

[Full-disclosure] Let's design a spy-proof communications infrastructure

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-06/msg00379.html>

- *From:* Glenn Everhart <Everhart@xxxxxxx>
 - *Date:* Sun, 29 Jun 2008 13:26:22 -0400
-

Colleagues:

It is unworthy that people should be spending energy criticizing others' qualifications, personal habits, ancestry and destination (as the wording goes).

I suspect that something much more useful can be possibly facilitated here (and elsewhere if anyone feels like it).

Let me suggest that it should be possible to construct something like a cell phone network which will run like a peer to peer network, with routing determined heuristically and pretty much unpredictably, with message encryption, and with small enough electronics to package in something no larger than current cell phones.

The current designs we have are the creatures of the old phone companies and presume things go through central offices. This has led to intrusions into user privacy by crooks and governments, and tends to make all manner of information we might not care to publish become effectively wide open to anyone who cares to steal it.

However, consider that many internet p2p networks have been worked out (and are still being) to hide some of this. Consider that the old usenet protocol has no idea of global source or destination (though its flood fill algorithm is I suspect way too slow, still, to be used for messaging or voice traffic). If a network is designed so that every member only has some idea of its neighbors and which of them might be closer to the desired endpoint than it is, each node only has or needs a very local idea of addressing – something that might be relatively useless to central authorities or to crooks.

The electronics to receive and send messages locally can be made very small and cheap. There are low power CPUs from places like TI and Atmel that run on microwatts, and WWV receivers can be had for \$1 in chip form in bulk (per messages I have gotten). We have GPS boxes that you hold in your hand able to receive satellite transmissions. A few years back this would have been thought energetically impossible.

[Full-disclosure] Let's design a spy-proof communications infrastructure

If we devised some private communicator, it might expect to function in a very large net so long as some path existed to other communicators. While truly global routing might require some relays to bridge areas with few people, in urban areas and quite a few not-so-urban ones direct communication should be workable, at low enough power on any single frequency (yeah, make it spread spectrum) that formal licensing would not be needed.

It should be noted that the address of any such system need not be fixed for huge times. To the extent you can get the systems to read, say, a time synchronization signal, systems might simply pick new addresses out of a suitably long number space. (If this is truly random, address collisions might be made so rare they can be ignored.) This would mean routing would need to be recomputed locally every so often but would make the notion of global address pretty well meaningless and unpredictable. (Use a heat source perhaps to generate random bits, so the randomness is from thermal noise. Nobody will be able to steal a key and figure the next address, or the last...). If a broadcast were available so each unit could sense nearby ones (where you make "nearby" as far away as you can) the constantly changing addresses won't cause problems discovering what else exists. If you have to scan an area, such discovery could be unsecurable. While I mention discovering where one is on a mesh, this might be tried with and without actual geographic coordinates. Nearness measured by a Hamming distance could be used for routing also. It might not be as efficient but if it worked it would mean routing gave eavesdroppers no hint as to physical location of anyone. If we want to keep private conversations private, this seems like a good thing.

Authenticating people is I think separable from this; I have some other schemes to handle that. For a communicator, encryption should basically make traffic snooping impossible and make routing snooping infeasible even with adversaries who listen to a lot of traffic. The lessons of Blackberry should be heeded here: make the encryption all end to end, not step by step, with no backdoors built in and with open source code so tampering with these principles can be quickly caught and negated.

Building such gadgets would be paid for by people wanting to use them, but note that the necessary infrastructure is just the existence of a large bunch of these things being used, sitting on peoples' belts or in pockets and passing traffic among one another. You start selling them in small offices or families, where the necessary groups will tend to be together a lot. Gradually people will notice that they can reach others.

How to address some particular person then?

I would suggest that some of the p2p research might be useful here. Perhaps have the gadget transmit a name or other identifier of the person there in some form. If for example we allow repositories of public keys, we might transmit "John Smith has address xxxxxxxxxxxx"

[Full-disclosure] Let's design a spy-proof communications infrastructure

where xxxxxxxxxx is encrypted by his private key. (This is not very good.)
If a few trusted nodes can be made, they can be used in setting up connections by finding the current addresses.

If I wanted to talk to John Smith and could find a partial address for him from some repository I might transmit some of my address encrypted by his public key and my name, and it might be noticed by John Smith's communicator and full address sent back. This kind of thing gets somewhat better, since not everything gets sent at once. It is still not great.

It is probably best for routing to have all units be able to be opportunistic routers, so that there would be a large and often – changing set of routers in

any area having information about some addressees. You will need some way to convert an identifier "name" to a network address, probably in several pieces to make it hard to fake.

It is probably worth thinking about a "web of trust" here and having ways to declare identifiers as trustworthy or others as to be shunned. Phil Zimmermann wrote much about this in conjunction with pgp, and such function may be necessary in some places to keep eavesdroppers from hammering parts of the network to try to analyze it. Here too I would suggest that distributing the decision function could make it harder to subvert.

This is all pretty schematic, but if a private communicator like this were devised, our networked conversations might be able to again be private as they were years back when you just went out behind the barn to speak privately, and could be pretty well sure nobody else heard.

I think a world in which it is harder for your every move to be tracked will be harder for anyone to take over and will tempt people less who now think they can watch your speech and predict you might do something they dislike.

However please if anyone wants to discuss this, I would ask that priority be given to what technically can or cannot work, what actually might protect or what will fail and perhaps be a boon to eavesdroppers, how much stego is needed in here, or other such topics. I suspect there is enough technical savvy around now to build something along these lines (and having said so in public, I may be said to have let the only important cat out of the bag). Anyone want to add or detract?

(The foregoing is not un-holey and certainly not all that would be needed.)

Can people here propose something that is still better?

[Full-disclosure] Let's design a spy-proof communications infrastructure

Glenn Everhart

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>