# The Evolving Meaning of Information Security

Whitfield Diffie
Stanford University

## ABSTRACT

When you are developing security systems, new penetration techniques seem to appear as responses to new security measures but in general the flow is the other way around: security exists and evolves because of the evolution of threats. Beginning with the rise of radio in the 20th Century attacks on communication networks have shown two forms: those that go for the big kill --- such as the breaking of Enigma --- and those that assemble small seemingly innocuous leaks of information into a comprehensive understanding of the target's behavior.

We will analyze the way in which these trends interact with others to create a situation in which what is possible in security and even the meaning of security in communication networks needs reexamination.

## Keywords

Information Security; Communication Security; Security Systems

## Bio

Whitfield Diffie best known for his 1975 discovery of the concept of public key cryptography, developed jointly with Martin Hellman, which revolutionized not only cryptography but also the cryptographic community and now underlies the security of internet commerce. This work was recognized in 1992 with a Doctorate in Technical Sciences (Honoris Causa) for the creation of a new field of science by the Swiss Federal Institute of Technology in 1992.

During the 1980s, Diffie served as manager of secure systems research at Bell-Northern Research, laboratory of the Canadian telephone system. In 1991, he joined Sun Microsystems as distinguished engineer and remained as Sun fellow and chief security officer until the spring of 2009.

Diffie spent the 1990s working to protect the individual and business right to use cryptography, for which he argues in the book Privacy on the Line, the Politics of Wiretapping and Encryption, written jointly with his Sun colleague Susan Landau. Diffie's role in this policy battle is extensively covered in Steven Levy's book Crypto.

As well as being a winner of the Turing Award, together with Martin Hellman, Diffie has won the ACM Paris Kanellakis Award, the IEEE Hamming Prize, and the Franklin Institute Levy Prize. He is a fellow of the Marconi Society, the International Association for Cryptologic Research, and the Computer History Museum. Diffie is an inductee of the National Inventors Hall of Fame and is particularly proud of receiving the National Computer Systems Security Award, given jointly by NIST and NSA.

Diffie is currently holds the position of consulting scholar at the Center for International Security and Cooperation at Stanford University and is on the advisory boards of a number of startups. His principal interest is the history of cryptography. Along with James Reeds and J.V. Field, he is the editor of Breaking Teleprinter Ciphers at Bletchley Park, an extensively annotated historical edition of the final report of the Newmanry, the group that attacked German systems above the level of Enigma.


*KDD '16, August 13-17, 2016, San Francisco, CA, USA*
ACM 978-1-4503-4232-2/16/08.
http://dx.doi.org/10.1145/2939672.2949031