Group Discussion Written Project

Is GIAC Enterprises' cryptography strong enough to protect our information?

Robert Comella, Brough Davis

June 6, 2010

Objective

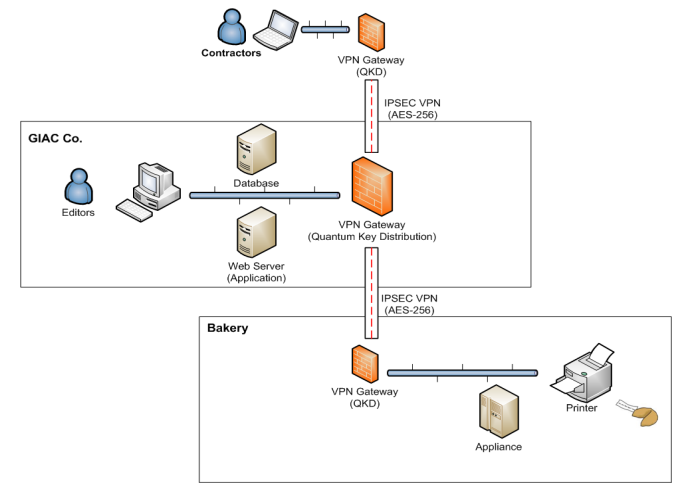
1. Is AES safe for GIAC's most proprietary and sensitive information?

2. Create a high level plan for the role of cryptography in the protection of GIAC information over the next five years. The key to success will be processes that allow GIAC to continue its successful and growing business.

Assumptions

- Malware Concern - All Local Data is Vulnerable
- HTTP Web Application (not SSL)
- Encryption - IPSEC VPN tunnels
  - AES-256
  - Quantum Key Exchange
- VPN L2L (lan-to-lan) tunnel between
  - contractors and corporate network
  - corporate network and remote bakeries

GIAC - Fortune Cookie Network



Quantum Key Exchange

Issues:
- New Protocol for QKD (BB84). Only 2 know commercial vendors that offer VPN QKD appliances
- Researcher finds loophole in implementations using 20% error buffer to hide inspection-replay attack

Recommendations:
- Probability of attack is low from large risk/expense to attacker
- Consider IKE/ISAKMP (Main Mode) implementation for key exchange
- Periodic Vendor Reviews for QKD implementation updates to reduce error margin. (reduce attacker hiding places)

AES-256

Issues:
- AES-256 becoming easier to crack (2^119 versus AES-192 at 2^176 and AES-128 at 2^128)
- AES-256 is broken...yet attack is still not realistic

Recommendations:
- Use AES-192 if optional
- Change keys more often (default devices are 24 hours

5 Year Plan

- Periodic (Quarterly) Vendor Review
  - AES-192 and/or Faster Key Exchange Lifetimes
  - QKD Error Margin Improvement or IKE/ISAKMP switch
- Defense in Depth
  - Consider integrating SSL/SSH into the Application between contractor-database and database-bakery appliance
  - Locking down Contractor Access with virtual appliance for VPN auth and web access/vulnerability