Controversy

Rejoinder: Independent One-Time Passwords

John Adams
Security Dynamics

In order for *Computing Systems* to remain a "Quarterly dedicated to the analysis and understanding of advanced computing systems," it is necessary to make the following clarification regarding an article in the Winter 1996 issue (Volume 9, Number 1). The article in question was entitled "Independent One-Time Passwords," and authored by Aviel D. Rubin of Bellcore.

In this article, Rubin compares two dissimilar technologies used to create one-time passwords. One product, which comes from Rubin's own Bellcore, is the S/KEY software authentication system. The other product is the SecurID token from Security Dynamics.

Rubin is misleading when he states that "One way to defeat it [SecurID] is to break the secret algorithm to predict the next number that will be displayed" [p. 17]. This makes it sound as if simply knowing the algorithm and observing a few displayed numbers allows an attacker to predict the next number. This is not the case; predicting the sequence of numbers for a given token requires knowledge of both the algorithm and the token's unique, 64-bit, seed number, which is contained in protected storage on the token.

Attacking the SecurID algorithm without knowledge of the secret seed value seems implausible. The algorithm has been analyzed by several noted cryptanalysts and they have discovered no such attack. They also estimate that such an attack, if possible, would require observation of a sequence of many thousands, if not millions, of displayed numbers. Given that the typical token only displays one number per minute, no attacker will plausibly have access to such a large sequence.

Secondly, Rubin states that an attacker can obtain the user's PIN by eavesdropping on an authentication session, and that the PIN is "sent in the clear each time." All authentication transactions between protected clients and the ACE/Server are encrypted, so eavesdropping provides no useful information. For remote-access environments, where the user is connecting to the protected client via an unsecured line, we have recommended the use of our PINPAD token, where the PIN is entered into the token and combined with the displayed value. The combined value is then transmitted over the line, again providing no useful information to an attacker.

These incorrect statements strongly dilute the whole discussion of SecurID technology.

More of Rubin's points need to be clarified as well. While the one-time password system described in Rubin's article is based on sound technology, and makes some significant improvements on the popular S/KEY system, two significant weaknesses remain: the system provides only single-factor authentication, and the single factor must be put in a form that is easily copied. The OTP system derives its one-time-passwords, in cryptographic fashion, from a secret key value. Knowledge of a user's secret key, however obtained, compromises that user. In addition, the one-time passwords are distributed in the form of a printed booklet. If the booklet is left unattended for any length of time, it may be copied by anyone with access to a copier.

SecurID is significantly stronger than the OTP system on both these counts. The user must enter a memorized PIN, in addition to the value displayed on the token. If a token is lost or stolen, any unauthorized person will have only three chances to guess the correct PIN, after three failures, the token is automatically disabled by the ACE/Server. The token itself is secure hardware, it cannot be copied or reverse engineered.

In conclusion, while the independent OTP system described by Rubin provides protection against simple password sniffing, it does not provide the strong, two-factor authentication of SecurID technology.

Again, I feel that it is important that these clarifications be made, not only to honor the efficacy of SecurID technology, but to defend *Computing Systems*' integrity and desire for informative, unbiased and fully researched contributions.