11º Fórum Espírito Livre

24 e 25 Set 2015 | Santa Teresa/ES

forum.espiritolivre.org

Realização

Rede Espírito Livre

INSTITUTO FEDERAL ESPÍRITO SANTO Campus Santa Teresa

Apoio

FAVENI

CLAIDS BISCOITOS

CAFÉ CARAMELLO

mozilla BRASIL

Associação Software Livre.Org

Sistema CFA/CRAs

ITAIPU BINACIONAL

CANAÃ 98,5

educaware

Serach

DualHosting

EASE MEDIA

ESPÍRITO SANTO Convention & Visitors Bureau

CRBio-02

Biohacking

Bio + Hacking == Ética Hacker aplicada a biologia

Quem eu sou

- Raphael Bastos aka coffnix
- Mantenedor da Slackzine (Zine Slackware-br)
- Organizador do Slackware Show Brasil (2011~2015)
- Organizador da II Oficina Livre – Pucminas (2007)
- Colaborador do SlackBook-ptBR - Livro do Slackware Linux (2007)
- Fundador do Slackware Users MG (desde 2007)
- Colaborador do projeto Funtoo Linux (desde 2013)
- Fundador do Área31 Hackerspace (desde 2013)

ATENÇÃO!!!!!

- Essa palestra **NÃO** é um aconselhamento médico.
- Tecnologias e pesquisas descritas são puramente experimentais e perigosas.
- **NÃO** tente fazer nada diferente do que foi descrito nesta palestra. (se fizer por favor documente)
- Sempre consulte seu médico para quaisquer problemas relacionados a saúde.
- Existem algumas imagens com procedimentos médicos nesta apresentação.

Objetivos

- Uma rápida viagem através da história da modificação corporal

  Pesquisa do Área31 Hackerspace sobre biochip implantável
- Riscos físicos do biohacking
- Insegurança (hacking)

Definições clássicas

HACKER:

- Uma pessoa que tem prazer em ter uma compreensão íntima do funcionamento interno de um sistema, computadores e redes de computadores em particular.

  O termo é freqüentemente mal utilizado num contexto pejorativo, em que "CRACKER" seria o termo correto.

Fonte: https://tools.ietf.org/html/rfc1392

Definições clássicas

BIOHACKING:

- Um termo novo, porém o significado do termo tem como origem a modificação corporal, que é uma prática quase ancestral em nossa espécie.

Fonte: http://www.oxforddictionaries.com/pt/definição/inglês-americano/hackerspace

Origem do Biohacking

- Origem no transhumanismo, termo este criado em 1957, pelo biólogo londrino Julian Huxley, que definiu o conceito como:

  “homem continuando homem, mas transcendendo, ao perceber novas possibilidades de e para sua natureza humana”.

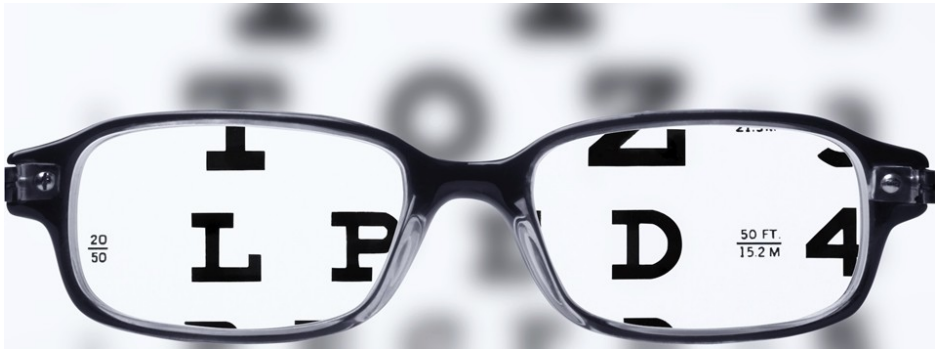
- Basicamente, qualquer modificação ou adaptação corporal é considerado um “BioHacking”.

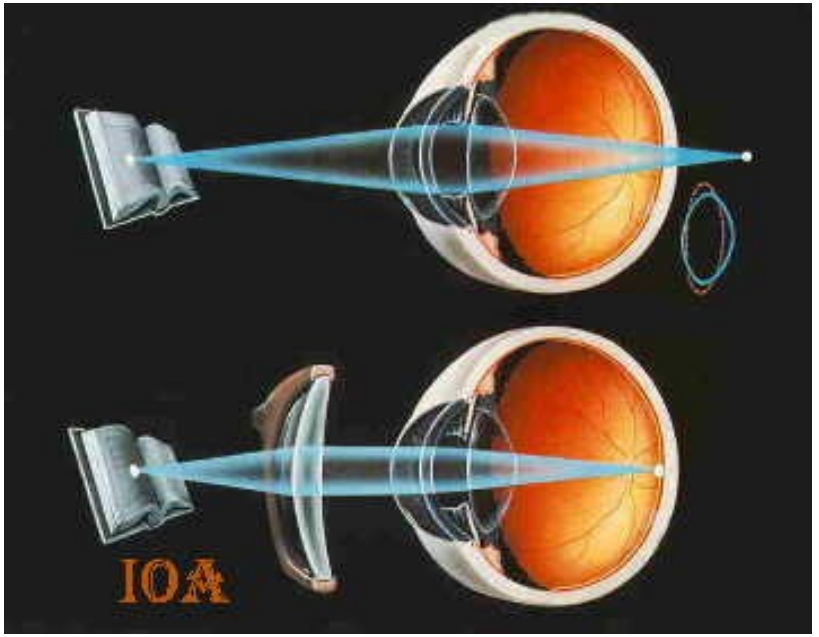
Transhumanismo

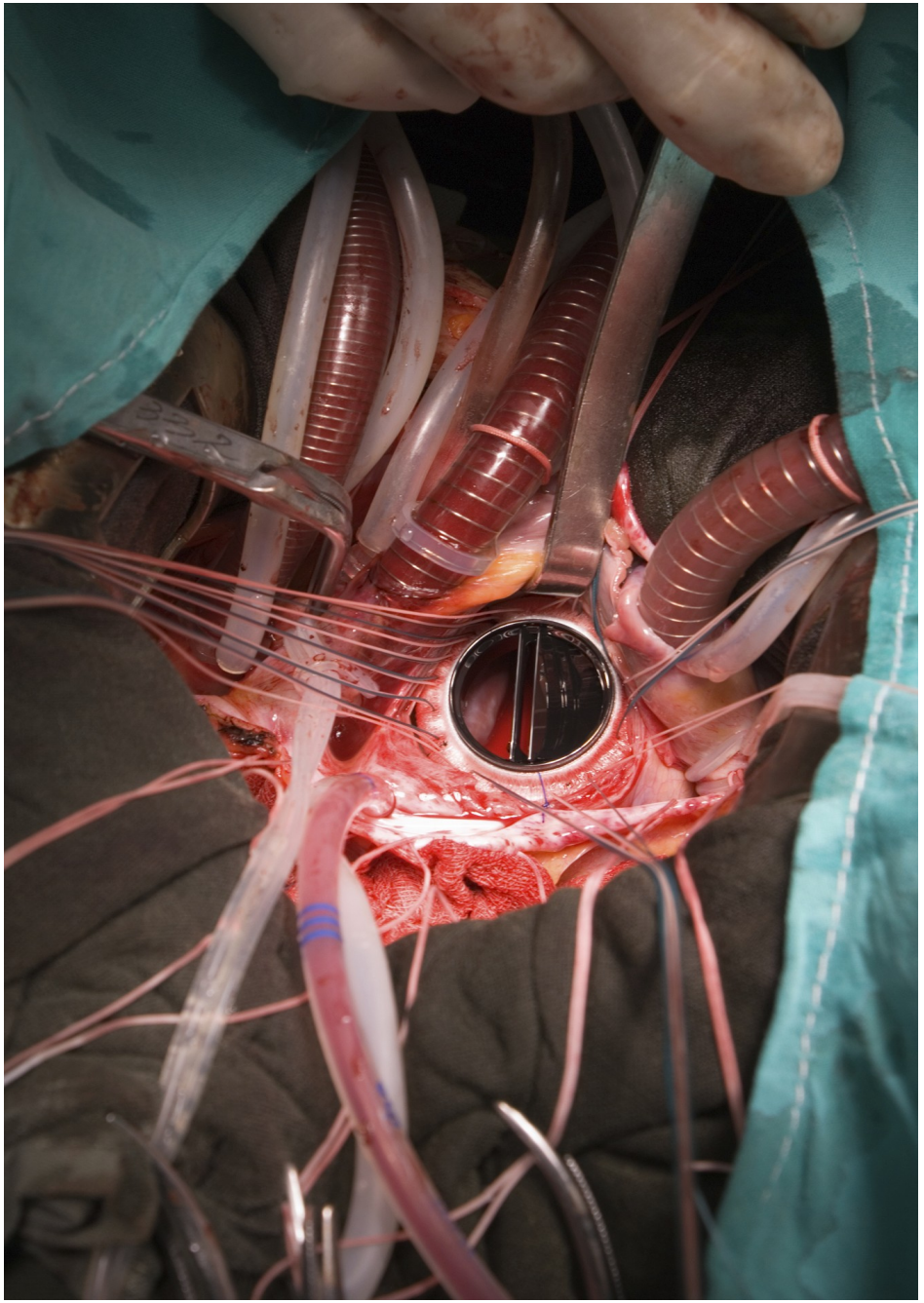
- Transhumanismo é a filosofia de que é possível, e também desejável, melhorar fundamentalmente a condição humana através do uso de tecnologias, especialmente da biotecnologia, da neurotecnologia e da nanotecnologia.

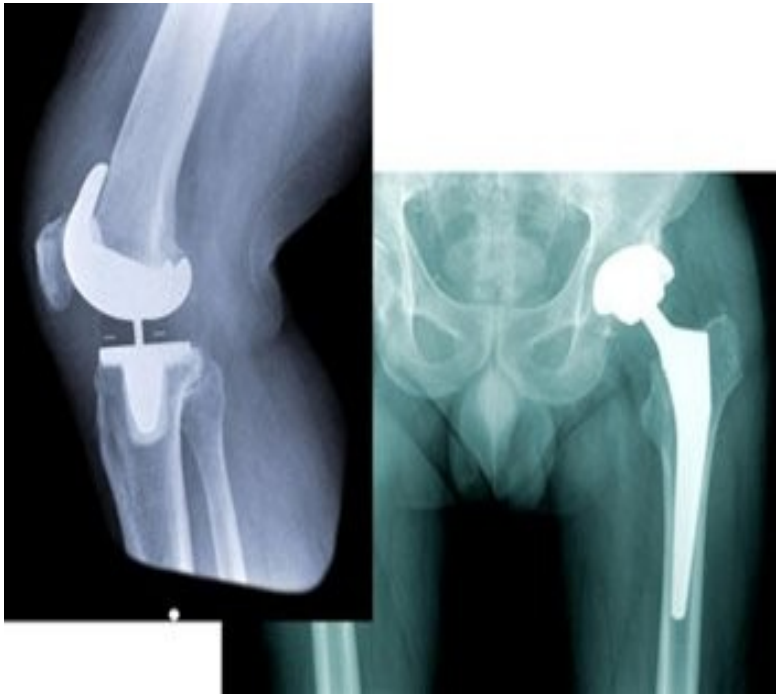
História do biohacking

- 3.300 A.C - Tatuagens mais antigas do mundo encontradas em múmias
- 1500 - Próteses básicas
- 1924 - **Eletroencefalograma (EEG)**
- 1927 - **Primeiro uso terapêutico da anfetamina**
- 1940 - Primeira cirurgia de implante de quadril
- 1952 - Válvula cardíaca artificial de bola
- 1958 - Primeiro marcapasso cardíaco implantável
- 1969 - **Descoberta do DNA**
- 1976 - Primeiros implantes neurais
- 1982 - Coração artificial
- 1984 - Implante coclear aprovado pela FDA
- 1990 - Joelho robótico controlado por microprocessador
- 1990 - Primeira terapia gênica (SCID)
- 1991 - Primeira nano estrutura sintética 3D
- 1997 - Primeiros implantes neurais para tratar doenças
- 1999 - Primeira nano máquina de DNA
- 2004 - Coração totalmente artificial aprovado pela FDA
- 2006 - Vacina de DNA (sucesso)
- 2007/2010 - Terapia gênica (sucesso)
- 2008 - Blade Runner (África do Sul) impedido de participar das Olimpíadas
- 2008 - Controle neural pelo cérebro humano.

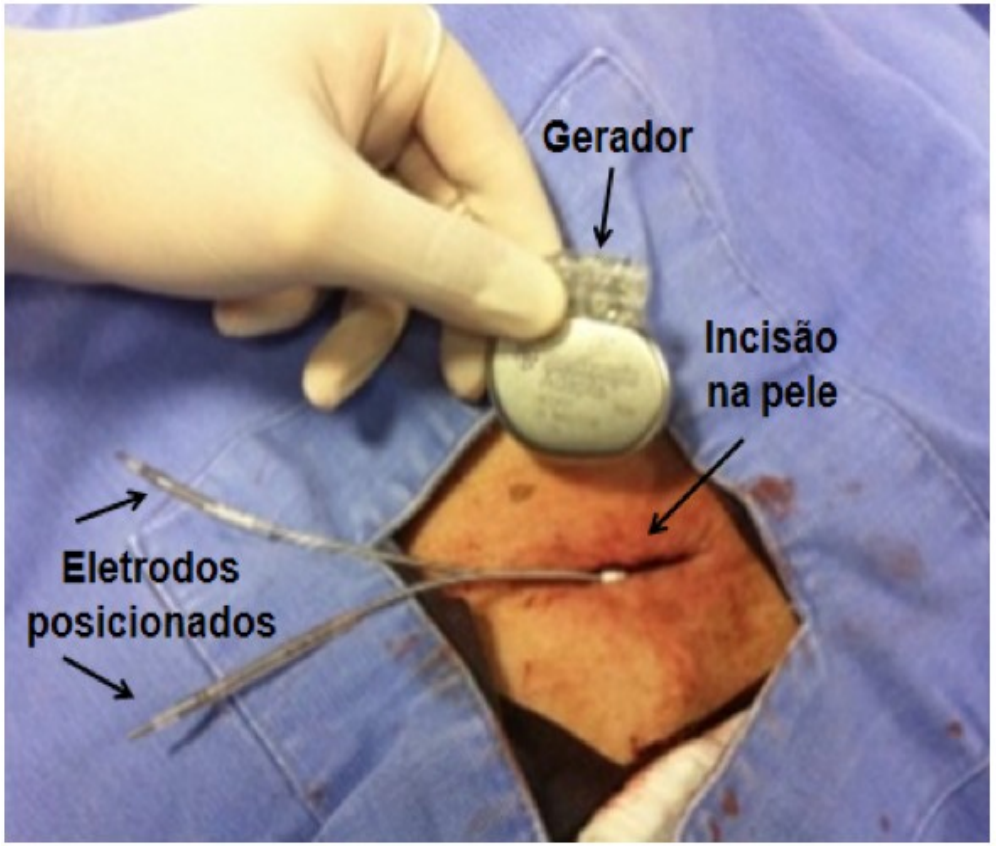

20
50
L P
D
50 FT.
15.2 M
4

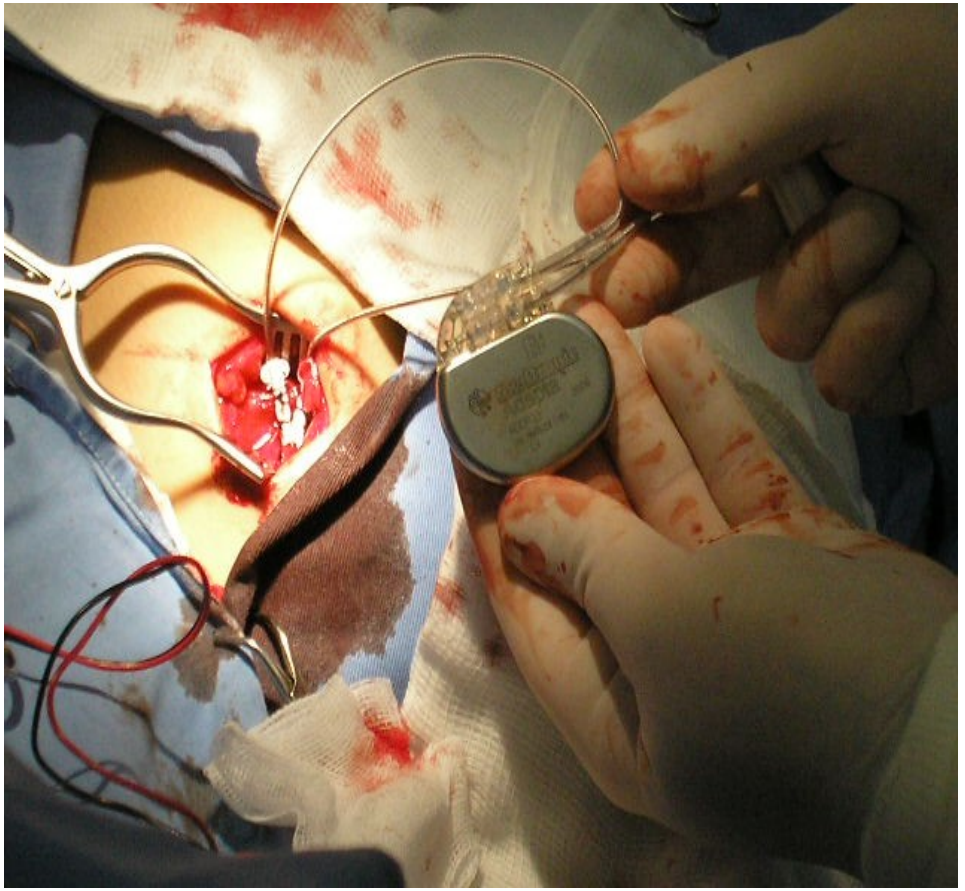

IOA

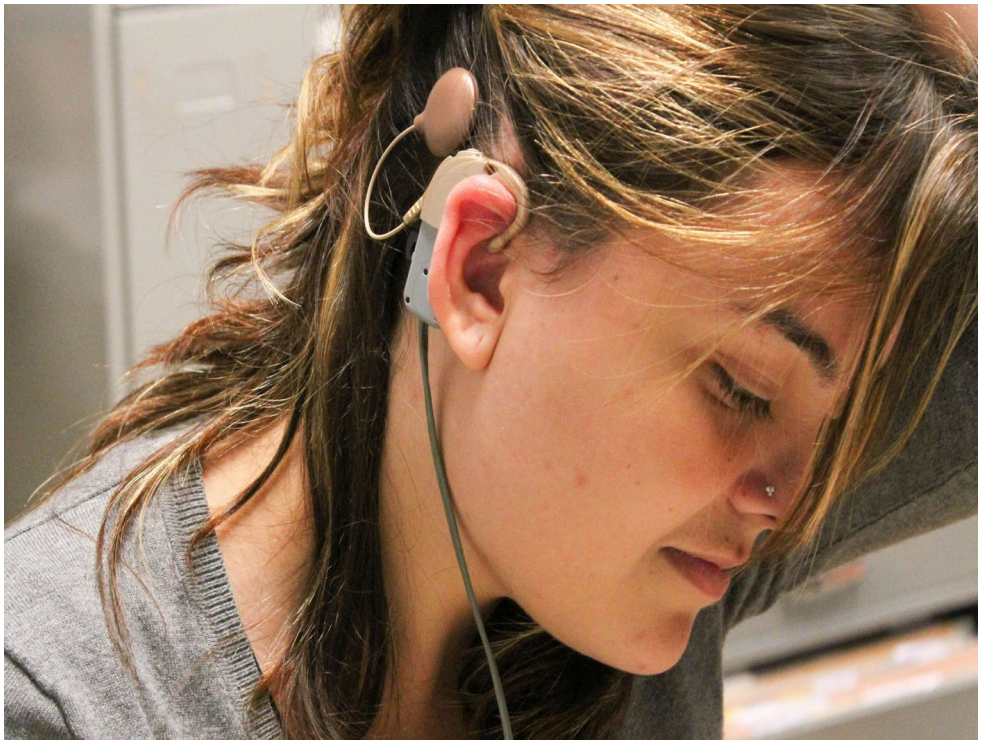


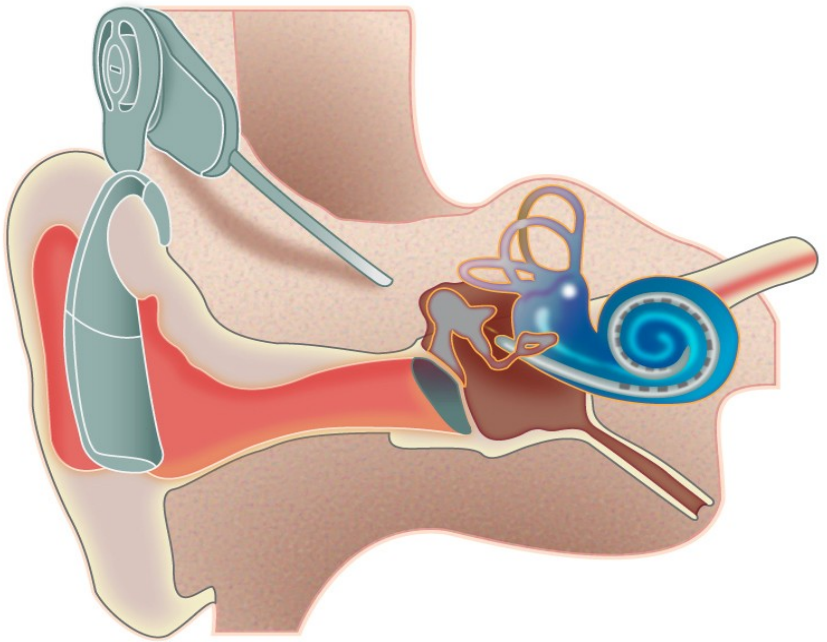


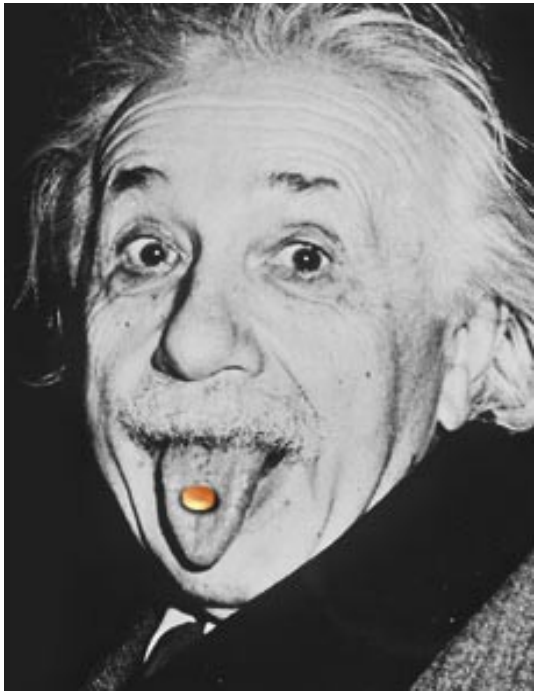

8
KBS


Gerador
Incisão
na pele
Eletrodos
posicionados



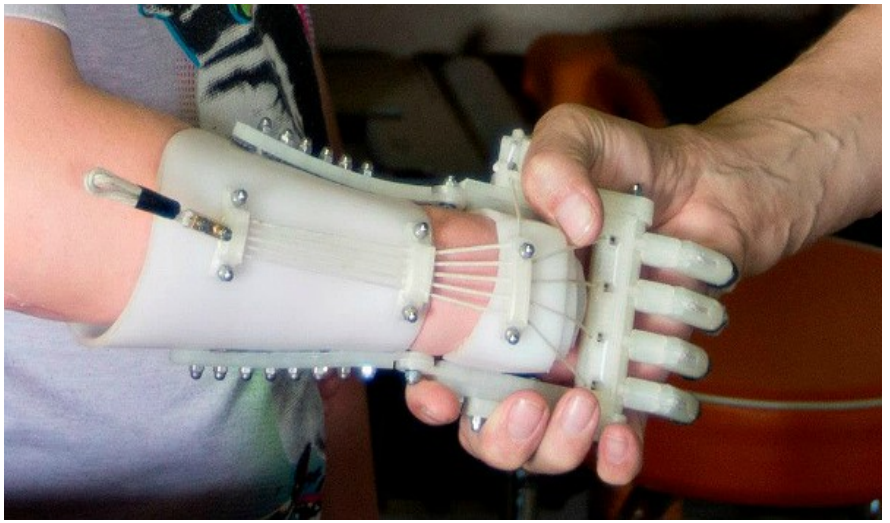






Stephen Hawking

Pai usa impressora 3D para construir mão biônica para o filho



Materiais bio-compatíveis

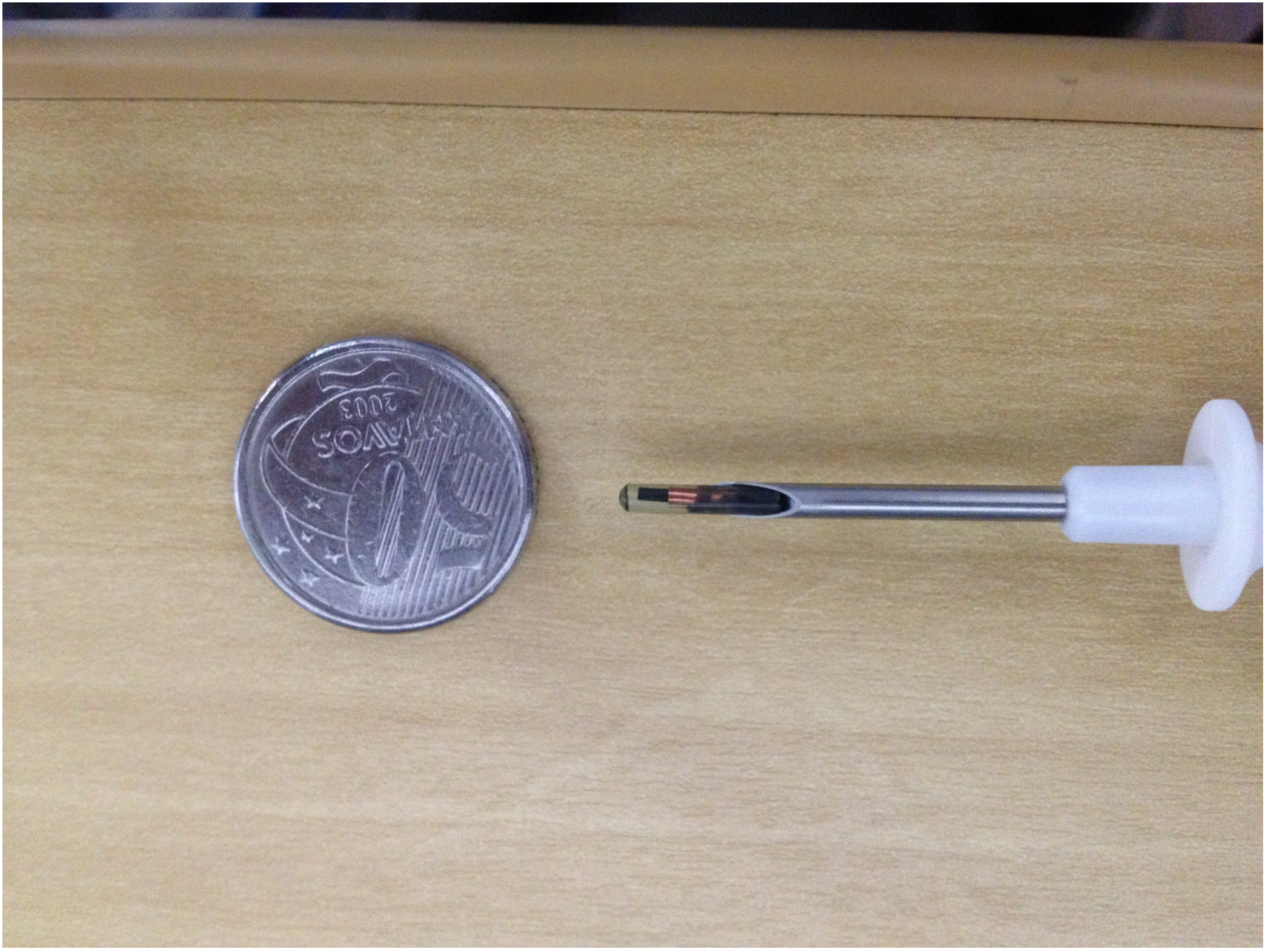
Metais

- Cromo
- Níquel
- Molibdênio
- Titânio
- Ligas de magnésio
- Ferro
- Cobalto

Polímeros

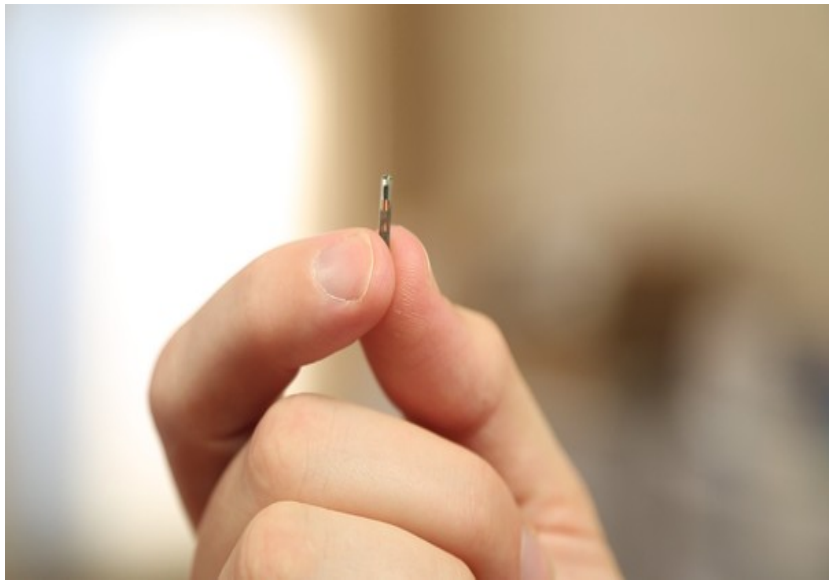
- Polietileno
- Trimetileno
- Carbonato
- Ácido poliglicólico
- Seda de aranha
- Poliéter-éter-cetonas
- Polysulfone

Biochip RFID/NFC implantável


2003

Descrição do Biochip RFID

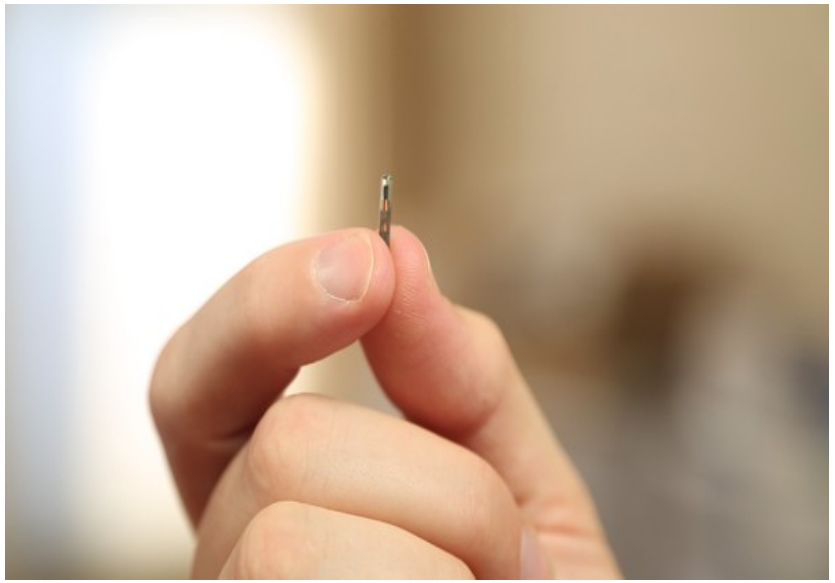
(125 KHz)



- 2,0mm x 1,2mm (cilíndrico)
- Tamanho de um grão de arroz
- Revestido em vidro **Schott 8625** (biocompatível)
- Identificador único e imutável
- Nenhum tipo de armazenamento
- Dispositivo passivo, não precisa de bateria e é completamente inerte
- Coisa do capeta..... **NOT!**

Descrição do Biochip NFC

(13.56 MHz)



- 2,0mm x 1,2mm (cilíndrico)
- Tamanho de um grão de arroz
- Revestido em vidro **Schott 8625** (biocompatível)
- Identificador único e imutável
- 888 bytes de memória programável
- Wireless Standard ISO 14443-A
- NFC compatível com o tipo 2
- Dispositivo passivo, não precisa de bateria e é completamente inerte
- Coisa do capeta..... **NOT!**

Onde e como é instalado

Implantação do biochip

Existem riscos físicos?

- Mesmo risco de se colocar um simples piercing
- Se feito corretamente por um profissional em um ambiente de estúdio limpo o risco é muito baixo
- Risco de rejeição do biochip (nenhum caso até a data atual)

E quanto a remoção? E se ele quebrar?

- Qualquer médico familiarizado com cirurgia básica pode facilmente remover o biochip com um pequeno corte de bisturi.

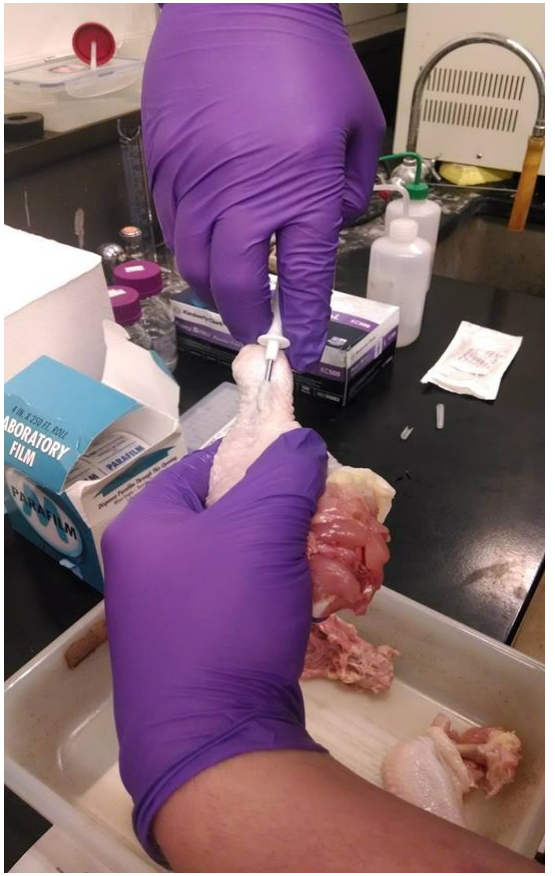
É doloroso? E sobre a cicatrização?

- Pode haver pouca ou nenhuma dor por alguns dias
- Dor similar a resultante de implantação de piercings em locais como a língua , nariz, ou cartilagem da orelha
- A cicatrização normalmente demora de duas a quatro semanas
- Não há qualquer problema em usar a mão levemente durante a primeira semana.

E quanto à privacidade?

- Leitura com distância máxima de 2cm
- O tamanho do dispositivo é extremamente pequeno
- A construção de um dispositivo leitor maior e mais poderoso que poderia ler o chip por alguns metros pode ser possível, no entanto, a real possibilidade de construção deste tipo de aparelho é bem remota.
- Rastreamento via satélite..... **NOT!**

Testes de resistência física



Resultados dos testes de resistência física

- Teste com silicone resultou em cerca de 15,2 quilos (185N) de força antes do biochip se quebrar

- Testes com carne de frango, ultrapassou a força máxima de 51 quilos (500N), sem danos

Aplicações atuais do biochip

- Autenticação (computadores, equipamentos eletrônicos diversos)
- Controle de acesso (catracas eletrônicas)
- Bilhetagem (metrô, ônibus, etc)
- Camada adicional de segurança
- Abertura de porta e ignição de carros e motos
- Acessibilidade a pessoas com dificuldades motoras ou de comunicação em geral

Riscos

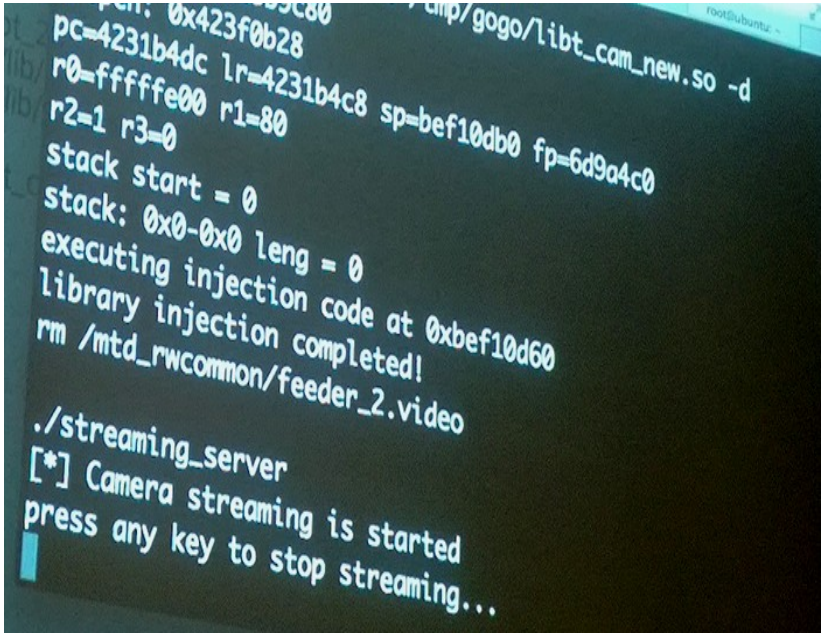
NÃO SEJA HACKEADO!

(don't want to be Owned)

Hard-coded PIN vulnerability found in smart toilets

A “Trustware SpideLabs” adverte que uma brecha de segurança no app para Android que controla o equipamento dá espaço para algum mal intencionado comprometer esses controles via Bluetooth. Usando o app ‘My Satis’, o hacker poderia, por exemplo, dar a descarga repetidas vezes – causando um grande desperdício de água – ou transformar o Satis num ‘vaso fantasma’, abrindo e fechando a tampa e ativando outras funçoes sem o conhecimento do usuário :-)

Smart TVs e geladeiras inteligentes são hackeadas e começam a disparar spam



“Um novo relatório indica que Smart TVs e geladeiras inteligentes são os novos alvos para a distribuição de lixo na internet. Depois desses eletrodomésticos serem hackeados, eles começam a enviar spam e e-mails maliciosos, de acordo com informações da empresa de segurança Proofpoint.”

Handheld clone ID Card

- Unit Price: US $25.00
- Free Shipping :D

http://www.dhgate.com/product/handheld-125khz-rfid-copier-id-card-clone/157446314.html

Solução ideal para clonar RFID

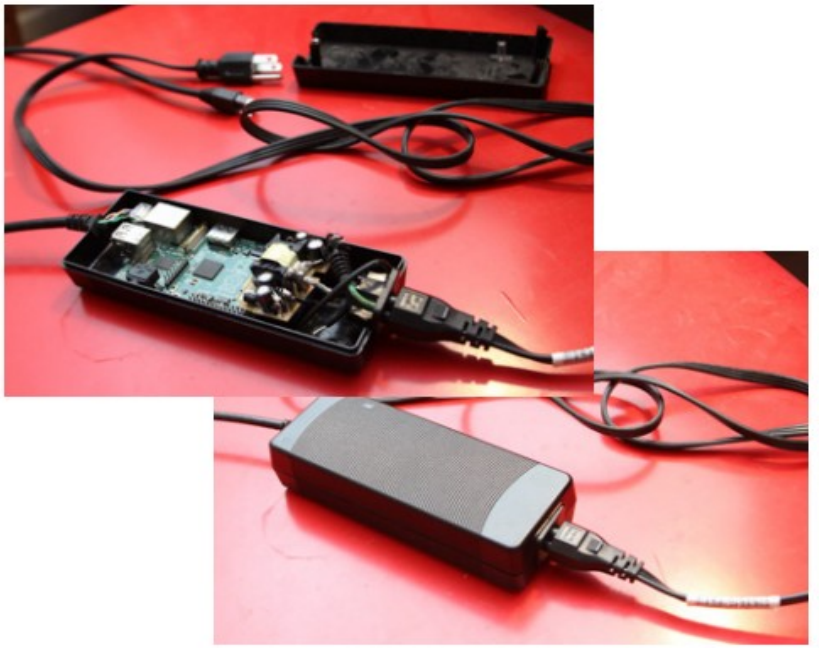
(Melhor alcance)

Clone RFID com baixo custo

Raspberry Pi

MAINTAINING ACCESS

- Raspberry Pi – cheap alternative (~$35) to Pwn Plug/Power Pwn
  - Pwnie Express – Raspberry Pwn
  - Rogue Pi – RPi Pentesting Dropbox
  - Pwn Pi v3.0



Formas possíveis de **hackear**

- Ataque malicioso para travamento intencional

  Modificação do capability container - NFC standard (E1 12 6D 00)

- Desbloqueio de TAG ou desativação de senhas

- Sobrescrita de dados no biochip com travamento posterior (ransomware biológico?)

Formas possíveis de **defesa**

- Bloqueio do capability container contra modificação acidental ou mal-intencionada
- Bloqueio da TAG (proteção por senha)
- Congelamento da TAG (static and dynamic lock bytes), fechando páginas de memória de usuário em um estado permanente (read/write)

Formas possíveis de **defesa**

- Utilizar o App do fabricante para ativação das defesas recomendadas pelo Área31 Hackerspace

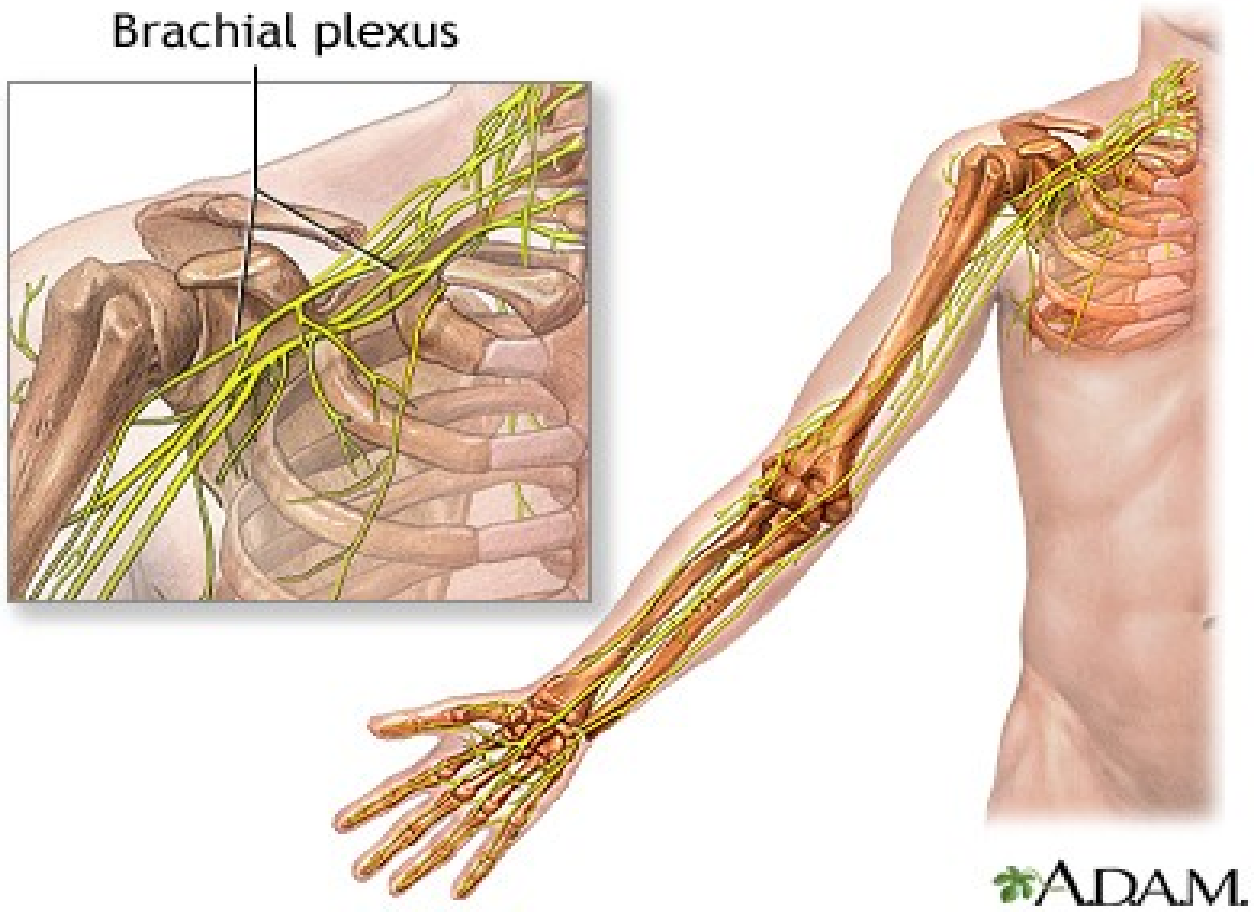
–> Dangerous NFC (BETA) <–

Suporte a TAGs NTAG213 e NTAG215

https://play.google.com/store/apps/details?id=com.dangerousthings.nfcs

Posso me proteger ???

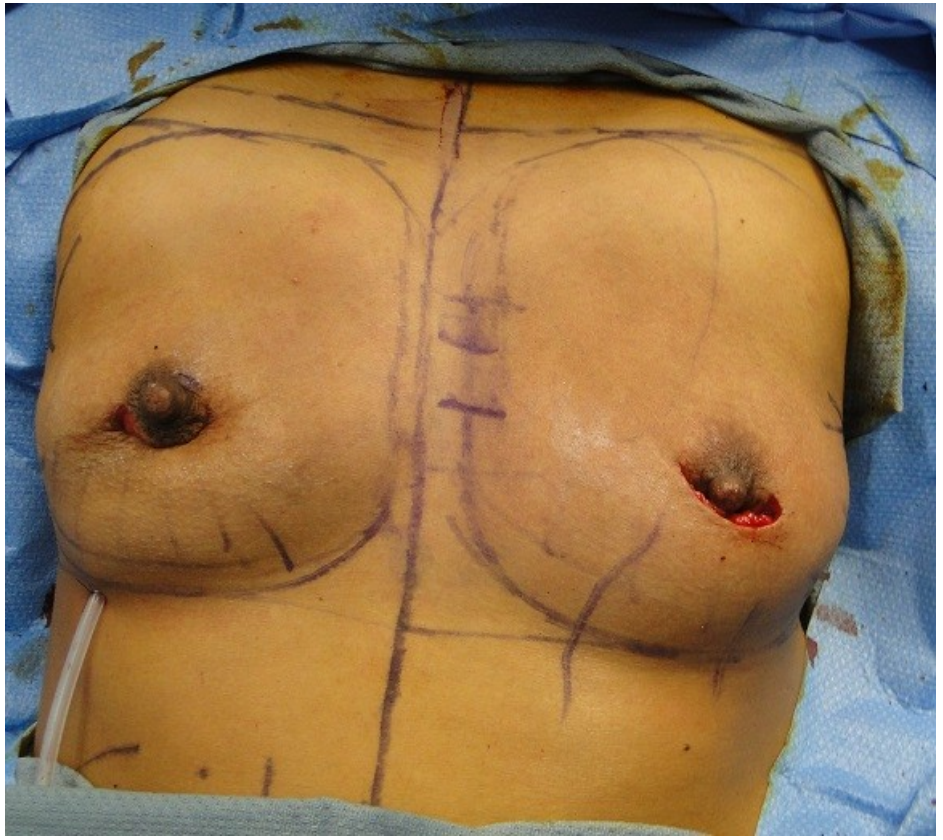
Sensores naturais



CUIDADO: O CORPO NÃO TEM BACKUP!

Risco: Infecção

Risco: Consequências imprevisíveis



Risco: Fanatismo religioso

Risco: **ESTUPIDEZ**

ESTE CARA..... NÃO SEJA ESTE CARA!

O que realmente importa

(Dispositivo implantável)

- **Possui baterias?** Não. O dispositivo é passivo.
- **Possui materiais tóxicos?** Não.
- **O tamanho é aceitável?** Sim.
- **Qual é a capacidade?** NFC 144 ~ 888 bytes
- **O custo é acessível?** Sim.
- **Emite calor ou radiação?** Não.

Custo médio

- **Marcapasso cardíaco** – US$ 23mil
- **Substituição Hip** – US$ 23mil (cada lado)
- **Prótese de perna** – US$ 36mil (cada perna)
- **Implante coclear** – US$ 40mil (cada orelha)

- **Biochip RFID** – apenas US$ 39 (unidade)
- **Biochip NFC** – apenas US$ 99 (unidade)

Realização

www.area31.net.br

Perguntas?

Obrigado!

Site: www.area31.net.br

Twitter: @coffnix

Skype: coffnix

Email: raphaelbastos@hackstore.com.br