Daryl Colquhoun has had careers as an academic and in IT. He was a long-serving member of the ASTC(NSW) committee and now works for Silverbrook, an industrial research company. He has a special interest in cryptography.

This is the first article in what we hope will become a regular column about security for technical writers.

Colquhoun's crypto corner

By Daryl Colquhoun

A few years back, we started receiving credit cards with a chip embedded in them, and at the same time each card has an associated personal identification number (PIN). Within the credit card machine, the card number and the PIN were encrypted so that when the machine communicated with the bank, it was supposed to be difficult to the point of being practically impossible for an eavesdropper to glean anything useful from the communication.

Let's analyse the security considerations behind this. Credit cards, as used in over-the-counter transactions, had always required a two-factor identification: you needed to possess something (the card) and you needed to know something. Formerly, the second factor had been 'how to write your signature' but this changed to a 4-digit number, which could easily be verified automatically, and more reliably than the old method where someone looked quickly at your written signature, or sometimes didn't even bother. Owing to the combination of chip and PIN, only you could use the card.

But a few years ago, a paper appeared called *Chip and Spin* by Ross Anderson et al of the Computer Laboratory at the University of Cambridge, in which the authors described a method by which someone could use the card without knowing the PIN! As described, it's a bit clunky, but it works. That is, it works when executed by a small group of academics. Have any criminals cottoned on to it? We don't know.

Here's one more anecdote. On 17 February 2012, the Networkworld website published an article about attacks on the RSA cryptosystem. (The RSA cryptosystem is behind the secure communications techniques used by many, many businesses for online transactions.) Networkworld said, "A group of prominent researchers published a paper blasting it [RSA] as woefully insecure". Is this true? No, not exactly. A group of prominent researchers, headed by the very prominent Arjen Lenstra, did publish a paper about RSA. It has the odd-sounding title *Ron is wrong, Whit is right* (alluding to Ron Rivest and Whitfield Diffie, big names in cryptography).

What the researchers did was, in fact, a lot of donkey work. They downloaded keys from millions of businesses and found interesting mathematical relationships between some of them. This means that if your bank uses one of the 'interesting' ones, it is possible for some attacker to tap the communications line and listen in ... and learn your password.

But this can occur only if your bank uses one of those bad keys. I don't think this makes the cryptosystem 'woefully insecure'; what it means is that some people have not implemented it as carefully as they should have.

What does this have to do with technical writers? We have bank accounts and are concerned to keep our transactions secure and private. Also, we read news websites and it's good to keep what they say in perspective. In the case of Lenstra et al, you don't need to read the original technical paper, which is heavy going. You can get to the bottom of it all if you read the detail in the website and the links, but a bit of background is useful. We technical writers do sometimes need to send information securely, as for example when we want to email a confidential document. If we do email such a document, we need to be sure that, for example, none of our company's IT people can read it. And lastly, sometimes we work on the design of websites that need to be secure.

So this column will help you learn a bit about how information can be secured, and I hope you will join me.