Build Safety of Software in 28 Popular Home Routers

Cyber-ITL
December 2018

Researched and written by: Parker Thompson, Sarah Zatko
{parker,sarah}@cyber-itl.org

Our findings in Brief

For many, wireless access points and home routers are just commodity appliances. However, an insecure access point or router can be as damaging to a user's security and privacy as an insecure web browser or document suite.

At CITL, our mission is to empower consumers to protect themselves by reporting on the security of popular products. As part of that, we recently evaluated 28 wireless access points and home routers.

While many access points and routers advertise features which claim to improve security, our evaluation focused on the fundamentals: how secure is the software that runs on these devices?

Our findings support two unsettling conclusions:

1. An old, seemingly forgotten bug in the Linux/MIPS stack has degraded the security of many access points and routers. We believe consumers should avoid purchasing products built on this architecture for the time being.

2. Though the Linux/ARM stack is completely unaffected by the aforementioned bug, for many devices it makes almost no difference: of the access points and routers we reviewed, not a single one took full advantage of the basic application armoring features provided by the operating system. Indeed, only one or two models even came close, and no brand did well consistently across all models tested.

These findings suggest an industry-wide failure to audit and test the security of the software running on these products. Indeed, our review shows that even the most basic practices are being largely ignored.

The absence of these security features is inexcusable: the features discussed in this report are easy to adopt, come with no downsides, and are standard practices in other market segments (such as desktop and mobile software).

For vendors, this state of affairs presents an opportunity for any brand wishing to distinguish itself: very little effort is currently required to earn a “best in class” designation.

For consumers, while none of the routers we reviewed scored well, the Linksys wrt32x scored the best.

Introduction

This paper focuses on the use of software safety features in 28 popular home routers. All of the devices reviewed were running Linux, either on MIPS or ARM architectures. There is a specific security issue with Linux MIPS systems that CITL discovered and describes in detail in another paper[1] that contributed significantly to the certain low scores within MIPS devices. Overall, our survey shows that most routers perform very poorly with regards to known, and industry standard, basic safety features, and that there is little consistency in terms of security practices even within the models of the same brand. One Linksys device scored noticeably better than any of the other devices reviewed, but still far behind best practices found in even default desktop environments. There is clearly opportunity here for any brand which wants to distinguish itself on the security front by employing basic safety features consistently across its product line.

The reviews here focus on a subset of the analysis capabilities CITL uses to measure security hygiene in the software development and build processes for ARM and MIPS. The MIPS issue referenced above contributes to the nearly total absence of basic stack Data Execution Prevention (DEP) hygiene. This paper will only briefly outline this issue, as it impacts the router analysis results. For those not interested in the full MIPS issue in our other paper, we provide a very brief overview of the issue, since it impacts the results for MIPS routers in this paper significantly, and then provide the the results of our survey of safety features present in popular home routers in the rest of this report.

The MIPS Vulnerability in Brief

In the course of adding MIPS binary analysis to CITL’s safety testing capabilities, we discovered a security weakness in MIPS Linux kernel versions from 2001 to 2016 and a new security hardening bypass introduced in their 2016 kernel patch security remedy that is still present to date. The issue from 2001 to 2016 resulted in stack based execution being enabled on userland

[1] https://cyber-itl.org/assets/papers/2018/Linux_MIPS_missing_foundations.pdf

processes. This was due to how Linux implemented floating point emulation for MIPS. Missing stack execution is concerning because it is a basic, vital, and well established safety feature.

One of the patches introduced in 2016 to enable non-executable stacks in Linux MIPS introduced a new fixed-location RWX (read, write, and execute) mapping. This provides a construct that can be used to bypass both DEP and ASLR (Address Space Layout Randomization) irrespective of whether a program opted into stack execution prevention or not. Given how few of the MIPS binaries have DEP and ASLR, the bypass is not terribly relevant at the moment as it is easier for an attacker to take advantage of relative offsets within an executable stack segment, but this will become more of an issue for MIPS systems if they improve their build time security practices to include default non-executable stacks and full ASLR.

We found that nearly every binary on a MIPS based device, which impacts this survey in addition to infrastructure and security systems, is still built in a way that results in an executable stack. This is a significant lack of basic security and safety hygiene. ARM devices generally appear to correctly have non-executable stack segments (i.e. they set the PT_GNU_STACK segment with correct RW permissions) which is expected basic security and safety hygiene for rudimentary Data Execution Prevention.

An Analysis of Security Hygiene for Home Routers Reviewed by Consumer Reports

CITL obtained firmware images for devices listed in the Consumer Reports home router buying guide (2018)[2]. Of the 14 models in the article, 10 had firmware images available publicly. For the purpose of this report we focus on the ten publicly available firmware images. This includes firmware images of home routers from Asus, D-LINK, Linksys, and NETGEAR. We further expand our analysis of router firmware images in the next section to include Synology, TP-Link, and Trendnet.

Of the 10 Consumer Reports models CITL analyzed, 7 were MIPS CPUs and 3 were ARM. For the images we processed all of the binaries within the root partition of the images. While our engine extracts hundreds of features, the analysis properties focused on in this report are the basic hardening and developer hygiene features. This includes Address Space Layout Randomization (ASLR), non-executable stack segments (DEP), correct ordering and marking of segments in the binary to prevent overwriting jump-tables for Linux systems (RELRO), and stack canaries to thwart stack overwrites (Stack Guards). While our extracted measurements include fine grained information for a range of features (e.g. numbers of stack guards observed relative to functions with stack assignments) this analysis focuses on basic: did the developer attempt to enable basic features or not on a per-binary measure.

[2] https://www.consumerreports.org/products/wireless-routers/ratings-overview/

The following table groups devices together by vendor and reports on percentages of binaries that incorporate essential hardening features. To illustrate how well, or poorly, vendors have done in comparison to Linux equivalents, the first line item represents statistics for a default installation of the 2016 Linux Long Term Support distribution 16.04.

Brand	Model	Count	ASLR (%)	Non Exec Stack (%)	RELRO (%)	Stack Guards (%)	CPU
Ubuntu Desktop - Reference	16.04, 64bit	5379	23.21	98.99	100	79.43	x86
Asus	rt-ac55u	334	0	0	1.8	0	MIPS
D-LINK	dir-850l	118	0	0	3.39	0	MIPS
D-LINK	dir-880l	128	0	99.22	7.81	0	ARM
Linksys	e2500	201	8.79	0	3.48	0	MIPS
Linksys	ea6100	414	5.82	0	0.97	0	MIPS
Linksys	ea6900	468	2.50	0.21	1.28	0	MIPS
Linksys	ea8500	484	2.26	99.79	2.07	0	ARM
Netgear	WNDR4300v2	228	1.52	0	2.19	0	MIPS
Netgear	r6100	170	1.96	0	2.35	0	MIPS
Netgear	r7000	457	0	99.78	21.44	13.43	ARM

The ‘Non Exec Stack’ column shows that across all MIPS-based devices, only one binary correctly, from a basic security standpoint, marks the stack as non-executable. By contrast, ARM binaries mark the stack segment as RW almost all of the time. Per our paper on this MIPS issue we expect the ARM toolchain, and ARM Kernel, do not suffer from the situations we documented on MIPS.

Whereas MIPS lacked basic stack-based DEP we found that nearly all the devices, both MIPS and ARM, generally lack other basic security and safety hygiene, such as ASLR and Stack Guards. Both of these defensive techniques have been widely known and deployed for over a decade. The data above shows that home routers are soft targets in comparison to the security hygiene present in modern desktop operating systems (e.g. Windows 10, OS X 10.13, and non-default, *hardened*, builds of Linux).

The data shows poor use of application armoring features across the board for these home router embedded devices: stack guards are almost completely missing (besides just 13.43% of binaries on the Netgear r7000), RELRO is only sporadically applied (with the best device covering less than a quarter of the system binaries), and the number of executables that have full ASLR is extremely low (less than 10% for all routers in this class). The fact that only a small number of binaries within these systems embody any form of correct basic hygiene is disconcerting. This lack of basic hygiene does not appear to be due to any inherent issue, such as the MIPS problem. If it weren't possible to institute these safety features, then the values would be 0 across the board. Instead, this poor showing implies an apathetic attitude towards applied consumer safety and security for the home router products analyzed.

While none of the analyzed systems do well, the Netgear r7000 does best on safety features, within the Consumer Reports selection, in a comparative analysis. In all of the router images we analyzed, as seen in the next section, the Netgear r7000 places second or third. While the Netgear r7000 is noticeably better than the other routers in the Consumer Reports selection that we analyzed, it is still well below even a standard unsecured common desktop Linux distribution from 2016, especially in regard to the Netgear r7000's total lack of ASLR.

To provide context for the build safety and hardening of the routers in the Consumer Reports review; version 16.04 of Ubuntu Linux has 100% usage of RELRO, 79% of all binaries have stack guards present, and 23% them are compiled with ASLR. The maximum values observed for these these routers are 21% RELRO, 13% stack guards, and 9% for ASLR. It is important to note that Ubuntu Linux is not even a hardened system with regards to these basic features yet still significantly exceeds the basic hygiene found in the home routers reviewed. Compared to other contemporary operating systems like Windows 10 and MacOS 10.13, Ubuntu Linux 16.04's 23% for ASLR is particularly weak - both of those operating systems have 99% of binaries compiled with ASLR.

Additional Home Routers

In addition to the Consumer Reports 2018 list of home routers, CITL collected data from other 'Best of 2018' home router lists. These included CNET[3], PCMag[4], and Trust Compass[5]. Below is an overview of the same basic hardening features for these 18 additional devices, again referencing the basic desktop distribution of an un-hardened Linux Ubuntu Long Term Support, dating back to 2016, in the first row for comparison.

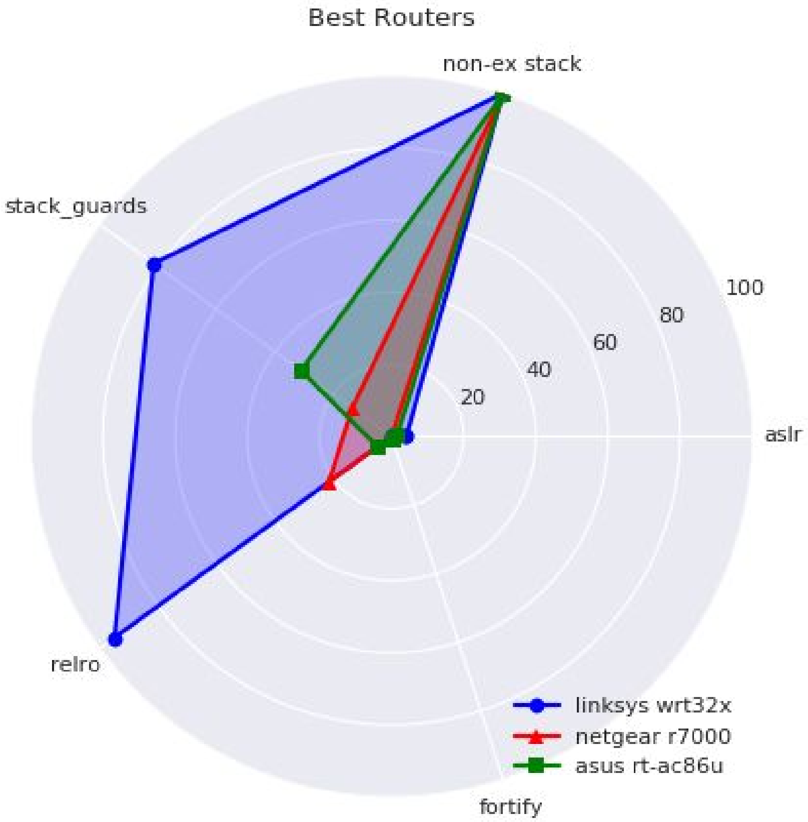
Brand	Model	Count	ASLR (%)	Non Stack Exec (%)	RELRO (%)	Stack Guards (%)	CPU
Ubuntu	16.04, 64bit	5379	23.21	98.99	100	79.43	x86
Asus	rt-ac3200	371	2.10	98.92	3.23	0	ARM
Asus	rt-ac68u	383	2.03	98.96	3.92	1.08	ARM
Asus	rt-ac86u	515	1.49	99.61	4.85	31.09	ARM

[3] https://www.cnet.com/topics/networking/best-networking-devices/
[4] https://www.pcmag.com/article2/0,2817,2398080,00.asp
[5] https://www.thetrustcompass.com/best-wireless-routers/

Asus	rt-ac88u	430	1.926	99.07	2.79	0.93	ARM
D-LINK	dir-842	129	01	0	4.65	5.47	MIPS
D-LINK	dir-890l	140	0	99.29	7.14	0	ARM
D-LINK	dir-895l	138	0	99.28	7.25	0	ARM
Linksys	wrt1900ac	503	4.15	99.8	3.18	0.62	ARM
Linksys	wrt32x	139	4.05	100	94.96	81.58	ARM
Netgear	r8000	440	0	100	22.05	13.65	ARM
Netgear	r9000	477	.44	100	17.82	0	ARM
Netgear	rbr50	340	.98	100	2.94	0	ARM
Netgear	xr500	421	07	99.76	6.89	9.28	ARM
Synology	rt2600ac	1835	6.72	99.56	16.68	5.48	ARM
TP-Link	ac1750	175	0	0	3.43	0	MIPS
TP-Link	ad7200	276	0	99.64	3.62	0	ARM
TP-Link	c3150_v2	160	0	99.38	14.37	0	ARM
Trendnet	tew-827dru_v2	197	0	0	77.66	0	MIPS

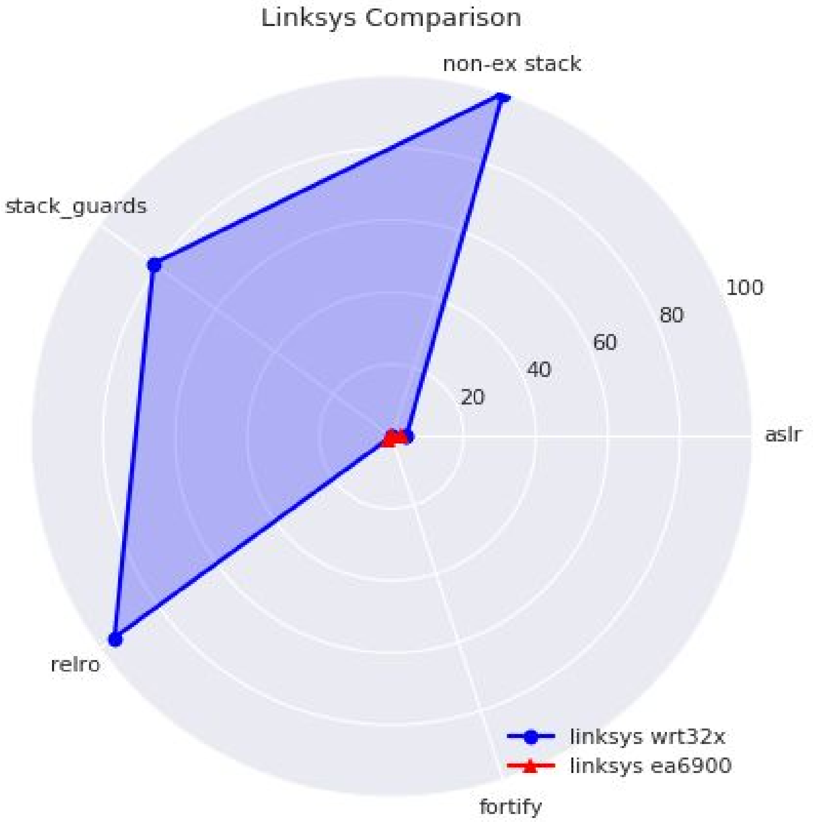
The Consumer Reports home router models we analyzed were made up of 3 ARM and 7 MIPS devices (30% ARM, 70% MIPS). The firmware we analyzed from the '*other* 2018' lists we collected were made up of 15 ARM and 3 MIPS devices (83.33% ARM, 16.67% MIPS). Thus bringing the total devices analyzed to 28 home router models, made up of 18 ARM and 10 MIPS systems (64.3% ARM, 35.7% MIPS). Although the ratio of ARM to MIPS devices increased, the overall use of basic hardening features was still poor. The Linksys wrt32x did better on basic safety and security build hygiene than the routers in the Consumer Reports article with the most consistent use of stack guards, RELRO, and non-executable stack marking, making it the best in class among its peers for security features. The Linksys wrt32x was still missing ASLR almost entirely, so there is still room for improvement. The router with the highest usage of ASLR across binaries was the Linksys e2500 from the first group, with a still extremely poor 9% ASLR. Given that ASLR is an easy safety hygiene feature to accomplish for binary applications, this is a major industry-wide security lapse.

One method CITL uses internally to visualize comparisons between different devices is radar charts. These charts show the percentage of binaries in the firmware image that have particular hardening features, and plotting more than one at a time allows easy comparison. Here are two samples from the above data that show the two extremes. Larger areas covered represent a binary that is better hardened. The following plot shows the three best secured routers out of all models that we reviewed.



In the above, the Linksys wrt32x, which scored better than the other home routers, can be seen to have significant coverage in RELRO and stack based DEP. There is room for improvements in stack guards, and ASLR is essentially non-existent. ASLR and DEP work best in tandem, so the lack of one impacts the efficacy of the other. That being said, the Linksys wrt32x is far better than either of the runners up, the Netgear r7000 and the Asus rt-ac86u. These still have very low values for ASLR, and additionally do far worse in terms of both Stack Guards and RELRO.

It’s interesting to note that the use of safety features is not consistent even within the same brand name. For example, the Linksys wrt32x was the overall “best in class” for these measurements, however other Linksys devices (wrt1900ac, ea8500, ea6900, ea6100, and e2500) fared far worse. The radar chart below shows how greatly security practices can vary within the same brand.



None of these safety features are difficult to enable, so the message the market should take from this is that the easiest step any brand can take to move towards a hardened and “safe” software build is to do the basics in safety and security practices for building and compiling software. At the moment, the field appears wide open.

Conclusions

The low scores on basic security hygiene for MIPS products can be attributed in part to the issues described in out other paper[6]. Due to this we expect security and safety issues for Linux MIPS systems may continue for some time in. Until Linux MIPS devices are on modern Kernels (Kernel Version 4.8 or greater) **and** Linux MIPS compiler toolchains such as GCC emit security safe defaults for primitives, like stack DEP (at present not the case as of testing of GCC 8), we do not see Linux MIPS devices as likely to embody basic hardening practices. Given the choice between a Linux based home router built on an ARM or MIPS processor at the present, and foreseeable future, we believe the consumer is statistically more likely to realize a higher safety and security build quality by choosing an ARM based Linux system. However, as noted above,

[6] https://cyber-itl.org/assets/papers/2018/Linux_MIPS_missing_foundations.pdf

the degree to which vendors care to enact basic hygiene varies widely even amongst their own offerings.

Security and Safety hardening of applications is a straightforward best practice to apply to products yet we observe this as a very unevenly distributed set of features in practice. By analyzing a large collection of devices on the market we observed how problematic the end result frequently is. Executable stacks, and anonymous regions, may have a specific historical technical explanation for why this basic vulnerability still persists within Linux MIPS, but when it comes to other safety features the ARM and MIPS systems are demonstrably equally poor. Some devices, such as the Linksys WRT32x, are noticeably better than their peers, but all vendors have room for improvement, especially when it comes to consistently applying basic safety features across different models in their product lines.

The haphazard security practices in IoT devices put their overall security stance well below that of desktop operating systems. From our research this is one of the reasons why botnet operators and other malicious actors are moving to IoT exploitation - the devices are numerous and largely insecure. This brief survey of one small corner of the IoT ecosystem shows why this trend is likely to continue unless vendors become more responsible in basic software security and hygiene practices.

This poor showing for home routers highlights the need for the basic testing measures prior to shipping a product. It is not difficult to check if the stack is marked non-executable, but doing simple safety checks of that nature does not appear to currently be a standard industry practice. It is not sufficient to assume that software compiled in a secure configuration - a post-compile check of the resultant binaries should be a standard step before release. Otherwise, surprises like the ones seen here are inevitable.

If vendors applied basic checks for software safety practices as part of their build and testing practices prior to shipping their products the industry could quickly see a noticeable improvement in product build safety.

Acknowledgements

Parker Thompson obtained router images, added MIPS analysis support, ran the CITL tools on all images analyzed, and wrote the first draft of the report.

Sarah Zatko produced the radar charts and review methodology, as well as writing the bulk of the text for the final report.

The authors wish to thank Peiter Mudge Zatko and Tim Carstens for their assistance in writing and editing portions of this report. We also thank Patrick Stach for his invaluable contributions in determining the cause and impact of the Linux/MIPS issues discussed above and in our separate report, *Linux MIPS - A soft target*.