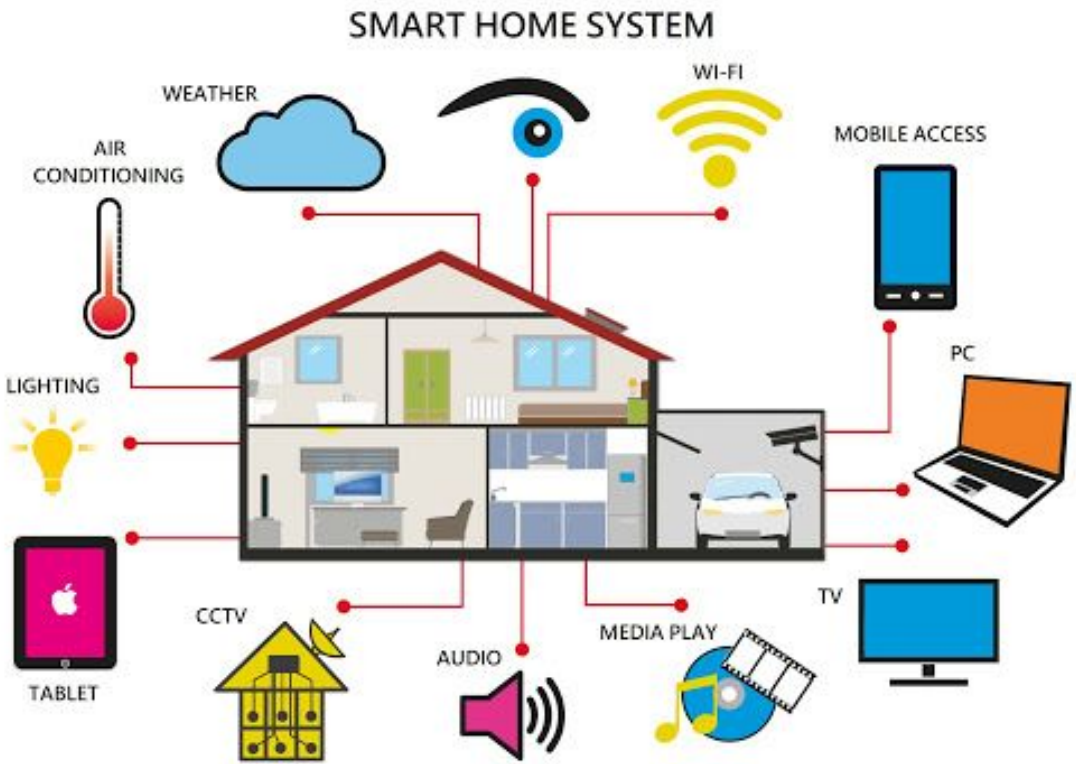
An Interdisciplinary Study on IoT Devices for Children

David Yifu Lang

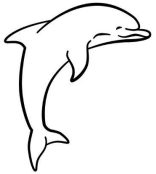

SMART HOME SYSTEM
WEATHER
WI-FI
AIR CONDITIONING
MOBILE ACCESS
PC
LIGHTING
TV
CCTV
MEDIA PLAY
AUDIO
TABLET

Background

End User Perception

- Often can be difficult for less technologically experienced users to understand the importance of following security standards
  - The most sophisticated security mechanisms are useless if they’re not being employed
- Can be attributed to the lack of reinforcement learning in security
  - Positive reinforcement: good security practices → not being attacked
    - No direct reward for good practices
  - Negative reinforcement: bad security practices → *possible* breach of security
    - Possibility of no consequences for bad practices

IoT Security Standards



"Dolphin" device emits ultrasonic sound undetectable by humans to activate VCA

Amazon Echo Dot for Kids

- Amazon’s child-friendly version of their smart home device
- Hardware is identical to the normal version; this product comes with an Alexa FreeTime subscription
  - Allows a user to enable FreeTime for certain devices, enabling child protection and filtering
  - Any Echo device can have FreeTime enabled

ROYBI Robot

- Smart toy designed to teach children a variety of topics, such as STEM topics and language
- Includes facial recognition capabilities
- App provides statistics on child's learning experience and will make suggestions on what to improve
- App has access to the mic and camera of the device, available for streaming
    - App user can speak through the device as well

Protecting Children

COPPA gives parents control over their child's data:

- What data is collected and how it is used
- Verifies parental consent
- Prohibits service from disclosing data to third parties, unless necessary
- View and delete collected data
- Prevent further use or collection of data
- Maintain the confidentiality, security, and integrity of the information
- Service retains information only for service use
- Collect no more than the necessary data for service

High-level Goals

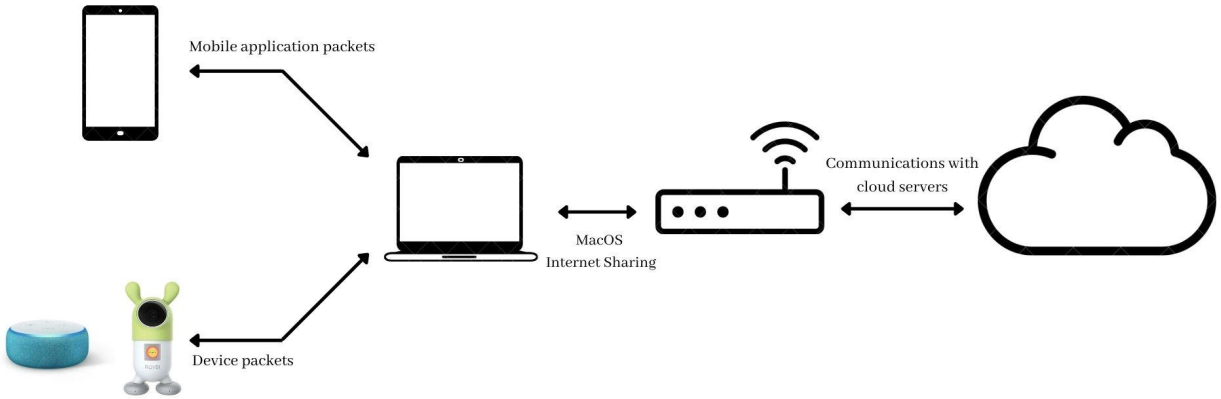
1. Develop a generalizable mental model of how parents understand cloud infrastructure and the IoT domain

2. Develop a threat model based on network analysis for possible attack vectors

3. Recommend security practices and mechanisms for safer IoT use

Methodology

qualtrics XM



End-User Study

Privacy Policy Findings

Amazon Echo Dot for Kids

- Records audio only when “wake word” is called
- Stored Amazon cloud services
- Application collects personal information, but Amazon will not sell to third-parties
  - Name, birthdate, contact info, voice, location, identifiers (ex. IP address)
- Children will not receive interest-based advertisements
- Adult users may revoke data collection permissions

ROYBI Robot

- Records audio and video only during lesson
- ROYBI service collects personal information, but *currently* does not sell to third-parties
- Stored on AWS
- COPPA-compliant
- All video, audio, and password data is encrypted
- Adult users can access data and delete their accounts, all data will be deleted after 90 days as well

ID	Age	Children's Age(s)	Occupation	Familiarity with Technology (Self-reported)
A	43	4	Data Analyst	Professional Experience
B	42	6	Accountant	Some Experience
C	45	6	Data Analyst	Some Experience
D	37	2	Sales	Moderate Experience
E	37	1, 3	Homemaker	Lots of Experience
F	42	3, 4	Quality Specialist	Some Experience
G	39	5	Coordinator	Lots of Experience
H	48	5	Clinical Pharmacist	Professional Experience
I	39	4, 6	Construction Superintendent	Professional Experience
J	39	0, 3	Physical Therapist	Some Experience
K	38	4, 6	Teacher	Professional Experience
L	38	2, 4	None	Moderate Experience
M	39	3	Lawyer	Lots of Experience
N	64	4	Mathematician	Professional Experience
O	35	1	Software Engineer	Professional Experience
P	26	0, 2, 4	Direct Sales	Lots of Experience

ID	Smart Home Owner	Child Smart Home Use	Smart Device Owner	Child Smart Device Use
A	More than 2 years	No	More than 2 years	Yes
B	More than 2 years	Yes	1-2 years	No
C	More than 2 years	No	N/A	N/A
D	N/A	N/A	More than 2 years	No
E	More than 2 years	Yes	More than 2 years	No
F	N/A	N/A	More than 2 years	No
G	More than 2 years	Yes	More than 2 years	Yes
H	More than 2 years	Yes	More than 2 years	Yes
I	More than 2 years	Yes	More than 2 years	Yes
J	More than 2 years	Yes	More than 2 years	No
K	1-2 years	Yes	Less than 3 months	Yes
L	1-2 years	Yes	More than 2 years	No
M	More than 2 years	No	More than 2 years	Yes
N	1-2 years	Yes	More than 2 years	No
O	N/A	N/A	More than 2 years	Yes
P	More than 2 years	Yes	More than 2 years	No

Device Review

- Pros
  - Simple design, easy to use
  - Parental controls
  - Amazon’s reputation
- Cons
  - Data collection
  - Spying, targeted advertising
  - Amazon’s reputation

- Pros
  - Good for at-home learning, especially during the pandemic
  - Natural language processing and facial recognition features
- Cons
  - Bad design, doesn’t feel friendly
  - Screen too small
  - Spying and facial recognition

Question	Disagree	Slightly Disagree	Slightly Agree	Agree
I have concerns for how my data is collected and stored on the Internet.	0	4	4	8
I find it important that collected data is kept private.	0	2	4	10
I thoroughly research into Internet-connected devices before making a purchase.	1	3	7	5
I am familiar with the Children's Online Privacy Protection Act (COPPA).	8	2	4	2

Security Concern	Count
Data Storage	10
Data Usage	6
Inappropriate Content	8
Privacy	12
Other	1
None	1

Dialogue Concerns	Count
Inappropriate Dialogue	4
Data Storage	4
How data is used	11
Privacy of Conversations	11
Other	0
None	4

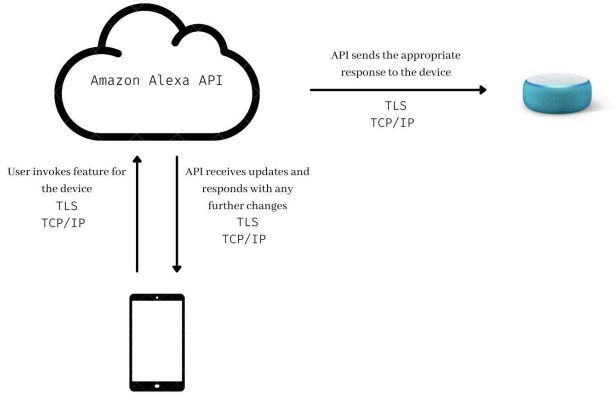
Findings

- Participants in a technical occupation demonstrated a deeper understanding of data collection and privacy, while those who were not demonstrated otherwise
  - Consequently, those who have less of an understanding tend to follow fewer security practices
- Participants' expectation of the contents on privacy policies did not align with the actual contents
  - Did not know exactly what data is collected, when it is collected, and how they use it
- Product design plays a role in user expectations
  - Less trust for ROYBI due to crude design
  - More trust for Amazon due to the company's reputation

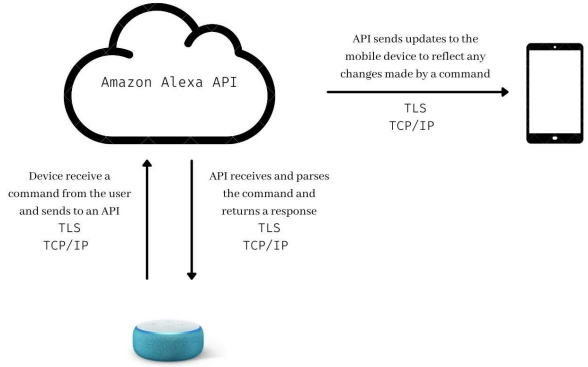
Device Taxonomy

Alexa FreeTime / Amazon Kids

- Allows parental controls for Alexa-enabled devices with FreeTime enabled
  - Helps manage Amazon Kids profiles
  - Set daily limits, add digital contents (e.g. e-books, apps, videos)
- Certain explicit phrases are not processed with FreeTime enabled
  - When mature content is requested, the device may either decline to answer or redirect the question to an adult
  - Requests containing explicit language is ignored
- Only kid-friendly Skills can be invoked with FreeTime enabled
  - Skills such as Spotify, The Washington Post, etc. are not available, as they contain contents that are inappropriate for children



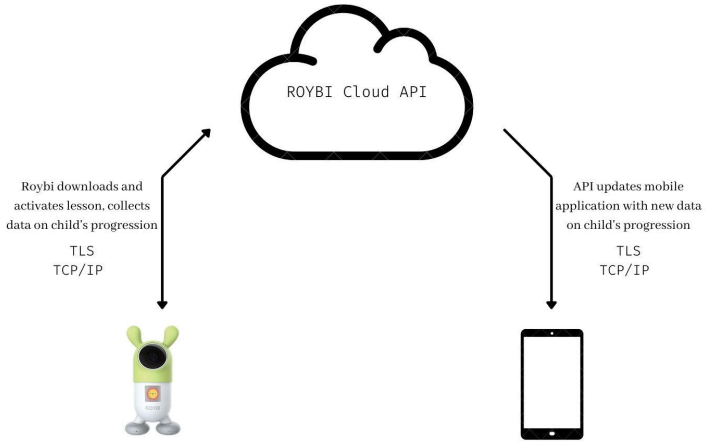
Mobile application command



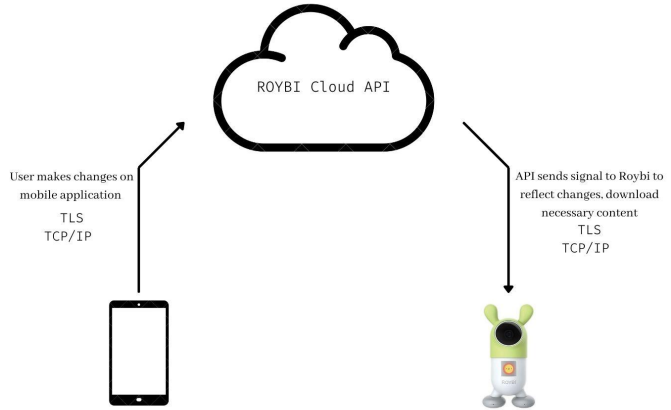
Voice command

Feature	Mobile Endpoint	Device Endpoint
Call	device-metrics-us-2.amazon.com cmds-tachyon.com (STUN)	avs-alexa-14-na-amazon.com cmds-tachyon.com (UDP)
Drop In	cmds-tachyon.com (STUN)	cmds-tachyon.com (UDP)
Announce	tp.cb7933e1d-frontier.amazon.com	avs-alexa-14-na-amazon.com
Play	tp.5fd53c725-frontier.amazon.com	Depends on *skill* invoked

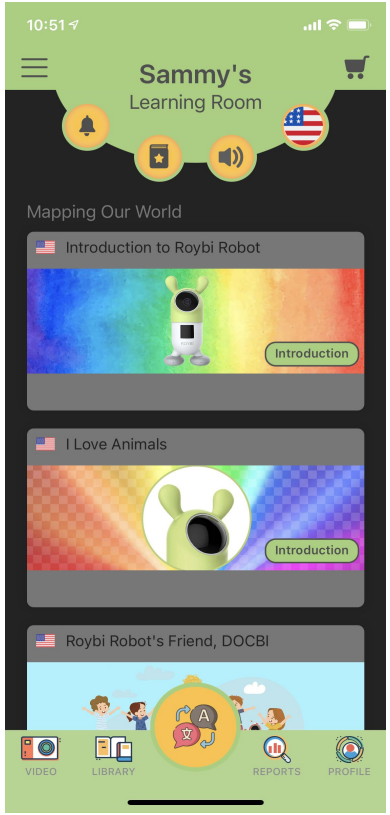
Mobile application feature endpoints

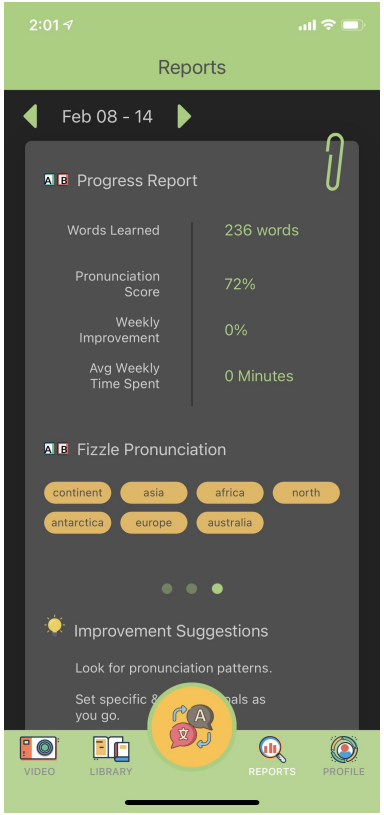


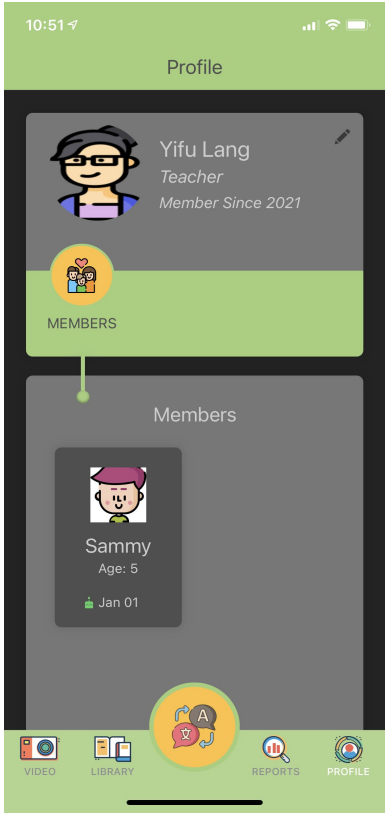
Roybi starts a lesson

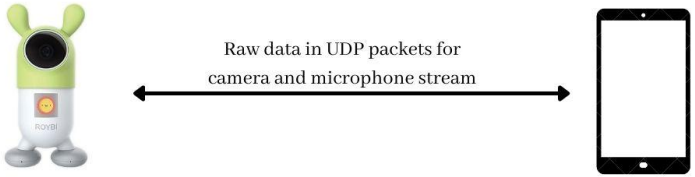


Parent makes update on mobile application


10:51
Sammy's
Learning Room
Mapping Our World
Introduction to Roybi Robot
Introduction
I Love Animals
Introduction
Roybi Robot's Friend, DOCBI
VIDEO
LIBRARY
REPORTS
PROFILE

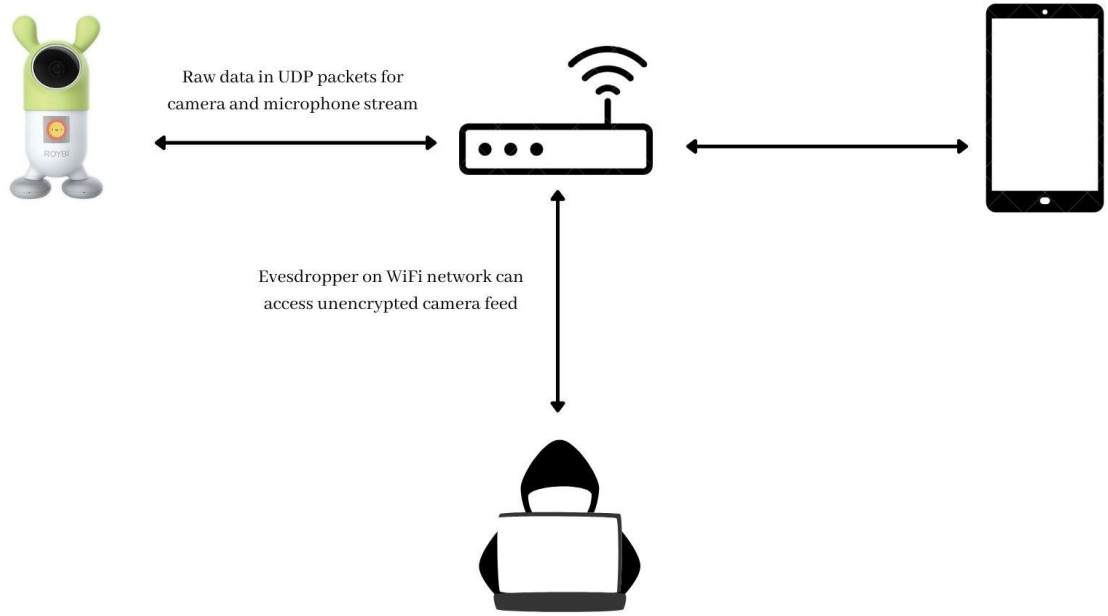

2:01
Reports
Feb 08 - 14
Progress Report
Words Learned
236 words
Pronunciation Score
72%
Weekly Improvement
0%
Avg Weekly Time Spent
0 Minutes
Fizzle Pronunciation
continent
asia
africa
north
antarctica
europe
australia
Improvement Suggestions
Look for pronunciation patterns.
VIDEO
LIBRARY
REPORTS
PROFILE

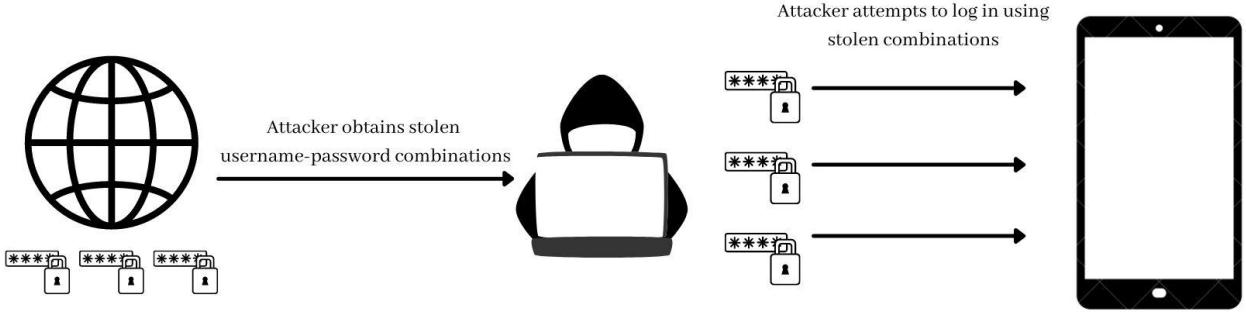

10:51
Profile
Yifu Lang
Teacher
Member Since 2021
MEMBERS
Members
Sammy
Age: 5
Jan 01
VIDEO
LIBRARY
REPORTS
PROFILE




```
0000  ea f7 77 a2 d7 20 cc 4b  73 5f 34 cc 08 00 45 00   ··w·· ·K s_4···E·
0010  01 9c 26 1d 40 00 40 11  80 d9 c0 a8 03 04 c0 a8   ··&·@·@· ········
0020  03 06 43 76 68 b7 01 88  49 86 f1 d0 01 7c d1 02   ··Cvh··· I····|··
0030  00 47 7f 7f ff ff 7f 7f  7f 7f 7f 7f ff ff 7f 7f   ·G····· ········
0040  ff ff 7f 7f ff 7f ff ff  ff ff 7f 7f ff 7f 7f 7f   ········ ········
0050  7f 7f ff ff ff ff ff ff  ff ff 7f 7f 7f ff 7f 7f   ········ ········
0060  7f 7f ff ff ff 7f ff ff  7f 7f 7f 7f ff 7f ff ff   ········ ········
0070  7f ff ff 7f ff ff ff 7f  7f ff ff ff ff 7f 7f 7f   ········ ········
0080  7f 7f ff ff ff ff ff 7f  7f ff 7f 7f 7f 7f 7f 7f   ········ ········
0090  ff ff ff 7f ff ff 7f ff  7f 7f ff 7f ff ff ff ff   ········ ········
00a0  ff ff ff ff ff ff 7f 7f  7f 7f ff 7f 7f ff 7f 7f   ········ ········
00b0  7f ff ff 7f ff ff 7f ff  ff 7f 7f ff 7f 7f ff ff   ········ ········
00c0  7f 7f ff ff ff ff ff ff  ff ff 7f 7f 7f ff ff ff   ········ ········
00d0  ff 7f 7f 7f 7f ff 7f 7f  ff ff ff ff ff 7f ff ff   ········ ········
00e0  7f ff ff 7f 7f 7f 7f 7f  7f 7f 7f 7f 7f ff ff ff   ········ ········
00f0  7f ff ff ff ff ff ff ff  7f 7f ff ff ff ff 7f 7f   ········ ········
0100  ff 7f 7f ff ff 7f 7f ff  ff 7f 7f ff 7f ff ff 7f   ········ ········
0110  7f ff ff ff 7f ff 7f 7f  7f 7f ff 7f ff ff 7f 7f   ········ ········
0120  fe ff 7d 7e fe fe 7e 7e  ff 7f 7e fe fe 7f 7f ff   ··}~··~~ ··~·····
0130  7f 7e fe ff 7e 7f ff 7e  7e fe ff 7e 7f ff 7e 7e   ·~··~··~ ~~·~··~~
0140  fe fe 7e fe 7f 7f ff 7f  7e fe fe 7e ff fe 7e 7d   ··~····· ~···~}
0150  fe 7f 7e fd ff 7e 7f ff  7e 7e fe 7e 7f fe ff 7f   ··~··~·· ~~·~····
0160  7f ff ff 7f ff ff ff 7f  7f 7f 7f 7f ff 7f ff 7f   ········ ········
0170  ff ff ff 7f 7f 7f 7f 7f  ff ff 7f ff 7f ff ff 7f   ········ ········
0180  ff ff ff 7f 7f ff ff 7f  7f 7f 7f ff ff 7f 7f ff   ········ ········
0190  7f 7f ff 7f ff ff 7f 7f  ff ff 7f 7f 7f ff ff 7f   ········ ········
01a0  7f ff 7f 7f 7f 7f ff 7f  ff ff                     ········ ··
```

```
0000  ea f7 77 a2 d7 20 cc 4b  73 5f 34 cc 08 00 45 00   ··w·· ·K s_4···E·
0010  01 9c 26 21 40 00 40 11  80 d5 c0 a8 03 04 c0 a8   ··&!@·@· ········
0020  03 06 43 76 68 b7 01 88  49 86 f1 d0 01 7c d1 02   ··Cvh··· I····|··
0030  00 47 7f 7f ff ff 7f 7f  7f 7f 7f 7f ff ff 7f 7f   ·G····· ········
0040  ff ff 7f 7f ff 7f ff ff  ff ff 7f 7f ff 7f 7f 7f   ········ ········
0050  7f 7f ff ff ff ff ff ff  ff ff 7f 7f 7f ff 7f 7f   ········ ········
0060  7f 7f ff ff ff 7f ff ff  7f 7f 7f 7f ff 7f ff ff   ········ ········
0070  7f ff ff 7f ff ff ff 7f  7f ff ff ff ff 7f 7f 7f   ········ ········
0080  7f 7f ff ff ff ff ff 7f  7f ff 7f 7f 7f 7f 7f 7f   ········ ········
0090  ff ff ff 7f ff ff 7f ff  7f 7f ff 7f ff ff ff ff   ········ ········
00a0  ff ff ff ff ff ff 7f 7f  7f 7f ff 7f 7f ff 7f 7f   ········ ········
00b0  7f ff ff 7f ff ff 7f ff  ff 7f 7f ff 7f 7f ff ff   ········ ········
00c0  7f 7f ff ff ff ff ff ff  ff ff 7f 7f 7f ff ff ff   ········ ········
00d0  ff 7f 7f 7f 7f ff 7f 7f  ff ff 7f ff ff 7f ff ff   ········ ········
00e0  7f ff ff 7f 7f 7f 7f 7f  7f 7f 7f 7f 7f ff ff ff   ········ ········
00f0  7f ff ff ff ff ff ff ff  7f 7f 7f ff ff ff 7f 7f   ········ ········
0100  ff 7f 7f ff ff 7f 7f ff  ff 7f 7f ff 7f ff ff 7f   ········ ········
0110  7f ff ff ff 7f ff 7f 7f  7f 7f ff 7f ff ff 7f 7f   ········ ········
0120  fe ff 7d 7e fe fe 7e 7e  ff 7f 7e fe fe 7f 7f ff   ··}~··~~ ··~·····
0130  7f 7e fe ff 7e 7f ff 7e  7e fe ff 7e 7f ff 7e 7e   ·~··~··~ ~~·~··~~
0140  fe fe 7e fe 7f 7f ff 7f  7e fe fe 7e ff fe 7e 7d   ··~····· ~···~}
0150  fe 7f 7e fd ff 7e 7f ff  7e 7e fe 7e 7f fe ff 7f   ··~··~·· ~~·~····
0160  7f ff ff 7f ff ff ff 7f  7f 7f 7f 7f ff 7f ff 7f   ········ ········
0170  ff ff ff 7f 7f 7f 7f 7f  ff ff 7f ff 7f ff ff 7f   ········ ········
0180  ff ff ff 7f 7f ff ff 7f  7f 7f 7f ff ff 7f 7f ff   ········ ········
0190  7f 7f ff 7f ff ff 7f 7f  ff ff 7f 7f 7f ff ff 7f   ········ ········
01a0  7f ff 7f 7f 7f 7f ff 7f  ff ff                     ········ ··
```


Raw data in UDP packets for
camera and microphone stream
Evesdropper on WiFi network can
access unencrypted camera feed


Attacker obtains stolen
username-password combinations
Attacker attempts to log in using
stolen combinations

Conclusion

Recommendations for Developers

- Preventing automated attacks
  - Prevent password stuffing, brute force, and dictionary attacks by verifying the client
- Encrypt everything, secure everything!!
  - We, and prior research, have found insufficiently encrypted or secure systems
- Multi-factor authentication
  - Virtually unbreakable, but may be a hassle for users
- Data collection transparency
  - Most people in our survey did not know when, how, and where data is collected

Future Work

- Diversify survey participants
  - Our participants were found through word of mouth and picked from an existing subject pool from the UCSC Baby Lab
  - Finding a wider diversity of participants helps us develop a better mental model
- Analyze more devices
  - Plenty of IoT devices available on the market, does not need to be a children's device
  - More industry examples helps up develop a better threat model
- In-person Interviews
  - This was the original plan, but had to be reconsidered due to the COVID-19 pandemic
  - Allows in-person interviews, and allows the children to play with the devices

Questions and Comments