# *Response: Independent One-Time Passwords*

*Aviel D. Rubin*
*Bellcore*

It is understandable that Security Dynamics is sensitive to any article that is critical of their SecurID card. After all, their success is based on their customers' confidence that their one-time password scheme is unbreakable. Thus, it appears to me that they read my article in *Computing Systems* with an overly-sensitive eye and misunderstood some of it. In this response, I will try to clarify some issues and address their objections.

The first objection is to my statement that "One way to defeat SecurID is to break the secret algorithm to predict the next number that will be displayed." Security Dynamics claims that this makes it sound as if it is easy to do this. It was not my intention to imply that this was easy. The two sentences preceding the quoted one state: "There are several strategies for breaking SecurID. The product is sold on the premise that these are infeasible." Whether or not breaking SecurID is feasible is a matter of faith. It is widely accepted in the security and cryptography communities that the only way to trust a cryptographic algorithm is to publish it and subject it to the scrutiny of the entire community. Otherwise, belief in the strength of the algorithm reduces to belief in the statements of the algorithm designer. The algorithm used by SecurID is not public.

I am not implying that SecurID is easy to break. Rather, I am simply stating that the only reason we have to believe that it is difficult to break is that Security Dynamics claims it.

I applaud the use of the PINPAD token, which hides the user's PIN when logging in from a remote site. However, I am confused by a statement earlier in that paragraph that states "All authentication transactions between protected clients and the ACE/ Server are encrypted..." If the transactions are encrypted, then that means that a secure channel exists between the clients and the servers. So what is the point of using SecurID at all? If encryption can be used to hide the PIN, then it seems that the same keys can be used for authentication, obviating the need for any SecurID.

The criticisms of my OTP scheme are valid, and these weaknesses are mentioned in my original article. I hope that I have clarified the misunderstandings that Security Dynamics had of my *Computing Systems* article.