The Internet of Things Old and Unmanaged

David Plonka
plonka@cs.wisc.edu

Elisa Boschi

This paper is largely an excerpt of an unpublished manuscript, originally prepared in 2005, amended with details and measurements for 2016.
It has NOT been peer reviewed. The authors take full responsibility for its content.

Abstract

The operation of the Internet is not usually informed by details about new types of Internet hosts such as customer premise broadband routers and other Internet-connected consumer products. Detecting and monitoring their arrival and effect is challenging. In this paper, we consider a particularly illustrative incident involving this class of host. In May 2003, we found that one IP address of a public Network Time Protocol server was the destination of a large scale flood of inbound traffic. To our surprise, we determined the sources of this flooding to be hundreds of thousands of real Internet hosts throughout the world – the root cause being serious flaws in the firmware of low-cost Internet products targeted for residential use. Because this situation was discovered before its peak and a subset of the flawed devices continue to operate even today, in 2016, we offer an empirical measurement of the lifetimes of such products. Based on this incident, we also consider how Internet consumer products are introduced and operated and propose ways in which we might address the threats that such things pose.

1 Introduction

Today, many consumer products are also Internet hosts. Some Internet products have become consumer products, such as broadband routers. Also, some consumer electronics products have become Internet hosts, *e.g.,* digital video recorders. Recent incidents resulting from engineering flaws in these products raise concerns about the Internet-wide effect of this emerging class of Internet hosts. These hosts are deployed rapidly and are owned and operated by inexperienced users having little incentive to reconfigure or update them once they are working. While one might argue that this has historically always been the case with Internet hosts, we suggest that special attention to these new hosts is warranted by their increased numbers, their significant ability to generate traffic, and their high rate of deployment.

These hosts can be involved in unwanted traffic and other abuse due to engineering flaws and their associated vulnerabilities. Competition-driven pressures have led some vendors to rapidly develop Internet hosts of dubious quality. Sometimes the product design and manufacture is delegated to "hidden" Original Design Manufacturers (ODMs). Because of competition for retail space (online or on-shelf), the vendors benefit from being the first to market with a new type of product. Engineering flaws have the chance to reappear when an existing product is wholly re-engineered solely to increase revenue – so-called "cost down" engineering. Superficial product reviews by the IT press result in recommendations of poorly engineered products. Still, admittedly, one must expect some flaws in even the best products.

To foster an informed community, and perhaps motivate its change, we believe there is value in publicly disclosing details of such flaws and the problems that result.

2 The Netgear SNTP Case Study

In May 2003, the University of Wisconsin campus in Madison (UW-Madison) found that its network was the recipient of a continuous large scale flood of inbound Internet traffic destined for one of the campus' public Network Time Protocol (NTP [6]) servers. The flood of traffic was at a rate of hundreds of thousands of packets per second, and hundreds of megabits per second.

Subsequently, we determined the sources of this flooding to be hundreds of thousands of real Internet hosts throughout the world. The root causes were serious flaws in the design of Netgear's low-cost Internet products targeted for residential use. Specifically, this unwanted traffic was traced to four models of residential broadband and wireless routers, which were found to have at least two problems. First, the University of Wisconsin's NTP server IP address was embedded in the firmware and was not configurable by the end user. Second, when these flawed devices do not receive a response to their Simple Network Time Protocol (SNTP [7]) queries, they retry continually at *one second* intervals.

Because this situation was discovered before its peak and the flawed devices continue to operate, we have a unique opportunity to examine the evolution of this incident. In Figure 1, we plot the estimated number of flawed SNTP clients observed utilizing the University of Wisconsin NTP server, 2003–2016. [1] The dots, colored blue, represent actual counts of active source addresses per day, and we use this as a proxy estimate of active client counts. By examining NTP clients' source port distribution (not shown), we expect a 5.5% exaggeration in address count due to non-Netgear clients and adjust our estimates accordingly. Netgear reported producing and shipping over 700,000 devices containing the flaw and changing the flawed code circa June 2003. Our measurements seem to confirm that peak, near November 2003. In response to questions from the community, we recounted on April 3, 2016, and find that an esti-

[1] Details of how these clients are discriminated is provided in [9].

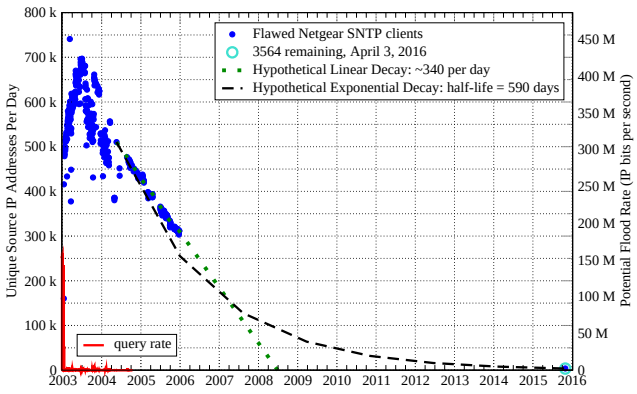

Figure 1: Flawed Netgear SNTP Clients, 2003–2016.

mated 3545 of these flawed Netgear SNTP clients remain. In Figure 1, we also plot hypothetical curves as straw men for the missing data, assuming the "births" of these devices largely subsided by 2005. If their "deaths" can be modeled by exponential decay, the mismatch to empirical data suggests the decay constant (λ) is greater than 2.

In Figure 1, we also show the and theoretical maximum amounts of bandwidth that could be consumed by the flawed clients' SNTP queries. These are labeled on the vertical axis on the right side. This is simply the number of active clients observed potentially querying at one second intervals, multiplied by 76 IP bytes per query. The actual bandwidth consumed by inbound queries is plotted in red (lower left), *e.g.,* exceeding 150 megabits per second in May 2003. This flood subsided when we resumed the servicing of these unexpected requests. We began counting the number of unique source IP addresses (IPs) per day in June 2003, and use this as an estimate of the number of flawed clients active on the Internet, worldwide.

We further analyzed the measurements to consider the daily client count on a source network by network basis. In Table 1 we show the top five source networks (Autonomous Systems) based on the number of flawed Netgear SNTP clients which they appear to host. For instance, Deutsche Telekom was the top ranked network [2]; it supplied the affected products to customers of its broadband services [11]. Cox Communications was highly ranked but we did not see evidence of such rapid deployment; instead, it likely happens to serve many consumers that bought the flawed equipment from a retail store. During the period from 2003 through 2005, each of the top five source networks had their source count decline to about 68% (range was 63% to 73%) of its peak value. During that time, the total number of flawed sources declined to 68% of its peak, as well. These early declines seem uniformly distributed across the source networks of service providers. As such, the decline observed may be the "natural" lifetime of these products. As of April 2016, the number of active Netgear clients appears to have dropped below four thousand in total. These top networks still remain in the top ten and Deutsche Telekom still hosts the most. (AT&T WorldNet is defunct and has become part of AT&T Internet Services.)

[2]Deutsche Telekom's service may change the clients' IP address daily; in Table 1, then, that estimated client count has an error of +50%, at most.

Table 1: Top Networks by Estimated Client Count.

Rank, 2003-2005	Client/Source Network (Autonomous Systems)	Est. Remaining Clients, 2016
1	Deutsche Telekom	437 (12.27 %)
2	Korea Telecom	84 (2.36 %)
3	AT&T Internet Services	146 (4.11 %)
4	AT&T WorldNet	*n/a*
5	Cox Communications	127 (3.55 %)
Total	all (450 in total)	3564 (100.00 %)

There are numerous factors which led to this prolonged problem. The Original Design Manufacturer did a poor job of engineering the product through ad hoc design and ultimately delivered unfinished code that was unfortunately deployed. Other factors are covered more completely in [9] and [10].

3 Remediation

The Internet is composed of networks operated by a great variety of organizations with diverse goals and rules. While good user service would require that the operators and administrators of the Internet follow some common rules for policies and operations, there is currently no way to enforce them.

Let's consider possible remedies which might help protect the Internet and its users from vulnerabilities and unwanted traffic generated by flawed consumer products.

Quality Engineering: It might be tempting to dismiss the aforementioned incident as merely an anecdote involving inept product development. One observation about these flawed products is that they differ from routers and other network elements in that they seem to be *Internet* products rather than *network* products. Consequently, they are inappropriately relying on the presence of hosts and services that happen to appear in the Internet that we see today, rather than relying only on features of a general IP-based network. Since it is unlikely that the quality of product engineering will improve merely at the suggestion, we should assume that these sort of engineering problems will continue to arise. As such, the Internet community would be best served by finding a way to avoid the flawed devices being widely deployed or finding techniques to contain the problems once they are deployed.

Internet Standards: The Best Current Practice (BCP) subseries [3] of the Request for Comments (RFC) series is a vehicle by which the Internet Engineering Task Force (IETF) [5] attempts to convey best practices. With respect to cases such as ours, RFC 4085 (BCP 105) [10] describes the problems and makes general recommendations about managing device configurations including: *(a)* disable unused

features, *(b)* provide user interfaces for features, and *(c)* utilize local services. Using *local services, i.e.,* in the customer premise or Internet Service Provider network, remains particularly appealing. This scales well and allows local control of device deactivation (*e.g., ala* a dead man's switch), reconfiguration, and reactivation without relying on Internet services, worldwide, that may not persist. This RFC, published in 2005, took one year and a half to develop; unfortunately, its impact seems quite low. Not surprisingly, since the IETF is not an enforcer, BCP RFCs, alone, are unlikely to be an adequate solution when an incident arises.

The Trade Press: In the process of working on this incident, we wondered what role the trade press played and could play. The situation seems somewhat bleak. One reviewer, who had recommended the flawed products, claimed that the publishers do not provide enough funding for proper product reviews. Ostensibly, this is what leads to reviewing the product simply by configuring and using it exactly as is suggested in its user manual. Furthermore, the manufacturers or vendors of the products are often advertising customers of the publication which carries the review, so the reviewer is not independent. Note that these flawed products received numerous "Editors' Choice" awards from the press. Also, many publications seem to have increased readership as a higher goal than accuracy in reporting. This is evidenced by the sensationalized headlines when our problem was publicly disclosed. The trade press further confused the issue with poorly researched descriptions of the problem and made negative exaggerations such as the claim, "Netgear Routers Wage War On University" [8].

Underwriting: Despite the remediation efforts and disclosure in this case, we have no evidence that they influence vendors or manufacturers to avoid such situations in the future. As Internet-specific consumer products continue to be developed, how best can we ensure that they are "Internet safe?" That is, how can we have some level of confidence that these products won't accidentally degrade the Internet itself? Other fields, such as structural engineering and consumer product safety, have matured to the point that the industries involved, or their governments, effectively impose and enforce standards that protect the communities which utilize the pertinent services or products. Thus we propose that, for some classes of Internet products, testing and certification, or *underwriting* is necessary, very much as it is for public safety regarding electrical consumer products. Consider the product safety testing and certification organizations, UL, FCC and CE. UL, Underwriters Laboratories is an independent product-safety testing and certification organization. FCC and CE mark are certification marks for electronic products sold in the United States and the European Economic Area, respectively.

If underwriting or Internet product marking were implemented, what aspects would the certifying organization be testing? What fail-safe features should we expect in an Internet product? We suggest that the IETF Standard and Best Current Practice documents be used as the basis for testing. In this way, the existing standards organization continues, as-is, to maintain the standards and best current practice documents, but the testing and conformance determination would be performed by a laboratory. Such certifications and labs do exist today [1, 2, 4]. We propose that, for Internet consumer products, they be employed either voluntarily by the manufacturer, or as a mandate from the retail product supply chain (such as a store considering carrying such a product), the insurance industry, or perhaps, ultimately, a government agency.

4 Conclusions

The unwanted traffic and vulnerabilities resulting from flaws in consumer products warrants special attention. In the case we've examined, this unwanted traffic arose accidentally as the result of engineering flaws. Because these products exhibit rapid deployment and are not easily reconfigured, it is difficult to design an effective solution once problems occur. While diligent engineering practices are certainly warranted when introducing this new class of consumer product Internet hosts, they are not sufficient to protect the Internet from the product flaws that will arise again. It is in the Internet community's interest to consider how to improve the process by which consumer products arrive on the Internet and also envision how we might limit the damage when it occurs.

In this short paper, we've suggested that the production and deployment of Internet consumer products should involve testing and certification. Furthermore, we propose that IETF standards and process could serve as a basis for such underwriting. While we advocate underwriting to mark high-volume consumer products as "Internet safe," we haven't proposed a method of enforcement. Consumer and insurer awareness is likely a key component to a successful certification program. Hopefully, the Internet community is willing and able to cooperate on such an initiative. Ignoring the danger presented by the continuous and increasing deployments of these new consumer products results in both risks to Internet users and to the performance of the Internet, itself.

Acknowledgments

We thank: Paul Barford, Arthur Berger, Nevil Brownlee, Dan Fox and Jan Galkowski for their helpful comments; Dale Carder and Gary Faulkner for updated measurements.

References

[1] InterOperability Laboratory Testing. `https://www.iol.unh.edu/testing/`.
[2] IPv6 Ready Logo Program. `https://www.ipv6ready.org/`.
[3] S. Bradner. RFC 2026, The Internet Standards Process – Revision 3, Oct. 1996.
[4] ICSA Labs. `https://www.icsalabs.com/`.
[5] Internet Engineering Task Force. `http://www.ietf.org/`.
[6] D. Mills. RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, Mar. 1992.
[7] D. Mills. RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, Oct. 1996.
[8] Netgear Routers Wage War on University. In *PC World*, Nov. 2003.
[9] D. Plonka. Flawed Routers Flood University of Wisconsin Internet Time Server. `http://www.cs.wisc.edu/~plonka/netgear-sntp/`, 2003.
[10] D. Plonka. BCP 105, RFC 4085, Embedding Globally Routable Internet Addresses Considered Harmful. `https://www.ietf.org/rfc/rfc4085.txt`, 2005.
[11] Personal conversation with Ruediger Volk.