Key Management

Cryptography ThreeA

Ed Crowley

Fall ‘08

Topics

- Key Management
- Key Distribution Centers

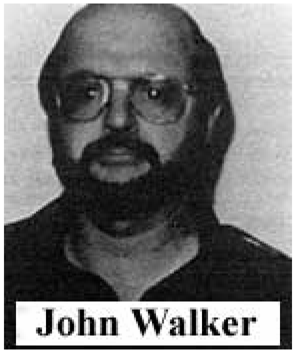
Focus

- Key Management Overview
- Key Management
- Automated Key Management
- Secret Keys

Key Management Overview

- Keys are analogous to the combination of a safe.
  - If combination becomes known, the safe provides no security.
  - Poor key management may easily compromise strong algorithms.
- Cryptographic security directly depends on:
  - Key strength
  - Effectiveness of associated mechanisms and protocols
  - Protection afforded to the keys.

Key Protection



Keys need to be protected against:

- Unauthorized modification
- Unauthorized disclosure
- Theft
- Loss
- Destruction
- Insecure storage
- Unauthorized copying

**See John Walker spy case at:*

http://www.fas.org/irp/eprint/heath.pdf

Symmetric Key Management Scaling

- Does not scale well.
  - A system with N users requires N(N-1)/2, number of keys
  - For example for a business to have a pair of secret keys for an office in each of the 50 states would require more than1,200 keys… (CD p.71)

Key Management

- Key management provides foundation for secure key:
  - Generation
  - Storage
  - Distribution
  - Destruction
- Refers to the establishment of cryptographic keying material to provide protocol security services, especially integrity, authentication, and confidentiality.

Automated Key Management

- Derives one or more short-term session keys.
  - Key derivation function may make use of long-term keys to incorporate authentication into the process.
  - Manner in which this long-term key is distributed to the peers and the type of key used is part of the overall key management solution.
- Manual key management can also be used to distribute long-term session keys.

Automated Key Management Technique

- Confirms the liveness of the peer and protects against replay
- Ensures that a fresh short-term session key is generated.
- Can improve interoperability by including negotiation mechanisms for cryptographic algorithms.
- Examples of automated key management systems include:
  - IPsec
  - IKE
  - Kerberos
- S/MIME and SSL/TLS also include automated key management functions

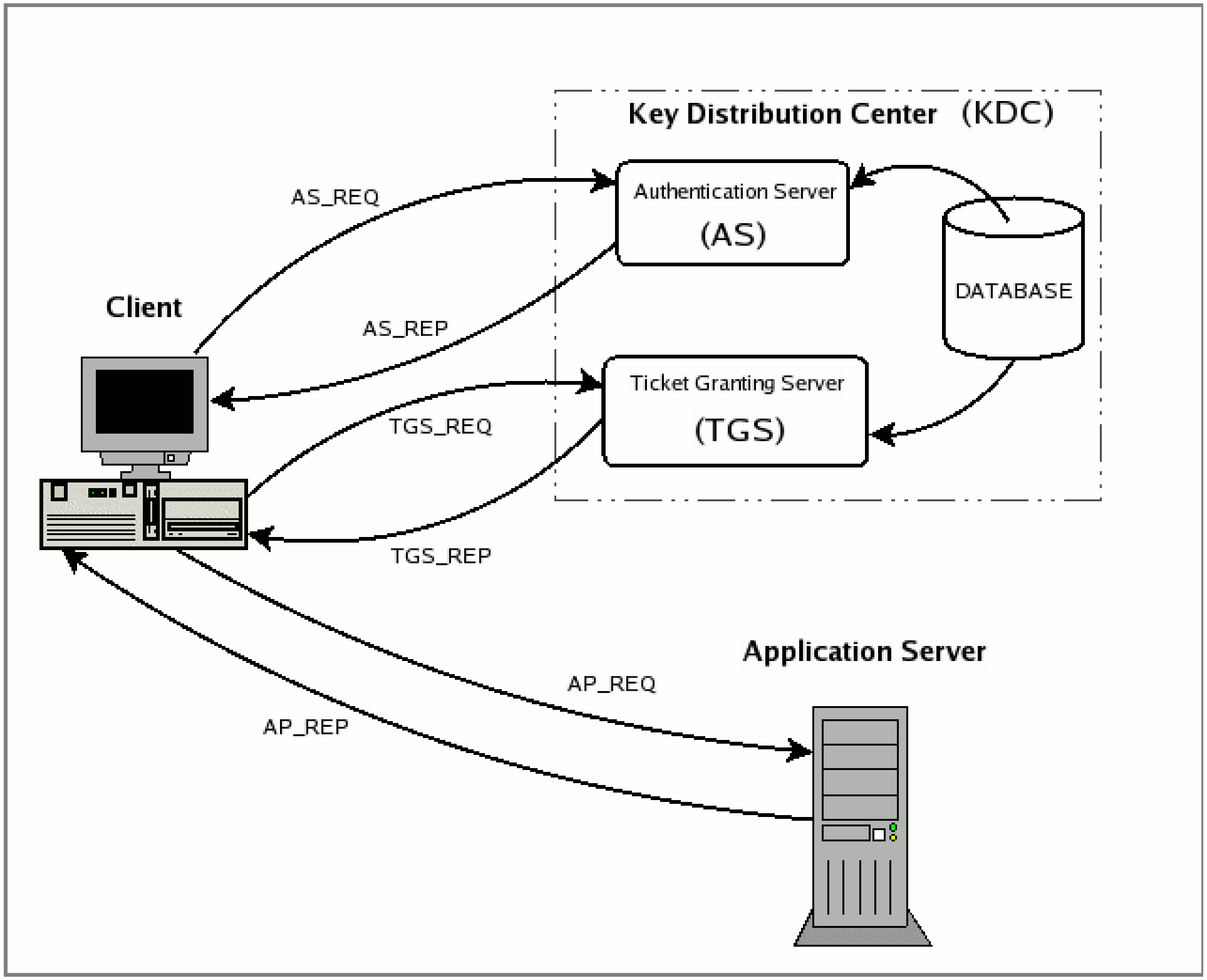
Symmetric Key Management Challenges

- Only works by prearrangement.
  - Cipthertext recipient must already have key.
- Key distribution/management challenges include:
  - How to deliver key to recipient without it being intercepted?
  - If two people have the key and it is compromised, whom is responsible?
  - If key is lost, cipher text cannot be recovered.
- Distribution problems can be dealt with through a trusted third party or a key distribution center (KDC)
  - Normally, KDCs operate with secret keys
  - For example, Kerberos employs a KDC

Symmetric Key Problem: Distribution

- Key distribution is a significant challenge
  - Only trusted parties should possess keys…
  - While secret keys can be distributed through a key distribution center (KDC), the KDC becomes a bottle neck and an attractive target
- Since they are shared, secret keys can’t provide nonrepudiation

Kerberos KDC Operation



Key Management Uses and Applications

- Policy Enforcement
- Separation of roles and duties
- Resisting repudiation
- Compensation for algorithm limitations
- Increases cost of attack and reduces value of success by frequent change (increasing effective key-length)

Key Management

- NIST’s Special Publication SP 900-57, Recommendation for Key Management at:

http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf

- IETF’s, RFC 42017, Guidelines for Cryptographic Key Management at:

http://www.rfc-editor.org/rfc/rfc4107.txt

Questions?

References One:

http://cis.gsu.edu/~rbaskerv/cis8680/Lessons/crypto/index.html

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/

http://www-106.ibm.com/developerworks/library/s-pads.html

http://www.math.temple.edu/~renault/cryptology/affine.html

References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.mspx

http://www.fas.org/irp/nsa/rainbow.htm

Appendix

- Who am I?

Who am I?

- Developed four, three credit hour, graduate level UH Security Courses
- Past Security Presentations at: University of Indiana in Pennsylvania's Network Security Workshop, Infragard, ISACA, ACM SIGITE, and American Association for Engineering Education
- Created/presented workshops at the New Jersey Institute of Technology and Sam Houston State University.
- Earned CISSP, NSA IAM & IEM, Security Certifications
  - Usual certifications from usual suspects (Cisco, CompTIA, Novell, and Microsoft).
- Former Network Admin and IS Director
- Graduate Military Police Academy
  - USARPAC German Shepard Sentry Dog School
  - Secret Clearance (expired)