Drive Encryption

Jason A. Lord, COO
d3 Services, Ltd.
www.WeAreCyber.com

Jason Lord

- COO at d3 Services, Ltd.
- 15 years in Forensics, IR and RE work
- Electrical Engineer by education
- Specialize in Cryptoforensics
- Previously with Symantec, Guidance Software, NGIT TASC and United States Marine Corps

Question

- Does drive encryption create a problem or just another thing to master getting around?
  - Security Answer
  - Forensics Answer

Strength in Encryption

- Single encryption algorithm, i.e., PGP
  - AES 256 key = 10^36
- Multiple encryption algorithm, i.e., TrueCrypt
  - AES, Serpent and TwoFish or combinations (128b keys)

Algorithm	Designer(s)	Key Size (Bits)	Block Size (Bits)	Mode of Operation
AES	J. Daemen, V. Rijmen	256	128	XTS
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	XTS
Twofish	J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, B. Schneier	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpent		256; 256; 256	128	XTS
Serpent-AES		256; 256	128	XTS
Serpent-Twofish-AES		256; 256; 256	128	XTS
Twofish-Serpent		256; 256	128	XTS

Weaknesses of Encryption

- Users
  - Sticky notes
  - USB keys
- Passwords
  - R3dkin1 --- really?
- Programs
  - Poor programing
  - Proper implementation

Probability

- Technology and programing are making it more difficult to conduct Digital Forensics
- Users typically save passwords or leave breadcrumbs, hints or photos
- RNGs provide passwords too difficult for typical users to memorize
- Sallie Mae vs Grandma Sally: Who is using drive encryption?
- Password recovery aids in drive encyption recovery (OS, IM, webmail, doc, zip, etc)

CONTACT INFO:

Jason A. Lord

jason.lord@d3-services.com

703-505-2524

www.WeAreCyber.com