Rapid Radio Reversing

Michael Ossmann

Great Scott Gadgets

SDR

and

non-SDR

CE
HackRF One™
GREAT SCOTT GADGETS™
RESET
3V3
DFU
1V8
RF
USB
RX
TX
ANTENNA
CLKOUT
CLKIN

SDR strengths

universal

frequency detection

modulation detection

replay

SDR weaknesses

learning curve

packets

speed

YARD Stick One™
r1-p1
P1
TXC 48.0
MJE2
CC1111-F32
49M0C8G
1436
LED1
LED2
LED3

transceiver IC strengths

learning curve

packets

speed

transceiver IC weaknesses

limited modulations

difficult to reverse

- frequency
- modulation
- symbol rate

use both

for their complementary strengths

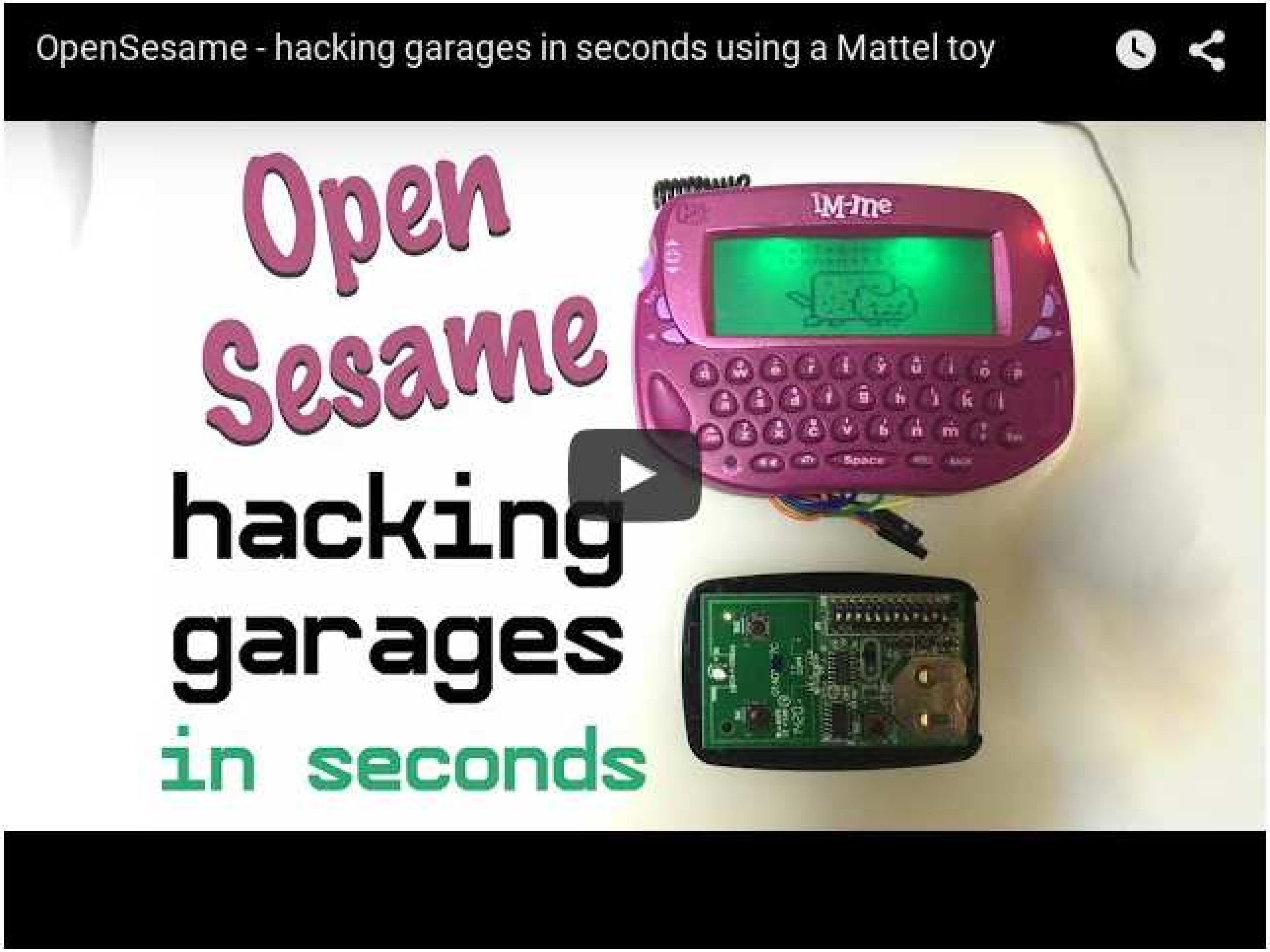
OpenSesame

OpenSesame is a device that can wirelessly open virtually any fixed-code garage door in seconds, exploiting a **new attack** I've discovered on wireless fixed-pin devices. Using a child's toy from Mattel.

Follow me on Twitter or join my mailing list to hear about future projects and research.

By @SamyKamkar

Live demonstration and full details available in the video:



Mike Ryan's Blog/ posts/

Blackbox Reversing an Electric Skateboard Wireless Protocol

About the author

4 comments

Recently at DEFCON 23 Richo Healey and I gave a talk about hacking electric skateboards. One of the skateboards, the Yuneec E-GO, uses a custom wireless protocol between its handheld remote and the board. We touched on how we reverse engineered the protocol during the talk, but I wanted to go into more depth on our methodology.

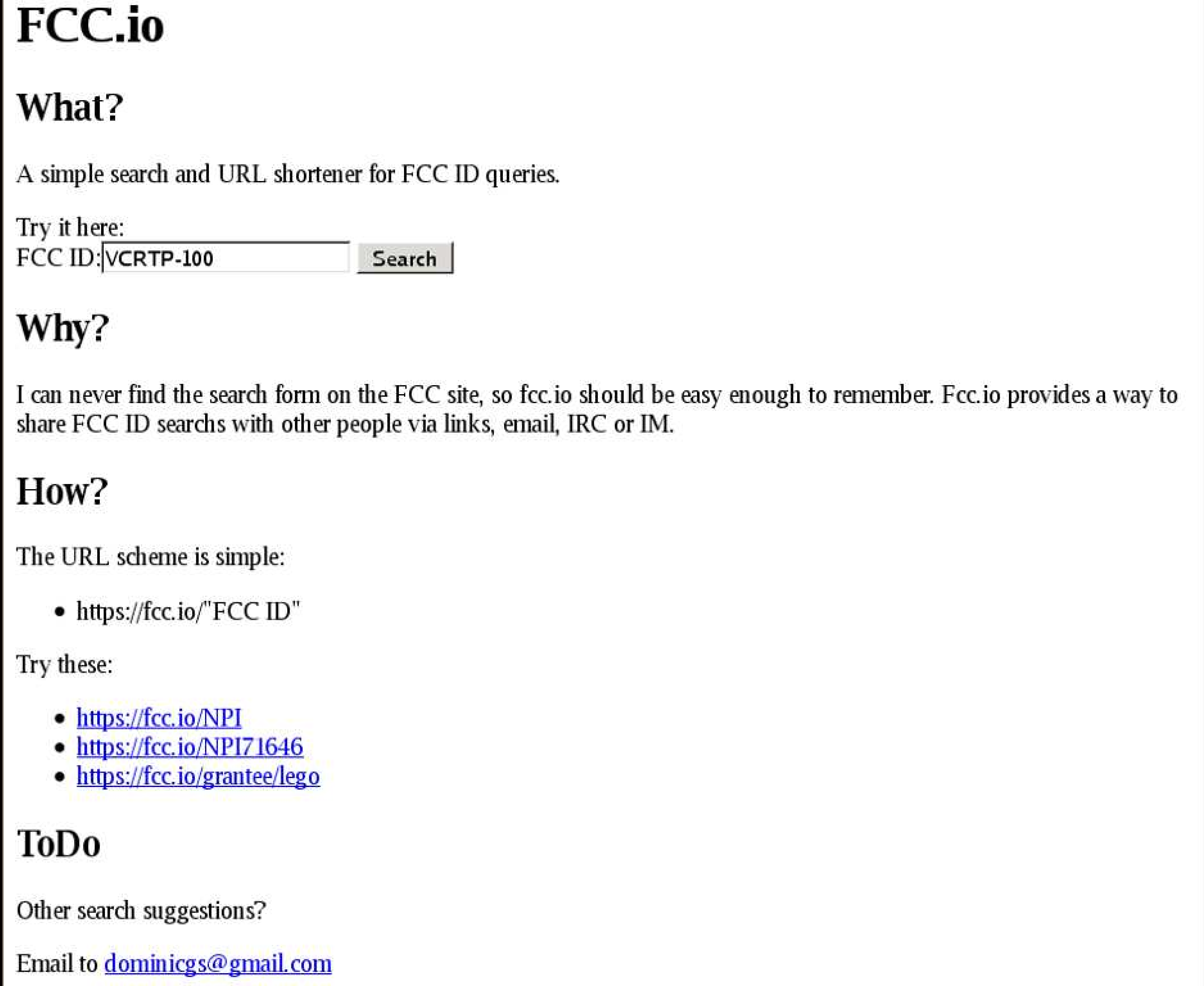
In short, this is the story of how we went from HackRF to skateboard jammer on Ubertooth. Read on for the gory details!

Finding the Signal

We theorized that the skateboard and remote used the 2.4 GHz band, which is well supported by HackRF One. Ordinarily one would use GNU Radio and a basic waterfall sink to look at spectrum, but GNU Radio can be a bit cumbersome.

Luckily we had a PortaPack to play with! The PortaPack sits on top of the HackRF and acts as a wideband spectrum analyzer (among other things). We tuned up to 2400 MHz and swept the spectrum in 20 MHz increments looking for our signal.

CompX
StealthLock
LEARN
1
2
3
4
5
6
7
8
9
0
CompX



FCC.io

What?

A simple search and URL shortener for FCC ID queries.

Try it here:
FCC ID: VCRTP-100

Why?

I can never find the search form on the FCC site, so fcc.io should be easy enough to remember. Fcc.io provides a way to share FCC ID searchs with other people via links, email, IRC or IM.

How?

The URL scheme is simple:

- https://fcc.io/"FCC ID"

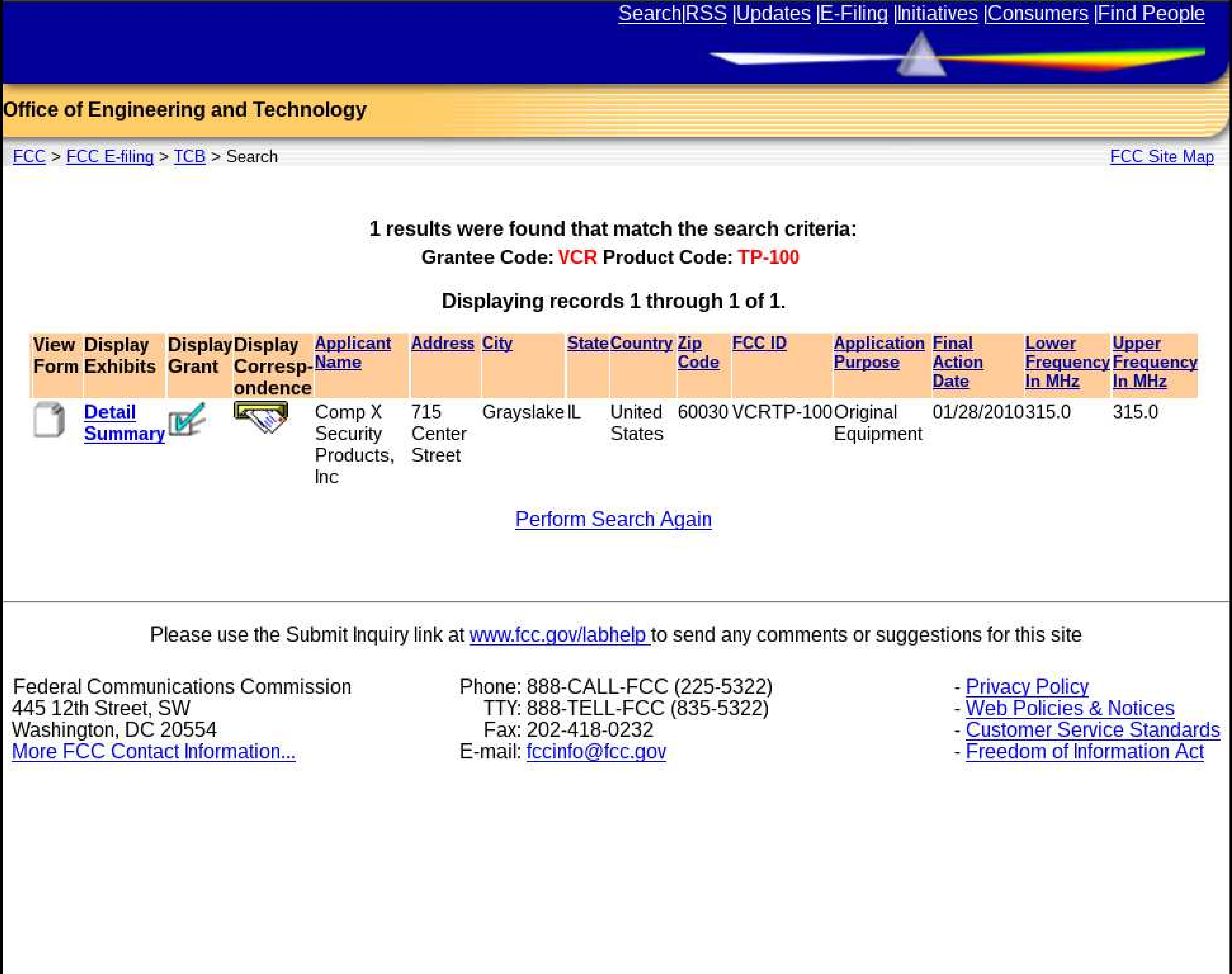
Try these:

- https://fcc.io/NPI
- https://fcc.io/NPI71646
- https://fcc.io/grantee/lego

ToDo

Other search suggestions?

Email to dominicgs@gmail.com



Search|RSS |Updates |E-Filing |Initiatives |Consumers |Find People

Office of Engineering and Technology

FCC > FCC E-filing > TCB > Search FCC Site Map

1 results were found that match the search criteria:

Grantee Code: VCR Product Code: TP-100

Displaying records 1 through 1 of 1.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Comp X Security Products, Inc	715 Center Street	Grayslake	IL	United States	60030	VCRTP-100	Original Equipment	01/28/2010	315.0	315.0

Perform Search Again

Please use the Submit Inquiry link at www.fcc.gov/labhelp to send any comments or suggestions for this site

Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
More FCC Contact Information...

Phone: 888-CALL-FCC (225-5322)
TTY: 888-TELL-FCC (835-5322)
Fax: 202-418-0232
E-mail: fccinfo@fcc.gov

- Privacy Policy
- Web Policies & Notices
- Customer Service Standards
- Freedom of Information Act

SDR in the future

better packet handling

better signal analysis

transceiver ICs
in the future

tricks for physical
layer reversing

http://greatscottgadgets.com/