Analysis of Security Concerns & Privacy Risks of Children's Smart Toys

Danelle L. Dobbins

Abstract— **This paper will examine smart toys marketed to young children that pose both security and privacy risks. Recently, Mattel's Hello Barbie and Talking Cayla have received wide publicity thanks to consumer watch groups and white hat hackers like Ken Munro. Future toys will be networked with additional toys and across the internet creating a smaller subsection of the Internet of Things, the "Internet of Toys." Microphone and camera recording capabilities are becoming a more standard feature in modern toys, as well as in the applications with which they interface with. The integration of these high tech features creates avenues for unsolicited data collection and tech-savvy pedophiles. While there are several government and data privacy standards such as COPPA, The Children's Online Privacy Protection Act that are aimed at protecting the youngest consumers are they really enough? This paper will analyze data privacy issues of toys and devices intended for children, suggest ways to mitigate their security risks, examine available security product offerings to date and explore current consumer legal protections in place.**

I. Introduction

New technologies and the rise of the internet of things will allow the children of this generation to experience seamless interactive technologies geared for entertainment and education unlike any previous generations. While these advancements create new markets and open a plethora of possibilities for the imagination, it is important to ensure these devices meet the highest of security standards. Toy producers and parents need to consider the threat of exposure to compromised websites, engaging with dangerous contacts, over-sharing of information, and cyber bullying when they purchase or create products that allow children to interact in the digital world. Artificial Intelligence companies such as ToyTalk and IBM's super computer Watson's participation in the physical/virtual toy world are already here. There are several opportunities for parents and toy manufacturers to limit the risk to children such as creating better authentication methods and providing software that allows for parent control.

Data privacy in regards to the internet of toys is of major concern. If your child's interactions with a machine are stored and processed on a remote server on the other side of the world what will be done with that data and who has access to it? While the Children's Online Privacy Protection Act was instituted in 1989 how applicable it is in today's world and are these laws are being adequately monitored and enforced by regulatory agencies such as the self-regulating Children's Advertising Review Unit.

The future is right around the corner, Hello Barbie and Tiggly the Dinosaur will become available later this year, companies are clearly preparing to capitalize on the new toy tech frontier. Are we ready as consumers to take on the risk that comes with the intelligent toy?

II. The Beginning & Future direction of the smart Toy

The Smart toy has been in development for quite some time. The New York Times in 2007 announced that several major toy companies; Mattel, Disney Hasbro, and Lego were underwriting a 5 year study at MIT Media Labs known as "Toys of Tomorrow." The project was meant to design "playthings as diverse as a toy piano that will sound like a Steinway, intelligent jogging shoes that can measure speed and distance, and small robots that will operate in antlike colonies reminiscent of the toy soldiers in the movie Toy Story." The industry knew that opportunity was on the horizon. Microsoft had just invested $30 million to develop the Actimate Barney doll at the time.

A brief glimpse into the work at the MIT Media Laboratory is available in a paper released in 1999 titled "Sympathetic Interfaces: Using a Plush Toy to Direct Synthetic Characters." The study examines the concept of a sympathetic interface for controlling a physical plush animal embedded with wireless sensors in a virtual world and how to optimize the immersive experience. The lab designed the interface to try to be sympathetic to the user in that it would examine context and try to anticipate or understand the user's intentions. The Plush creature when handled by a user generated raw data that was processed in real time and associated with a gesture recognition model to make the motion more fluid rather than literal in the virtual world as to not seem erratic. The doll was tested on over 400 participants and was well received.

Fast forward to present day and we find that several companies are very interested in today's networked intelligent toy market. An article featured in Computer World titled "Google's Internet-connected toys patent sparks privacy concerns, visions of IoT Chucky" examines a patent filed by Google in February of 2012 that recently surfaced in May of 2015. The patent was filed for an anthropomorphic device that can be configured to control one or more media devices. If the

device detects a social queue or recognized movement it will respond with its own human-like movement response and/or transmit the demand to the media device causing the media device to change state. The device would include a motor, camera, speakers and microphones. See Figures A& B.

Figure A.

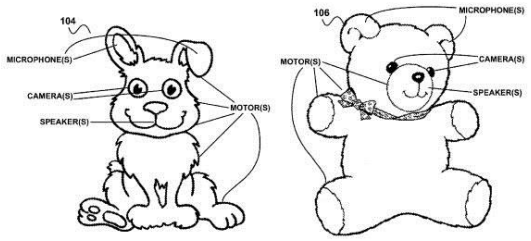
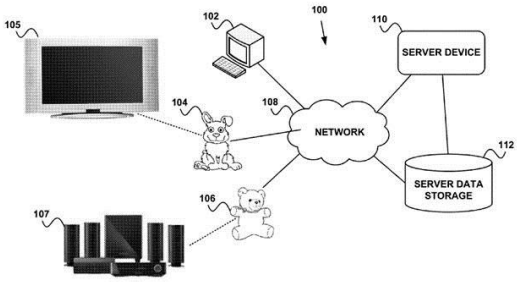


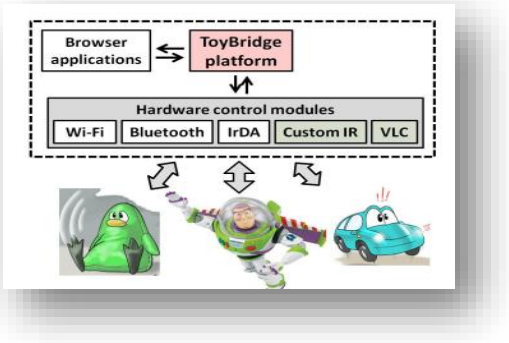
Figure B.



The article states a spokesperson for Google down played the patent by suggesting it was in the company's best interest to file patents in the event that an invention did come to fruition. Not all patents are guaranteed products. However, it is known that Google is very interested in the IoT space and is working on developing "Brillo" an Android system designed for low power devices with very small amounts of RAM.

Disney is no doubt a majoy player in the intelligent toy space. A white paper from a Disney Research Center in Zurich, Switzerland explores the functionality of Toy Bridge, a middleware platform that was developed to integrate physical world smart toys with online activities (Figure C). Browser applications aren't permitted to control hardware so the toy applications would use sockets to communicate with the ToyBridge OS Service, which consists of hardware modules responsible for controlling the toys.

Figure C.



The ToyBridge-to-toy interface depends on the type of toy used. For example, the Lego Mindstorms NXT Toys are connected via standard infrared blue tooth interface. Buzz Lightyear remote controlled robots, however function by a proprietary infrared communication protocol which cannot be implemented using standard infrared hardware and libraries.

Ideally, there would be a seamless toy-to-browser interface that would make full use of smart toys' radios, sensors, and actuators. Some of the challenges that come with the wireless ToyBridge platform are online user authentication, identity management with real world toys, maintaining low costs for toys with such advanced capabilities, and offloading complexity to a computer by sending its data to that ToyBridge-running computer for processing. Smart Toys would need to be able to identify and interact with one another passively and/or actively. Further opportunities for toy development include green toys powered by solar energy, and utilizing the power of a network of toys to make toys delay tolerant.

The Toy Talk Platform is currently in the process of being integrated with Toy Bridge middleware. Toy Talk uses a form of VLC, visible light communication in which a bi-directional LED transmitter and receiver is used to exchange information. LED technology has been used in toys previously and is desirable because of the small size, low cost, and low energy needs. The future Internet of Toys will merge online gaming and social networking into a seamless experience. To illustrate the paper provides the following example; you visit a theme park where you can interact in the physical world with your toy and other toy owners and continue the experience in the virtual world after the visit. Toys would react differently with one another based on familiarity and the frequency of interaction. The paper argues that authenticating into social networks using physical toys would be safer, although it fails to elaborate with further evidence.

III. Tech Companies on the Smart Toy Front

A recent TechCrunch article did a feature story on ToyTalk. ToyTalk is based out of San Francisco led by former Pixar Alums which creates entertainment applications for iPads such as Winston Zoo and SpeakaZoo. They just released Speakalegend, a character-driven touch and play app. ToyTalk may easily become the front runner in toy technology, as they

have just announced licensing deals for their speech recognition technology with at least a dozen major brand children's toy companies.

ToyTalk has prided itself on its voice recognition technology development. It is far more challenging to analyze a young child's voice relative to an adult as well as engage in conversations rather than responding to commands similar to iPhone's Siri. The company may be worth as much as $15 million. ToyTalk devices will surely outpace Teddy Ruxpin, a teddy bear toy popular in 1985 and still on shelves in 2010 known for reading pre-recorded stories and recreating the stories with his pal Grubby. They are also set to surpass LeapFrog's personalized read-back stories where it is possible to add in your child's favorite food or color with a simple USB link to a computer because ToyTalk technology will enable full conversations.

Elemental Path is another tech toy producer to watch out for. They will begin rolling out the CogniToys line in which the toys will be able to connect to the artificial intelligence of IBM's Watson super computer. The company raised capital by featuring the product on Kickstarter and was so well received they quickly surpassed their funding goals. The first toy in the CogniToy line is in the form of a green dinosaur that can provide age-appropriate answers to thousands of questions asked by children when the toy's belly is pushed. The toy is advertised mainly to help kids with rhyming, spelling, vocabulary and math. The loveable green dinosaur starts processing the input immediately as it is received. It was set to be released in May of 2015, but at the time of this paper I was unable to find any retailers selling the green dinosaur smart toy known as "Tiggly" (Figure D).

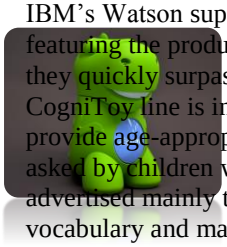


Figure D. Tiggly the Dinosaur

KickStarter Video:
https://www.kickstarter.com/projects/522717158/cognitoys-internet-connected-smart-toys-that-learn

Disney Playmation was officially introduced to the world in a press release on June 2, 2015 in Glendale, CA. In a collaboration with Hasbro the "digital gets physical and imagination becomes real." The smart technology includes action figure toys, wearables, wireless technology, and motion sensors that allow kids to go on different missions and become the heroes of the story. The toys and wearables interact with an application that let the consumer know their points earned, new powers unlocked, and the next mission. A third party study commissioned by Disney found that parents have nostalgia for the way they used to play and have a desire to keep their kids physically active. The online study of 2,000 families found that parents are open to their kids growing up in a rich technology environment and 9 out of 10 parents were very on board with a technology that could keep play active.

The first product line to be released will be the Avengers. Playmation is purposefully not tied to an internet connection so play can take place anywhere from living rooms to the outdoors. The Avengers pack also comes with multiplayer modes to take on missions together or challenge one another in competitive play. The launch of the product line will take place in October of 2015. While Avengers will be the first on product series to be released, the Starwars line is set to debut in 2016 and Frozen in 2017.

A link to the press release demo of the toy can be found here: http://youtu.be/O34Nd4vkpro

IV. Hacking Smart Toys with Ken Munro

Ken Munro, a white hat hacker, is on a mission to put smart toy security to the test. He has successful hacked the My Friend Cayla doll available in the United Kingdom. On his penetration testing website he speculates how the Cayla doll compares to Hello Barbie which will be released later this year in 2015.

The Cayla doll uses Bluetooth and requires no Bluetooth authentication leaving the doll extremely vulnerable if the hacker is within range. Munro says that even if Cayla was already paired the potential hacker would just have to offer a stronger Blue tooth signal to the doll to initiate a new pairing. The doll comes with an app to talk/interact with the owner of the toy, but if the app is compromised the doll can essentially be used as a Bluetooth headset in which the hacker could talk to the child and hear the responses, a security nightmare.

The Cayla doll does all of its processing on the smart phone app she pairs with, however if she hears any of 3,000 known

words she will query a local database for a faster response. Munro reports it is extremely easy to hack the database and modify its contents if you have high enough admin privilege on the android device where the app is stored. It also would not be hard to work around the pin authentication because the doll talks over a data connection for questions she does not know locally, thus it would be fairly easy to do a Man in the Middle Attack because the communication is unencrypted. A hacker could even offer their own API to compromise the doll.

While there is a bad word filter on the Cayla doll it only works for content spoken to her not vice versa. It is also easy to remove the filter from the database by hacking the doll.

Hello Barbie has yet to be released, but ToyTalk will be creating the smart technology behind the device. Munro says so far one of her stronger features is that you have to push a button on her belt for the doll to actively record. Munro is looking forward to seeing if Hello Barbie is hackable and comparing her vulnerabilities to the My Friend Cayla doll.

To see a BBC news feature with Munro talking about the doll visit: https://www.youtube.com/watch?v=YrGFqOcl3Bo

V. MITIGATING THE RISKS

While there are no guarantees in ensuring every single smart toy vulnerability is addressed there are several opportunities to make the intelligent networked toy world more secure. If the toy uses VOIP technology it should have a password protected console. Some VOIP providers will have a built in option for activating parental control software. Alternatively there are 3rd party vendors that offer this service such as Parental Skype Recorder, which will record all conversations that take place while using Skype allowing parent to review interaction. In order to protect children's identities it is important to not give away details such as name, age, and the type of device possibly indicating that it is a child's toy in a VOIP profile to make it harder for hackers or identity thieves to pin-point targets.

If the device uses remote control technology it is very important to ensure that all data transmissions are adequately encrypted. 256 bit AES encryption should be used for communications over the internet. Toy makers could offer authentication servers to secure the authentication connection between the toy and the computer over the internet.

Any toys that use a wireless connection are prone to wi-fi vulnerabilities. It is important to change your default user name for a wi-fi set up. It is possible to have the router generate a difficult security key for the WLAN. If needed, upgrade the encryption to WPA2 with TKIP+AES algorithm. Ensure that you also have firewall software and antivirus current on devices. The default SSID should always be changed when configuring the WLAN, default settings are prime indications of an easily hackable target. The Public broadcasting of the Wi-Fi SSID should also be disabled and the wireless access point firewall should be enabled to allow for the blocking of anonymous internet requests for pings. Another suggestion is to position the WAP in the center of the home rather than near a window. You can check the WAP logs to check that no unknown systems have connected. It is also possible to enable MAC filtering on the WAP and disable remote login and administration of the WAP.

Toy Companies should ensure that toys comes with some form of parental control settings that enable parents to determine or approve their child's friends list so they are fully empowered to know who their child is interacting with. It would also be ideal to allow parents the ability to schedule when the toy could be used so the child was supervised. An auto generated email log that details who the child was talking with and for how long would also be a nice feature to allow further review.

There are numerous products that allow for Parental control both free and paid options depending on the needs of the parent if the device requires a computer to interact. A few examples are McAfee Family Protection 2.0, Net Nanny 6.5, PureSight Owl, SafeEyes, ZoneAlarm Guard, CellSafety 2.0 and Minor Monitor.

Currently, toy manufacturers are not required to disclose security vulnerabilities and therefore carry no liability. Because they do not have to report such factors it is unknown how well companies are testing the security of their products.

VI. DATA PRIVACY AND LEGAL CONCERNS

There is a lot of value in information. The Toy Industry Association is an advocacy group geared to preserve the right for the toy industry to communicate with children in a responsible manner. Children's online privacy has become of greater importance and one of the main concerns of the toy industry is that legislation will reduce their ability to obtain the necessary data to improve content and impede company's ability to personalize individual children's experiences. If the data were required to be anonymous it would hinder a marketer's ability to offer targeted advertising on e-commerce sites for young consumers. While toy companies just like any other business need to generate profits the BBB created a self-regulating agency that further develops and monitors such advertising standards.

CARU – Children's Advertising Review Unit of the Better Business Bureaus is a US self-regulatory agency that was established in 1974 by the National Advertising Review Council. CARU reviews TV, radio, comic books, and internet advertising for truth, accuracy, and sensitivity to children's susceptibility. When an ad is found to be misleading CARU seeks change only through voluntary cooperation. The results are publicly recorded in a case database. Agencies who meet CARUs guidelines are deemed in compliance with COPPA and essentially insulated from FTC enforcement action as long as they comply with program requirements. CARU has an advisory board of industry leaders and experts that continually work to develop the guidelines

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in 1998 and created to limit the collection of personally identifiable information for children under 12. COPPA has been in effect since April 2000 and requires websites to post a complete privacy policy, notify parents directly about their information collection practices, and obtain verifiable parental consent before collecting personal information from their children or sharing it with others.

There was a survey performed by the FTC in April 2001 of 144 websites that primarily target children which demonstrated most of the websites complied with the display of the privacy policy, but there were several delinquencies in other provisions of the law. For example, half the sites failed to publicize that they were prohibited from conditioning a child's participation in an activity or disclosing more personal information than deemed necessary for the activity as well as informing parents of their right to review, delete and refuse further collection and use of their child's personal information. The FTC has tried to educate websites, but no further studies have been done by the FTC in the past 14 years that were noted on the primary website on this matter so it is hard to gauge how compliant companies which are geared for kids entertainment that maintain a virtual presence really are.

VII. CONCLUSION

There are both positive and negative aspects to consider as the smart toy continues to evolve. It will provide new ways of learning and interacting, but with it comes security and privacy risks. While there are several steps consumers can take to protect themselves there really needs to be a formal agency that approves and reviews the security of the new Internet of Toys and the legality of data those toys harvest, process, and monetize. There will always be zero day attacks and unknown unknowns, but there is room for improvement in protecting the youngest consumers with a higher standard of safety.

REFERENCES

[1] "Children's Online Privacy Protection Rule ("COPPA")." Children's Online Privacy Protection Rule ("COPPA"). Federal Trade Comission. Web. 26 July 2015. <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>.

[2] Eric, Hayes. "Playing It Safe: Avoiding Online Gaming Risks." United States Computer Emergency Readiness Team. Web. 22 June 2015. https://www.us-cert.gov/sites/default/files/publications/gaming.pdf>.

[3] Johnson, Michael Patrick, Andrew Wilson, Bruce Blumberg, Christopher Kline, and Aaron Bobick. "Sympathetic Interfaces." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems the CHI Is the Limit - CHI '99 (1999): 152-58. Print.

[4] "Marketing to Children." Marketing to Children. Web. 22 June 2015. <http://www.toyassociation.org/#.VYdp0_lViko>. Markoff, John. "Toy Makers To Sponsor Design Lab At M.I.T." The New York Times. The New York Times, 14 Oct. 1997. Web. 24 Sept. 2015. <http://www.nytimes.com/1997/10/15/business/toy-makers-to-sponsor-design-lab-at-mit.html>.

[5] Munro, Ken. "Fight! Fight! Hello Barbie vs My Friend CaylaPen Test Partners." Pen Test Partners. 18 Feb. 2015. Web. 22 June 2015. <https://www.pentestpartners.com/blog/fight-fight-hello-barbie-vs-my-friend-cayla/>.

[6] Perez, Sarah. "Led By Pixar Alums, ToyTalk Launches Its First Paid Kids App, Begins To License Tech." TechCrunch. 6 Sept. 2014. Web. 22 June 2015. <http://techcrunch.com/2014/09/26/led-by-pixar-alum-toytalk-launches-its-first-paid-kids-app-begins-to-license-tech/>.

[7] Rubenking, Neil. "Keep Your Child Safe Online." PCMAG. 13 Dec. 2011. Web. 22 June 2015. <http://www.pcmag.com/article2/0,2817,2346997,00.asp>.

[8] Schmid, Stefan, Maria Gorlatova, Domenico Giustiniano, Vladimir Vukadinovic, and Stefan Mangold. "Networking Smart Toys with Wireless ToyBridge and ToyTalk." Disney Research, Zurich, Switzerland. Web. 22 June 2015. <http://www.disneyresearch.com/wp-content/uploads/Networking-Smart-Toys-with-Wireless-

[9] Sciretta, Peter. "Playmation: Disney Reveals New Way To Play, But What Is It?" Film RSS. 2 June 2015. Web. 24 Sept. 2015. <http://www.slashfilm.com/playmation/>.

[10] Siew Yong; Lindskog, D.; Ruhl, R.; Zavarsky, P., "Risk Mitigation Strategies for Mobile Wi-Fi Robot Toys from Online Pedophiles," *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on* , vol., no., pp.1220,1223, 9-11 Oct. 2011doi: 10.1109/PASSAT/SocialCom.2011.194 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6113285&isnumber=6113084

[11] Storm, Darlene. "Google's Internet-connected Toys Patent Sparks Privacy Concerns, Visions of IoT Chucky." Computerworld. 25 May 2015. Web. 22 June 2015. <http://www.computerworld.com/article/2926333/data-privacy/googles-internet-connected-toys-patent-sparks-privacy-concerns-visions-of-iot-chucky.html>.

[12] Takahashi, Dean. "Elemental's Smart Connected Toy CogniToys Taps IBM's Watson Supercomputer for Its brains." VentureBeat. 23 Feb. 2015. Web. 27 July 2015. <http://venturebeat.com/2015/02/23/elementals-smart-

connected-toy-cognitoys-taps-ibms-watson-supercomputer-for-its-brains/>.