Schneier on Security

Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure

C. Ellison and B. Schneier

Computer Security Journal, v 16, n 1, 2000, pp. 1-7.

Public-key infrastructure has been oversold as the answer to many network security problems. We discuss the problems that PKI doesn't solve, and that PKI vendors don't like to mention.

[PDF (Acrobat)] [plaintext]

Categories: Miscellaneous Papers

← Protecting Secret Keys with Personal Entropy

A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish →

Sidebar photo of Bruce Schneier by Joe MacInnis.

Search

Powered by DuckDuckGo

Go

Blog Essays Whole site

Subscribe

About Bruce Schneier

https://www.schneier.com/academic/archives/2000/01/ten_risks_of_pki_wha.html

CRYPTOGRAPHY

Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure

By Carl Ellison and Bruce Schneier

Computer Security Journal • Volume XVI, Number 1, 2000

Risk #1: “Who do we trust, and for what?”
Risk #2: “Who is using my key?”
Risk #3: “How secure is the verifying computer?”
Risk #4: “Which John Robinson is he?”
Risk #5: “Is the CA an authority?”
Risk #6: “Is the user part of the security design?”
Risk #7: “Was it one CA or a CA plus a Registration Authority?”
Risk #8: “How did the CA identify the certificate holder?”
Risk #9: “How secure are the certificate practices?”
Risk #10: “Why are we using the CA process, anyway?”

Critique

Response To "Ten Risks Of PKI" by Aram Perez
https://sites.google.com/site/aramperez/home/10-risks-of-pki