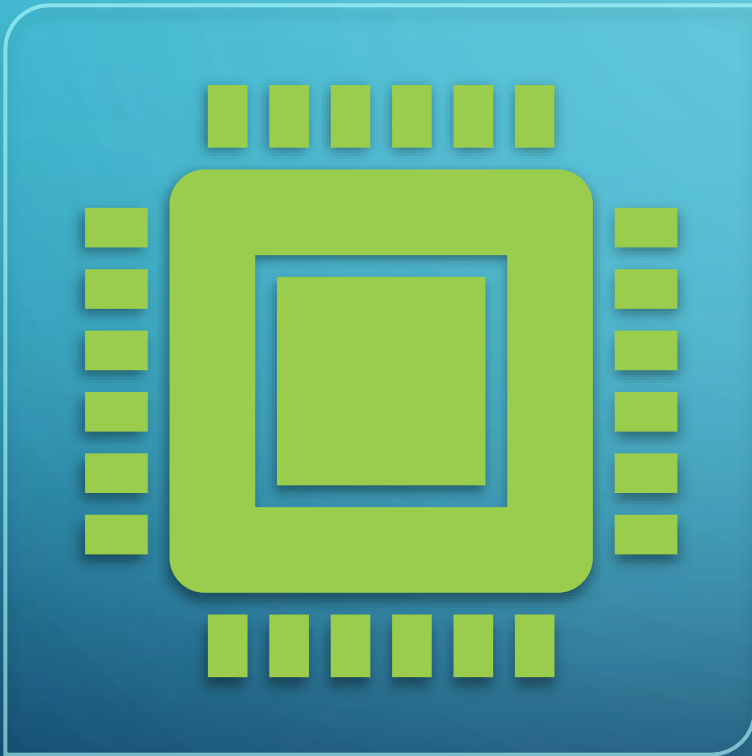
### **xG3 Implant v2**

- The xG3 v2 injectable biomagnet. The xG3 v2 is diametrically magnetized, which provides strong lifting capabilities.

### **Spark 2 Chip Implant**

- The VivoKey Spark 2 is a 2mm x 14mm cylindrical chip implant. The Spark 2 is a product designed and manufactured by VivoKey Technologies, makers of the only cryptobionic implants capable of performing strong cryptographic functions in vivo. The Spark is a 13.56MHz ISO14443A and NFC Type 4 compliant, readable by all NFC reader devices including all NFC capable smartphones and USB readers that are capable of reading ISO14443A chips. There is nothing to program, and it is cryptographically secure.

# CLONING RFID



- Super simple and quick!
- Tools are portable and easy to conceal
  - Proxmark 3
  - Chameleon Tiny
  - Smart phones



# IMPACT TO ORGANIZATIONS

- **DOS attacks with RFID**
  - Used to impede others from entering or general disruption
- **RFID WEB EXPLOITATION**
  - Data can be written directly to a card or RFID chip. Can be scanned by a smart phone or computer and sent to a malicious site.
- **SQL Injection with RFID**
  - Access systems are often vulnerable to SQL injection and payload can be passed via RFID
- **Buffer Overflow with RFID**
  - Can cause a crash of overflow the buffer of the application to inject a payload
- **Malware**
  - Delivered directly to the computer or a smartphone



**DEMO TIME!!**



**...WHAT COULD GO WRONG?**

makeameme.org

QUESTIONS?

