PRODUCT SECURITY AND EVALUATION
CYBER ATTACKS

01

How would your new products stand up to cyber attacks?

Are you sure that the products and devices you plan to buy and deploy really do meet the high standards of security you demand? Whether you are buying or selling – failing to identify vulnerabilities could have a major impact on your business or organisation. And when it comes to fast-emerging technologies such as the IoT or Artificial Intelligence (AI), too many products are being rushed to market with too little attention to security.

02

The Internet of Broken Things

In a recent survey of over 16m smart home networks worldwide, security firm Avast found that 40.3 percent had more than five smart devices connected and 40.8 percent of these had at least one vulnerable connected device. As more vendors race to take a slice of this fast-growing IoT market, we should not be surprised by the headlines of IoT breaches and the targeting of IoT devices for botnets. It's clear that people are buying products that could compromise the security of their network and beyond. At Context, we've already found security holes in things, from a smart printer with an unauthenticated firmware update process and an alarm with baked-in guessable webserver credentials, to an IP security camera with a plethora of security problems.

But it's not only tech start-ups that are guilty of paying lip service to security. Some of the most high-profile technology vendors, third-parties and end-user companies have been found to come short when it comes to marketing or deploying insecure products.

03

The way forward

The solution is remarkably straightforward:

— **Analyse products and software for vulnerabilities before they are released or updated if you want to maintain brand reputation and customer confidence**

— **Test third-party products or software before you adopt to avoid exposing your organisation to attack**

Each assessment should be tailored to your product using the appropriate threat model and specific requirements. Whether you're after a light-touch or an in-depth evaluation, it is important to determine the scope based on the likely threats and impact of a breach.

In addition to conventional penetration testing techniques, it may be necessary to perform a full holistic assessment of a major new technology or platform. This could also include reverse engineering, protocol analysis, vulnerability research or development of a proof of concept capability. For example, recent research projects undertaken by Context include exploring attacks on HTTPS via malicious proxies, reversing the string encryption in the Pangu 9.3 jailbreak and attacking smartphones using binary SMS.

THE FURBY EFFECT

CONTEXT RESEARCHERS HELP *WHICH?* TO CALL TIME ON INSECURE CONNECTED TOYS

Don't Feed Them After Midnight: Reverse-Engineering the Furby Connect

Context has worked with leading independent UK consumer body *Which?* to highlight vulnerabilities in internet or Bluetooth connected products. Our research team helped to provide evidence and demonstrate how easy it is with the right skills to hack into off-the-shelf children's toys. As part of this work, Context researchers looked at the security of the popular Furby Connect, a furry, robotic creature with expressive LCD eyes that can speak, sing, dance and connect via Bluetooth to the Furby World smartphone game.

Like many other consumer smart devices and toys that use Bluetooth Low Energy, we found that the Furby does not implement any of the standard Bluetooth security features and does not use authenticated pairing or link encryption. As a result, anyone in wireless range of the Furby can connect to it while in use and send control commands without any physical interaction.

Our Context researchers fully reverse-engineered files used by Furby, which include programmable action sequences, lip movements and animation commands, making it possible to display custom graphics and animations on Furby's LCD eyes. We also found that Furby firmware updates appear not to require to be signed by the manufacturer. This meant that maliciously installed firmware could potentially gain access to the toy's microphone, turning the toy into a remote listening device, for example.

Basic safety and security measures should be standard in all connected consumer devices and should be the absolute priority with any toy.

But IoT's great potential spans all sectors from consumer and domestic to retail, manufacturing, energy, transport, health and public infrastructure. With the advent of IPv6, the number of available individual addresses is a staggering 340 trillion, trillion, trillion. But along with the huge opportunity comes the security challenge.

The industry is trying to catch up and in February 2019, the ETSI Technical Committee on Cybersecurity (TC CYBER) announced a global standard for cybersecurity in the IoT, which addresses the exploitation of poor security and consumer privacy. This is a good step forward, but we can expect to see more IoT breach headlines before many manufacturers wake up and take IoT security seriously.

For the full Furby case study, read our detailed blog: Don't Feed Them After Midnight: Reverse-Engineering the Furby Connect

context

contextis.com
@CTXIS