



THE 1997 RSA DATA SECURITY CONFERENCE

SPEAKER BIOGRAPHY

DEVELOPERS' TRACK

Cryptography's Future: Opportunities and Threats

Speaker: **Bruce Schneier**

President Counterpane Systems

101 E.Minnehaha Parkway

Minneapolis, MN 55419

Phone: 612-823-1098

Fax: 612-823-1590

Email: schneier@counterpane.com

Company Background: Counterpane Systems is a virtual company, with two full-time employees and six part-time contractors. Counterpane provides expert consulting in design and analysis, implementation and testing, threat modeling, product research, training, and intellectual property. Clients include Canon, Compaq, Disney, Hughes Data Systems, Intel, Intuit, MCI, Merrill Lynch, Microsoft, Mitsubishi, National Semiconductor, Netscape, Oracle, Silicon Graphics, Stac Electronics, and Xerox. Contracts range from short-term expert opinions and design evaluations to multi-year design and development efforts. More information can be found at <http://www.counterpane.com/>.

Presentation Overview:

From encryption to digital signatures to electronic commerce to secure voting--cryptography will change the world. It is the enabling technology that allows us to take existing business and social constructs and move them to computer networks. In this presentation, Mr. Schneier will take a look at the future of cryptography: how it works in practice, where the business opportunities are, and where the risks are. This overview will be invaluable to anyone making decisions about cryptography.

Speaker Background:

Bruce Schneier is president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. He has worked for hundreds of clients on five continents, in such areas as computer hardware and software, commerce, communications, and entertainment. Mr. Schneier is the author of *Applied Cryptography* (John Wiley & Sons, 1994 & 1996), the seminal work in its field that has sold over 50,000 copies. His papers have appeared at international conferences, and he has written dozens of articles on cryptography for major magazines. He designed the Blowfish encryption algorithm, still unbroken after years of cryptanalysis.

PRESENTATION