Ordine degli Ingegneri di Pisa
T.A.G. - Talent Garden Pisa
via Umberto Forti 6, Montacchiello (PI)
20 ottobre 2017 – 14:00 – 19:00

IISFA European Chapter

Breve storia dell'Internet delle Cose

14 anni di storia di un nuovo universo, con una "autopsia" del suo primo abitante: Nabaztag

Marco A. Calamari
marco.calamari@ordineingegneripisa.it

IISFA – International Information Systems Forensics Association: Italian Chapter

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/

- **Marco Calamari, classe 1955, ingegnere nucleare, si cimenta a rotazione tra attivita' di consulenza tecnica informatica, Computer Forensics, editoriali e di formazione.**
- **Membro di: IISFA, AIP, Opsi, Hermes Center, PWS**
- **Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.**
- **Fondatore del *Progetto Winston Smith* e del *Centro Hermes per la Trasparenza ed i diritti digitali*.**
- **Dal 2003 scrive su Punto Informatico ed altre riviste la rubrica "Cassandra Crossing", che ha superato le 400 uscite. (www.cassandracrossing.org)**

Di cosa parleremo

L'Internet delle Cose e' troppo giovane ed evolve troppo rapidamente per avere una storia condivisa.

Esistono solo alcuni fatti rilevanti dell'IoT (Internet of Things – Internet delle Cose), la definizione di cosa rende un oggetto una ToIoT (Thing of Internet of Things – Cosa dell'Internet delle Cose) non e' condivisa o non esiste.

Per questo motivo ho cercato di definirle ambedue, anche se, sottolineo, si tratta di definizioni personali.

Questo ha richiesto:

Primo: dare una definizione esatta di IoT and ToIoT.

Secondo: trovare idee, oggetti e fatti importanti che permettano di costruire una "storia".

IoT: oggetti, computer, software, internet

Oggetti: e' la parola con cui iniziare l'analisi.

Smartphone, tablet, laptop, automobili, lavatrici, ferri da stiro, tutti questi oggetti possiedono una singola funzione, che usiamo quando vogliamo per fare cio' che vogliamo.

Per questo noi percepiamo l'oggetto come "semplice" perche' lo identifichiamo con la singola funzione che svolge.

Tutto questo e' cambiato da quando questi "oggetti" hanno iniziato a contenere software "embedded"..

Contenere software e' una caratteristica essenziale affinche' un oggetto sia parte dell'IoT, ed e' anche la causa di tutti i problemi e le preoccupazioni che l'avvento dell'IoT ha provocato.

Eventi importanti

Cominciamo ad elencare i fatti importanti per costruire una timeline, che non e' una "storia" ma e' un buon inizio per costruirla.

Prometto che viaggeremo alla massima velocita' tra questi fatti, come il *"Viaggiatore del Tempo"* del romanzo "La Macchina del Tempo" di H.G. Wells.

1991: Mark Weiser pubblica su "Scientific American" l'articolo *Il computer per il 21mo Secolo* che descrive, pur senza dargli un nome, l'avvento del "Disappearing Computer" il computer che scompare.

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."

Eventi importanti - 2

1998: sempre Mark Weiser costruisce una fontana davanti il suo ufficio il cui getto rappresenta l'andamento del mercato azionario.

Ma fatto ben piu' importante, quello stesso anno introduce la definizione che mancava:

"Ubiquitous computing is roughly the opposite of virtual reality. Where virtual reality puts people inside a computer-generated world, ubiquitous computing forces the computer to live out here in the world with people."

Eventi importanti - 3


Credit: RFID Journal

1999 – il termine "Internet of Things" - Internet delle Cose viene (sembra) coniato da Kevin Ashton, direttore esecutivo di *"Auto-ID Center"*:

"I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is stil often misunderstood."

Կարեւոր փաստեր-Նաբազթագ

2005: nasce Nabaztag

E’ la traslitterazione (non la traduzione)

del termine armeno

Lepre - “Նաբազթագ".

Concepito da Rafi Haladjian e Olivier Mével, e prodotto in oltre 100,000 esemplari dall’azienda francese Violet; Violet dopo poco falli’, vittima del suo stesso successo, e venne acquistata da Mindscape. Successivamente anche Mindscape fu ceduta, ed i suoi asset (hw & sw di Nabaztag), furono acquistati da Aldebaran Robotics e divennero abandonware.

Il mio coniglio (anzi i miei 6) sono la sola cosa computerizzata che in 30 anni di convivenza mi abbia fatto fare bella figura con la mia signora. Il motto di Nabaztag e’ (non per nulla) "If you can even connect rabbits, then you can connect anything" (credit: @kinivazquez)

Eventi importanti - 4

Nabaztag possiede un bottone sulla testa, due orecchie con fissaggio magnetico mosse da motori passo-passo e dotati di encoder per leggerne la posizione via Software, 5 LED RGB, un lettore RFID, una scheda audio con microfono ed una scheda WiFi.
E' controllato da un server remoto, originariamente programmato in Ruby on Rails, su cui ogni proprietario di Nabaztag deve caricare plugin e "programmarli".

Nabaztag puo' muovere orecchie e fare coreografie con i LED, puo' leggere oroscopi, previsioni del tempo ed indici azionari dal web e dirvi l'ora, anche con battute spiritose. E' possibile "sposare" due conigli cosicche' se si muovono le orecchie ad uno, l'altro inizia a cantare, lampeggiare e sposta le orecchie nella stessa posizione. Commovente e divertente anche se non facile da spiegare ad un cliente in ufficio!

Eventi importanti - 5

2015: viene presentato Amazon Echo / Alexa

Anonimo come il monolite di "2001: Odissea nello spazio", costa ai suoi acquirenti circa 150 euro e permette di ospitare un'intelligenza artificiale controllata da Amazon in casa, mettendola quindi in grado di ascoltare, con 6 orecchi sopraffini, tutto quello che viene detto.

Intelligenza Artificiale e Internet delle Cose si fondono nel vostro soggiorno allo scopo di vendervi piu' cose possibile, ma anche di carpirvi piu' dati personali possibile, e quest'ultima cosa passa largamente inosservata...

La definizione di IoT

Internet of Things

e' la materializzazione di quanto era stato definito a livello teorico

Ubiquitous Computing

e successivamente

Pervasive Computing,

Ambedue venivano considerate in passato positive e desiderabili conseguenze delle tecnologie informatiche.

La maggior parte delle persone, ancora oggi, e' rimasta di questa opinione … ma ne siamo sicuri? Io no.

Breve storia dell'IoT

Storia e problematiche dell'IoT

I 5 eventi che abbiamo visto, tutti avvenuti nel non breve periodo dal 1991 al 2015, sono abbastanza per raccontarci in generale la storia dell'IoT.

In effetti l'IoT e' meglio descritta non da una "storia" ma da un elenco delle opportunita' che offre e dei problemi che causa.

La piu' importante opportunita' dell'IoT e' data senz'altro dall'essere formata da oggetti complessi e potenti, contenenti sensori, potenza di calcolo e molto software, che rendono non percepibile la propria complessita' interna.

Ma non sorprendentemente, i problemi derivano appunto dall'essere formata di oggetti complessi e potenti, contenenti sensori, potenza di calcolo e molto software, che rendono non percepibile la propria complessita' interna.

Storia e problematiche dell'IoT -2

Nascondere la propria complessita' ed essere potenti sono caratteristiche contenute nella nostra definizione di IoT; non possiamo quindi considerarle problemi da eliminare; non potremmo farlo senza cancellare l'IoT completamente.

D'altra parte contenere software, che e' intrinsecamente flessibile, puo' anche permettere di mantenere le prestazioni degli oggetti dell'Iot riducendone i problemi.

Ma i produttori lo vorranno fare?

Ad aggravare il problema della complessita' nascosta, queste grandi quantita' di software vengono inserite in oggetti familiari (es. televisore) che non consideriamo parte dell'IoT ma piuttosto evoluzione di oggetti semplici e preesistenti che facevano solo una cosa, e che oggi la fanno semplicemente meglio.

Il software nella IoT

In maniera molto grossolana ma efficace, la quantita' di software si puo' misurare contando le linee di codice sorgente che il programmatore ha usato per scriverlo.

Come ben sappiamo, queste linee, trasformate da appositi compilatori od interpreti, diventano il software che, tramite i computer (ordinari od embedded), utilizziamo coscientemente tramite i programmi "normali" ma anche, senza accorgercene, utilizzando gli oggetti "smart" dell'IoT.

Percio' quando utilizziamo coscientemente il software con i programmi per pc, tutto fila (piu' o meno) liscio, ma quando lo facciamo interagendo con gli oggetti dell'IoT, quindi in maniera non percepibile, strane cose, anche "brutte" possono accadere...

Dove sta il problema ?

- **Nel 1969 siamo andati sulla Luna con meno di 10.000 linee di software, e per lo Shuttle negli anni ‘90 ne sono bastate 400.000.**
- **Un pacemaker ci salva la vita con 100.000 linee, tante quante ne aveva Photoshop 1.0, che pero’ oggi e’ cresciuto a 3.500.000.**
- **Nel 1971 la prima versione di Unix aveva 10.000 linee, mentre Debian 5.0 (Lenny) nel 2009 ne aveva 65.000.000 (incluse pero’ le applicazioni).**
- **Nel 1991 Windows 3.1 contava 2.000.000 di linee, nel 2001 Windows XP 43.000.000**
- **Un “vecchio” caccia supersonico F22 “Raptor” si contentava di 2.000.000, mentre un aereo da trasporto Boeing 787 ne vuole 9.000.000 ed il famigerato F35 45.000.000**

Quanto software?

- Il rover "Curiosity" ha esplorato Marte con “solo” 5,000,000 di liee di programma.
- Il Large Hadron Collider, il piu’ grande strumento mai costruito dall’uomo, per trovare il bosone di Higgs ha avuto bisogno di 50,000,000 di linee.
- Ma una moderna autovettura di fascia alta contiene certamente piu’ di 100,000,000 (dicasi centomilioni) di linee di codice.
- Per fare un confronto, si consideri che il DNA di un topolino puo’ essere descritto con “solo” 120,000,000 di "linee di codice".

Considerando la loro complessita’, questi sono ancora da considerare "Oggetti"? O non sarebbe meglio chiamarli "Soggetti"?

E perche’ cosi’ tanto software? Cosa fa e per chi lavora? Per il proprietario o per il suo fabbricante?

Evoluzione di oggetti semplici

Ferro da stiro

Dal 1700 ad oggi: 0 linee di codice

Telefono fisso
dal 1850 al 2000: 0 linee di codice

Smartphone

Dal 2005 ad oggi: da 1.000.000 a 30.000.000 ...

… per merito di un sistema operativo che contiene Linux

Fiat 500.

Dal 1960 ad ora: da zero a 50.000.000 di linee

Televisione
Nel 1935: zero

Televisione

Nel 1954: stessa tecnologia, ancora zero

Televisione a magnifici colori del 1984.
Malgrado la data infelice, e' bella, usa nuove tecnologie e non e' affatto "pericolosa".
Infatti niente software; ancora zero linee

Televisore moderno
Ti vede e ascolta e riferisce al suo creatore.
Il manuale lo dice anche, ma nessuno lo legge.
Contiene piu' di 30.000.000 di linee di codice

Televisione prossima ventura

Vi ascolta, vi vede ed agisce di sua iniziativa.
Sa cosa vi piace, e' piu' di un sistema esperto, forse avra' un'intelligenza artificiale.
Usa il cloud, e non c'e' limite alla quantita' di software che puo' "contenere". La vorrete in casa?

~~La prestazione~~ il problema finale

Le tre leggi di Zuboff dicono:

Prima Legge, qualunque processo che possa essere automatizzato, sara' certamente automatizzato.

Seconda Legge: qualsiasi cosa che possa essere informatizzata, sara' certamente informatizzata.

Terza Legge: qualunque applicazione possa essere utilizzata anche per sorveglianza e controllo, sara' certamente utilizzata per sorveglianza e controllo.

(sorveglianza == intercettazione di dati personali)

Nabaztag sul lettino

Նախագիծ

Նախագիծ Opera

Genealogia dei Nabaztag

Durante l'evoluzione dei conigli, nell'IoT, vennero prodotte tre versioni di Nabaztag.

Nabaztag (o Nabaztag v1) contiene:

- Un micro controllore PIC18F6525
- Una scheda WiFi BenQ 802.11b
- Un digitalizzatore audio ML2870a PCM
- Un convertitore ADPCM
- Due motori passo-passo e relativi encoder per il movimento delle orecchie
- Un controller TLC5922 per i LED multicromatici
- Poca, ma davvero poca, memoria; 48 kB per il programma, 3.840 Byte per i dati.

Genealogia dei Nabaztag - 2

Il firmware monolitico del v1 gestisce direttamenteil traffico TCP/IP ed il driver Wi-Fi.

Implementa una “macchina virtuale” in grado di eseguire fino a 64kb di bytecode, cross-assemblato esternamente da un assemblatore dedicato.

Per l’interazione con il server (ricordiamo che il Nabaztag e’ un client) esiste una API per programmare azioni, comportamenti e coreografie, disponibile per molteplici linguaggi di programmazione, tra i quali Java e Perl; questo permette a sviluppatori terze parti di sviluppare ed offrire ulteriori applicazioni.

Genealogia dei Nabaztag - 3

Nabaztag:tag (o Nabaztag v2)

In vendita dal 12 Dicembre 2006, Nabaztag:tag supporta lo streaming di audio MP3, anche da Internet Radio e da podcast.

Ha un microfono incorporato, che permette tra l'altro l'attivazione vocale di eventi preprogrammati.

Ha un lettore di RFID per riconoscere alcuni modelli di tag RFID (i.e. ISO/IEC 14443 Type B) e quindi "identificare" gli oggetti su cui sono attaccati.

E' dotato inoltre di una uscita audio jack e di una "manopola-coda", che permette di regolare il volume.

Genealogia dei Nabaztag - 4

Mentre il Nabaztag viene aggiornato solo in modalità "push" (il dispositivo viene chiamato dal server appena un nuovo contenuto e' disponibile per essere riprodotto), il Nabaztag:tag usa anche la normale modalita' client "pull" (ossia è lui ad interrogare il server).

Nell'Ottobre 2008, Violet lancia gli RFID Children's Books in joint venture con Penguin Publishing House. Contenevano un RFID che permetteva di farli (apparentemente) leggere al Nabaztag

Vengono anche messi in vendita i tag RFID adesivi Zstamps ed i Nano:ztags (graziosi conigli in miniatura contenenti un tag RFID). La scheda WiFi e' sostituita da una SoftMAC che supporta la crittografia WEP/WPA e contiene nel firmware gli stack TCP/IP e 802.11.

Genealogia dei Nabaztag - 5

Karotz (o Nabaztag v3)

Karotz viene rilasciato nell'Aprile 2011 da Mindscape. E' dotato di webcam, di porta USB (che puo' essere usata anche per l'alimentazione oltre che per collegare periferiche) e di 256 MB di RAM on board. Un pc con le orecchie.

Karotz e' fortemente integrato con Facebook e Twitter.

Dopo appena pochi mesi, nell'Ottobre 2011, Mindscape e' acquistata da Aldebaran Robotics, che annuncia "*Insieme continueremo questa meravigliosa avventura*".

Ma inspegabilmente, nell'Ottobre 2014, Aldebaran Robotics annuncia "*La fine dell'avventura dei Karotz … i server … cesseranno di funzionare il 18/02/2015*".

Genealogia dei Nabaztag - 6

Nel 2016 una nuova API per il Karotz, "Free Rabbits", viene creata da una iniziativa di appassionati.

In precedenza altre comunita' di volontari gia' avevano rilasciato, con iniziative simili, numerosi cloni di software per il server di gestione dei Nabaztag v2.

Successivamente alcuni dei software suddetti vengono adattati per suportare anche il Nabaztag v1.
Per questa versione e' richiesta pero' una modifica al firmware, perche' il nome del server era cablato in esso senza possibilita' di modificarlo, possibilita' presente invece nei v2 e v3.

Genealogia dei Nabaztag - 7

Genealogia dei Nabaztag - 8

L'Autopsia

Autopsia di un Nabaztag

Il Nabaztag:tag e' e' di gran lunga il piu' comune tra le specie di conigli che abitano l'IoT.

La sua popolazione e' stimata in 100.000 "abitanti", su una popolazione totale di conigli connessi (v1+v2+v3) di oltre 150.000.

L'autopsia quindi verra' effettuata su di un Nabaztag:tag v2, grazie anche alla collaborazione del Progetto Winston Smith, e di un video di RobotShop.com

PROGETTO WINSTON SMITH

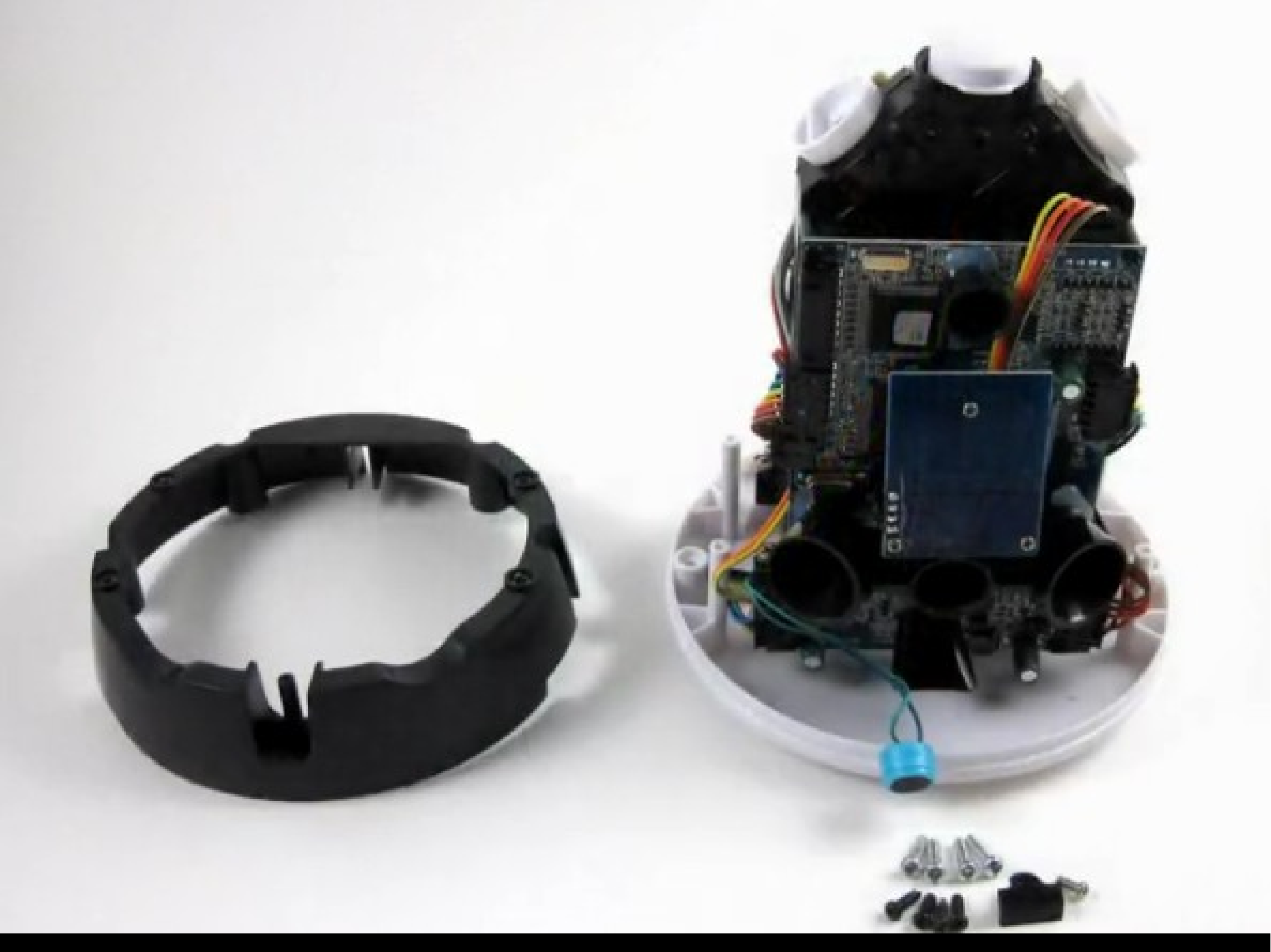

Magnetic ears are easy to remove.

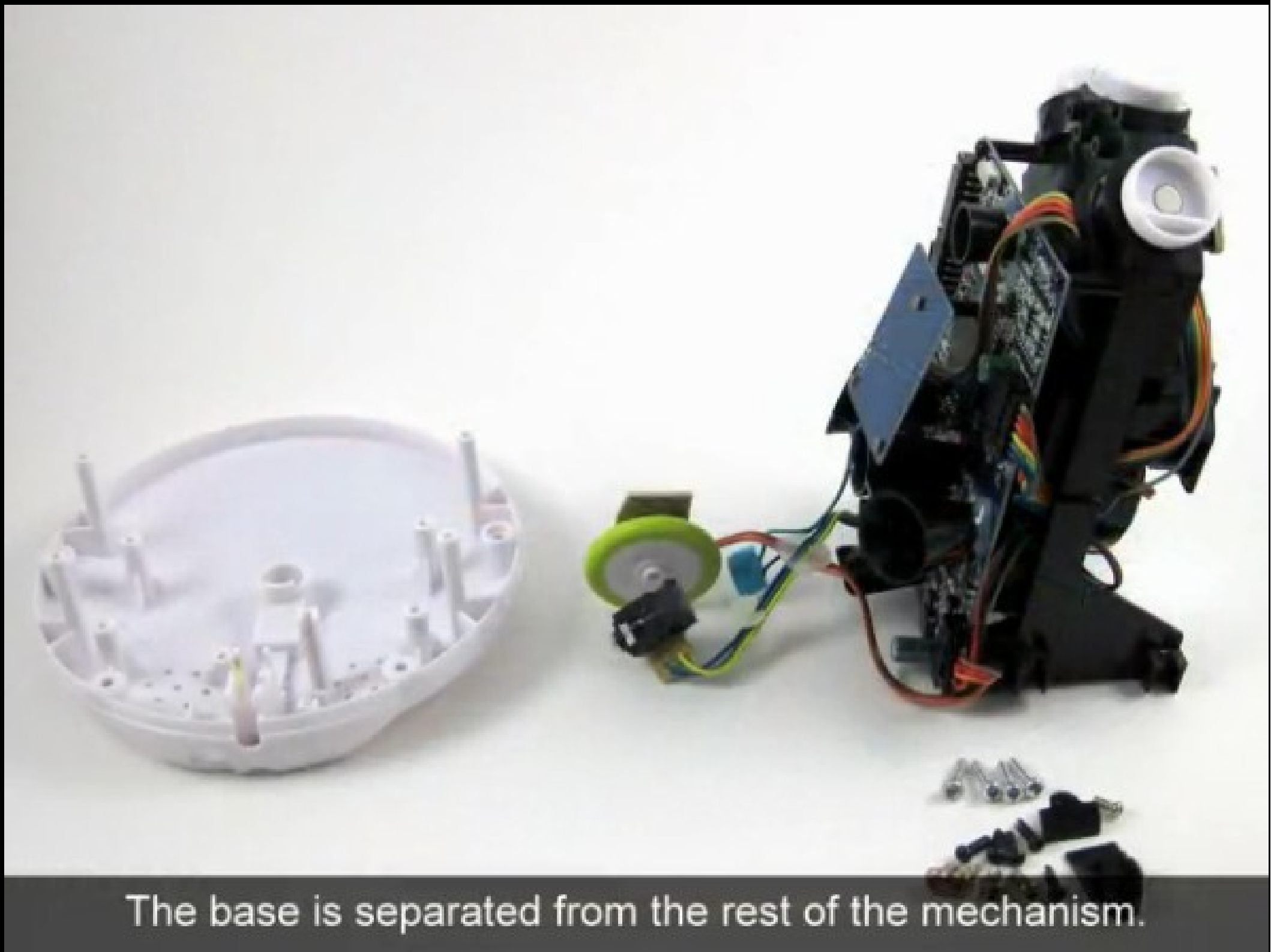
Nabaztag Bottom

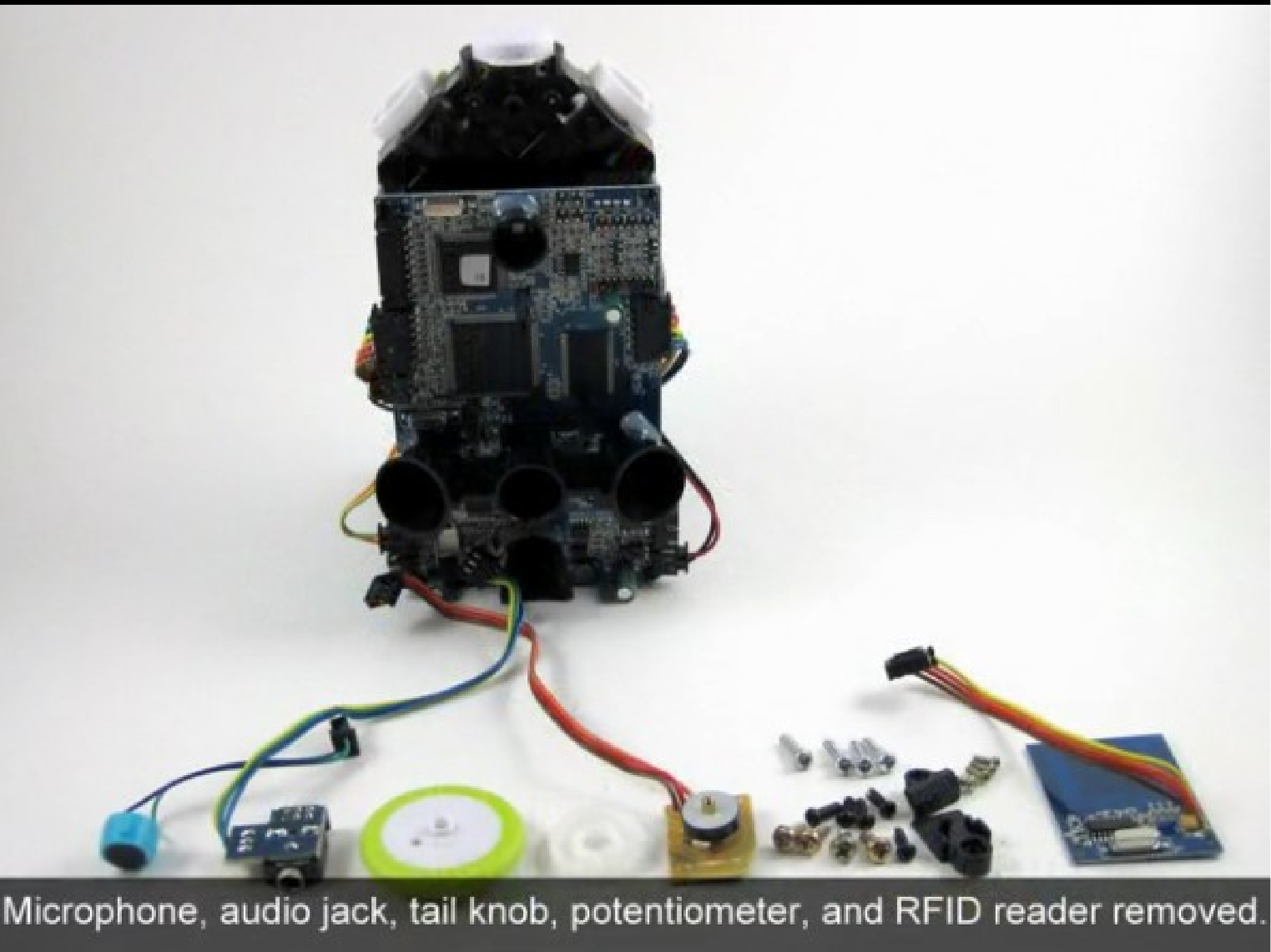

GTAG
02
R-TAGTAG
B digital apparatus
Let's remove the triangular security screws.


A First Look at Nabaztag's Guts


Let's take more screws off.

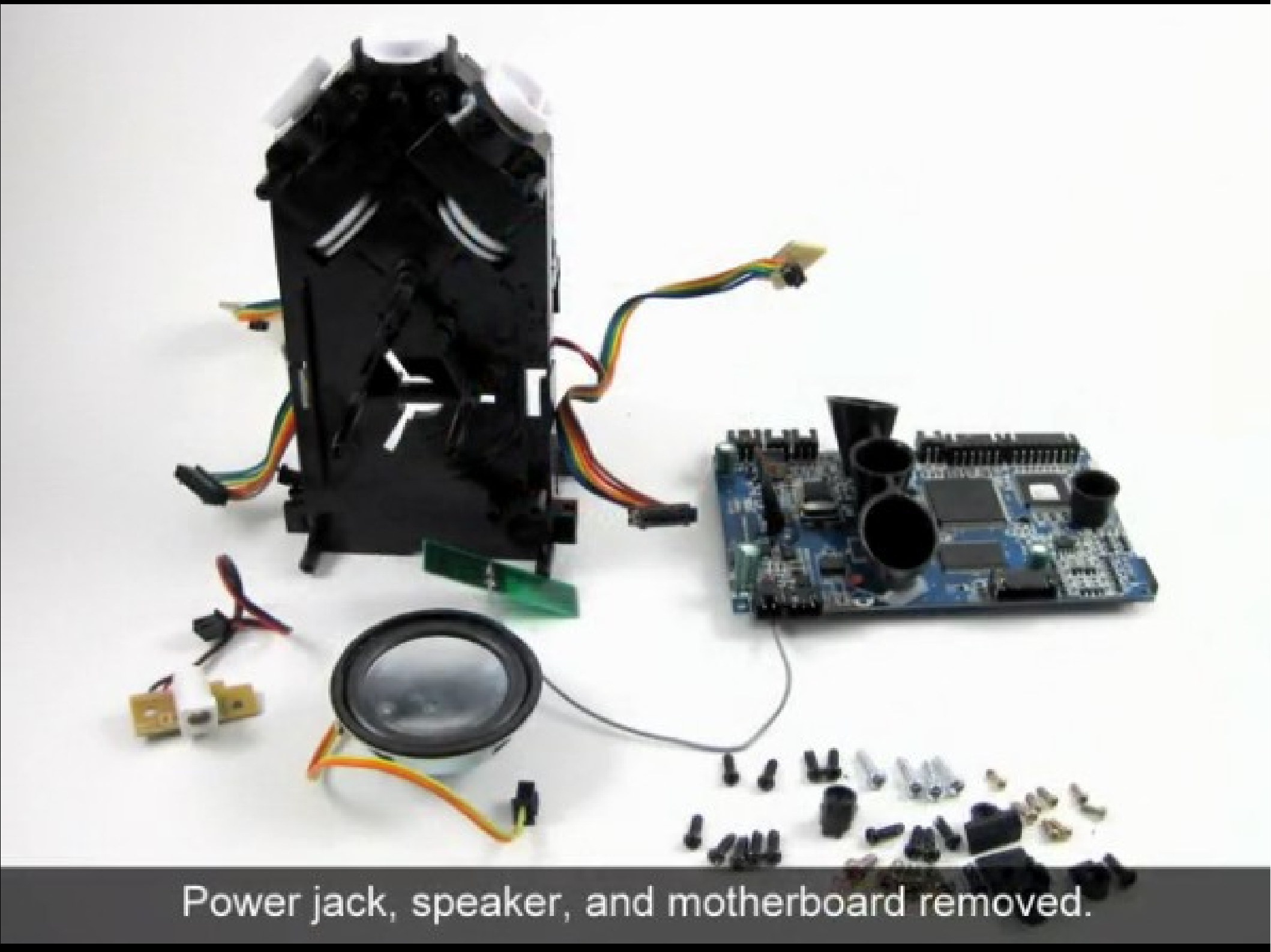



The base is separated from the rest of the mechanism.

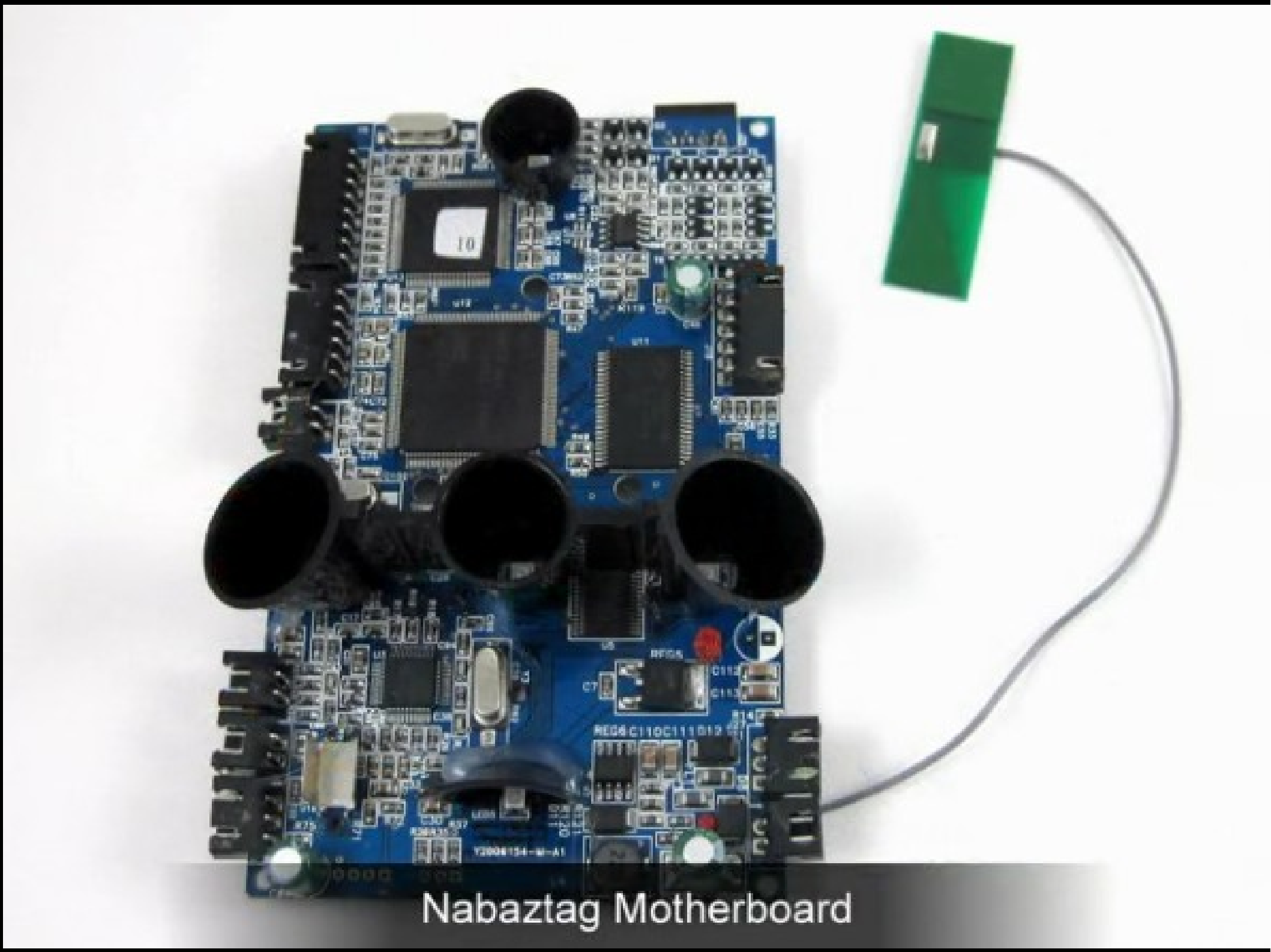


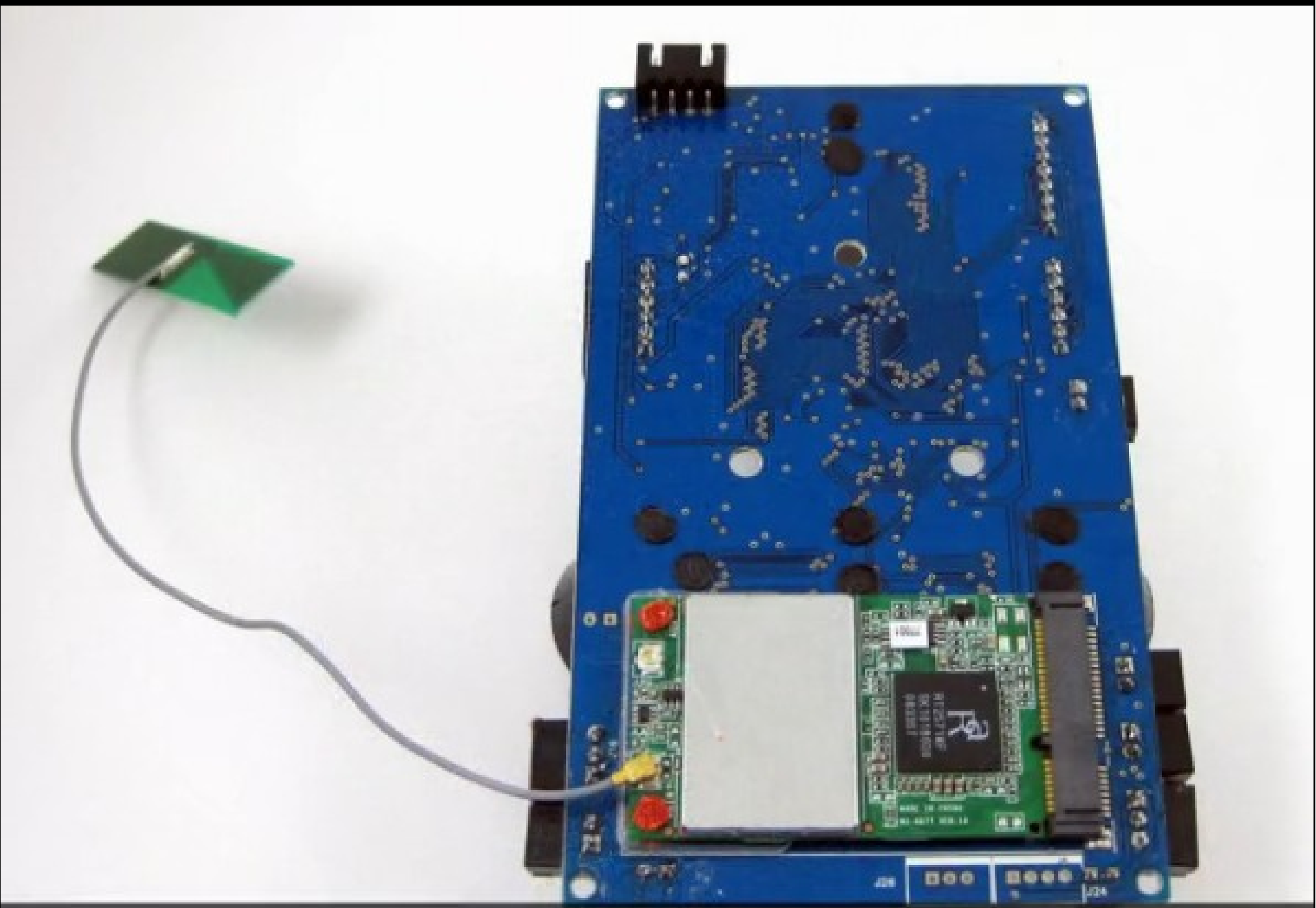
Microphone, audio jack, tail knob, potentiometer, and RFID reader removed.


Let's remove the rest of the electronics.

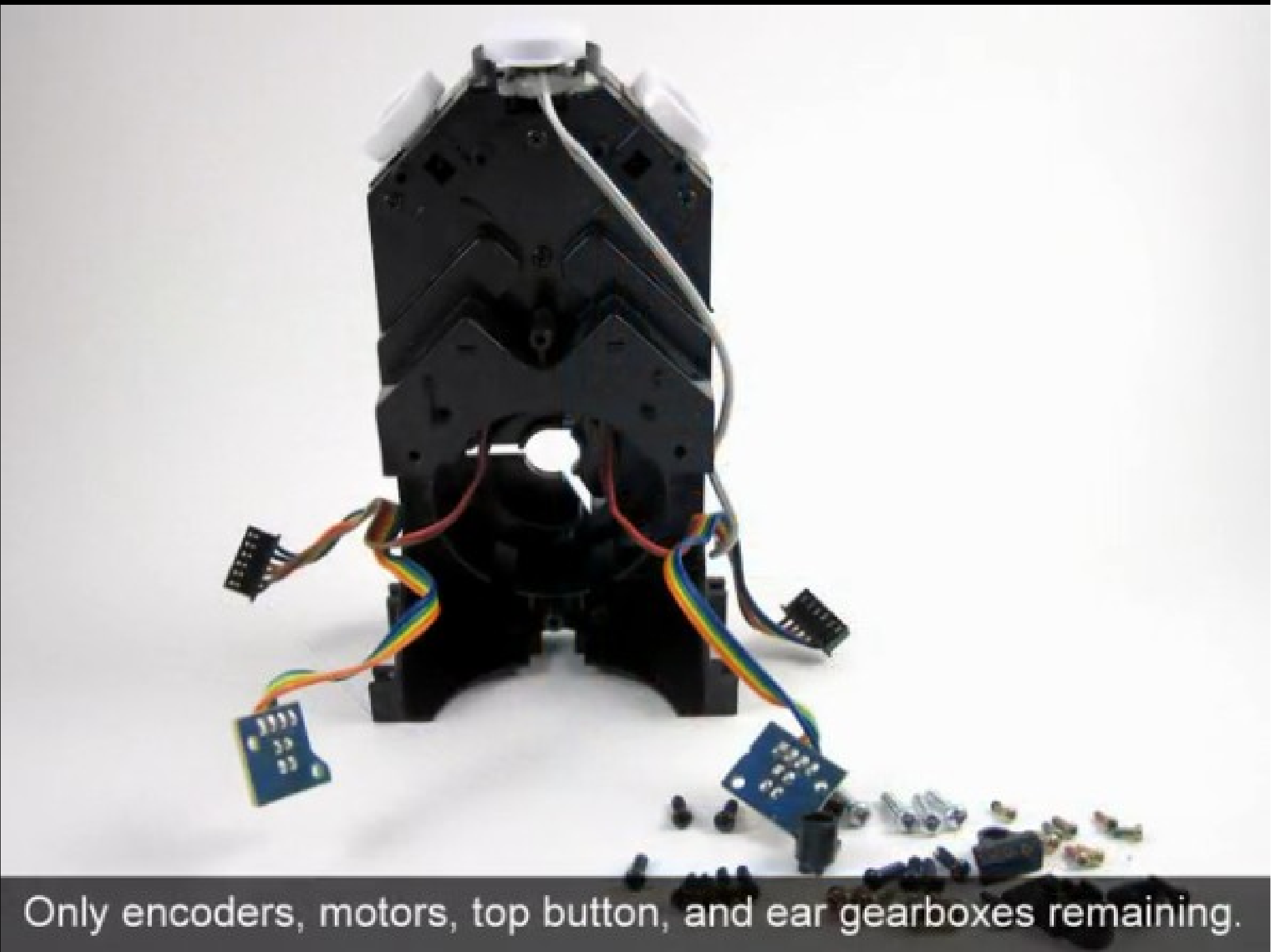


Power jack, speaker, and motherboard removed.

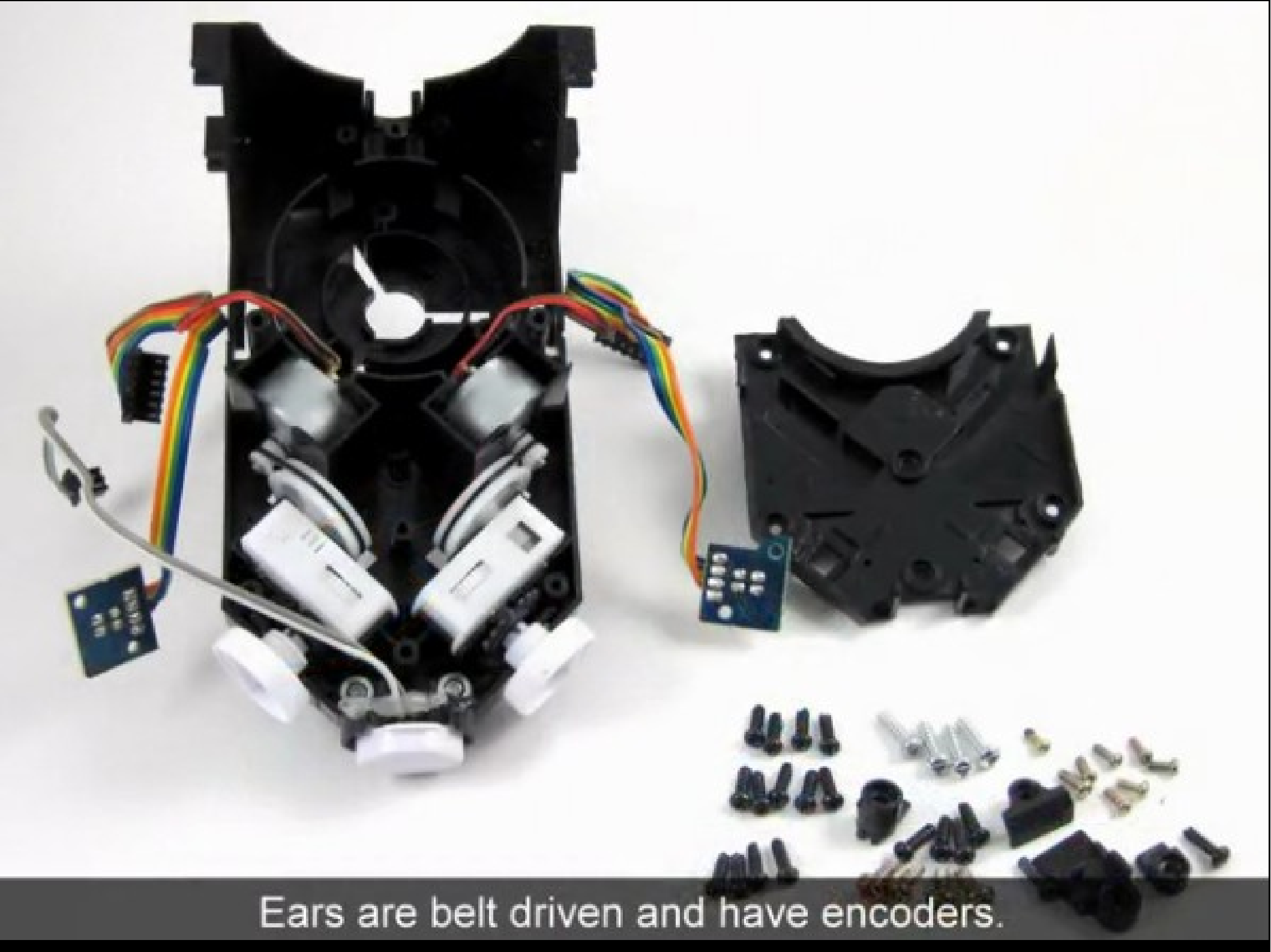

Nabaztag Motherboard



The back of the motherboard sports the WiFi card.



Only encoders, motors, top button, and ear gearboxes remaining.


Ears are belt driven and have encoders.


Motors, gearboxes and top push button removed. Nothing is left!


Nabaztag Disassembled!

… ma l'autopsia non finisce qui

(ricordatevi del software)

Nabaztag software

Vi ricordate del software negli oggetti IoT?

Il software che rende Nabaztag cosi interes-sante e coccoloso?

Come ogni sistema client/server il Nabaztag ha una parte client (il firmware), una parte server ed un protocollo di comunicazione/API che li “collega”.
Uno spoiler - le cose piu' interessanti accadranno in quest'ultimo.
Per non dilungarci tratteremo del solo Nabaztag:tag (v2); in effetti il Nabaztag (v1) e' un sottoinsieme del Nabaztag:tag (v2), e Karotz (v3) una versione estesa, ma l'architettura eì del tutto simile.

Dopo aver terminato l'autopsia, cercheremo infine di trarre delle conclusioni a questa chiacchierata.

Nabaztag software design

Sylvain Huet ha sviluppato la maggior parte del firmware di Nabaztag.

Sebastien Bourdeauducq ha sviluppato il driver Wi-Fi.

Antoine Schmitt e' il progettista dei comportamenti e Jean-Jacques Birgé ha realizzato i suoni.
Insieme hanno relizzato Nabaz'mob opera, un concerto per 100 Nabaztag.

Maÿlis Puyfaucher ha fornito la voce francese, ed ha realizzato i testi di tutte le frasi originali pronunciate da Nabaztag.
Non esistono informazioni su chi abbia sviluppato il protocollo ed il software originale dei server, oggi non disponibili per la bancarotta di Violet ed i vincoli della cosiddetta "proprieta' intellettuale".

Nabaztag: the Client

Nabaztag:tag (v2)

Il firmware e' memorizzato in 128 KB di flash ROM "sicura" ed in 8KB di Boot Flash ROM.

Il firmware e' crosscompilato esternamente in un blob binario.

Contiene una macchina virtuale capace di eseguire fino a 64 kB di bytecode.

Esiste un linguaggio pseudo-Assembler dedicato per la programmazione di movimenti, azioni e coreografie.

Coreografie & plugin possono essere anche scaricati dal server ed eseguiti nella VM.

Nabaztag: il software Server

Nabaztag:tag (v2)

Dopo la scomparsa di Violet and Mindscape, parecchie comunita' spontanee iniziarono a sviluppare cloni del software lato server e dei relativi plugin.

Per il Nabaztag:tag (v2) i software piu' diffusi sono OpenNab, scritto in PHP, and openJabNab, scritto in PHP & C++.

Ad oggi oltre una dozzina di questi server sono in funzione, e tengono desta una buona parte della popolazione dei conigli "smart", come il server italiano OpenZNab.it
Sono manutenuti da comunita' spontanee, che spesso gestiscono anche maillist e forum informativi.

Home

OpenNab
About
ChangeLog
Download and Install
User Documentation
Developer Documentation
OpenNab on SourceForge

languages
english
français
italiano

OpenNab

Set your bunny free!

Welcome to OpenNab software website!

OpenNab is an open PHP-based framework for the Nabaztag™ bunny.
The Nabaztag is an electronic device connected to the internet and performing a wide range of functions.
In its standard operating mode, the Nabaztag connects to the web servers of its originating company, Violet.

With OpenNab, you set your bunny free by having it connected to your own server and no longer depend on a 3rd party.

OpenNab

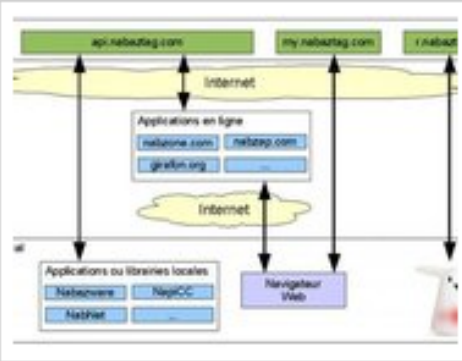
Brought to you by: oaz

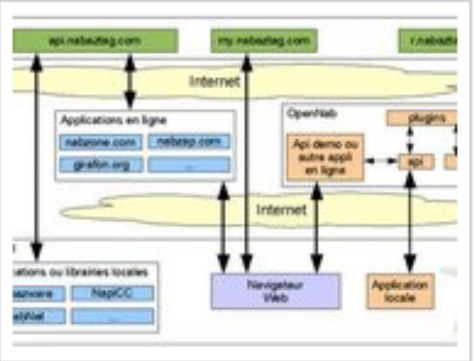
★ Add a Review
3 Downloads (This Week)
Last Update: 2013-04-29

Download
opennab_0.09.zip

Browse All Files

Tweet G+ Like 1





Recommended Projects

- Nabaztools
- NabazLab
- Nabaztag API .NET wrappe

sourceforge DEALS

Report inappropriate content

openJabNab Admin

Your nabaztag is not connected on this server ?

If you want to join the openJabNab solution, you need three steps :

- Setup your bunny : How to setup my bunny ?
- Create an account : Sign Up
- Add the bunny to your account
- Choose and setup the plugins : Plugin list

Recent News

Nabaztag V1 is now supported

Nabaztag V1 are now officially supported by openjabnab.fr Currently, there is a limited number of plugins for those bunnies, but I'll increase it in the coming months

19 Jan

First version for Nabaztag V1

From 8 December 2014, the first version for the Nabaztag V1 will be test. If you want to participate, send a message through the contact form with the MAC address of your bunny. Do not hesitate to report problems or suggest improvements. Thank you all for

06 Dec

Sign In

Sign in using your registered account:

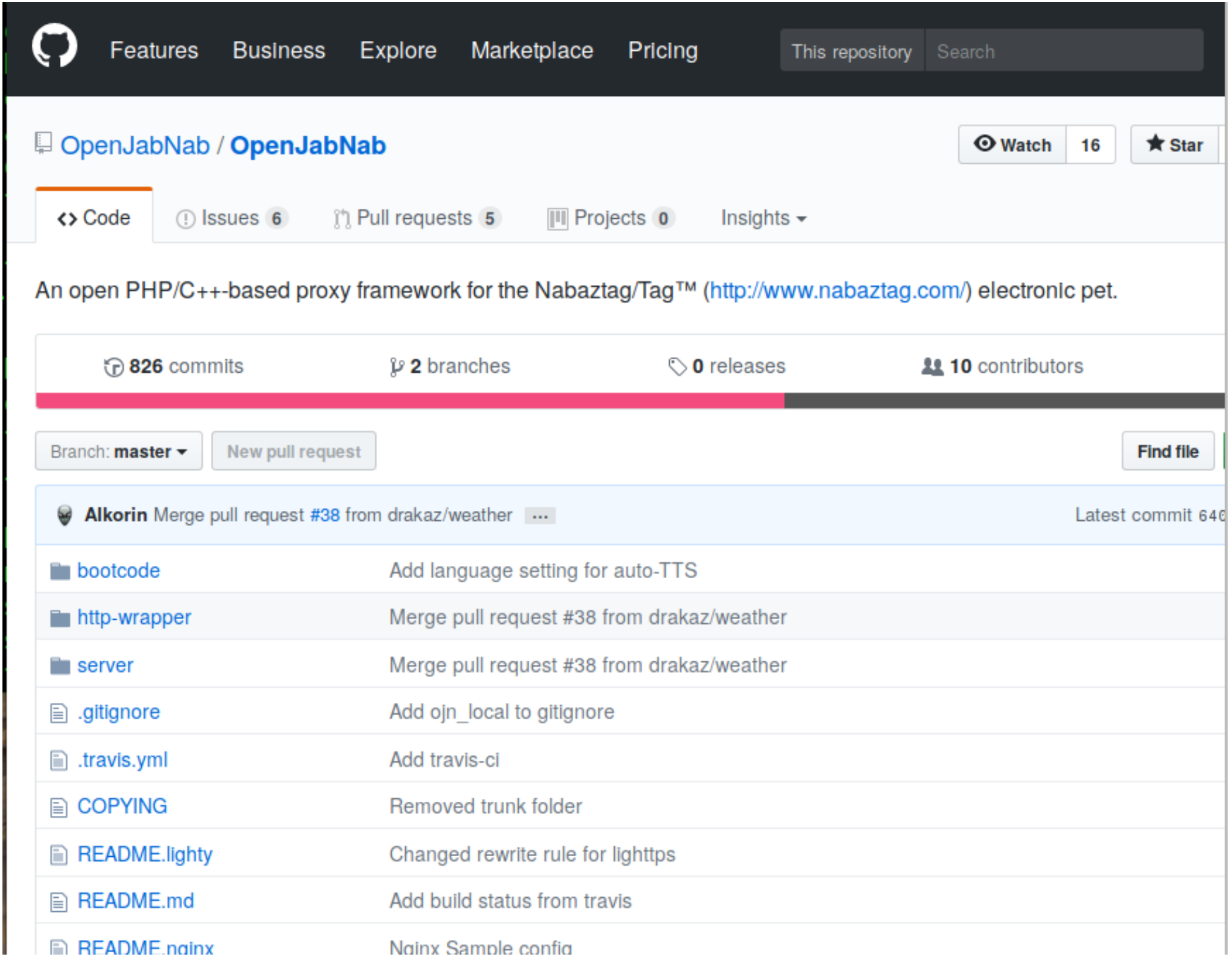
Username

Password

Sign In

Don't have an account? Sign Up
Remind Password

Social


Features
Business
Explore
Marketplace
Pricing
This repository
Search
OpenJabNab / OpenJabNab
Watch
16
Star
Code
Issues 6
Pull requests 5
Projects 0
Insights
An open PHP/C++-based proxy framework for the Nabaztag/Tag™ (http://www.nabaztag.com/) electronic pet.
826 commits
2 branches
0 releases
10 contributors
Branch: master
New pull request
Find file
Alkorin Merge pull request #38 from drakaz/weather
Latest commit 646
bootcode
Add language setting for auto-TTS
http-wrapper
Merge pull request #38 from drakaz/weather
server
Merge pull request #38 from drakaz/weather
.gitignore
Add ojn_local to gitignore
.travis.yml
Add travis-ci
COPYING
Removed trunk folder
README.lighty
Changed rewrite rule for lighttps
README.md
Add build status from travis
README.nginx
Nginx Sample config

- marco
- giusy
- sofia

Configurazione nabaztag 'marco'

Configurazione nabaztag

Configurazione

Nome: marco Conferma

Plugin singola pressione: Oroscopo

Plugin doppia pressione: Nessuno

Conferma

Voce TTS: Giulia Conferma

VioletAPIToken: 8a3d0d9402fd1bd1788c644a7a8dbb58

VioletAPI: (•) Attiva ( ) Disattiva Conferma

Tipo API: ( ) Pubblico (•) Privato Conferma

Disconnetti nabaztag

Plugins

PLUGIN	OPERAZIONI	
Orologio	Disattiva plugin	Configura / Utilizza
Colore respirazione	Disattiva plugin	Configura / Utilizza
Compagni d'orecchie	Disattiva plugin	Configura / Utilizza
Oroscopo	Disattiva plugin	Configura / Utilizza
Memo	Disattiva plugin	Configura / Utilizza
Musica	Attiva plugin	
Nabcast	Attiva plugin	
Notizie	Attiva plugin	

FREE RABBITS

Welcome

We cannot find your Karotz right now, maybe you have not installed our TimeButton software?

Install the TimeButton software on your Karotz, press the button on its head and start to explore the new world of Karotz!

If you have installed the software before, press the button on your Karotz so we can update your IP-address and find your rabbit again.

La météo à 7 jours


Random Sound


Weerbericht Nederland

Nabaztag: protocollo di rete

Nabaztag:tag (v2) + OpenJabNab

A causa della mancanza di documentazione, il protocollo di rete e' stato in parte sniffato e sottoposto a reverse-engineering.

Si e' verificato che tutte le comunicazioni usano il protocollo XMPP Jabber, con crittografia TLS.
Tuttavia si e' scoperto che quando un blob binario, ad esempio un file MP3, deve essere trasferito, questo viene fatto encodando l'oggetto in Base64, e poi trasferendolo con l'uso di HTTP in chiaro.
Inoltre, per la scarsa potenza di calcolo lato client, quando un messaggio di testo deve essere letto dal coniglio, viene prima inviato al server che lo rasterizza in un file MP3, poi trasferito fuori dalla sessione XMPP usando HTTP in chiaro.

Nabaztag: un semplice attacco

Non e' difficile intuire che un firmware complesso, sviluppato tra l'altro in condizioni economiche critiche, possa contenere molti bug pronti ad essere utilizzati da degli attaccanti ben motivati.

D'altra parte, il protocollo di comunicazione parzialmente in chiaro e' un bersaglio troppo ghiotto per non essere sfruttato.
Quindi "avveleniamo" il nostro router casalingo con ARPspoof e catturiamo una sessione client/server.

Durante la sessione catturata, al coniglio veniva fatto semplicemente dire "Ciao".

La sessione registrata, letta tramite Wireshark, fornisce facile accesso all'HTTP e all'HTML scambiati.

Nabaztag: un semplice attacco - 2

Inoltre, il file MP3 encodato Base64 era facilmente identificabile nello scambio di dati HTTP, e copiabile senza difficolta'.

Usando ancora ARPspoof per "avvelenare" nuovamente il router, e poi usando Iptables per realizzare un attacco MITM locale, ed il proxy BURPsniffer, e' stato preparato un "diabolico meccanismo" in grado di sostituire, nel flusso dati server -> client, l'oggetto HTTP contenente l'MP3 rasterizzato con uno diverso.
In questo modo al coniglio veniva trasmesso un file MP3 che invece di fargli dire "Ciao" gli faceva dire "*Sono posseduto dal demonio; per liberarmi dovete pagare un Bitcoin*".
La sessione veniva ripetuta, e cosi' il coniglio salutava in maniera ben diversa il suo proprietario.

~~La prestazione~~ il problema finale - 2

Ogni oggetto IoT e' zeppo di software e fa di tutto per nascondere la sua complessita'.

Questa complessita' "nascosta", che rappresenta buona parte del software, svolge funzioni che l'utente non puo' vedere (e di cui perltro non gliene frega niente)

Come prova indiscutibile che gli oggetti dell'IoT lavorano in realta' per i produttori ele .com, terminero' questa presentazione con l'abstract di un costoso corso per assicuratori, e dandovi una link.

"Thanks to the Internet of Things, the world of insurance is ready to enable new business models that generate opportunities unthinkable in the past.

This is especially possible due to the increased availability of real-time information.

Connected objects, in fact, collect large amounts of data, which can be used to better customer profiling and to optimize risk analysis."


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Q&A time

Grazie per l'attenzione

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ------------+