No product can be 100% secure, but you can take steps to limit the possible vulnerab

exclusive

Using the nom de guerre RenderMan, a Canadian hacker has set out to m

The internet of things is growing. Hardly a day goes by without new products that automatically and independently communicate with each other via the internet. The adult industry has also launched several innovations in this segment, and it is all but guaranteed that the number of these high-tech toys will only increase in the future. But at the same time, there is a growing risk: Sex toys could become the target of hacker attacks. Internetofdon.gs is a product that was started with the intention of preventing such a scenario – a collaboration of researchers, hackers, and producers who want to protect products and data against unauthorised access. Of course, the project is still in its earliest stages right now, but the man who set the ball a-rolling, a hacker using the pseudonym RenderMan, explained to EAN which dangers lurk in the world wide web and how companies can prepare themselves.

"Hi, RenderMan. You recently launched a project called Internet of Dongs, a website dedicated to sex toy security in the age of the internet of things. What made you start this project?

RenderMan: Several years ago, I gave a talk at some hacker conferences that included a few slides about the first Bluetooth vibrators that were coming onto the market. The idea of connected sex toys opened up a whole world of new threats and vulnerabilities that no one seemed to consider much at the time. It sat in the back of my mind to do a project auditing sex toys until this year. I finally decided to look into doing it and found the market was much further than I expected. What I found was very scary and concerning. I felt the need to expand the project from a one-off audit to a group that could help influence and advise vendors on how to make their devices secure and private from the beginning.

Before we go into more detail about the project, could you tell us a bit about your background?

RenderMan: I'm a hacker who lives and works in western Canada. By day I am a penetration tester (I break into stuff) for a financial institution. I've been doing security research for many years and been speaking all over the world for the last decade or so. I just dive into whatever interests me.

My last project was illuminating vulnerabilities in the world wide air traffic control system. I'm a man of many talents and use my projects to learn new skills.

> "MANY DEVICES NOW ALLOW FOR REMOTE CONTROL OVER THE INTERNET WHICH IS A VERY BIG CHANGE IN THE THREATS."
>
> RENDERMAN

Internet of Dongs can be a bridge between manufacturers and designers on one side and researchers and hackers on the other side. What would the actual collaboration look like?

RenderMan: We are still sorting out a lot of the details of this collaboration. The project has sort of grown organically as we figure out the market, the attitudes and challenges. What we are hoping for is to work with vendors to educate them about the information security concept of "responsible disclosure". This would involve them setting up a public single point of contact for researchers and hackers to privately report their discoveries to the vendors. In turn, the vendors have an established policy and process to evaluate the discovery and to fix any issues that are confirmed in a timely fashion. This also includes being in communication with the researcher throughout the process and allowing for public disclosure of the vulnerabilities after the issue has been fixed. It's a process that has worked well for information security in other branches of the Internet of Things, so it's a matter of working with this branch to do the same.

Have the manufacturers of IoT sex toys paid enough attention to security up until now? What are the most common weak spots?

RenderMan: IoT devices in general have not gotten the attention to security in their design, but unlike a fridge or thermostat, sex toys are a much more private and intimate item where security and privacy should be a high priority. Before this project, there's been almost no work on the security of these devices, which is scary in and of itself. The most common technical issues we have noticed so far is lack of encryption in communications which allows for eavesdropping and

improperly implemented encryption that is easily defeated and provides a false sense of security. Another major non-technical issue we've noticed is the amount of data that these devices and associated apps collect and send to third parties for unknown purposes without proper disclosure to the user.

Society is getting more and more open about sex toys. Even though most people don't want to publicly announce it when they use one, it doesn't seem like a big deal if such information gets leaked... So why even bother? What makes hacked sex toys dangerous?
RenderMan: The latest generation of connected sex toys has connectivity outside of the room it's being used in. Many devices now allow for remote control over the internet which is a very big change in the threats. While the fact that you use one may not be of concern, other information such as whom you've invited to remotely control the device could be something you don't want public. Other things like location information, the contents of video and text chat functions are things most people wouldn't want public either. There are also other concerns and dangers that we have to worry about. For instance, if I could hijack a sex toy remotely and now I'm controlling it instead of the person the user is expecting and gave permission to, is that now a sex crime? Are we ready as a society to deal with internet enabled sexual assault? I'd prefer that it remain theoretical and not something we see on the evening news.

Without getting too technical, how do you check the security of sex toys or IoT devices in general? Or, put differently: How does someone hack a vibrator?
RenderMan: Each device has its own threat landscape so methods adjust accordingly. In general, though, many of the devices now use Bluetooth to communicate with an app on the user's smartphone or computer. From the app it then communicates to the internet for remote control or other functionalities. Usually the first steps entail examining the data being sent between each point and looking for potential issues. In addition, injecting or manipulating parts of that traffic can be done to see if systems can be "tricked" into behaviour it was not designed for. Another part of the process is to take apart the app and other software used and examining it line-by-line for issues and even sometimes the hardware device itself looking for issues. It's a matter of peeking under the hood, understanding how it works and seeing if there's anything dangerous being done.

> "WHAT WE ARE HOPING FOR IS TO WORK WITH VENDORS TO EDUCATE THEM ABOUT THE INFORMATION SECURITY CONCEPT OF 'RESPONSIBLE DISCLOSURE'."
>
> RENDERMAN

Which steps should manufacturers and designers take to make their products more secure? Is there something like a secure product in the IoT?
RenderMan: No product can be 100% secure but you can take steps to limit the possible vulnerabilities. Designers should realise that once you add connectivity, you are now hundred milliseconds away from over three billion potential attackers. Understanding that and putting security first can go a long way. In addition, ensuring that you involve security experts in the design and development process will do wonders to stop problems before they start. Very often it seems that these vulnerabilities exist simply because no-one involved knew any better or didn't know to ask certain questions. They are industries that are brand new to connectivity and don't understand the threats until it's too late.

Are there ways for the users to protect themselves on their own or must they rely on the manufacturers to provide a secure product?
RenderMan: The average user has little they can do to analyse these devices themselves and has to trust the manufacturers, even if they may not have security or privacy at the front of their mind. The best thing to do (besides visit https://internetofdon.gs and check out reports) is to ask questions. Ask vendors what data they may collect and store. Ask them about their privacy policies and if they have ever had a security audit of their product. We've yet to find one who has had one, but the more people who ask, the more it seems like a good idea to do so. Finally, just ask if you are comfortable with using a product that has these risks. If you are not, there's still a huge number of manually operated sex toys out there that you can enjoy.

Which innovations and developments will shape the future of sex toys? What seems most interesting and promising to you?
RenderMan: The field of teledildonics is a fascinating one. I think that bi-directional interactive toys (movement on one toy makes the other react and vice versa) combined with telepresence and VR is going to be an amazing revolution. The ability for people to safely and remotely explore their sexuality in new and interesting ways within an immersive environment will be a major shift in sexual identity politics and societal attitudes towards sex.

What is next steps for Internet of Dongs?
RenderMan: Building up our connections to vendors and getting them to work with researchers and hackers rather than seeing them as a threat is going to occupy a lot of our time. In addition to that, we will continue to work to acquire and test new devices in order to find and get vulnerabilities fixed in existing products and to generally act as a watchdog over this branch of the IoT.