The Internet Of Dongs

Hacking Sex Toys For Fun And No Profit

Hackfest 2016
RenderMan and Murdoch Monkey

Disclaimer

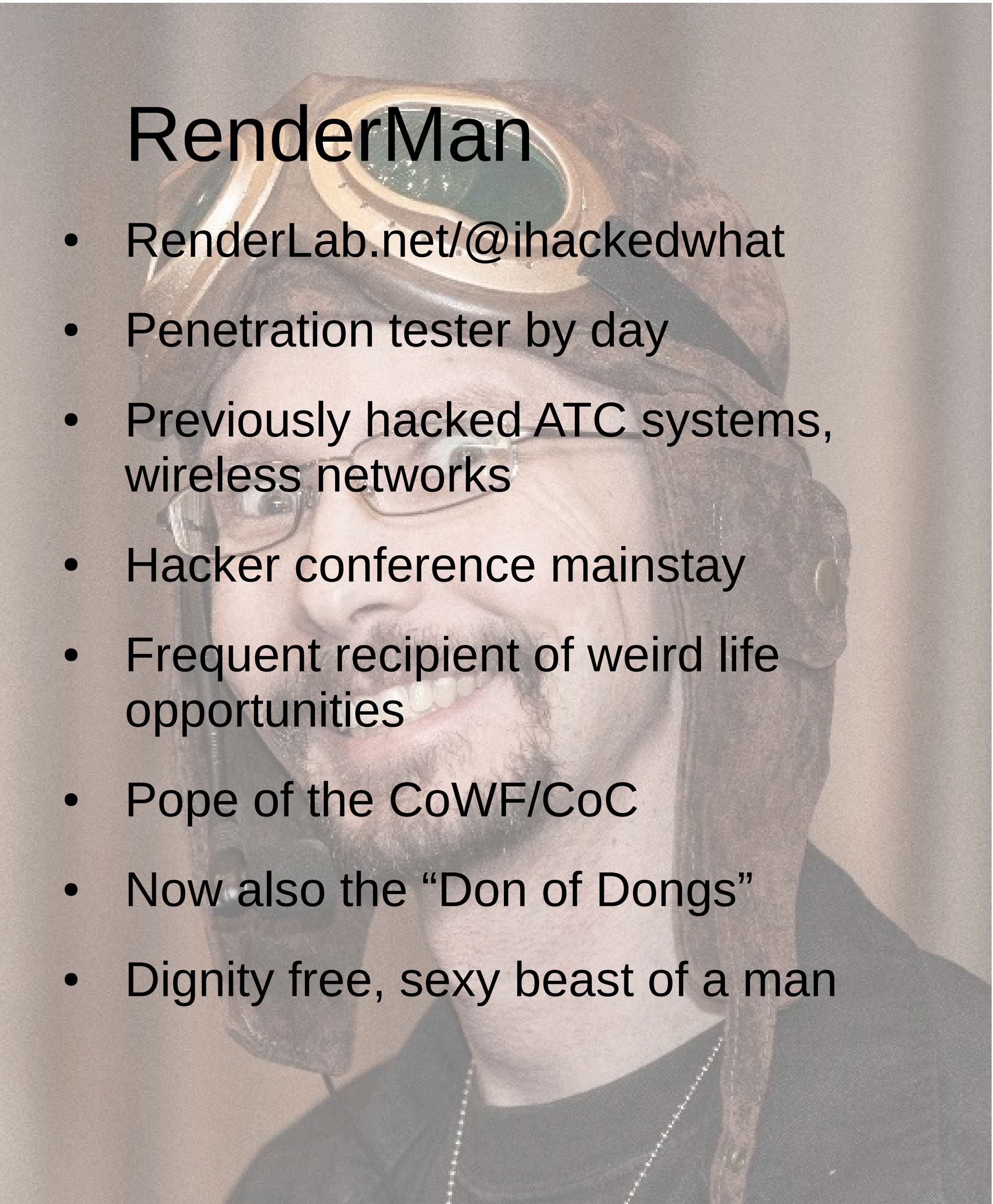
- This is a serious talk
- No intent to offend, We’re all adults here
- Any double Entendre’s, any innuendo is completely unintentional
- Will do my best to keep it PG-13/SFW, but no promises
- Not responsible for any children's future therapy bills
- If you find anything funny in this talk, it is because you are a terrible, terrible human being

HELLO

my name is

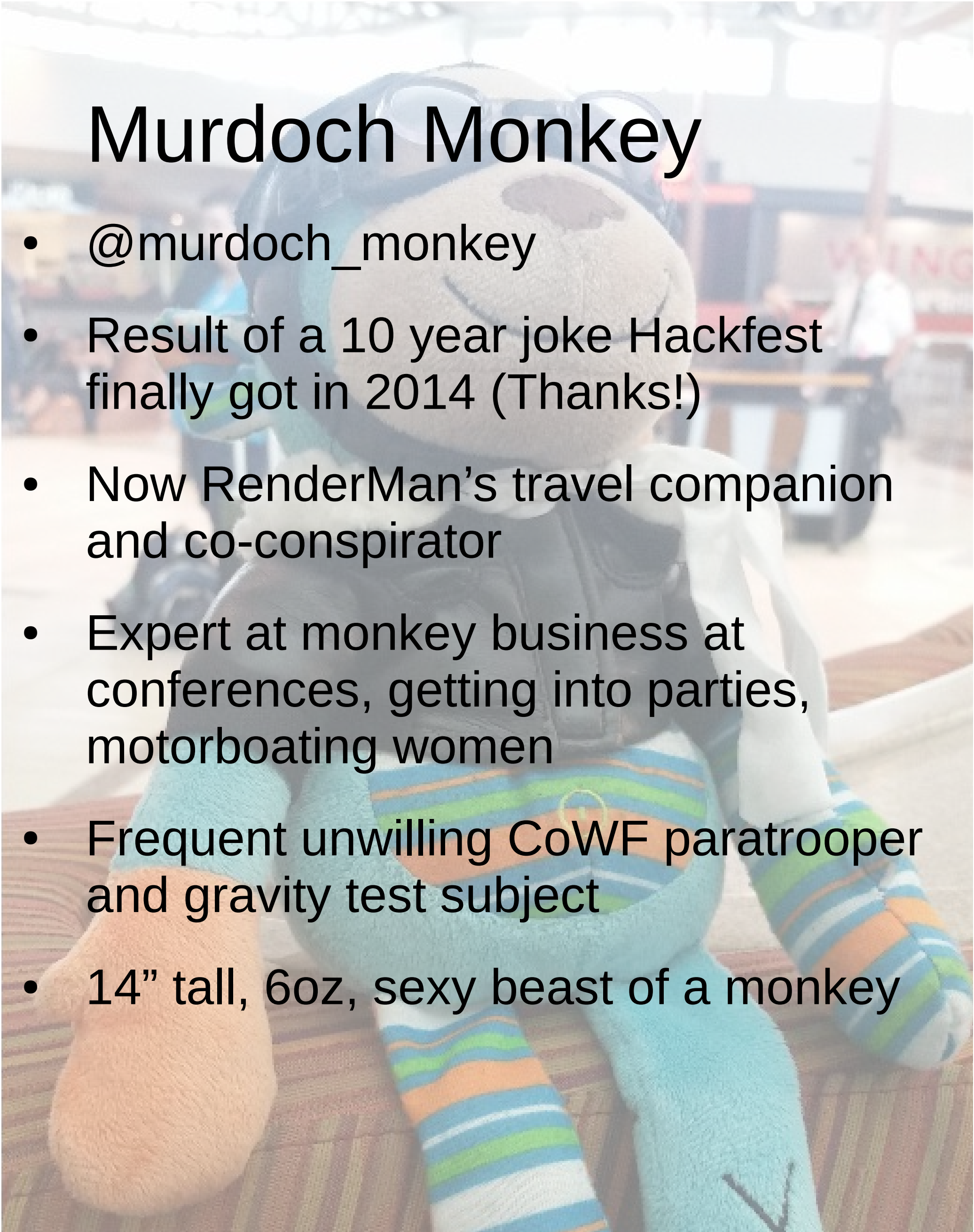
inigo montoya
you killed my father
prepare to die

Who Are These Nuts?



RenderMan

- RenderLab.net/@ihackedwhat
- Penetration tester by day
- Previously hacked ATC systems, wireless networks
- Hacker conference mainstay
- Frequent recipient of weird life opportunities
- Pope of the CoWF/CoC
- Now also the “Don of Dongs”
- Dignity free, sexy beast of a man



Murdoch Monkey

- @murdoch_monkey
- Result of a 10 year joke Hackfest finally got in 2014 (Thanks!)
- Now RenderMan’s travel companion and co-conspirator
- Expert at monkey business at conferences, getting into parties, motorboating women
- Frequent unwilling CoWF paratrooper and gravity test subject
- 14” tall, 6oz, sexy beast of a monkey

Yeah, We’re A Badass Team

Thank You Hackfest!

Internet of Things

- The industry movement to “connect everything”
- Fridges, thermostats, toasters, door locks, etc
- Often industries who’ve never had to deal with challenges associated with connectivity
- Security is a frequent issue with these devices (too much to discuss)
- Every day is another stupid hard coded password, open telnet port, or other stupidity
- IoT devices harnessed for record breaking DDoS attacks in October, 2016

Internet of Things

- More devices hit the market every day
- Faster than security vendors can test them
- Manufacturers often do not an update method or just simply don’t care to fix it
- DDoS attacks now becoming a serious threat
- Groups like I Am The Cavalry” working with industries to help them build in security from the beginning (automotive, medical)
- It’s a huge uphill battle

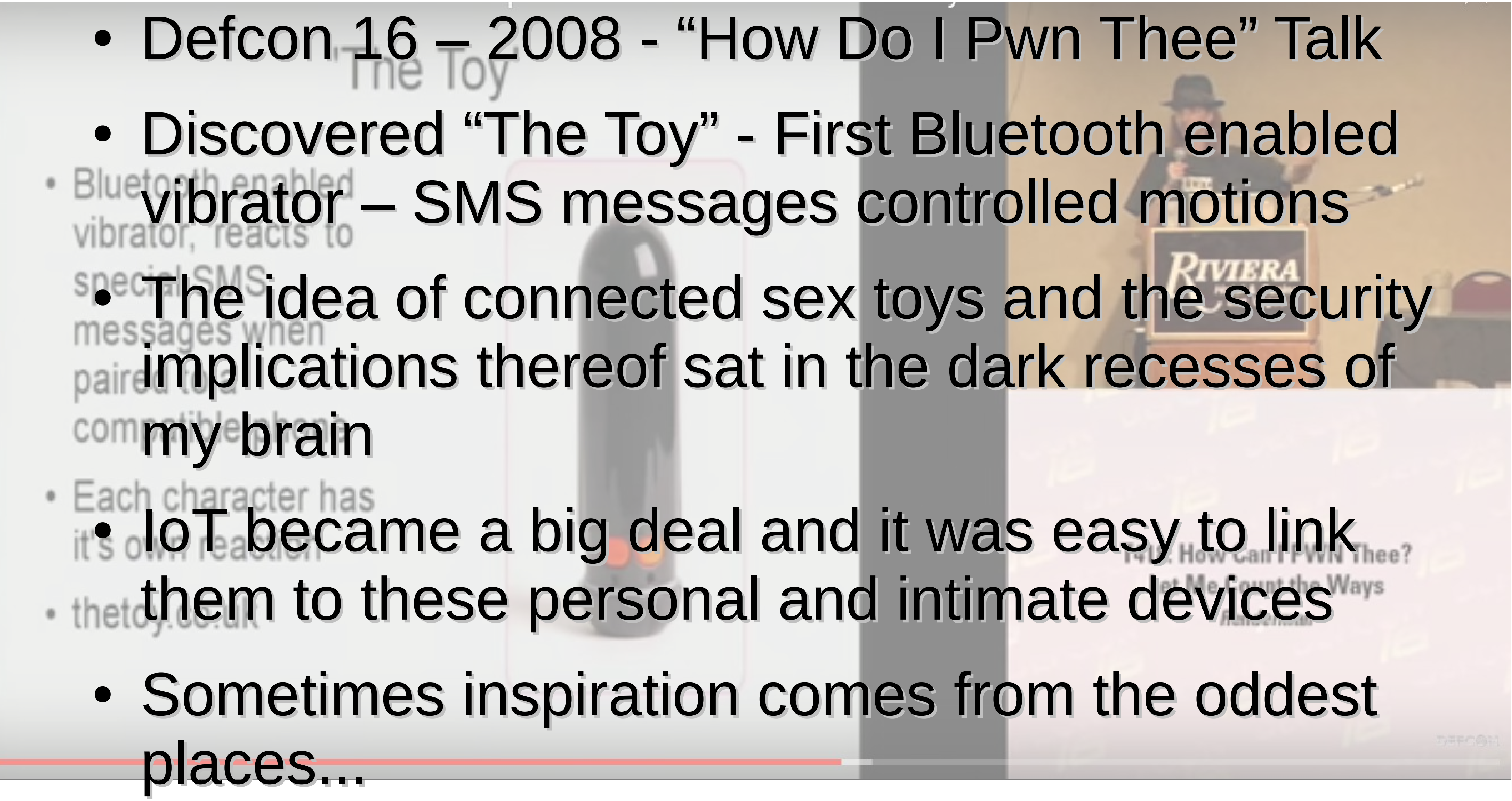
Why Internet Of Dongs?

- IoD is a branch of IoT
- “Dong” is the unit of currency in Vietnam, not often blocked by web filters (SFW possible?) and a really fun word to say!
- Domains were available for .net and .org. Found out about .gs later, worth the cost
- Rather apt name for exploration of this branch of IoT
- Maintains my desire for respectful, scientific based research into “touchy” subject, but still had a great hook for presentation descriptions
- How many people have I gotten to say “Dong” this week?
- Face it: Sex is what drives the Internet...

The Ultimate Goal of IOT

https://youtu.be/IKBJxZf-Dgs

How Did This Start?



- Defcon 16 – 2008 - “How Do I Pwn Thee” Talk
- Discovered “The Toy” - First Bluetooth enabled vibrator – SMS messages controlled motions
- The idea of connected sex toys and the security implications thereof sat in the dark recesses of my brain
- IoT became a big deal and it was easy to link them to these personal and intimate devices
- Sometimes inspiration comes from the oddest places...

How Did This Start?
With A Stupid RomCom Movie!

https://youtu.be/4SLXKtOmcR4

Stop Laughing!

- This scene raised some serious questions
- What potential was there for physical harm?
- Embarrassment is a huge factor for an otherwise private thing
- Sources of interference causing unforeseen actions?
- The Kid did not have Katherine Heigl’s permission to work the remote; Did he commit a sex crime?
- Doesn’t seem as funny anymore does it?

Rape By Deception

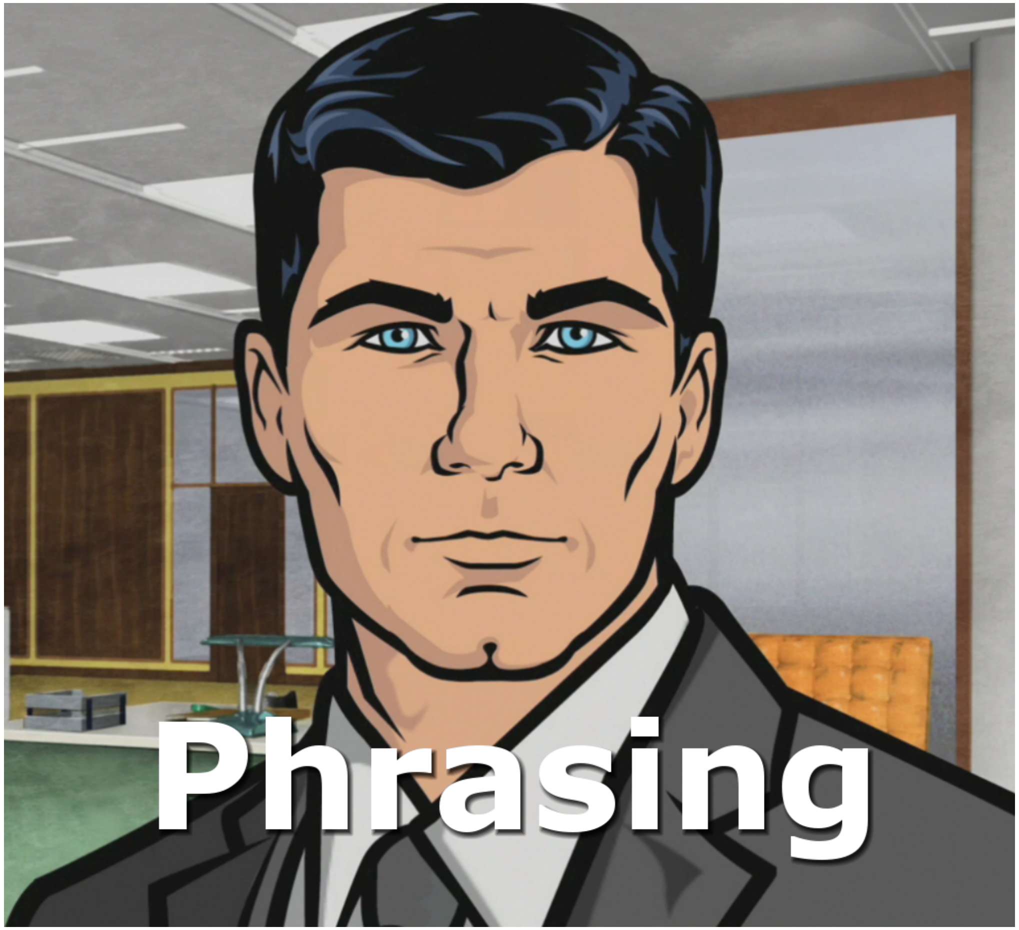
- Several cases where person thought their sexual partner was someone else (brother, intruder, etc)
- Usually dismissed on some technicality
- IANAL: Could be other cases, laws, in other places
- It’s been an issue in the past and considered by the courts. Largely seems unresolved so far
- Permission was given, but under false pretenses
- IoD: Same bits, but the origin and control matter for consent
- Is hijacking a remote control of a connected sex toy a form of sexual assault?

How Did This Start

- “The Ugly Truth” scene really put the risk in perspective for me
- Kept talking about it for years, mentioned it to a store owner during a sex toy take-apart I was running at our local science museum (long story)
- Gave me a couple We-Vibes and the needed push to finally dive in (Thanks Brenda @ Travelling Tickle Trunk)
- Looked around at what was available - **Mind Blown**

Why Internet of Dongs

- Serious implications are just under the surface, past all the giggling
- Privacy issues
- Device security issues
- Relationship blackmail/extortion/etc
- Physical harm?
- As a decent human being, I had to do something
- I have no dignity, so why not become the face of Teledildonics Security?



Teledildonics

- The name for technology enabling remote controlled sexual activity
- Not masturbation - Someone/thing else is controlling sensations
- Coined by Ted Nelson in 1975 (also coined hypertext among others)
- One of those ideas in the background, driving internet technology development

Ted Nelson
From w3.org history of the web article

Internet of Dongs

- Connected sex toys – Another branch of IoT
- Noticed no real security research had been done
- Some reverse engineering, some basic replay attacks, nothing comprehensive
- Security vendors have been unwilling to take on this “controversial” type of device for research
- Quickly found it was more than simple device research, now also consumer advocate, security policy designer, and a bunch of stuff I didn’t expect

Been A Crazy Few Months

- Originally a personal project, get a few speaking gigs and laughs out of it
- Research into the field showed industry was way more advanced than I thought, way more devices
- Obtained a few devices through Travelling Tickle Trunk
- Initial research showed some very obvious and terrible security and privacy practices
- Initial overtures showed most vendors have a complete lack of a vulnerability reporting framework or plan in place
- Made contact with major security vendor about partnering on acquiring all devices and publishing a collaborative exhaustive testing of the market
- Discussion went all the way to CEO who approved it !.........

Been A Crazy Few Months

- .....And the board overruled him (too controversial)
- Back to square one, but had a few devices now
- Could still investigate software components without the devices (Android since iOS is a bitch to RE)
- Exhaustively searched Google Play and websites for every device I could find with remote capabilities/cloud integration
- Began automated static testing and some simulator based dynamic testing
- Had more than enough for a “State of the Dong” talk for Defcon 24, but......

Been A Crazy Few Months

- ......Follower and Goldfisk put in a nearly identical talk, Mirrored my results perfectly
- Holy crap, I’m not the only one?
- Met with them and others, realized others wanted to collaborate under the IoD banner
- Began to re-tool for handling larger volume of devices, researchers and software formats
- Launched early due to We-Vibe Lawsuit resulting from Follower and Goldfisk’s Defcon talk*

*More on that later

Been A Crazy Few Months

- Already had domains, setup a basic framework for blogging/posting for now
- Now can handle multiple user/researcher submissions and output aggregate reports*
- Brought a few researchers into the fold
- Now realized sponsorship would be needed for device acquisition, shipping, test devices, etc
- Tried the high road, lets try the low road....

*Once I get the templates build for Dradis

Internet of Dongs – Sponsored by Pornhub

- More difficult to email than expected, but got a response very quickly
- Still in discussions with them about how they can help/support the IoD but love the idea and support us fully
- Try explaining this to your mother

Lovense – First Industry Partner

LOVENSE

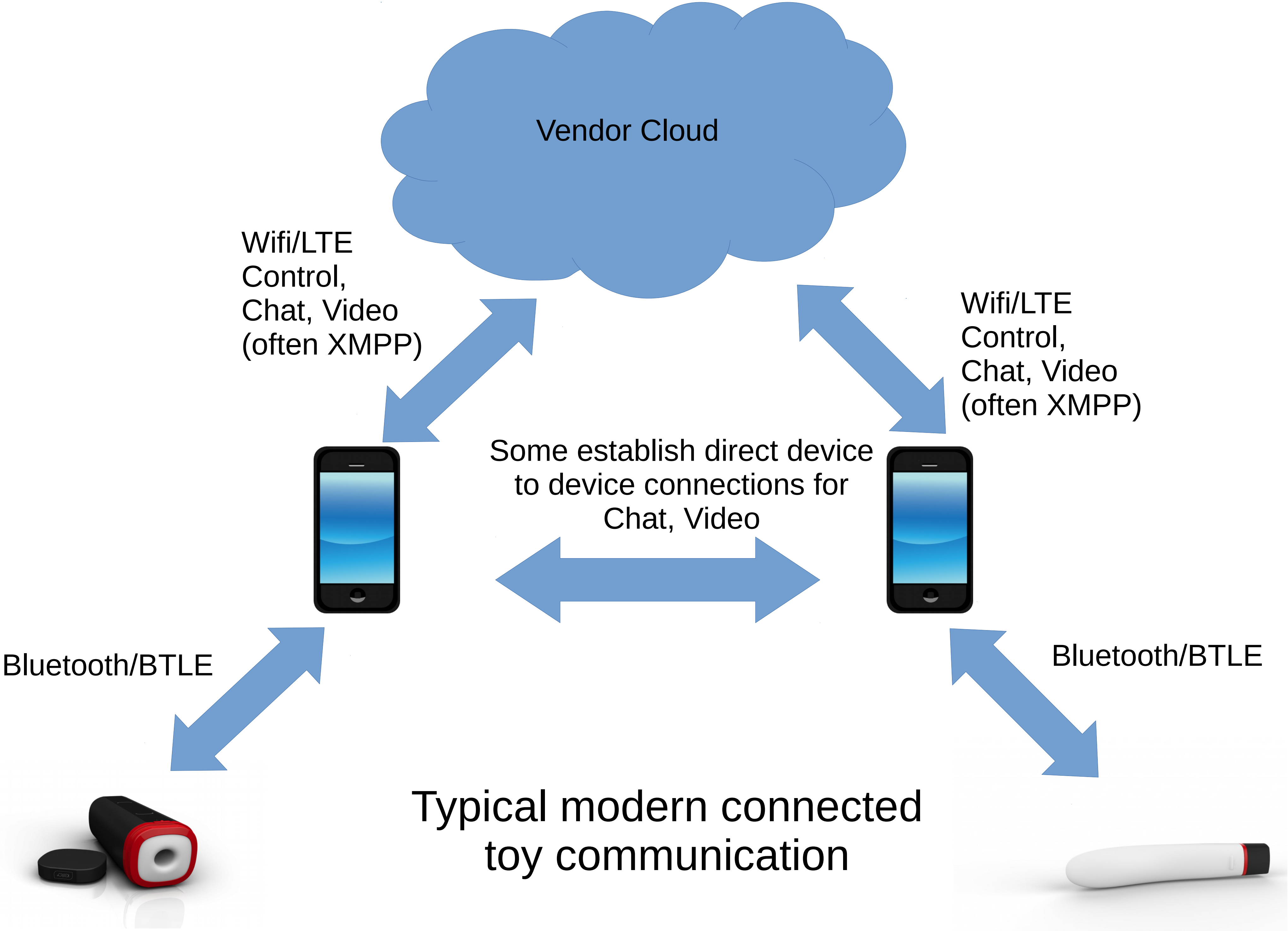
- Qdot connected me with Eddy @ Lovense
- Had to convince the CEO, but prevailed
- Working with them to develop vulnerability disclosure framework and internal processes for secure development
- Committed to user privacy and security

Internet of Dongs

- https://internetofdon.gs - @internetofdongs
- Setting up as a hub for researchers to pool results and present a single point of interactions with industry/vendors
- Building bridges with industry to help them build security disclosure programs
- Establish best practices for vendors to follow in developing devices and a process for vulnerability reporting and disclosure
- Non-judgmental, just want to see people be able to enjoy these products safely, securely and privately

Basics of IoD Devices

- Vast majority are Bluetooth/BTLE devices
- Pair to smartphone for local control and as a gateway for remote control
- A few have desktop applications as well
- Often using XMPP for control channel as well as chat functions
- Often Text, Audio, and Video chat functionality
- Almost always some interaction with vendor servers at some level for remote control functions



Vendor Cloud

Wifi/LTE
Control,
Chat, Video
(often XMPP)

Wifi/LTE
Control,
Chat, Video
(often XMPP)

Some establish direct device
to device connections for
Chat, Video

Bluetooth/BTLE

Bluetooth/BTLE

Typical modern connected toy communication

This Is A Weird Place

- This research is not for the easily embarrassed or easily shocked
- I’m very open minded, non judgmental, sex positive, but I’ve been stunned a few times
- Here are some examples

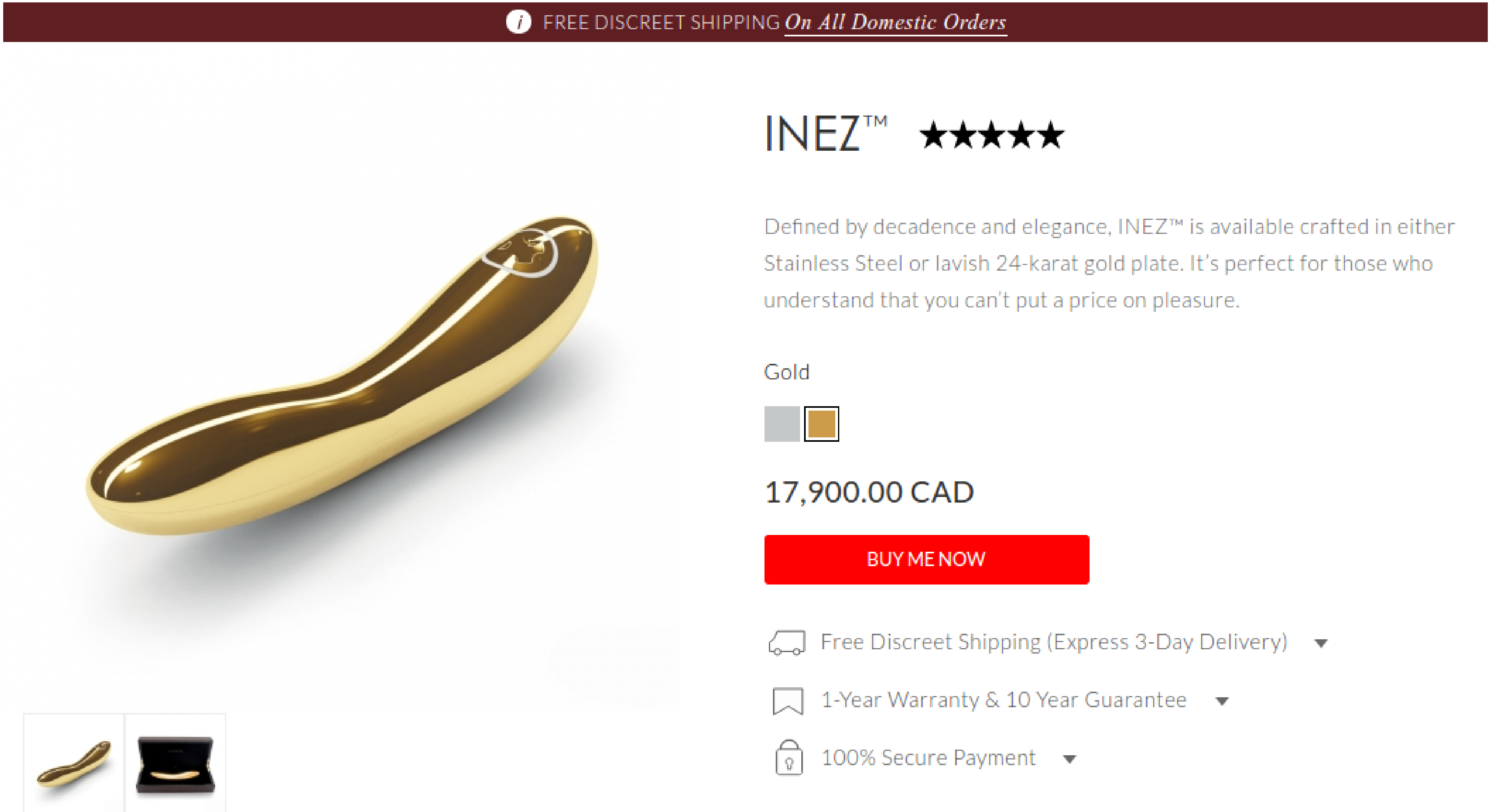
Twerking Butt

- Pornhub Branded Twerking Butt
- It twerks, it vibrates, it massages
- VR googles and Syncs to VR porn
- Yes, There’s an app for that

Pornhub, PLEASE send me a couple, it’s a moral imperative that these be hacked!

Lelo INEZ: A $17,900 Vibrator

- So, this exists: 24k Gold & Free Shipping!



FREE DISCREET SHIPPING *On All Domestic Orders*

INEZ™ ★★★★★

Defined by decadence and elegance, INEZ™ is available crafted in either Stainless Steel or lavish 24-karat gold plate. It's perfect for those who understand that you can't put a price on pleasure.

Gold

17,900.00 CAD

Free Discreet Shipping (Express 3-Day Delivery)

1-Year Warranty & 10 Year Guarantee

100% Secure Payment

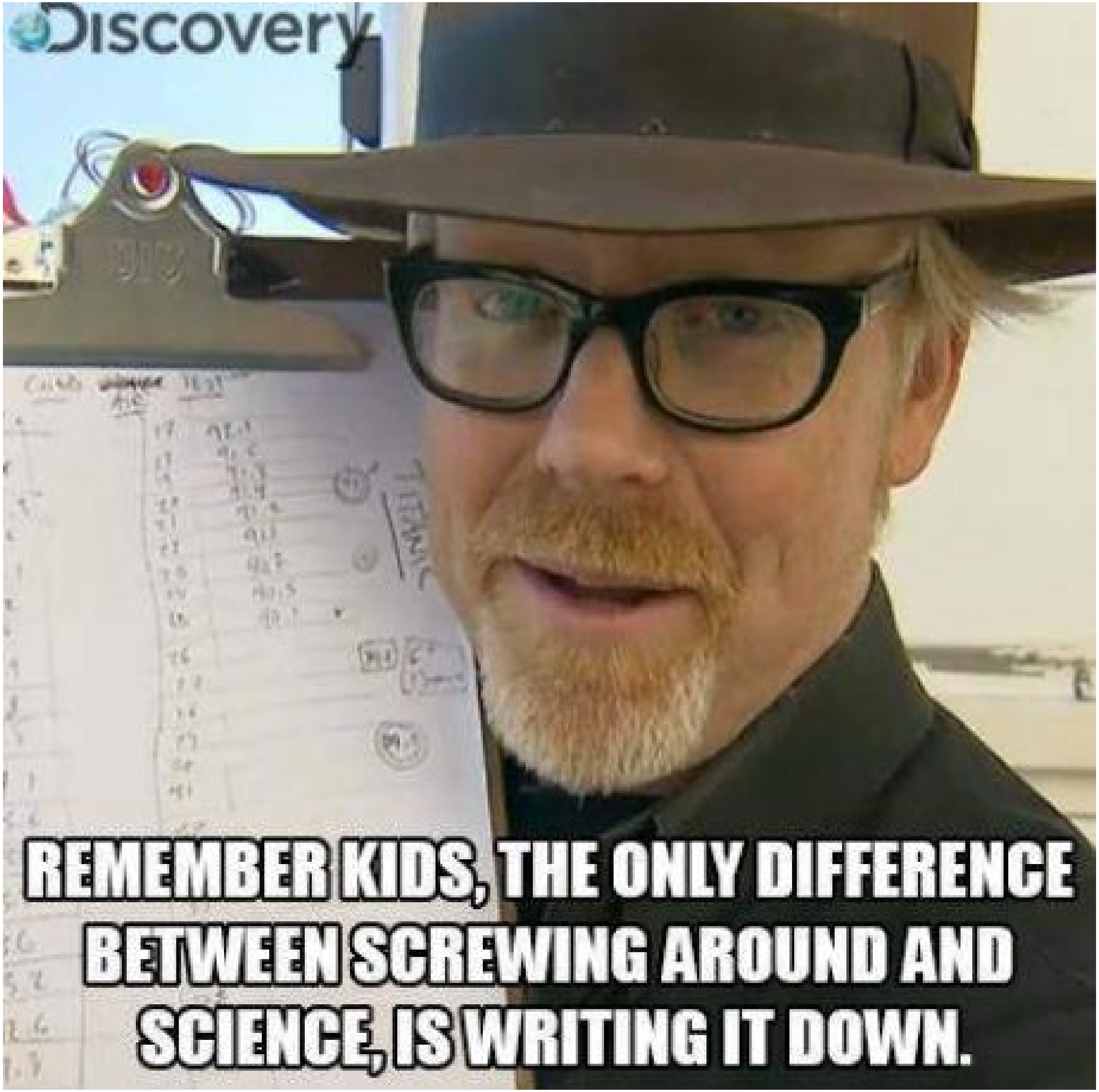
Software Oddities

- Who else has to deal with software with functions like this:

```
private static OrgasmService ORGASM_SERVICE;

public static final String GET_ORGASMS = "/orgasms";

public static final String SEND_ORGASM = "/orgasm"

          public class OrgasmUtils
          {
            public static final int AFTERNOON_DELIGHT = 1;
            public static final int EARLY_RISER = 0;
            public static String FILENAME = "ohs.txt";
            public static final int NIGHTCAPPER = 2;
            public static ArrayList<Orgasm> OHS = new ArrayList();
            public static final String OH_GOAL = "oh_goal";
            public static final int TWILIGHT_ZONE = 3;
```

It’s All For A Good Reason

- This may be funny, but there are serious concerns
- Security and privacy concerns are prevalent in any product
- Sex Toy users should have every protection (maybe more) than any other consumer
- Like most IoT vendors, an industry of non-connected, manually operated devices is going online and doesn’t know about the risks
- Yes, it means I have a bag full of sex toys and I know what you think that means, but I take this seriously.
- This is Science.....


Discovery
REMEMBER KIDS, THE ONLY DIFFERENCE BETWEEN SCREWING AROUND AND SCIENCE, IS WRITING IT DOWN.

Privacy Issues

- I assume most people have sex toys, NBD
- Assuming or someone has one is different than knowing, and with whom, when, how, etc.
- Many apps have text, audio, video chat capabilities that could be very, very private
- Connected devices usually have a login or unique identifier.....
- All Android Apps require location permission*
- Location, private info being leaked to other users, 3rd parties

Example Findings

- Not everyone uses SSL/TLS!!
- If they do, no one knows how to do SSL/TLS properly*
- User enumeration
- User private information disclosure
- Partner disclosure
- Excessive permissions
- Embedded API keys

*Both client side and server side

SSL Fail

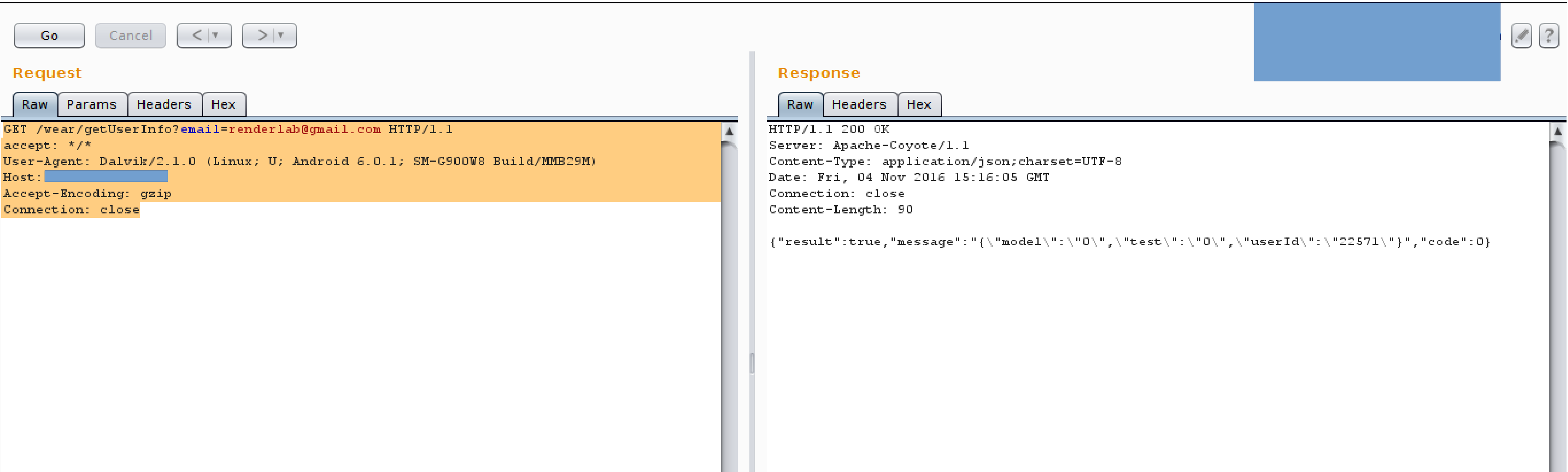
- Many apps/platforms do use SSL at least partially, ALOT use it poorly
- ALLOW_ALL_HOSTNAME_VERIFIER
- Turns off SSL certificate checking; ANY SSL certificate is accepted. Making MitM soooooo easy. WTF!
- How many shared networks are these devices used on, really?
- How many people know if this hotel has client separation turned on? Is the hotel doing any DPI or other logging? NSA?

User Enumeration

- Multiple vendors have this issue
- Poor coding, lack of any tokens, not AUTHENTICATED, minimal rate limiting
- No limit to number of queries
- Can query against lists of emails to see who has an account
- Example:

User Enumeration Zero Day

- Actual vendor, report has been filed
- Query returns ‘True’ or ‘False’
- No auth, tokens, anything
- Minimal rate limiting



```
GET /wear/getUserInfo?email=renderlab@gmail.com HTTP/1.1
accept: */*
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; SM-G900W8 Build/MMB29M)
Host: [redacted]
Accept-Encoding: gzip
Connection: close
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Date: Fri, 04 Nov 2016 15:16:05 GMT
Connection: close
Content-Length: 90

{"result":true,"message":"{\"model\":\"0\",\"test\":\"0\",\"userId\":\"22571\"}","code":0}
```

User Enumeration Zero Day

```
GET /wear/getUserInfo?email=renderlab@gmail.com HTTP/1.1
accept: */*
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; SM-G900W8 Build/MMB29M)
Host: <REDACTED>
Accept-Encoding: gzip
Connection: close
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=UTF-8
Date: Mon, 17 Oct 2016 22:49:46 GMT
Connection: close
Content-Length: 89

{"result":true,"message":"{\"model\":\"0\",\"test\":\"0\",\"userId\":\"null\"}","code":0}
```

User Enumeration Zero Day

- Personal Address book - ~275 addresses

User Enumeration Zero Day

- Personal Address book - ~275 addresses
  - I have some friends with surprising personal activities
  - One was another friend doing BT LE research, did not know about my IoD work
- Ashley Madison Dump

User Enumeration Zero Day

- Personal Address book - ~275 addresses
  - I have some friends with surprising personal activities
  - One was another friend doing BT LE research, did not know about my IoD work
- Ashley Madison Dump
  - Extracted all .gc.ca and .gov addresses
  - Won’t say if I found anything, they’ve suffered enough
- In all ~10000 emails queried, handful of ‘True’ returns
- Easily scripted, easy starting point for further compromise and data mining

User Information Disclosure

- Some apps are more ‘social’ than others
- Some have search features to find ‘friends’
- Others have ways to share custom vibe patterns
- Sometimes the server provides more info than it should or was intended to be shared by the user with others
- Another real example....

Example

Base64 encoded pattern name

{"result":true,"message":"","code":0,"data":[{"id":"d79cd4b8b4c2457a9ea096caa879e8ac","created":"2016/10/27 23:29","updated":"2016/10/28 00:09","name":"8J+YmPCfmJjwn5iY\n","text":"c3lyaWVsbGUudGF5dXVuQGdtYWlsLmNvbSB0YWxrIGRpcnR5IGFuZCBjb250cm9sIG1lIPCfmJjw\nn5iY8J+YmCB2aWJlIHdpdGggbWUgbWF5YmU/\n","path":"/UploadFiles/wear/pattern/20161027/d79cd4b8b4c2457a9ea096caa879e8ac","author":null,"email":"USEREMAIL@gmail.com","timer":"00:08","likeCount":1,"status":"active","playCount":11,"duration":480,"createdTime":1477636197000}

Users Email Address **NOT** displayed in the app entry

Username of author, optionally displayed (user selected, not email address)

User Information Disclosure

- An anonymous username now has it’s associated email address disclosed to others
- Maybe not everyone wants other users to know their email
- Cam Model sites now integrating remote control toy functions into their sites, are details about the models details or location being leaked?
- Are viewers/controllers details being leaked back to the model or third parties?
- Stalking, harassment, extortion, etc

Partner Disclosure

- Many device app allow you to “Pair” with another user and allow remote control
- Larry Pesce at Defcon 22 showed one vendor where you could see a users partner and force “Unpairing”
- Datamining potential is amazing:

Query:

```
POST /WebService/VibeSvc.svc/getpartnerinfo HTTP/1.1
{"Username":"yourvagina"}
```

Response:

```
{"Message":"", "PartnerNickname":"haxorthematrix" ,"Profile
PhotoURI":"","Status":"true","ThumbnailProfilePhotoURI":""}
```

Excessive Permissions

- Been focused on Android for the most part so far
- Some apps are better than others, most leave alot to be desired
- Some defy all logic in what permissions they need:
  - android.permission.WRITE_SECURE_SETTINGS
    - Allows an application to read or write the secure system settings. Not for use by third-party applications
  - android.permission.READ_CONTACTS
    - Allows an application to read the user's contacts data.
  - android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
    - Allows the app to download files through the download manager without any notification being shown to the user.
  - android.permission.AUTHENTICATE_ACCOUNTS
    - Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.
  - android.permission.USE_CREDENTIALS
    - Allows the app to request authentication tokens.
- Notice Location permissions is not on this list...

Bluetooth and Location Permissions

- Android 6+ now requires location permission for all Wifi and Bluetooth connections
- WTF!!!! Made no sense to me and many online
- Got the answer straight from the horses mouth
- Permission is needed for lookup of device address in Google location services as part of a larger location aware functionality. i.e. connecting to wifi projector in board room also establishes audio, lighting control, etc
- Many apps don’t call for location data outside this, but Some do.....

Embedded API Keys

- Poor coding practice to leave unencrypted API keys in apps
- Allows an attacker to interact with the backend directly
- From We-Connect v2.2.2.2 SystemDefaultHolder.java file:

```
private static final String DEFAULT_SECRET = "tZ9o1i5fRHqFyS11OqOkMHu5IvtfjG";
private static final String DEFAULT_XMPP_CERTIFICATE_TYPE = SecurityType.NONE.toString();
private static final String DEFAULT_XMPP_PORT = "443";
private static final String DEV_CHAT_HOST = "dev-chat.sic-apps.net";
```

- API Secret, No SSL security, Known URL and port
- Many others have similar issues

Side Note: We-Vibe Lawsuit

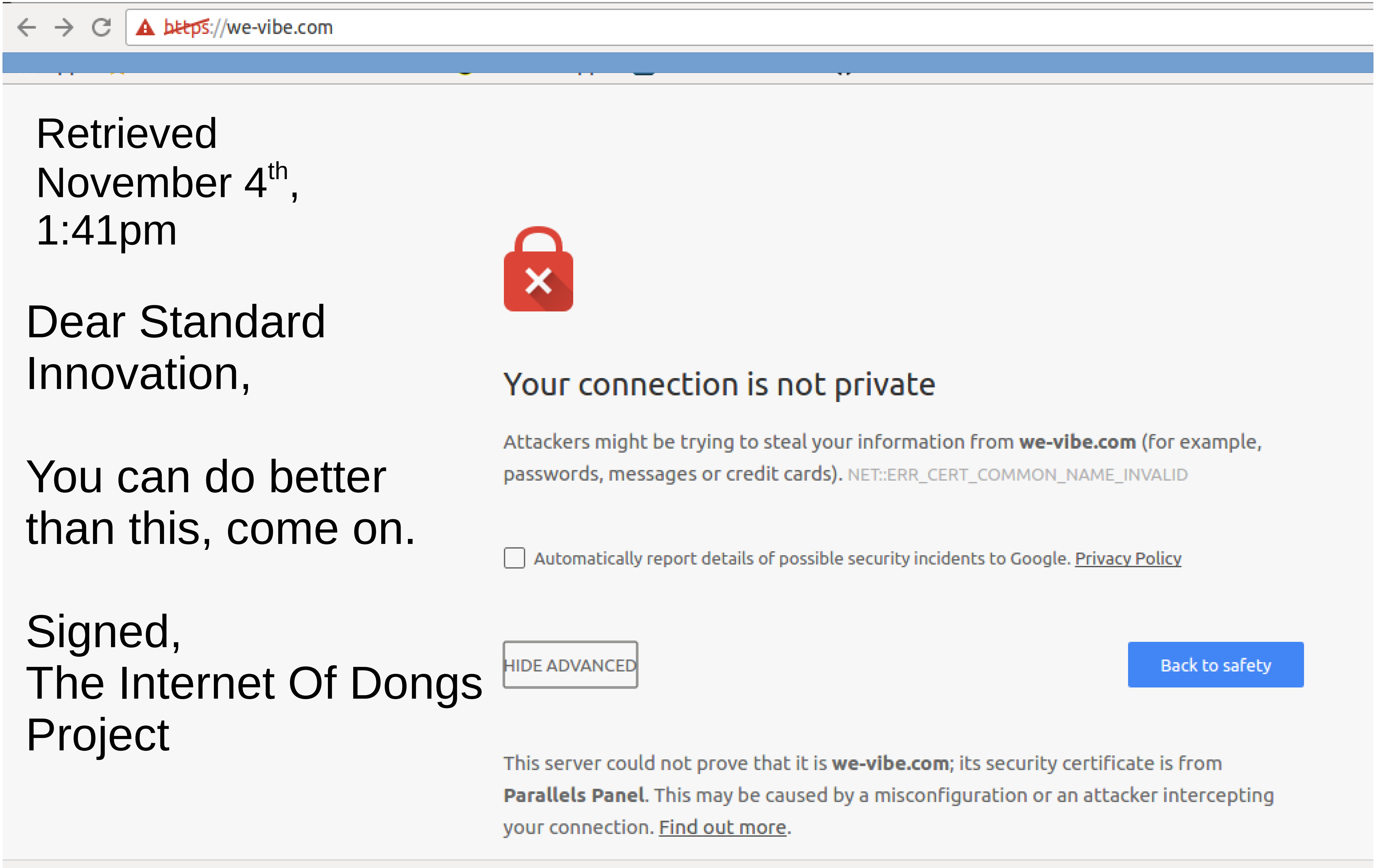
- Standard Innovations sued in September 2016 in a class action
- Result of Goldfisk and Followers Defcon 24 talk
- Issue is with lack of disclosure about data collected and sent through company servers
- App lacked a privacy notice, sued for lack of disclosure
- “If I had known it was doing this, I wouldn't have bought it”
- No evidence of maleficence, just legal notice oversight

Side Note: We-Vibe Lawsuit

- We-Connect was one of the better apps before the lawsuit
- Standard Innovation stepped up after and really locked down their app
- No more need for user accounts
- Allow opt out of anonymous usage data
- Appear to do certificate pinning!
- Some issues remain...

http://we-vibe.com/blog/we-connect-app-and-privacy-update/

Oh FFS Standard Innovation!



Retrieved November 4th, 1:41pm

Dear Standard Innovation,

You can do better than this, come on.

Signed,
The Internet Of Dongs Project

Your connection is not private

Attackers might be trying to steal your information from **we-vibe.com** (for example, passwords, messages or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically report details of possible security incidents to Google. Privacy Policy

This server could not prove that it is **we-vibe.com**; its security certificate is from **Parallels Panel**. This may be caused by a misconfiguration or an attacker intercepting your connection. Find out more.

Other Issues

- Google Play and Apple App Store have banned some apps – No automatic update mechanism
- Data collection of users location in places where sex toys are illegal
- Physical harm: Can you turn it to 11? Can you overload the battery?
- Waiting for the first divorce case to cite data from one of these apps

Others Research

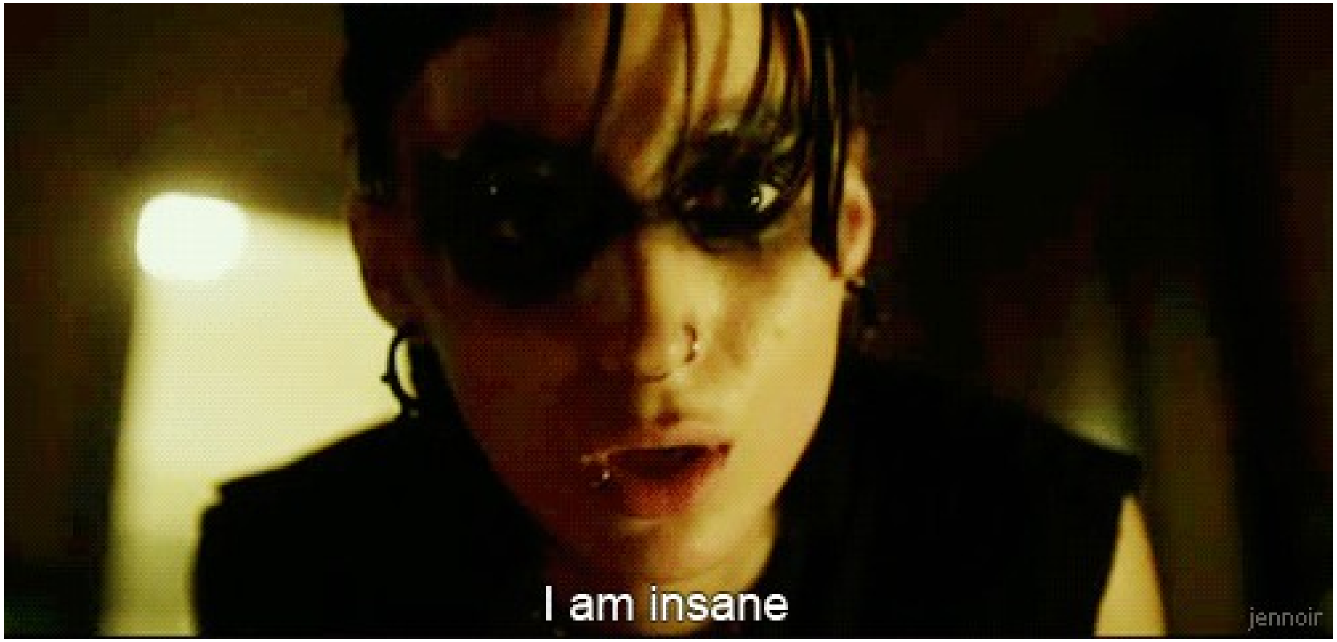
- A few others have looked into these devices over the years
- I’m re-testing and verifying their work and putting together formal reports for responsible disclosure
- Will be posting Larry Pesce’s Defcon 22 presentation, which was not previously available, on https://internetofdon.gs **after** I disclose vulns to the vendor which was not previously done (bad Larry, no doughnut)

Closing Thoughts

- As I hope I convinced you, there are some serious issues here
- Not regulated like medical devices, no oversight or standards for security
- It’s only going to get more serious as technology progresses, new threats no one has anticipated
- Get over any discomfort over the nature of the device and look at it technically
- We need to educate and work with this industry before it gets really bad

How To Help

- This got much bigger, much faster than planned
- Issue grew in importance and scale as well
- I cannot do this alone
- I suck at community building



How To Help

- Send us Dongs https://internetofdon.gs/dongwishlist/
- Connect us with vendors, stores, other advocates
- Do your own research, route your reports through IoD
  - Need an iOS app reverse engineer!!!
- We need non-dong help too!

How To Help

- Need a logo (I have ideas, just need to make them pretty)
- Need to learn some more about XMPP
- Need policy writers, help with IoD responsible dong disclosure framework
- Need help with Dradis report template creation
- Need help with workflow automation to handle reports
- Need help with email server setup
- Need test mobile devices (Android 5+ w/ BT4.0)
  - Busted screens, sim slot, bad battery, etc
  - Useful as rooted test platforms for us though!

Thanks Hackfest!

Contact IoD:

https://internetofdon.gs

@internetofdon.gs

info@internetofdon.gs

Comments, critiques about this presentation are requested!

Contact RenderMan
Renderlab.net
@ihackedwhat

Contact Murdoch Monkey
@murdoch_monkey

Thank You

- Thanks to Pornhub and Eddy @ Lovense for their support, dongs
- Qdot, Larry Pesce, Goldfisk, Follower, cryptoishard
- Brenda at Travelling Tickle Trunk - http://www.travelingtickletrunk.com/
- The CATSA screener in YEG for selecting my carry on for hand inspection (priceless)
- Many, Many others who have helped, contributed and supported but for obvious reasons, dont want to be names