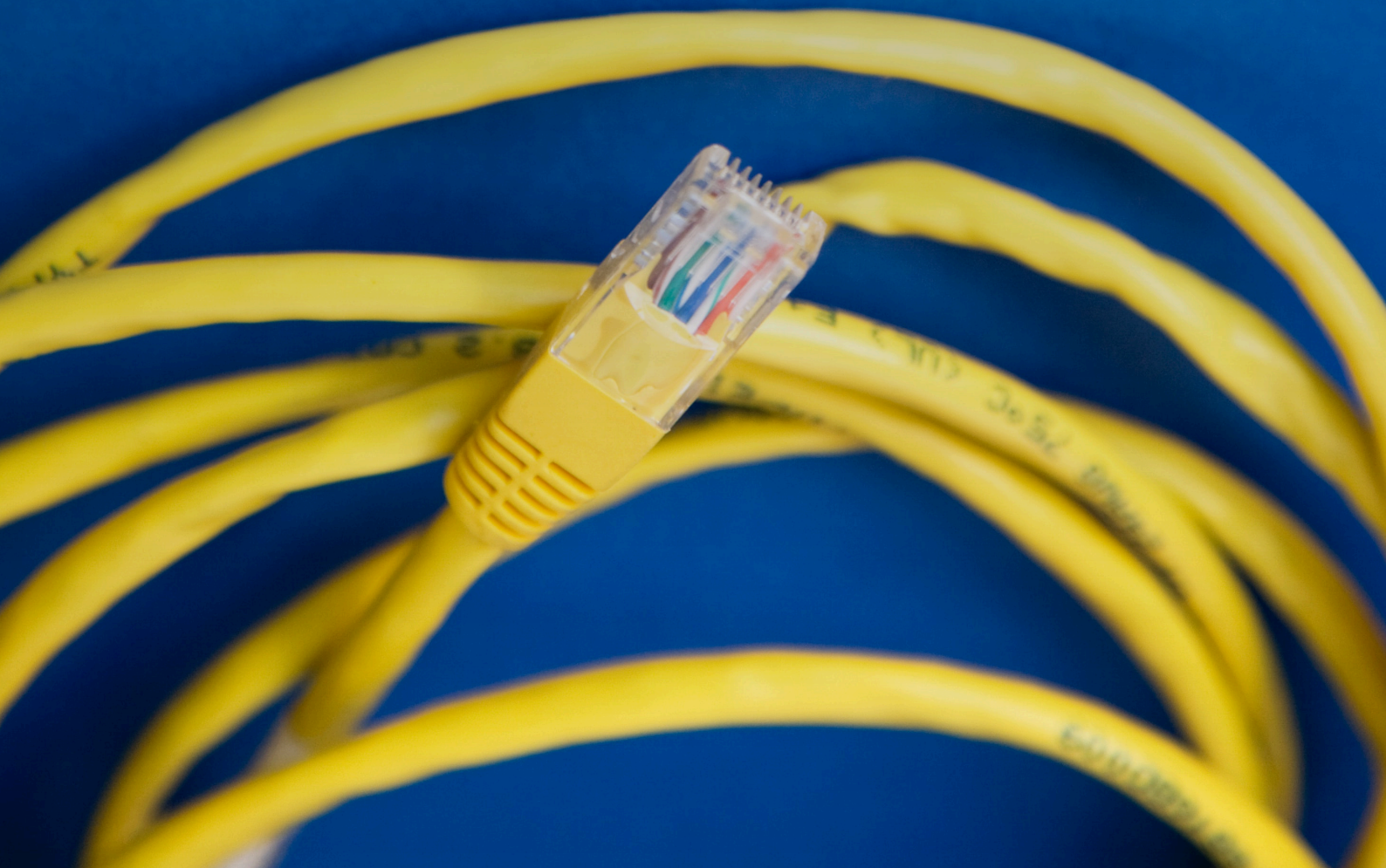
UCL

Security Recommendations for Consumer Routers

K. Demetriou and N. Healy
Centre for Doctoral Training in Cybersecurity
University College London



Introduction

Consumer routers are some of the most prevalent devices in the home with 26.7 million fixed broadband connections in the UK at the end of 2019 according to Ofcom[1]. Consumer routers (alternatively known as home routers, wireless routers or customer edge routers) establish a connection between a local computer network and, typically, an Internet Service Provider's (ISP) own backhaul network[2]. Routers are usually provided by ISPs to customers. While these devices facilitate convenient access to the Internet with little to no required technical knowledge or manual tuning by the consumer, the security posture of consumer routers is questionable. The widespread installation of consumer routers, the economic and social importance of the Internet access they enable, along with the prevalence security vulnerabilities, renders these devices likely targets of future exploitation. The Mirai botnet campaign demonstrates the impact the exploitation of embedded systems, like consumer routers, can have[3].

Case Study: Mirai

Embedded systems are special, purpose-built computer systems with specific applications, usually embedded within another object or system. Consumer routers are one form of embedded system. In 2016, the Mirai malware targeted internet-connected cameras and video recorders, other kinds of embedded devices, to build a network of hundreds of thousands of compromised devices. This network was then used to conduct a distributed denial of service (DDoS) attack against Dyn, a Domain Name System (DNS) provider. Disruption of Dyn's name-resolution service meant that Internet users were unable to access popular websites including Twitter, Etsy, GitHub and Netflix[4]. Mirai also affected ISP services when, in November 2016, 900,000 Deutsche Telekom customers experienced connection problems caused by Mirai-infected ISP-provided routers[5].

1. Telecommunications market data update q1 2019, Jul 2019.
2. H. Singh, W. Beebee, C. Donley, B. Stark, and O. Troan. Basic requirements for ipv6 customer edge routers. RFC, 7084:2070–1721, 2013.
3. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al. Understanding the mirai botnet. In 26th {USENIX} Security Symposium ({USENIX} Security 17), pages 1093–1110, 2017.
4. S.A. O'Brien. (2016) Widespread cyberattack takes down sites worldwide. CNN.
5. B. Krebs. (2016) New Mirai Worm Knocks 900K Germans Offline. Krebs on Security.

The events of Mirai demonstrate how routers, as a gateway to the home network, act as a point of convergence between the home network and the wider Internet and as a place where crime might take place. Governments and other actors are increasingly acknowledging the security risks associated with embedded devices like consumer routers. Since 2017, the UK government has conducted a programme of work intended to improve security for consumer IoT products[6]. The Department of Digital, Culture, Media and Sport also published a Code of Practice for Consumer IoT Security in 2018[7], and announced plans to introduce legislation to regulate the security of consumer 'smart' products in January 2020[8].

In this context, this policy briefing reports on findings from research conducted about a specific embedded device – home routers. From January 2020 to June 2020, researchers from the UCL Centre for Doctoral Training in Cybersecurity systematically reviewed literature for recommendations on how to improve the security of these devices. This briefing begins by briefly describing the method used for the review, before summarising the research's key findings. The final section analyses the findings of the research and suggests how this research should help guide further work in this problem space.

Method

This policy briefing is based on a systematic review conducted from January – June 2020 by two researchers based within UCL's Centre for Doctoral Training in Cybersecurity[9]. A systematic review is a formal method for identifying and analyzing literature, involving the creation of a search protocol and following a set of clear and pre-documented steps. We surveyed both academic publications and grey literature, primarily publications by government and router manufacturers. The initial searches identified 2,045 pieces of academic literature and 229 pieces of grey literature. After several stages of review, we identified 19 academic papers containing novel recommendations to improve router security, which we clustered around six themes, 5 academic papers and 61 pieces of grey literature containing what we characterised as 'established recommendations' to improve router security. These 'established recommendations' are common practices recommended to consumers to improve security across digital devices e.g. to change default passwords.

6. United Kingdom Department of Digital, Culture, Media and Sport. (2018) Secure by Design: Improving the cyber security of consumer Internet of Things Report.
7. United Kingdom Department of Digital, Culture, Media and Sport. (2018) Code of Practice for Consumer IoT Security.
8. P. Lester. (2020) New law proposed to help protect millions from unsecure smart devices. Which?
9. K.P. Demetriou & N. Healy. (2020). Security Recommendations for Consumer Routers. Manuscript in preparation, University College London, London.

Key Findings

After reviewing the full text of the final set of papers and grey literature items, we have identified 19 papers proposing novel solutions to router security issues, with a further 5 papers and 61 pieces of grey literature containing mainstream or otherwise "common" recommendations. Of the latter, the most common recommendations were to leverage network encryption (found in 67% our our identified literature), change default router username and password combinations (50%), change the default wireless network name (29%), use strong wireless network passwords (29%), enable built-in router firewalls (26%) and keep router firmware up to date (23%). All remaining recommendations had a level or support lower than or equal to 20%.

Our thematic analysis of the "novel" solutions previously discussed has surfaced six themes among the 19 papers examined. Five papers selected for inclusion respond to vulnerabilities specific to Internet of Things (IoT) devices. Five papers deal with security issues related to network access, including vulnerabilities associated with network encryption. Four papers proposed solutions in response to problems associated with router firmware. Four papers address security issues associated with home routers' current processing and functionality limitations and one paper specifically looked at vulnerabilities associated with the IPv6 network protocol.

Analysis

This section analyses the findings of our research and suggests how this research should help guide further work in this problem space.

Lack of practical solutions to router security issues in existing research

Many novel studies are not practical solutions to security issues in consumer routers. More precisely, no existing approaches in academic literature are feasible when considering factors such as cost, user experience or computational performance. In many cases, existing proposals only represent partial solutions to the identified security issues that may not be applicable under various technical or other circumstances. Future research could adopt a more holistic examination of this research question. Further research could seek to identify "well-rounded" approaches to improve router security that can function within real-world constraints or to blend existing methods to the same end.

Cloud infrastructure as an area of promising research

A promising area identified from our research is the concept of outsourcing consumer router functionality away from router firmware, to dedicated Cloud infrastructure located at the premises of Internet Service Providers (ISPs). This approach presents an opportunity to improve the security posture of consumer networks while reducing manufacturing costs and enabling advanced capabilities such as fine-grained traffic shaping. Compared to existing consumer router architectures, cloud infrastructure allows for security or performance subroutes to be implemented on demand, perhaps paving the way for rapid incident response across entire ISP fleets. However, we only identified two papers discussing this approach and only one with demonstrated practical feasibility. Future research should build on this existing work, and stakeholders shouldmac consider ways to support the development and commercialization of this concept.

Effects of existing security recommendations remain unclear

Despite the popularity of certain security recommendations, such as changing WiFi® passwords, we did not identify any studies that investigated how effective these prompts are or to what extent end-users seek or become exposed to such advice, be it from the documentation supplied with their device or from auxiliary grey literature sources. Future research could attempt to quantify the effects of mainstream security recommendations. Ultimately such studies may be helpful in crafting future messaging and directing future funding and expertise.

Lack of existing analysis of user behaviour around router security

A major omission in existing academic research was analysis of user behaviour around consumer router security. One paper collected in the initial sift of papers examined whether altering router interface design could lead to security improvements, but this paper was excluded from our research as it was outside the allotted time band for the project. Further to this, only two papers identified in our review tested their security recommendations with users. Researchers could engage users of consumer routers to fill this gap and aim to trial security improvements already identified by existing work with users.

Common recommendations, but some disagreement within security literature for consumers

Our search strategy captured two forms of grey literature concerned with router security: publications by government and publications by router manufacturers. Typically this literature is targeted towards users of consumer routers. Within this literature, we identified 44 unique recommendations for improving router security and seven of these recommendations were repeated in more than 10 different sources. Many of these recommendations reflected common principles within computer security e.g. recommending the use of strong passwords. However, there was disagreement between authors on some suggestions. For example, papers disagreed whether the use of MAC address filtering and hiding the network SSID would improve consumer router security. The UK government should support manufacturers to review and standardize security guidance given across the industry, drawing upon existing research where available.

Default security configuration of consumer routers could be improved

As described previously, most of the recommendations identified in the grey literature to improve router security consisted of alterations that consumers could make to the default configuration of their devices e.g. making use of network encryption; changing the default username and password for the router administration; and changing the default SSID. Manufacturers and/or ISPs could improve the default security configuration of consumer routers. For example, manufacturers could require users to reset the default username and password when first logging into a router's admin interface. Additionally, ISPs could facilitate these security improvements via more robust defaults and configurations, for example, by changing the default SSID of routers they distribute.

This project was funded by the UK EPSRC grant EP/S022503/1 that supports the Centre for Doctoral Training in Cybersecurity delivered by the UCL Departments of Computer Science, Security and Crime Science, and Science, Technology, Engineering and Public Policy.