All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Alternatives to encryption for securing open channels

Encryption is and has always been problematic for many different parties and reasons. But there are alternatives for securing open channels. The first step to understanding this is in understanding what encryption and the alternatives might achieve – or in other words, what is meant by “securing” these “open channels”.

Traffic crossing open channels

Open channels, for the purposes of this discussion, are communications media that can have traffic examined and injected by those with access. Not all channels are open to everyone, and this is an important aspect of protection. As an example, a local unencrypted WiFi connection can be surveilled (examined) by anyone who can receive the radio communications and decode them by turning the electromagnetic signals into meaningful bit sequences (i.e., understand the protocol). They can be injected by those who have a radio capable of causing reception to be heard and understood by the WiFi receivers. From across the World you cannot typically do this, so there are physical limits on who can do this based on the physical access to proximate spaces. Similarly, cable connections, DSL connections, and so forth are open to those with physical access to intervening physical infrastructure between sources and destinations.

The power of encryption and what it stems from

Encryption leverages mathematical properties of transformations on content to make it easy to observe and inject meaningful content by those possessing relevant 'keys' and hard(er) for those not having those keys to do the same thing. “Better” encryption is characterized, among other things, by the computational leverage gained by having the keys vs. not having them. If it is a billion times harder without the keys than with them, that's “better” than if it's only 100 times harder. At some point, the leverage is so high that encryption can only be circumvented in practice (i.e., by breaking into endpoints, causing key generation to be less effective, and/or exploiting other implementation weaknesses) rather than being directly attacked by finding ways to computationally compensate for the leverage.

The power of these methods are that they directly alter the content so that any copy of it anywhere is meaningless. For clarity, content, encryption, presence, absence, quantity, quality, timing, path, and other indicators may also inform. From an integrity perspective, altered or improperly effectively encrypted content tends to fail end-point integrity tests, and thus injection is normally defeated, even if channel capacity is reduced. Without encryption, the methods available are based on either (1) preventing access to the informative set of relevant content, or (2) preventing meaningful use of the content available. If all of the content transmitted can be observed and understood in context in time to meaningfully apply it, the open channel can be meaningfully observed and if timely injection of meaningful content can be undertaken, injection can defeat the integrity protection of the mechanism.

The notions of induction and suppression of signals to cause different behaviors by targets is the very definition of deception. In other words, encryption counters deception.

A few alternatives and how/why they work

"Horses for courses" describes the situation here. Depending on the situation particulars, different methods will be more or less effective in defeating deception. Starting at a basic level, deception (induction and suppression of signals to cause effects) is countered by not fooling yourself into belief of safety. Encryption does not make you safe and never has. Such methods are readily defeated by going around them (e.g., defeating endpoints and exploiting revealed information). Excessive trust in encryption is also self-deception and to be avoided. So even if you have and use encryption, reliance on it should be limited. The same is true of any other method you may apply. Recognize that anything can be defeated; there is no perfect protection. All of the alternatives, including encryption are only forms of leverage in a competitive/cooperative environment. Recognize the game you are in if you hope to win.

Preventing access to an/the informative set of information implies that what you wish to control is not everything always everywhere. Further, one person's information (i.e., treasure) is another person's data (i.e., trash). In principal, win-win can be achieved by giving them what they want while protecting what you want. Remember there may be many of "them" and they may want different things. The counter-intelligence question then comes down to what is important to protect and how do you protect it, and at least the first part of that is generally an issue of operations security (OPSEC) when it comes to operations.[1]

How to protect it and how well?

If you have done your OPSEC job reasonably well, you know what to protect, against whom, for how long, and why. Now come the strategies for protecting it – the it in this discussion being content in transit over open channels. Here are some basics:

- **Keep it away from them:** The content set to harm you may be harder to assemble if different parts of it are sent in different ways (careful for common mode failures), at different times, intermingled with other things, through different intermediaries, as part of different things.
  - **Example:** Send the User ID from Email address A to B and text the password from Cell number C to D. Since they need both to succeed unless they are all-seeing, they will not get enough to do harm. If they alter one in transit, you can try strategies to figure out which one they are attacking and then defeat them.
- **Make it hard(er) to understand:** Meaning is largely a function of context. Controlling the context may be used to effect the utility of the content.
  - **Example:** Q: Did you go to see the guy about the thing? A: He said it was in the place with the space. If you don't know the context, it's pretty meaningless, but if you do, you know just what to do next. Alteration is likely senseless →detected.
- **Reduce the time of utility:** Information is often less useful with less time to use it.
  - **Example:** Let's meet at the Starbucks across from Taylor hall in 10 minutes. Unless you are within 10 minutes of the target, you are at a distinct disadvantage. If the signal is altered, you won't meet, you will know something went wrong, and when you next meet, you may reasonably find out that the signal was altered.

1 See "Frauds, Spies, and Lies and How to Defeat Them" at http://all.net → Books for more details.

- **Don't inherently trust what you get:** Verify content through redundancy. This comes in many forms, over time, space, matching against reality, based on experience, etc.
  - **Example:** Saturday, December 27, 2015 does not exist. It's either Saturday or December 27, 2015 because they are different days. The redundancy provides a cross check on the content, and more complex cross-checks are readily available. Consistent alteration is far harder than single alteration, and it gets harder to do systematically with more diversity.
- **Adapt (change) over time:** If you do the same thing every day and every time, it's easier to watch and interfere.
  - **Example:** Set up a new email address in a few minutes and go with it. For whatever reason, events caused email outages between partners under a short deadline. They got new gmail accounts, used them for a few hours, and got it done.
- **Mix them all together:** These approaches tend to work reasonably well together.
  - **Example:** Every 6 hours, get a new gmail account and exchange it by sending a text to the throw away cell phones you use to communicate. Once a week, meet at a new location to exchange new cell numbers used for no more than 1 day each. Use texts to indicate locations based on mutual experience and in person determine the general area to be in so you can make the meeting place close.

I'm not a spy or a drug dealer – get serious

I know this methodology sounds like what drug dealers likely do these days to avoid the police, and I want to note that they do it successfully. It's similar to the tradecraft used since... for a long time, with dead drops and secret signs, and all of that cloak and dagger stuff, but updated to the modern era. Is it excessive for your needs? Only use it when you have to. Only use parts of it, and only the ones you think are required for the situation.

Were you looking for a more “corporate” solution? Don't! The very nature of a “corporate” solution is that, for the most part, it has to be manageable and controllable and observable by folks you don't know and only trust because the company says to. Lo and behold, insiders are responsible for ~75% of the harm in information-related attacks (historically) and many corporations, or portions thereof, are required by law (or by extra-legal means) to defeat the very protections that cryptography is/was designed to afford. And when company executives want to have confidential discussions regarding possible cybersecurity issues, they very often do so using personal cell phones to avoid the very insider-related threat their corporate solution had that they suspect may have produced the problem that is the reason they called.

Summary:

Tradecraft is the meat and potatoes (salad and vegetables?) of safe communications in open channels, and this has been true for as long as intelligence (i.e., spying) has existed. It is from ancient times and is used and works for the same reasons today as it was then. The technical means are different, but the realities are pretty much the same. Which is why we need human intelligence and not just technical measures to be effective in the World. And no, I am not helping the terrorists by telling you and them this. They already know this and they are already using it. Encryption and cyber security is being systematically weakened. If you want to protect yourself, you need to adapt to the changing realities of the cyber-world.

