Shonak Nathwani CS133 Professional Skills Term 2

Critique

The article "Why Don't We Encrypt Our Email" was written by Stephen Farrell in January 2009. It was published the same month in the journal, "Practical Security" by the IEEE Educational Activities Department. The purpose of the article is to briefly inform readers about the different functionality in common Multi User Agents and the security related issues that are frequently ignored by users when using them. This critique will address the appropriateness of ideas and structure in the article.

Farrell's article assumes fairly strong technical competence of the reader in the field of computer security from the beginning of the article. This is showed through the immediate use of terms such as "Mail User Agents" and "Web-based mail client" (Farrell 2009, p.82).

In assessing the structure of the article, it is instantly surprising upon first look of the article, how seemingly long-winded it is to answer a relatively simple question. And for the most part, it is. There are many concepts that Farrell ploughs through to try and explain to the reader, many of which don't help in answering the question posed in the title. One example of this would be Farrell's divergence to explaining the two MUA integrated protocols, S/MIME and OpenPGP, and how these have not been incorporated mainstream MUA program operations. He doesn't entirely describe *why* the protocols "remain unused" (though he partly answers this under the following section), but *how* "these protocols are deployed" (Farrell 2009, p.83). Having said this, as the article goes on, he begins to input his own opinion, and takes a less technical stance, which helps him evaluate all of his ideas and helps him answer the question of the article.

Going back to the structure, as well as removing sections of the article that are irrelevant to the topic being discussed, Farrell could also have included a very concise glossary of the technical acronyms. Many of the technologies mentioned are abbreviated (e.g. MUA, MTA, PEM, MIME etc.), and even for a computer science professional new to this particular topic, it could be tiresome to traverse through the entire text to remind themselves of a definition - so a glossary would have been useful. Additionally, important quotes aren't highlighted frequently enough (only once, on page 3) and several images could have been included to show the different MUAs, for example. In adding these extra components, the article would have been more readable and easier to understand.

Farrell's language and writing style certainly deserves to be praised. He uses useful analogies to describe his point, such as when he says that mail encryption is "the difference between a postcard (most email) and a closed letter (encrypted mail)" (Farrell 2009, p.82). Also, the frequent use of rhetorical questions simplifies the points that Farrell is puts across. His final paragraph is a highly appropriate summary of his article, where his judgement adds great value to his points, especially the final, damming sentence, where he criticises MUA developers (such as Microsoft) for not incorporating users' encryption needs.

Many of the appropriate parts of the article are accurately referenced in the "References" section at the end. However, with the reference to the medical study on page 83, the study appears to have been undertaken at least 2 years before it was published. In this time, there could have been significant advances in the computing industry, particularly in the area of encryption. Indeed, in 2008 (after the medical study was carried out), Microsoft Office Outlook 2007 - Microsoft's MUA offering - benefited from a major update to its encryption, with the inclusion of encryption using configurable symmetry and cipher-block chaining (Oiaga 2008). Considering Outlook 2007 has a "75% - 80% market share in the corporate email market" (Greiner 2007), this could potentially skew the evidence that Farrell reported of people who could not "use the standard MUA security features" (Farrell 2009, p.83). The article could have featured more in depth studies with various expert opinions or organisations, for example from Mozilla with their MUA offering of Thunderbird. The reader being more aware of the stance of these software development companies in regards to email encryption should have been more of a priority for Farrell than discussing the technicalities behind encryption itself.

In summary, the article would successfully inform a computer security -enthusiast about the reasons for not sending encrypted email, and for the most part, information that Farrell has cited from other authors is up to date and based upon concrete computing theory. He explains many of the concepts of encryption with great detail, and uses numerous examples and analogies to put his point across. However, the article may be misleading to the casual reader in the sense that he article is too technically focused and its title does not reflect this. A more suitable title would be “Email: Why Our Software doesn’t Encrypt Our Messages”. And regardless of the target audience, the structure should have been more fragmented in order to captivate the readers with different styles of engagement. This is especially important as already it doesn’t appear that this article reaches out particul arly well to those who are less technically competent, due to the amount of technical jargon. In general, though, the article was an interesting read and offers a solid contribution to the field of computational research.