Roke
Part of the
Chemring Group

Walking the walk of IoT security

What we found from hacking a home

The world is still finding its feet in securing the Internet of Things. Only real-world knowledge will help us accurately guide manufacturers towards secure and user-friendly devices, and what better way to gather this by hacking a standard family home? Roke's resident expert in Cyber Security, Mark West reflects on the valuable insights we came away with and what this means for manufacturers and consumers.

Business is booming for manufacturers of internet-connected devices. However, a quick browse of recent news stories surrounding the Internet of Things (IoT) paints a vivid picture of ongoing security troubles. The same question is raised time and time again: "How are we going to secure the IoT?" A lot of thoughts and ideas have been raised, but anyone can talk the talk. Meanwhile, the real challenge is putting this into practice.

WHY SECURE INTERNET-CONNECTED DEVICES?

We all store information on our home computer networks that could cause significant financial damage or distress if it fell into the wrong hands via insecure IoT devices. For the risk to businesses, the numbers speak for themselves: a cyber attack can have a devastating effect on the bottom line, with share prices reported to drop by an average of 1.8% on a permanent basis. It doesn't take much to imagine the reputational damage associated with a breach of an IoT device.

Another interesting aspect to this is how increasingly cyber-savvy consumers are influenced in their buying decisions of IoT devices. In addition to factors such as convenience and interactivity, consumers are likely to be positively influenced by the security of a device, with one study finding 39% of consumers had made a buying decision based on privacy concerns. Manufacturers with a strong reputation for cyber security can tap into this growing consumer awareness, which is likely to increase if there is some way of knowing just how secure a device is, much like a gas safety certificate.

Walking the walk of IoT security

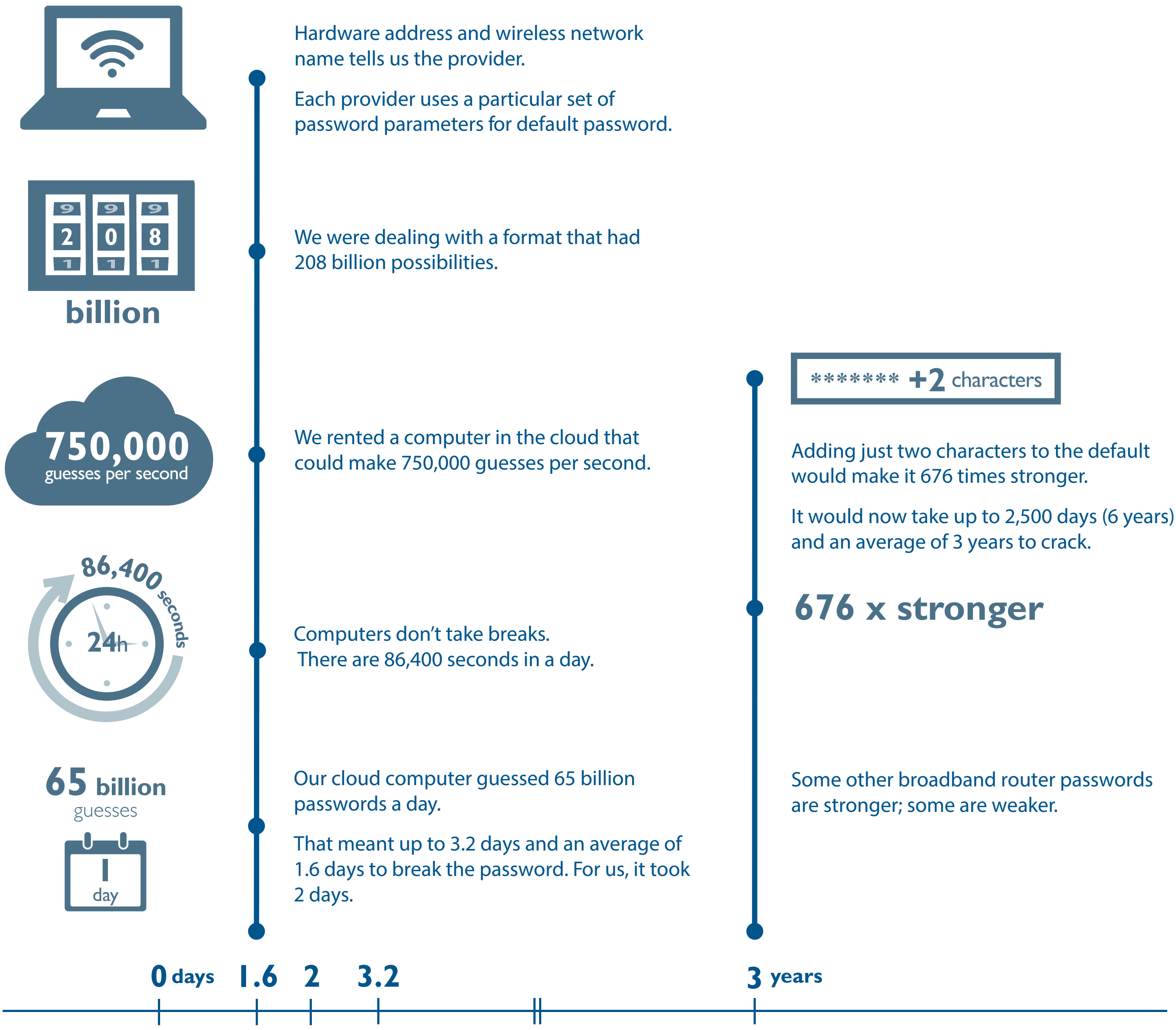
First and foremost we need to understand the reality of IoT insecurity in everyday life. As part of our research into this issue, we pulled together a team of our cyber security experts to conduct a cyber security assessment of a standard IoT-equipped suburban family home.

The success of this experiment required getting into the mind-set of common hacker motivations. We therefore focused on identifying ways in which hackers could try to gain access, and once on the network look for useful information. Here are some of our discoveries.

PASSWORD SECURITY MATTERS

The critical security factor was passwords. It was easy to identify the provider of the broadband router via the default network name. We also checked that the wireless network was not protected with a common, dictionary password. We therefore assumed that it had the default password. We also knew that, for each provider, the default format follows a well-known format – so we cracked it.

If the password had been changed from the provider's standard format, we would break the password by trying common dictionary words, simple variants and any other keywords based on knowledge of the target. This is relatively quick, so if it fails, with enough time brute-force can be used to cycle through endless combinations of the default password format. Had that failed, we would assume that it's got a non-default, strong password and give up.



Hardware address and wireless network name tells us the provider.

Each provider uses a particular set of password parameters for default password.

We were dealing with a format that had 208 billion possibilities.

We rented a computer in the cloud that could make 750,000 guesses per second.

Computers don't take breaks. There are 86,400 seconds in a day.

Our cloud computer guessed 65 billion passwords a day.

That meant up to 3.2 days and an average of 1.6 days to break the password. For us, it took 2 days.

Adding just two characters to the default would make it 676 times stronger.

It would now take up to 2,500 days (6 years) and an average of 3 years to crack.

Some other broadband router passwords are stronger; some are weaker.

Cracking a broadband router password: This is an 'offline' attack. We need to capture some specific data from the network, which we can then take away and use to break the password – we don't need to try to connect to the network until we've recovered the password.

Needless to say, end-users have an important part to play when it comes to protecting their home. Manufacturers can help by setting strong default passwords, informing (or enforcing) a password change from the default setting, and explaining the importance of a strong password more fully (see infographic). We strongly recommend following password guidance directly from the National Cyber Security Centre. In dense urban environments with a large number of networks, hackers are much like a burglar looking for an open window: if a network can be easily cracked, then why not? It is worth noting that once a password is recovered, this immediately becomes a candidate for access to any on-line service that we know the user has.

INSIDE THE NETWORK

Once on the network, eavesdropping allows us to see more by decrypting traffic between a device and the router. We can also 'scan' the network, sending packets to devices to find out more about them. We'd be quite cautious about being detected if scanning an office, but in a home setting we can do this with impunity.

Devices often have individual usernames and passwords to control access. Once we knew which device was sending what information, we tried to access specific devices and learn more about what they were doing – and this led to some surprising revelations.

Most hacking is done remotely and we identified several instances where devices were made globally accessible, providing better access for a hacker and increasing the number of attack points on the network. Devices can make use of a mechanism called Universal Plug and Play (UPnP) to ask the home router to make the device accessible from the Internet – in other words, anyone, anywhere in the world with Internet access would be able to try to talk to the device.

We observed devices with cameras and microphones making themselves Internet accessible. Where we were able to crack or recover passwords, we could watch and listen. It doesn't take much imagination to understand how this surveillance could be applied for nefarious means.

In the case of smart TVs or media streaming devices that let you watch online content on your TV, these generally do not contain personal details and strong security is understandably a lower priority. Yet we could remotely control the media streaming device, which might enable us to trigger a smart home assistant device, leading to all sorts of outcomes.

This study has also raised awareness of ways that manufacturers can help make passwords more effective:

- Always use TLS (HTTPS).
- Have strong default passwords and encourage setting a strong password.
- Limit the rate at which log on attempts can be made. Careful consideration is vital here, since an attacker can deliberately use such mechanisms to deny the user access to their own device.

SECURITY RATINGS FOR CONNECTED DEVICES

With the lack of cyber security best practice or test and accreditation schemes, how are manufacturers to know what is expected of their devices until they are breached? How are consumers able to choose suitably secured devices? This is what the industry is focusing on, and right now Roke is working to develop cyber security accreditation as part of the 5*Stars consortium for cyber security ratings of connected vehicles. We're confident that it won't be long until consumers will select independently assured cyber secure devices, and manufacturers must be ready for this shift.

PLAYING THE HACKER

Everything we did made use of freely available tools and techniques, closely replicating a hacking scenario. However, as a responsible cyber security consultancy we also conducted the experiment with consent, adhering to guidance from lawyers specialising in the relevant laws, including the Computer Misuse Act. Real hackers on the other hand are a different kettle of fish. They are not constrained in this way and might, for example, target the 'back end' servers used by a service as a way of gaining access to a large number of devices – something which we were unable to investigate.

SUMMARY

This experiment has highlighted several areas that can be addressed in order to improve smart home security. Still, there is no avoiding the fact that securing internet-connected devices poses a real technical challenge. As a cyber security consultancy and founding member of the IoT Security Foundation (IoTSF), Roke offers specialist advice and support to manufacturers wishing to create secure and user-friendly devices, walking the walk of IoT cyber security.

REFERENCES

1. CGI. (2017). The cyber-value connection. Available at: www.cgi-group.co.uk/white-paper/the-cyber-value-connection

2. Chang, YaPing et al. (2014). Influence of Characteristics of the Internet of Things on Consumer Purchase Intention. Social Behavior and Personality: an international journal, Volume 42, Number 2, 2014, pp. 321-330(10)

3. IOT Security Laboratory. (2015). Consumers make buying decisions based on privacy. Available at: http://iotsecuritylab.com/consumers-make-buying-decisions-based-on-privacy/

PROFESSOR MARK WEST

EXPERT IN CYBER AND INFORMATION SECURITY

Mark heads Roke's Information Security practice. He plays a central role in Roke's partnership with the Cyber Security Challenge and the University of Southampton's Cyber Security Academy. He specialises in Internet standardisation as well as EU and UK/US collaborative research programmes, also providing consultancy to commercial, defence, national security and Open Government Data projects.

Owing to Mark's knowledge of Internet protocols and architecture, he has been chosen as technical authority on many diverse projects for the UK Government, where he has been responsible for the design and evaluation of secure systems.

Mark has more than 25 years of experience as a software engineer.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
www.roke.co.uk • info@roke.co.uk

03968