RSAC Studio

Connect to Protect

Smart Toys: Are They Too Smart?

Oren Yomtov
Security Researcher
Synack Inc.
@orenyomtov

#RSAC

Smart Toys


PLAYMATION STARTER PACK
PLAYMATION
STARTER PACK
AVENGERS
REPULSOR GEAR
2 POWER ACTIVATORS
2 SMART FIGURES


Toymail

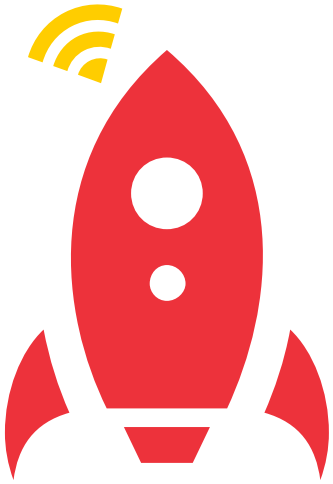

CAUTION - ELECTRIC TOY
Hello
Barbie
HELLO
HELLO
HELLO
PRESS BELT
& TALK


DDY KRUEGER
PREME EDITION
EPLICA METAL
GLOVE
GANT DE
FREDDY KRUEGER
SUPREME
I CAN TALK!

Background

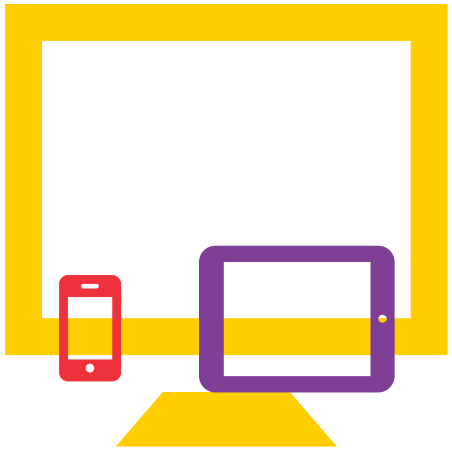
- Started breaking things in 2007
- Israeli Intelligence Corps
- Security Researcher at Synack

Smart Toy =



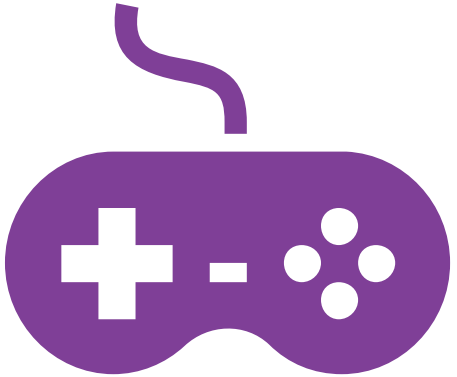
Physical Toy

+



Any Screen

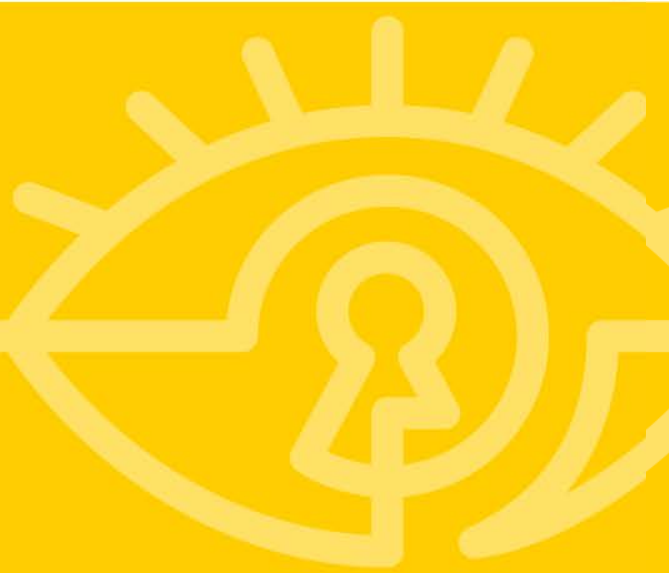
+



Game Software

Users

Manufacturers



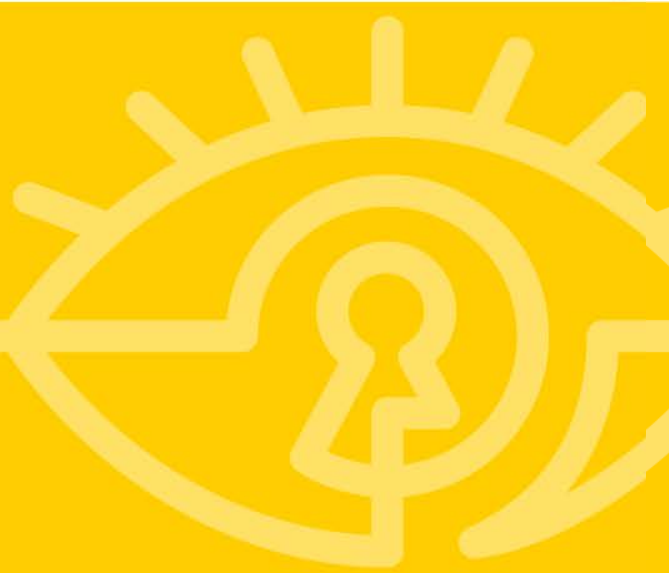
Users


Dear Diary,


WARNING
AUDIO SURVEILLANCE
Barbie
IN OPERATION
HELLO
HELLO


VIDEO
RECORDING
IN PROGRESS


Power
Internet
WAN
Wi-Fi
LAN1
LAN2



Manufacturers

The Washington Post

The Switch

VTech says 6.4 million children profiles were caught up in its data breach

By Hayley Tsukayama December 1, 2015

Man Hacks Monitor, Screams at Baby Girl

by KEITH WAGSTAFF

Welcome to the Internet of things. Creepy things.

Last week, Fox 19 reported that a man hacked into an Internet-enabled baby monitor in a home in Cincinnati, Ohio, and started screaming “Wake up baby!” at a 10-month-old girl.

Fox 19

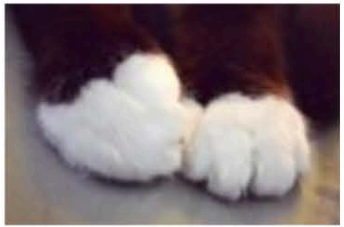
BuzzFeed

LOL

News Videos Quizzes Food DIY More Get Our

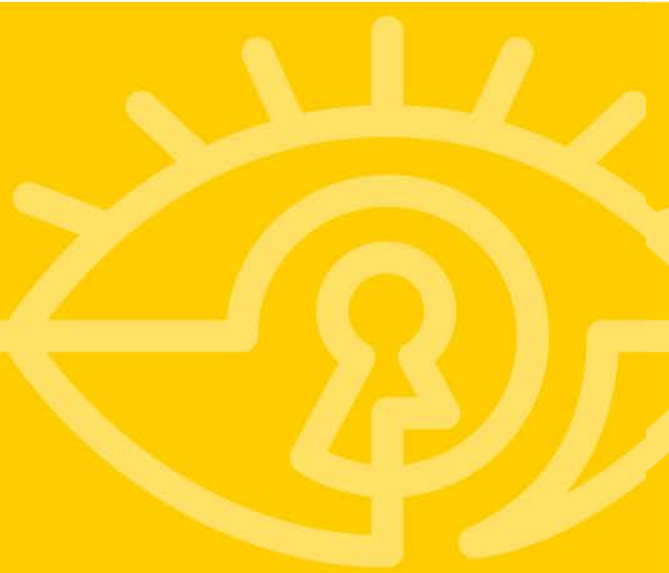






7 Creepy Baby Monitor Stories That Will Terrify All Parents

"You're being watched."



Attack Vectors

HTTP

HTTP

- HTTPS
- Certificate validation
- Certificate pinning

Web API

Toy

Server

Web API

- SQL injection
- Broken authentication
- Path traversal

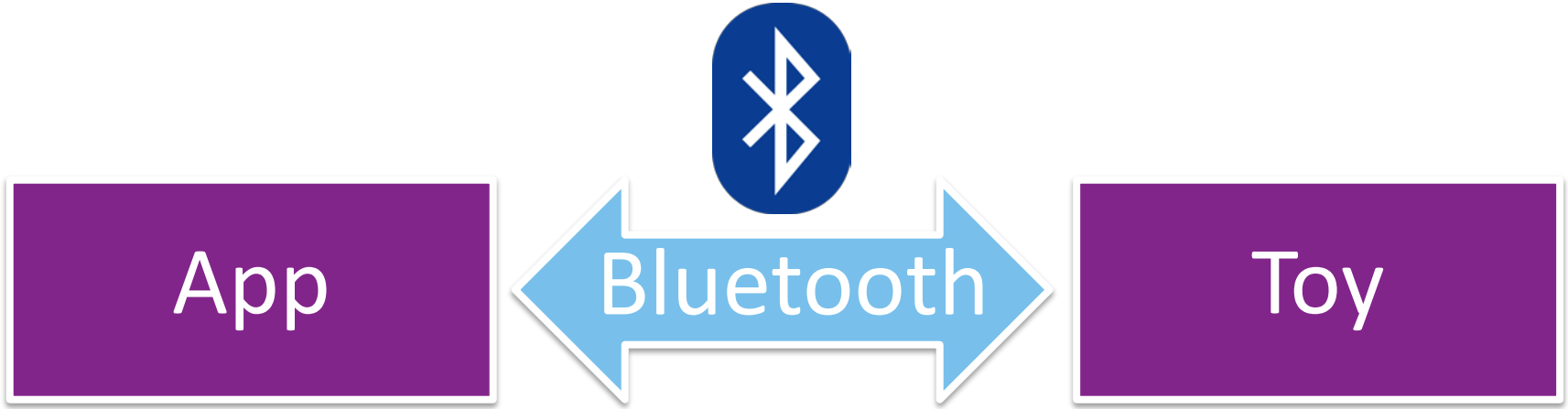
- For more information, visit [OWASP Top 10]

Firmware / Software Update

Firmware / Software Update

- Firmware signing
- Transport security (HTTPS)
- Encryption

Bluetooth



Hardware

Toy

TECHNIQUES

hardware - spoiler!

serial consoles found on 12 of 14 devices

Hardcoded Secrets

App

Toy

Hardcoded Secrets

- API Keys (e.g. AWS)
- URLs not meant to be exposed to end-users
- Credentials
- Encryption keys


Researchers
Press

RSAC Studio

Connect to Protect

Smart Toys: Are They Too Smart?

Oren Yomtov
Security Researcher
Synack Inc.
@orenyomtov

#RSAC

RSAC Studio

Connect to Protect

Your Part in Securing Our Connected World – Are You Ready?

Michele D. Guel
Distinguished Engineer, Infosec
Cisco Systems
@MicheleDGuel

#RSAC

A Typical Connected Day in 2017

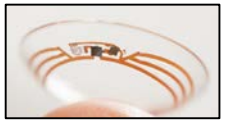




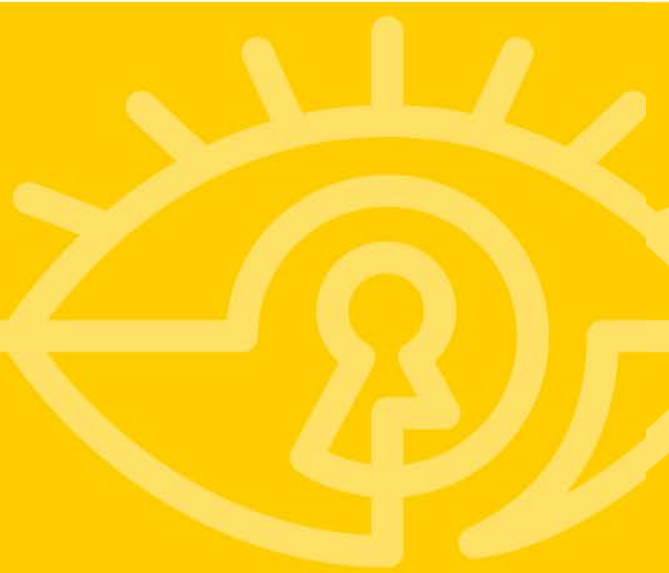







What if every aspect of your life was digitally captured?



Opportunities & Challenges

What are the Opportunities?

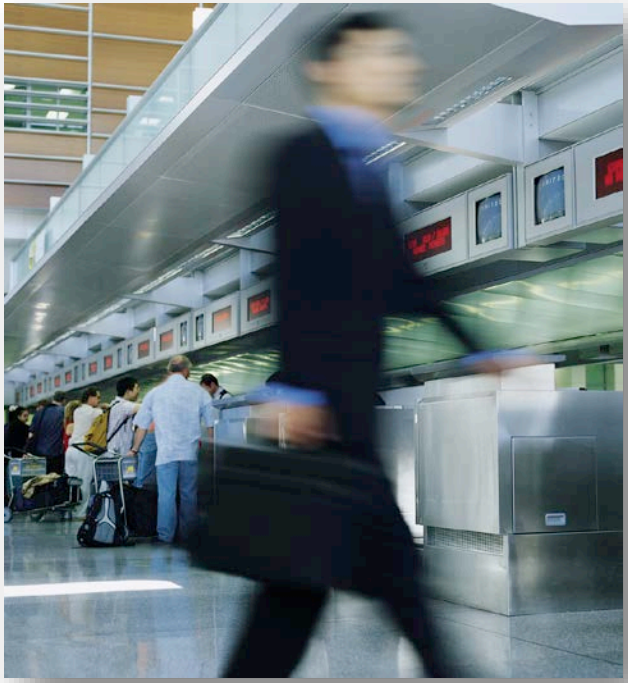
- Data driven decisions
- Increased automation
- Higher productivity
- Efficient use of resources
- Exponential connectedness
- Limitless possibilities

What are Challenges?

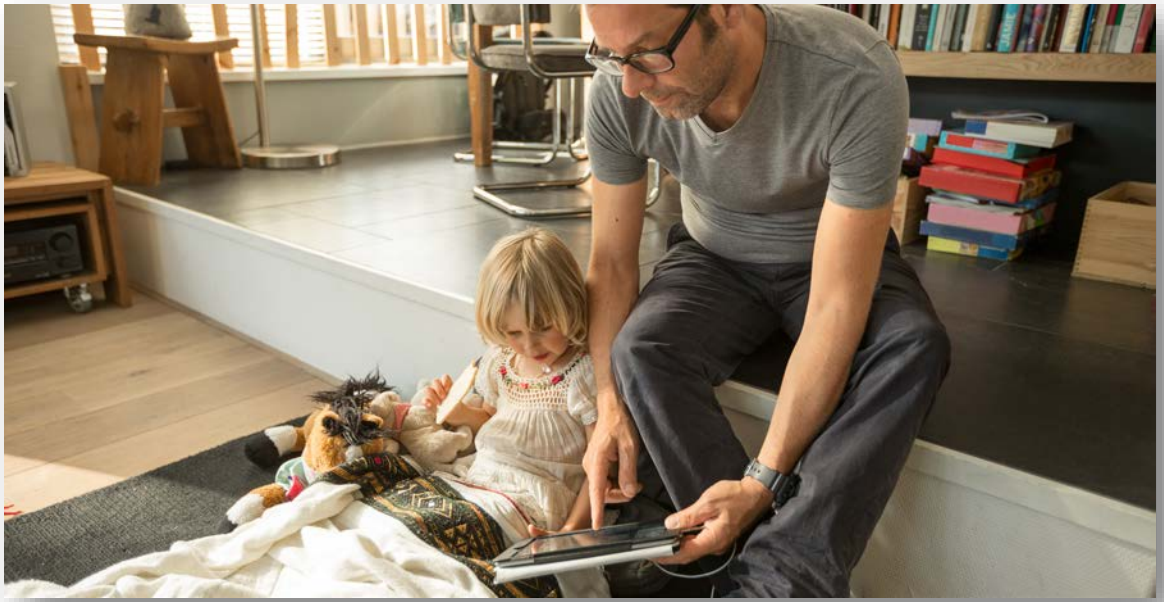
- Loss of privacy
- Loss of humanity
- New, unforeseen attack vectors
- Increase risk of targeted attacks
- Increase need for new laws and regulations
- Exponential expansion of threat landscape

IOT is Moving at Warp Speed

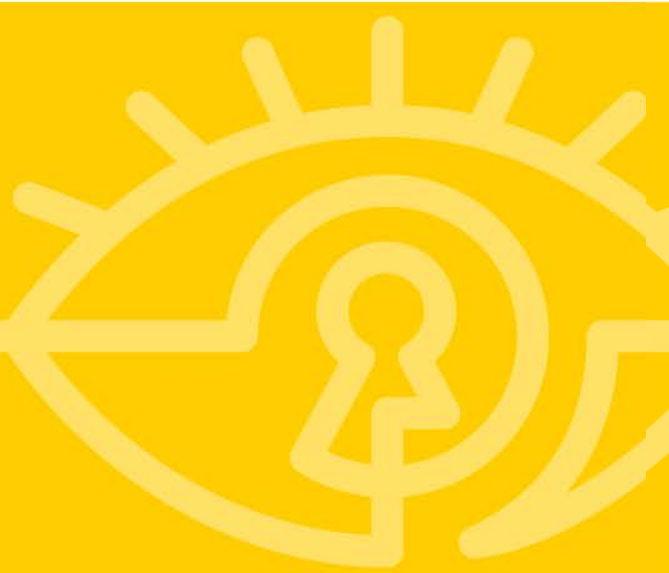
"As is often the case, consumer demand for new and exciting technologies have far surpassed the implementation of security measures."



cisco



How Connected Do You Want to Be?



Our Part

As Individuals We Can…

- Hold vendors accountable
- Don’t use applications with weak security
- Understand privacy laws
- Get educated on new technologies
- Encourage your kids to pursue STEM

As Employees We Can…

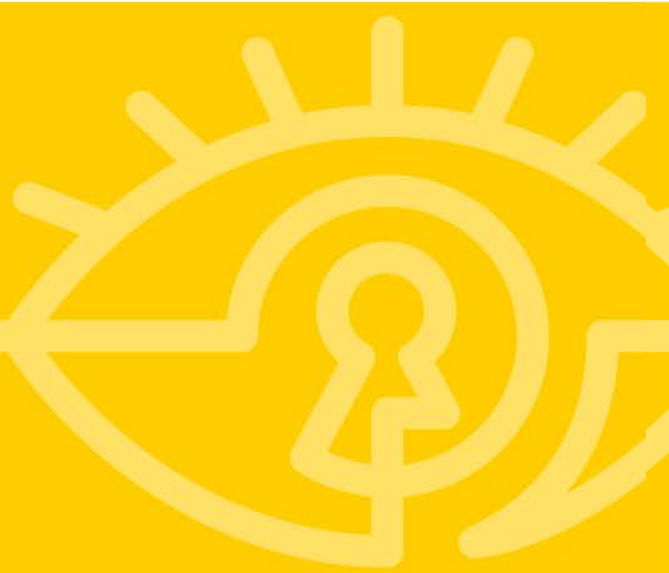
- Hold vendors accountable
- Develop & adopt standards for application integrity and trustworthiness
- Develop and adopt standards for IP enabled devices
- Develop and adopt seamless and scalable identity for people, process and things

Apply What You Have Learned Today

- Within 30 days:
  - Identify where sensor/smart technology is in use
  - Become more proactive about privacy of data
- Within 60 days:
  - Form a strategy around securing sensor/smart technology
  - Understand changing privacy laws that pertain to your organization and your personal data

Apply What You Have Learned Today

- Within 180 days:
  - Implement policy regarding use of sensor/smart technology
  - Ensure IoT projects are reviewed by security architecture team



Thank You