An Alternate View of the World: If We Didn't Dodge the Bullet

C Matthew Curtin, CISSP
Interhack Corporation

If not for a series of events in 1996-1999, identity theft would be a much bigger problem than it is today.

Preventing Identity Theft Today

- Exposure is most common threat
  - – Lost tape
  - – Application that leaks data
- Simple to mitigate with cryptography
  - – Data exposure isn't necessarily breach
  - – Codified into regulation today
    - e.g., HIPAA Security Rule
    - e.g., Payment Card Industry Data Security Standard

Cryptography, One Decade Ago

- Interntional Tarrifs in Arms Regulation (ITAR)
- Cryptography considered a munition
- Export of American products limited to 40-bit; special exception for 56-bit
- Federal standard, DES, 19 years old
- Height of the Crypto Wars

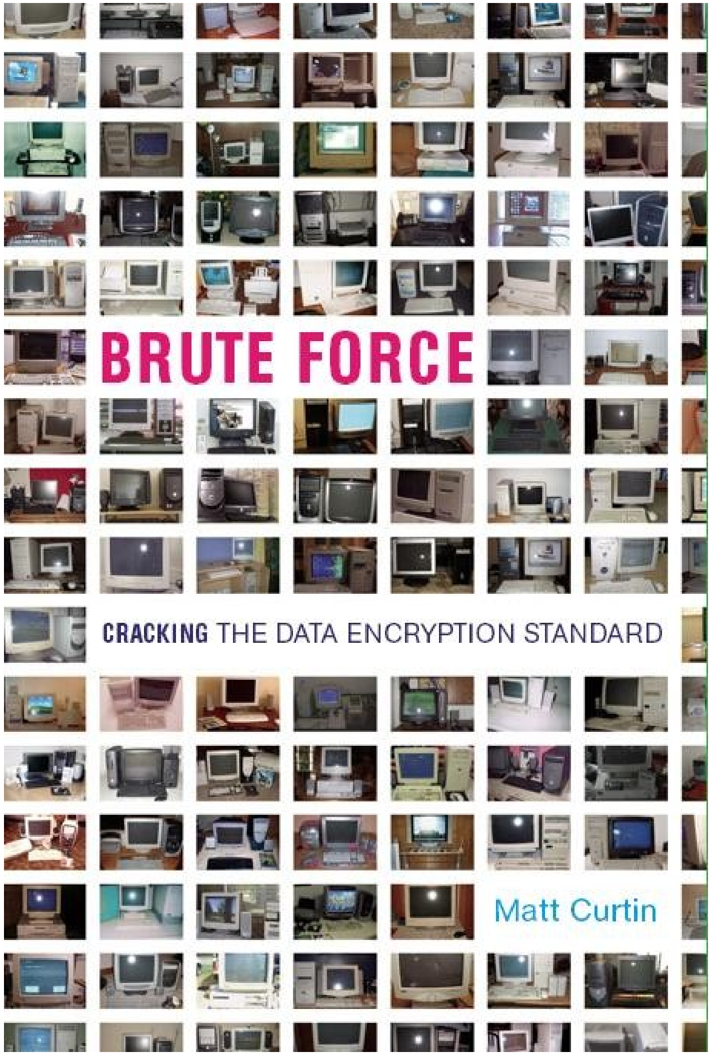
“DES Is Secure Enough”

- DOJ testified to Congress
  - 56-bit message will take a $30MM supercomputer 1 year, 87 days.
- RSA DES Challenges
  - Jun 1997, DES message cracked in 140 days
  - Feb 1998, DES message cracked in 39 days
  - July 1998, DES message cracked in 56 hours
  - Jan 1999, DES message cracked in 22 hours

Bizarro-Today

- Cryptography a “dual-use” product, still subject to limits
- Only viable market concentrated around 56-bit DES?
- Cracking DES keys with a network of PCs would take about five hours
- Our most viable protection would be no real protection at all

For More Information



- *Brute Force: Cracking the Data Encryption Standard* (Copernicus Books, 2005)