Cyberthreats under the Bed

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2018)." Cyberthreats under the Bed ", IEEE *Computer, 51(5),* 92-95.

Made available courtesy of IEEE: https://doi.org/10.1109/MC.2018.2381121

Abstract:

Internet-connected toys provide an often-overlooked avenue for breaching personal data, especially of those most vulnerable. Government and private measures can minimize the risks, but responsibility for monitoring smart toy usage ultimately lies with parents.

Keywords: IoT | child identity theft | internet-connected toys | smart toys

Article:

According to Juniper Research, the size of the global smart toy market was $5 billion in 2017.[1] Smart toys employ sensors, cameras, microphones, data storage, voice recognition, GPS, and more. These technologies make toys more fun and engaging but also provide more vectors for cyberattacks.

In early 2017, a security vulnerability was discovered in CloudPets, a line of stuffed animals that connect via Bluetooth to a smartphone, enabling parents and children to send voice messages to and from each other from a distance. Exploiting the flaw, hackers were able to access children's personal information, photos, and voice recordings stored in the cloud. According to one security researcher, more than 820,000 user accounts were compromised including 2.2 million voice recordings. At one point, the hacked information was held for ransom.[2,3]

Two years earlier, Hong Kong–based toymaker VTech had experienced an even larger cyberbreach. Through a flaw in its website, hackers obtained access to photos and chat logs from the accounts of more than 6.3 million children in the US, Canada, Europe, Latin America, Australia, and New Zealand.[4,5]

SLOPPY SECURITY

In part due to limited technology budgets, many smart toymakers have weak security and privacy policies.[6,7]

VTech, for instance, had secured its toys' user data with outdated protocols.[8] It's standard practice to hash passcodes—transform them into a different set of digital characters—to make databases more secure. VTech reportedly used the hashing algorithm MD5, whose developer had publicly announced back in June 2012 that it was obsolete due to software limitations and dramatic increases in computing power since the algorithm was first released.[5,9]

Toymakers sometimes fail to make serious eff orts to strengthen security and privacy even after experiencing significant attacks. For instance, after its massive data breach, Vtech did little to fix the security problems. Instead, it revised the terms and conditions of its user agreement to shift the responsibility of any future data leaks onto parents, prompting outrage among security experts.[4]

CHILD IDENTITY THEFT

Information held by smart toy manufacturers can be more sensitive and valuable than credit card data. In VTech's case, the breached data included parent names, email addresses, passwords, secret questions and answers used to verify account information, IP addresses, mailing addresses, and download histories, as well as information about the child such as name, gender, and birthdate.[5,10]

One study found that children are 51 times more likely to be targeted for identity theft than adults.[11] Child data is specifically sought by cybercriminals because children are unlikely to find out that they have been a victim of identity theft until they apply for credit, which could be decades later. In testimony to the House Ways and Means Subcommittee on Social Security, a Federal Trade Commission (FTC) official noted that "children's SSNs [Social Security numbers] are uniquely valuable because they lack a credit history and can be paired with any name and birth date."[12]

Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child present exploitation risks.[6]

CHILD-PROTECTION EFFORTS

Government and consumer watchdog organizations have taken measures to protect children from toy-related security breaches and privacy violations as well as to highlight the risks posed by certain toys.

Regulatory initiatives

In some jurisdictions, regulations have been established to protect children from harmful effects attributed to smart toys.

In the US, the FTC expanded compliance with the Children's Online Privacy Protection Act (COPPA) in June 2017 to include smart toys and other Internet-connected devices aimed at

children. The extended rule explicitly deems such devices to fall under the protected category of "websites or online services."[13]

In Germany, wireless devices with hidden cameras or microphones are illegal. In February 2017, the country's Federal Network Agency classified the My Friend Cayla doll (created by the US company Genesis Toys), which connects wirelessly to the Internet to answer questions, as an "espionage apparatus" after learning that hackers could listen to children's conversations and steal their personal data through its unsecured Bluetooth connection. The agency told parents of children with a doll to destroy its internal microphone and banned future sales.[14–16]

Some are hopeful that the EU's General Data Protection Regulation (GDPR), which aims to generally strengthen and unify consumer data protection in all member countries, will address privacy and data security issues related to smart toys.[17] GDPR enforcement begins on 25 May 2018.

Raising public awareness

Government agencies and private watchdog groups are raising public awareness of smart toys' security and privacy risks.

In a July 2017 public service announcement, the FBI's Internet Crime Complaint Center warned consumers that hacking smart toys could lead to a breach of sensitive information including a child's name, school, likes and dislikes, and geographic location, potentially leading to identity theft.[18,19]

The Norwegian Consumer Council examined various Internet-connected toys including My Friend Cayla and raised four key concerns:[20]

- lack of safeguards—anyone can easily take control of the toys;
- illegal or improper terms of service—users are required to consent to changes in the terms without notice, the use of personal data for targeted advertising, and information sharing with third parties;
- privacy violations—for example, anything told by a child to My Friend Cayla is recorded and transmitted to the manufacturer's technology partner, Nuance Communications; and
- hidden marketing targeted at kids—for example, preprogrammed spoken phrases endorse different products such as Disney movies.

The UK consumer watchdog Which? likewise tested seven smart toys and discovered security vulnerabilities in CloudPets along with the Furby Connect, i-Que Intelligent Robot, and Toy-Fi Teddy. The organization urged retailers to stop selling these and other toys with security flaws.[21,22]

These and other public interest groups are making a concerted effort to produce positive policy outcomes. In 2016, for example, more than 18 privacy groups filed complaints with the FTC and the EU concerning smart toys. How successful these attempts will ultimately be remains an open question given consumers' sometimes heedless rush to acquire any "smart" device.

Experience suggests that many smart toy manufacturers ignore or only pay lip service to security and privacy concerns. Their products thus could be even more vulnerable to cyberattacks than other Internet of Things devices, providing an often-overlooked entry point for hackers. In addition, security flaws in Internet-connected toys expose children to identity theft, which might not be revealed for years, as well as surveillance of the family by cybercriminals.

Manufacturers might lack the capabilities, resources, and motivation to strengthen the security built into their smart toys. Regulatory efforts to address this issue are nascent, a gap that various government agencies and consumer watchdog groups are trying to fill. For now, however, the obligation to monitor smart toy usage and protect children's personal data largely lies with parents. The expectation of understanding smart toys' security and privacy risks might be unrealistic for most parents. As a general rule, however, parents should be wary of toys with recording technology, connect to the Internet, or ask for personal data. Returning "creepy" dolls and other suspect smart toys to vendors for refunds and exchanges, or refusing to purchase them, will likely motivate toymakers to improve their products' security.

REFERENCES

1. "Smart Toys: Market Summary 2017," Juniper Research; www.juniperresearch.com/resources/infographics/smart-toys-market-summary-2017.

2. S. Larson, "Stuffed Toys Leak Millions of Voice Recordings from Kids and Parents," CNN Tech, 27 Feb. 2017; money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html.

3. T. Hunt, "Data from Connected CloudPets Teddy Bears Leaked and Ransomed, Exposing Kids' Voice Messages," blog, 20 Dec. 2017, www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages.

4. L. Kelion, "Parents Urged to Boycott VTech Toys after Hack," BBC News, 10 Feb. 2016; www.bbc.com/news/technology-35532644.

5. L. Eadicicco, "Everything to Know about a Massive Hack Targeting Children's Toys," *Time*, 1 Dec. 2015; http://time.com/4130704/vtech-hack-childrens-toys.

6. J. Kestenbaum, "The FTC and FBI Are Shining the Spotlight on Your Kid's Smart Toys," *The Hill*, 8 Aug. 2017; thehill.com/blogs/pundits-blog/technology/345119-the-ftc-and-fbi-put-the-spotlight-on-your-kids-smart-toys.

7. "10 Tips to Protect Your Kids' Toys from Hackers This Holiday Season," Vanderbilt Univ. News, 14 Dec. 2017; https://news.vanderbilt.edu/2017/12/14/10-tips-to-protect-your-kids-toys-from-hackers-this-holiday-season.

8. J. Keane, "VTech's Hacked Toys: How Not to Rebuild Your Reputation after a Cyber Atack," *Paste Mag.*, 15 Feb. 2016; www.pastemagazine.com/articles/2016/02/vtechs-hacked-toys-how-not-to-rebuild-your-reputat.html.

9. Z. Whittacker, "MD5 password scrambler 'no longer safe,'" ZDNet, 7 June 2012; www.zdnet.com/article/md5-password-scrambler-no-longer-safe.

10. H. Kuchler, "Toymaker VTech Hit by Cyber Attack," *Financial Times*, 29 Nov. 2015; www.ft.com/content/2bcf9ee6-9701-11e5-95c7-d47aa298f769.

11. R. Power, "Child Identity Theft; A Lot of Questions Need to Be Answered, but the Most Important One Is 'Has It Happened to Your Child?,'" blog, Carnegie Mellon Univ. CyLab, 1 Apr. 2011; www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html.

12. Federal Trade Commission, "FTC Testifies on Children's Identity Theft," press release, 1 Sept. 2011; www.ftc.gov/news-events/press-releases/2011/09/ftc-testifies-childrens-identity-theft.

13. S.A. Reiter, "FBI and FTC on Privacy Risks Stemming from 'Smart' Toys," Lexology, 27 July 2017; www.lexology.com/library/detail.aspx?g=78ff6c12-ed11-45d9-8fb2-48a1f8595f9c.

14. S. Fogel, "Germany Bans Creepy Doll over Privacy Concerns," Engadget, 17 Feb. 2017; www.engadget.com/2017/02/17/germany-bans-my-friend-cayla-doll.

15. S. Bernando, "The Latest Hack Is Targeting Your Kids' Smart Toys," blog, Experian, 6 Dec. 2017; www.experian.com/blogs/ask-experian/the-latest-hack-is-targeting-your-kids-smart-toys.

16. A. Petroff, "Germany Tells Parents to Destroy Microphone in 'Illegal' Doll," CNN Tech, 17 Feb. 2017; money.cnn.com/2017/02/17/technology/germany-doll-my-friend-cayla/index.html.

17. E. Silfversten, "A Smart Toy Could Have Personal Details for Life, Not Just for Christmas," blog, RAND Corp., 21 Dec. 2017; www.rand.org/blog/2017/12/a-smart-toy-could-have-personal-details-for-life-not.html.

18. FBI Internet Crime Complaint Center, "Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children," alert no. I-071717(Revised)-PSA, 17 July 2017; www.ic3.gov/media/2017/170717.aspx.

19. A. Newcomb, "FBI Warns Parents of Privacy Risks with Internet-Connected Toys," NBC News, 18 July 2017; www.nbcnews.com/tech/security/fbi-warns-parents-privacy-risks-internet-connected-toys-n784126.

20. BEUC, "Consumer Organisations across the EU Take Action against Flawed Internet-Connected Toys," press release, 12 June 2016; www.beuc.eu/publications/consumer-organisations-across-eu-take-action-against-flawed-internet-connected-toys/html.

21. R. Smithers, “Strangers Can Talk to Your Child through ‘Connected’ Toys, Investigation Finds,” *The Guardian*, 14 Nov. 2017; www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

22. “Connected Toys Have ‘Worrying’ Security Issues,” BBC News, 14 Nov. 2017; www.bbc.com/news/technology-41976031.