PullString

How PullString Makes IoT Safer

Securing online experiences on web/mobile is hard enough, but what about the onslaught of IoT devices? Welcome to the world of PullString. This is the story of how they launched one of the most successful of more than 550 Bug Bounty programs on HackerOne ahead of their incredibly innovative IoT product launch.

PullString was founded in 2011 as ToyTalk. Today, PullString is the broader technology platform powering computer conversations in text, voice and video and ToyTalk is a brand for their COPPA (Children's Online Privacy Protection Act) compliant family of products in the kids entertainment space. Although many toys have had simple recorded phrases over the years, Hello Barbie was something entirely new.

Martin Reddy, cofounder and CTO at PullString explained, "No one had done this before — take a doll, put in a chip, connect to WiFi and hit an API. Our customers immediately saw the importance of that." The API in particular was key to PullString's IoT strategy. It required realtime response to make a conversation with a user flow.

From the dawn of time, children have talked to their toys, but now toymakers can make the toys talk back. Interactive characters that understand and respond to children can be much more than just fun. They are educational, inspirational and maybe even lifechanging. Even CNET agreed that the future of playtime is going to mean more intelligent interactive toys. More than toys, they are now imaginary friends who speak in personalized dialogue that evolves and grows along with the child. However, any connected device that children can use needs the highest possible levels of privacy and security.

Dr. Reddy and his entire engineering team worked extremely diligently to ensure that their category-defining interactive IoT offerings would be as secure as possible and have taken measures such as:

1. Hardware Root of Trust - If the hardware is not secure, then nothing is. Disable unnecessary access, such as for debugging after that.

2. Security built into the Architecture and not bolted on - The architecture should reflect security built into the earliest designs. It pays off later.

PullString

As this was an entirely new product category, with high expectations in responsiveness by children, they knew they were stretching the boundaries of the possible. Vulnerabilities would be inevitable with something this innovative.

At the same time, COPPA is very clear on directives, such as the fact that companies need to inform parents on precisely what kind of information is being collected on their children and how it will be used. To be certified as COPPA compliant, items on the market for kids must prove that they are safe from malicious actors over the internet and the child's private data won't fall into the hands of intrusive marketers.

PullString leveraged HackerOne's bug bounty program, inviting hackers to hack their products, APIs and website. HackerOne connected PullString directly to "white hat" hackers who helped them harden their security and close vulnerabilities. HackerOne also streamlined interactions between the company and the independent hackers, handled all the external payment arrangements and provided expertise on how to run the Bug Bounty program. To prepare, PullString launched privately and handled 18 reports over 4 days to get the team ready for a public launch. Pullstring successfully handled the 223 reports that came in over the next 3 days without accumulating a backlog of reports.

PullString's engineering team has responded with incredible agility during the Bug Bounty program, which prepared security teams for quick assessments and responses. PullString ended up with one of the most successful launches on HackerOne. Their team addressed issues quickly and efficiently, and never got overwhelmed by bug reports. Freelance security experts in the HackerOne community were able

to tease out 62 potential vulnerabilities in the first month and help PullString harden their code. They received less than five reports per month after that on the same scope.

Unique, valid reports came from 57 different hackers - a much larger team than could have been assembled in any other way. The vulnerabilities were considered high quality - fully 98% of valid high quality vulnerabilities earned a bounty and only 2% received noncash thanks alone. Most importantly, PullString stood above their peers in their willingness to work with independent security researchers to find every last vulnerability they could.

The 50+ person years' worth of investment in engineering a highly scalable and secure platform will make the PullString platform stand apart from new entrants in the field of computer conversation as PullString opens up its platform to power computer conversation for enterprises.