What's In It For Me?
Revisiting the reasons people collaborate

Richard L. Barnes

August 2022

The M-TEN call for papers correctly observes that many proposed approaches to network management in the presence of encryption require collaboration "across the encryption boundary" — between an "inside" entity that can see unencrypted user content and an "outside" entity that can see only ciphertext. A collaboration, however, only makes sense when there is a problem of mutual interest to the collaborating parties. For most of the problems that tend to be labeled "network management", it is not clear that any such mutual interest exists. What problems does encryption create that are meaningful to the people who would need to collaborate on a solution?

In any collaborative effort to solve a problem, all of the collaborators need to see:

- Benefits to solving the problem
- Costs that are proportional to the benefits
- Safeguards against bad behavior by other collaborators

The last of these items is especially essential in the Internet. Thanks to the magic of interoperability and dynamic discovery, the party with whom you are "collaborating" is often just some other information system that your system happens to have encountered in the wild — not someone that you have any reason to trust. It is also exceptionally important when we are talking about encryption, since the "outside" collaborators are being trusted with information that would otherwise be protected.

When we talk about collaboration to deal with problems raised by encryption, for the most part the party on the "inside" of the encryption boundary is an *application* that a user interacts with. The user provides the application with their information so that they can get whatever benefits the application provides. The application applies encryption so that users' information isn't exposed to anyone who isn't supposed to have it.

Given this situation, the questions above need to be answered through a more human lens:

- What *user-meaningful* problem is being solved?
- What does the user have to give up in order to solve the problem?
- How can the user be confident that they're not going to be harmed?

Moreover, the answers to these questions need to be *general*. Applications ship one program to many users, so the trade-offs involved in a collaboration need to make sense for all of those users. It's not enough to have some niche cases where there are a few users for whom giving up privacy for some network benefit would be acceptable.

On the specific question of network management: Users don't care about network management. Users mainly care that the network works well in a few well-defined ways. Do web pages load quickly? Is my video quality good? These aspects of network management largely just come down to normal bandwidth and latency considerations, and obvious things like buffer bloat — not anything for which the network needs any of the user's private information.

(There are obviously cases where users delegate certain security functions to the network, sometimes quite invasive security functions, such as when enterprise-managed devices opt in to TLS-decrypting firewalls. These are in fact collaborative cases, but within the scope of M-TEN, it's important to note that these cases are solving users' security problems, not network management problems.)

The empirical evidence to date does not indicate that encryption is causing any user-meaningful network management problems. Despite a number of IAB and IETF sessions premised on the idea that there are problems to solve, no problems have arisen that have resulted in changes to encryption technologies or their application. On the contrary, for several years now, encryption has been nearly universal for web traffic as well as traffic generated by other applications, and the network has not collapsed. Even the financial health of network operators seems unharmed; Verizon's net income, for example, has increased by more than 30% in the few years since TLS 1.3 was standardized!

The Internet certainly has network management problems that need collaborative solutions. But it doesn't seem that encryption is at the heart of any of these problems, or that collaboration across the encryption boundary is called for.