A Long, Slow Conversation

Jon Millen

Abstract

Cathy has always been an inspiration for me, because of the example she has set for quality in her research work, and more personally for her interest in my own attempts in the same area. In all her professional activities, I admire her humility, energy, constructive ideas, and commitment to serving the research community.

Cathy Meadows and I have had a long-time interest in symbolic methods for cryptographic protocol analysis. We were co-authors on one paper, along with Dick Kemmerer: Three systems for cryptographic protocol analysis, in *J. Cryptology* in 1994 [1]. That paper compared the NRL Protocol Analyzer, the Interrogator, and Inatest, the tool used by Kemmerer. As a bonus of that, I gained the Erdös number of 3, since Cathy was a 2. Since then, we have influenced one another over many years in another way, one which might be described as a long, thoughtful theoretical conversation. Here are three examples of that.

Cathy wrote a paper called "Using Narrowing in the Analysis of Key Management Protocols" in 1989 [2]. Narrowing is a form of term rewriting that allows substitutions for variables. Cathy realized its applicability for symbolic protocol analysis, in the NRL tool. I saw this as potentially useful in the Interrogator, which did something similar, but more *ad hoc*. I had been having a problem with search termination in the Interrogator at the time. Cathy's paper led me and a co-author at MITRE to write "Narrowing terminates for encryption" in 1996 [3]; this paper assured termination for my adjusted algorithm and rules.

Another example of how a paper by Cathy influenced my own work involved a connection between multilevel databases and survivability. Cathy's paper was "Extending the Brewer-Nash Model to a Multilevel Context" in 1990 [4], about the aggregation problem: combining data available at a low sensitivity level could sometimes lead to a higher-level result. The "NSA phone book" was a simple popular example of that - individual phone numbers were considered unclassified, but the book was classified. When aggregation is possible, security levels must be assigned to all sets of "datasets" (security-marked data objects), since one cannot assume that the maximum or lattice join of the individual levels will suffice. Cathy proved that there was a maximum flow policy between datasets that respected the given level assignments.

In a survivability context, I noticed an analogy between a set of datasets and a set of system components, such that the "security level" of a component set could be taken as the set of system services supported by those components. The current set of supported services should be preserved when the system is reconfigured by reallocating components to services, as a result of the failure of some components. This condition turned out to match the flow policy condition abstractly, so Cathy's result implied the existence of an optimal "Local reconfiguration policy" strategy in 1999 [5].

One more example, this one going in the opposite direction: I published a paper with a partial result that left a question open, and Cathy responded with a paper that answered the open question and extended the result. This was “On the freedom of decryption” in 2003 [6]. Some protocol analysis techniques modeled symbolic encryption without an explicit decryption operator. They assumed that decryption was not useful, even for an attacker, unless it was applied to an encrypted term, so that decryption was simply a matter of stripping off the encryption operator. This is not true in general – my paper had a counterexample – but it was a safe assumption as long as encryptions in the protocol were protected by combining the secret with a recognizable data item. This is normally done in real protocols. However, I could prove my result only for symmetric encryption, and left the public key case open. But then Cathy and Christopher Lynch came out with “On the Relative Soundness of the Free Algebra Model for Public Key Encryption” in 2005 [7], which wrapped up the result for public key protocols as well.

Everyone who does research would like to know that their results are read and appreciated by at least a few people, and even better, that they stimulated further thought and progress. In our long slow-motion tennis game of ideas, Cathy has always been an inspiration for me because of the example she has set for rigor and thoroughness in her research work, and more personally for her interest in my own attempts in the same area. It has also been my pleasure and privilege to have worked with her in other professional activities, where I admired her humility, her energy, her constructive ideas, and her commitment to serving the research community.

References

1. R. Kemmerer, C. Meadows, and J. Millen, Three systems for cryptographic protocol analysis, *J. Cryptology* 7(2), 1994, 79-130.
2. C. Meadows, Using Narrowing in the analysis of key management protocols, *IEEE Security and Privacy* 1989, 138-147.
3. J. Millen and H-P. Ko, Narrowing terminates for encryption, *IEEE Computer Security Foundations,* 1996.
4. C. Meadows, Extending the Brewer-Nash model to a multilevel context, *IEEE Security and Privacy,* 1990.
5. J. Millen, Local Reconfiguration Policies, *IEEE Security and Privacy,* 1999.
6. J. Millen, On the freedom of decryption. *Inf. Process. Lett.* 86(6), 2003, 329-333.
7. C. Lynch and C. Meadows, On the Relative Soundness of the Free Algebra Model for Public Key Encryption. *Electr. Notes Theor. Comput. Sci.* 125(1), 2005, 43-54.