Net.info: A Provider-to-Subscriber Secure Communication Channel

Steven Bauer, MIT

Net.info is a project underway at MIT with the goal of developing an architecture and implementation for a new communication channel between ISPs and their downstream users.[1] There does not currently exist a trusted, secure and easy to use channel for communicating information between access networks and their connected end users. It is currently surprisingly difficult for access providers to communicate notifications, alerts and other types of relevant network information with their attached users. Similarly users, applications, and measurement tools have no convenient channel for pushing information upstream to their network access provider such as communication failures or measurement test results. *Net.info* creates the possibility of enabling a virtuous cycle of feedback between access providers and users that results in rapidly improving the security of the network and the quality of experience of users.

Some of the specific kinds of information that should be able to flow between network access providers to end users over a secure, authenticated and trusted channel include:

1. Network service information (e.g upload, download speeds, data caps, traffic alerts)
2. Network quality reports generated by end user applications and measurement tools
3. Notifications of botnet and malware infections
4. Mandated network disclosures (e.g. FCC mandated network management information)
5. Copyright Alert System notifications[2]

Our *net.info* project acts as a coordination point where such information would be readily accessible. The information is available both in human readable forms (unstructured or semi-structured) accessible with any web browser and in structured formats (e.g. JSON, CBOR, etc.) for use by software systems (e.g. system status bar notifications, mobile apps, and edge based measurement tools such as FCC's Measuring Broadband America program).

Today, access networks attempt to push notifications to their users via one of the following communication methods: email, phone, text messages, mail courier, inline web notifications[3] and walled gardens. In addition to being expensive, most of these channels are vulnerable to different types of attack. Notably, malicious hackers have exploited the first four of these using social engineering tactics to worsen, not improve, end user security.[4] Users, applications, and test measurement tools rarely seek to communicate information directly upstream with their current network access provider.

---

[1] The choice of the name reflects the desire to make this broadly and easily adoptable. Most obviously, *net.info* concatenates "network" and "information" in a short domain name currently reserved by ICANN that is globally accessible. We believe users could become readily accustomed to typing net.info into web browsers or using applications that displayed net.info information and notifications.

[2] See https://en.wikipedia.org/wiki/Copyright_Alert_System

[3] See RFC 6108: Comcast's Web Notification System Design.

[4] For example, we are personally aware of two incidents where end-users were called and partially talked through the installation of malware -- both with the justification that their computer was infected and needed to be "cleaned up."

We next consider some motivating examples of how *net.info* could facilitate efficient and secure exchange of information between access providers and their attached users and thus how net.info can be a key building block in efforts to measure and improve quality of experience.

1. Network service parameters:

It is currently exceedingly difficult for end users or measurement tools to identify basic service information such as the upload and download speeds of their broadband access link. While this information is readily available when signing up for a broadband service it changes over time as service is gradually upgraded. At least for the authors of this report, learning the current service levels of their residential broadband service involves a complicated procedure of logging into their broadband account and comparing the service name on their billing information with a lookup on a zip code specific mapping of service names to speeds on a different part of the provider's website.

Especially at a time when over 80% of households already have broadband service in the United States, real time and easy access to this basic service information is arguably more important that broadband labeling efforts aimed at point of purchase time periods. It is unfortunate that when tens of millions of broadband speedtests are run each year users are not capable of easily comparing their actual performance with the advertised speeds of their service.

One of the reasons that the FCC's Measuring Broadband America project only releases its data and reports once a year is that the procedure for validating panelist service information is run by the FCC and ISPs only once a year and only covers the one month of the report period. This limits the analysis that is conducted by the FCC to a single, hopefully representative, month as well. Singapore on the other hand releases data from their very similar, albeit smaller, broadband measurement effort every three months with data from every month included.

The adoption of *net.info* would enable testing tools such as the FCC's measurement devices and the popular speedtest.com to acquire accurate service information automatically. This facilitates both regulatory and user monitoring of broadband performance.

2. Network quality reports

Significant improvements in the quality of applications, operating systems, and hardware have been driven by the wide adoption of automated crash-dump / error-reporting that sends feedback when applications go awry. Software providers in this fashion gain insight into the real-world environments, situations, and problems their users experience. Microsoft was reportedly able to fix 29% of Windows XP bugs due to automated collection and analysis of crash reports.[5]

Feedback on network quality from users and applications to the access provider could similarly create a feedback loop driving continuous improvements in network quality. Regular applications as well as purpose build measurement tools could submit these network quality reports. As a concrete example that combines multiple pieces of *net.info*, consider a new measurement tool that implemented a constant bit rate test from the Model Based Metric

[5] K. Glerum, K. Kinshumann, S. Greenberg, G. Aul, V. Orgovan, G. Nichols, D. Grant, G. Loihle, and G. Hunt. 2009. Debugging in the (very) large: ten years of implementation and experience. In Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles (SOSP '09).

framework.[6] The tool would first calculate an appropriate data rate to test based upon the download speed discovered over *net.info*. The provider's *net.info* server might suggest a set of appropriate test servers located in their network or other nearby networks. After selecting a server and conducting the test, results that deviated significantly from expected results could be reported upstream over the *net.info* channel to the access provider. While individual reports are unlikely to be investigated by access providers, the aggregate accumulation of reports might provide a strong signal that quality problem have arisen. Network quality reports facilitate providers' ability to localize problems both in their own network as well as other off-net locations that are affecting the experience of their users.[7]

3. Botnet mitigation

In September 2014, the Messaging Anti-Abuse Working Group (MAAWG) reported the percentage of subscribers that participating network operators had identified as being infected with a botnet.[8] Around 1% of subscribers were detected as being infected with malware, and attempts were made to notify almost all those infected. The study does not report on the methods, costs or effectiveness of the mitigation efforts, but it is noteworthy that the incidence of infections was not substantially reduced over the eight quarters. A persistent supply of up to 500k bots poses a significant threat to Internet security.

We believe that *net.info* has the potential to drive down by one or two orders of magnitude the number of subscribers infected with a botnet or malware that can be detected by their ISPs. There are two key elements: 1) building an authenticated, secure, and trusted channel (that is not vulnerable to social engineering attacks that worsen instead of improve the problem); and 2) significantly reducing the response time between when an infection is identified and when it is addressed. By design, net.info focuses on the communication of information about the infection, while leaving the response to that infection to be determined by other elements of the ecosystem.

Design requirements:

Precisely defining the architecture, APIs and message formats are the subject of ongoing research. We believe *net.info* will be able to meet the following key design requirements:

- Designed to be adopted and used by human users, applications, libraries, and platform/operating system providers
- Designed to provide information in human readable, accessible, and multilingual formats and in structured formats that are easily parsed by software systems
- Designed to support both a push and pull mode of communication
- Designed to be secure against man in the middle attacks (such as a compromised wireless access point in the user's home.)
- Designed to work across complex network topologies that can exist between user devices and the network access provider (e.g. multiple NAT boxes, multiple hops both wired and wireless, proxies, alternative DNS providers, Carrier Grade NAT, IPv4 and IPv6 etc.)

---

[6] See https://tools.ietf.org/html/draft-ietf-ippm-model-based-metrics-06

[7] Some large broadband providers in the United States already work to identify problems and notify content and application providers of issues that are effecting the quality of experience of their subscribers.

[8] See https://www.m3aawg.org/for-the-industry/bot-metrics-report