Analysis of Arguments on Plaintext Features in US Encryption Products.

Michael Rafferty

December 6, 2000

In July of 1999 the director of the FBI gave a speech concerning encryption[1]. The speech focused on the need for law enforcement to be able to read communication, and how this is threatened by commercially available strong encryption. As a solution to this problem Mr. Freeh proposed a feature he referred to as a "Plain Text" feature. This feature would allow a law-enforcement agent with a search warrant to somehow recover the original plain-text used to generate encrypted data. Mr. Freeh's argued that such a feature was necessary for law-enforcement officers to do their job. He encouraged software companies making programs capable of encrypting information to provide a "Plain Text" feature. Mr. Freeh argued that these features do not harm either the individuals using the products or the corporations producing the product.

Several points were made in the speech in support of those claims. In this document I will analyze those points, and provide arguments against them. My arguments will establish that "Plain Text" features may be a threat to the viability of a product on the international market, to the security of the individual using a product, and to the reputation of American encryption programs. Mr. Freeh made several assumptions in his speech, this paper will analyze a couple of them and discuss what would happen if those assumptions were false. I make the assumption that if the good made possible by the "Plain Text" feature outweighs the harm that the feature would cause, then the feature should be implemented. I will demonstrate why in this case more harm than good would come of the system.

The most basic point in the speech was that for law enforcement to have the ability to access the plain text of encrypted data was good. If this is not true, then the entire speech is irrelevant, and "Plain Text" features should not be implemented because they do not provide any benefit. Argument on this issue revolves around the status of electronic communication; is electronic communication equivalent to a phone call, or equivalent to a USPS letter, or

does it fall somewhere in between those two extremes. If it is similar to a phone call then existing wire-tap laws suggest that the feature would be good. On the other hand, if it is equivalent to a letter then reading the communication in transit should not be allowed. Given existing laws and opinions on electronic surveillance it would seem that it is considered closer to a phone call. If that is accepted then allowing access to that feature would be good. The potential for good must now be weighed against the harm which the feature could cause.

Mr. Freeh now brings up several points against "Plain Text" features, and briefly argues against and dismisses each point. A few of his arguments do not support his dismissal of those points, and examination of these shortcomings will expose problems with the proposed feature. One of Mr. Freeh's assumption is that criminals and foreign governments will not be able to use the "Plain Text" system to spy on communication. How reasonable this assumption is depends on how the feature is implemented, and if the feature is known about. While there could be many ways to implement a "Plain Text" feature the commonly proposed systems all involve key escrow or a mathematical process which makes it easy to determine a decryption key. Key escrow systems make a central storage location which can be broken into. The other "Plain Text" feature implementation is a mathematical decoding process, that may be more difficult to figure out; however, if it is broken then it is much more difficult to recover from. Also the decoding process would be difficult to protect from discovery if someone trying to break the code has access to the encryption program. Other feature designs may be possible, but this covers the normal implementations of those features.

First I will address two of Mr. Freeh's arguments as they pertain to the profitability of the software, and the reputation of US software for not being subject to government interference.

The first argument against "Plain Text" features which is discussed is the impact of "Plain Text" features on the value provided by a program. Mr. Freeh claims that "Plain Text" features will not affect the value of US software. He states,

> "People who buy American software products don't make a purchase decision because of some embedded security feature in the products. They buy them for spreadsheets and all the other things that make them desirable." [1]

The problem with this statement is that it ignores encryption software, all of which are bought primarily because of superior encryption ability.

Mr. Freeh next addresses the claim that foreign countries are making encryption software would be unassailable by court orders by stating:

> "We know for a fact that encryption products made in many, many countries are unreliable—and you can rest assured that the police and security services in some of those countries have the ability, without a court order, to get into that particular product." [1]

This is certainly true, many countries do not produce reliable encryption products, and many countries already have the ability use similar features. However, this argument doesn't actually address the claim. Even if many countries don't have reliable encryption products, there are a couple that do. Also, there are many available encryption products which are developed by many people from several different countries; it is possible to examine to source of those programs and show that they are free from "Plain Text" features. For example Secure SHell (SSH), the current standard product for encrypting remote connections to a unix machine, is maintained by a company in Finland. [2]

Mr. Freeh's argument on this issue also brings up the issue of industry reputation. Mr. Freeh comments that other countries have this ability already, as a reason not to use their products; what he doesn't comment on is that most other countries will feel the same way about US law-enforcement having that ability. Right now US software is used internationally in part because foreign users are confident that the US government is not using the software to spy on them. Introducing "Plain Text" features will remove part of that certainty.

This issue of reputation could also seriously impact US software industry outside of encryption by raising awareness of the possibility for the US to use software to spy. Mr. Freeh assumes that no "Plain Text" feature will be used without a court order. This is quite possibly true, or at least it is probably nearly always true, and any other accesses will not be usable for anything that law-enforcement cares about. However, foreign governments will look at that ability and may assume that the US government is going to use the "Plain Text" feature to provide companies with a competitive edge. If that assumption is made the foreign governments will encourage companies in that country to develop software which would not carry that risk with it. Once that begins, the foreign companies would probably develop more software putting them in direct competition with several areas of the project.

Now that I have explored the possible effects of "Plain Text" features on US software companies, I will look at the effects that "Plain Text" features would have on US consumers using the system. Mr. Freeh claims that he is in favor of strong encryption to protect our trade secrets from the "23 countries that are actively using their external services to steal our trade secrets....[1]" The implication is that he believes that "Plain Text" features do not weaken encryption. Unfortunately, the purpose of a "Plain Text" feature is to create a way for a third party to decode encrypted data, without permission of one of the two parties involved. If the FBI was the only third party to be able to use the

feature this would be fine; however, no systems currently exist which supports that restriction without making it much easier for outside parties to break into the data. Also, if a "Plain Text" feature is created by applying some form of powerful encryption to the encrypted data, it will be possible, and depending on the use of the feature it may be worth it for a foreign power to spend the money to crack the "Plain Text" feature.

Also, Mr. Freeh assumes that the US products with the "Plain Text" feature will be used by the criminals that are being chased. While that will happen at least at first, the criminals will begin working with foreign encryption products, or those products which do not have the feature. I have already shown that at least some encryption products exist out of this country, many of which would be available over the Internet.

As I stated earlier it is likely that wide-scale creation of "Plain Text" features would cause a loss of foreign market share for US computer software companies. It would encourage foreign development of competition for local companies, as well as possibly encouraging US users to switch to non-US products to avoid the problems. It would encourage non-US companies to look on US products with distrust, and would weaken the encryption in use by US citizens, possibly allowing foreign governments to access documents. All these are potentially very severe problems caused by implementing "Plain Text" features; they work against Mr. Freeh's stated desire for ". . . a policy that allows American companies and consumers to use the strongest possible encryption. . . "[1]. Also, unless there is a remarkable effort to limit access to sites covering encryption, the people the FBI is trying to catch will just avoid using programs with the "Plain Text" feature. This will strongly limit the good caused by the system, especially over a long period of time. When compared to the problems listed earlier this paragraph, the potential damage to the security of product users, US company product sales, and US company reputation outweighs the limited,

and likely temporary, benefit caused by the availability of information.

References

[1] Freeh, Louis J *Encryption and Electronic Surveillance*, FBI Press Room — Director's Speeches. July 1999

[2] SSH web-page *SSH — Products* SSH Communications Security. 200