Thursday

1

Sources

- "Divertible protocols and atomic proxy cryptography" by M. Blaze, G. Bleumer, and M. Strauss. EUROCRYPT '98.
- "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage" by G. Ateniese, K. Fu, M. Green, and S. Hohenberger
- "Identity-Based Proxy Re-encryption" by M. Green and G. Ateniese

2

Credits

- Kevin Fu (~~MIT~~ UMass)
- Matt Green (JHU)
- Susan Hohenberger (~~MIT~~ JHU)



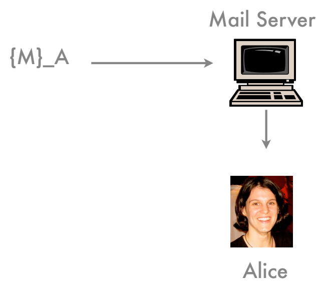
3

First Translations

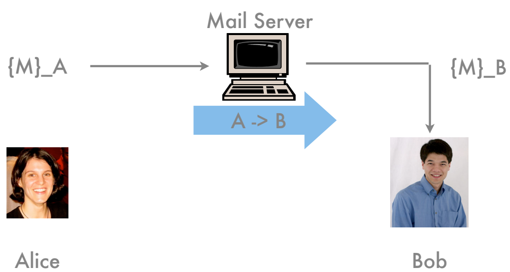
Susan => Alice
Kevin => Bob
Matt => Charles

4

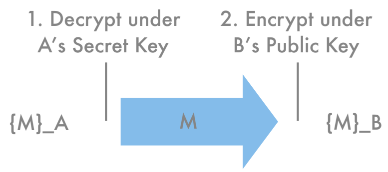
PRE: An Example



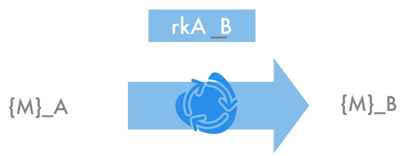
5



6



7



1. Plaintext NOT revealed
2. rk_A->B does not reveal secrets

8

PRE and RFIDs

- The RFID stores encrypted data
- Encryption can be read by A
- The reader transforms the encryption for A into one for Bob
- This effectively addresses the revocation problem in RFIDs

9

Blaze, Bleumer and Strauss

Alice: $SK = a, PK = g^a$	Bob: $SK = b, PK = g^b$

$$\{M\}_A = Mg^r, g^{ra}$$

$b/a \bmod q$

$$\{M\}_B = Mg^r, g^{rb}$$

10

- Bidirectional
- Requires interactive proxy-key generation (both Alice and Bob must provide their secrets)
- Secret key leaked by colluding with the proxy
- Transitivity (from A->B, B->C the proxy can compute A->C)

11

A Simple PRE Scheme (1)

Alice: $SK = a, PK = g^a$	Bob: $SK = b, PK = g^b$	
$e() : G_1 x G_1 \rightarrow G_2$	$Z = e(g, g)$	$M \in G_2$

$$\{M\}_A^1 = MZ^k, Z^{ka}$$

12

A Simple PRE Scheme (2)

$$\{M\}_A^2 = MZ^k, g^{ka}$$

$$g^{b/a} \in G_1$$

$$\{M\}_B^2 = MZ^k, Z^{kb} = e(g^{ka}, g^{b/a})$$

13

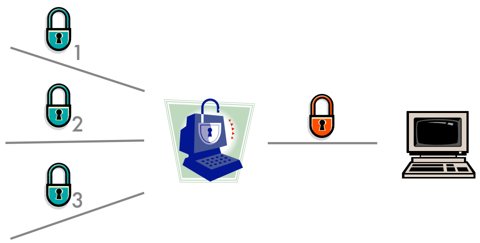
VPNs

14

Old Key <> New Key

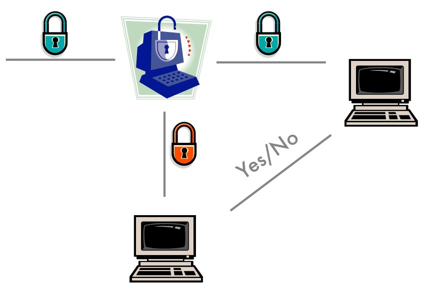
15

Key Management



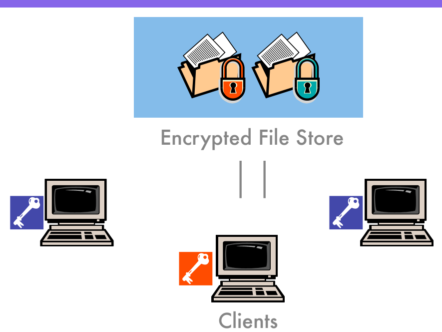
16

Spam of Encrypted Data



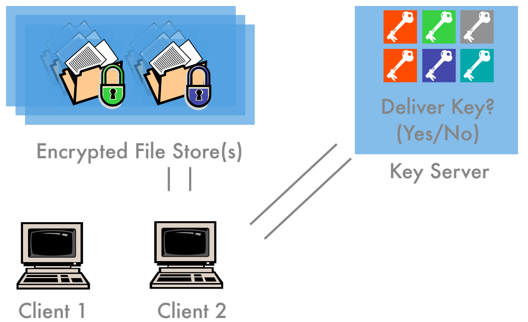
17

Encrypted File Storage



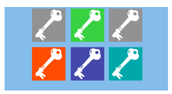
18

Using a Key Server



19

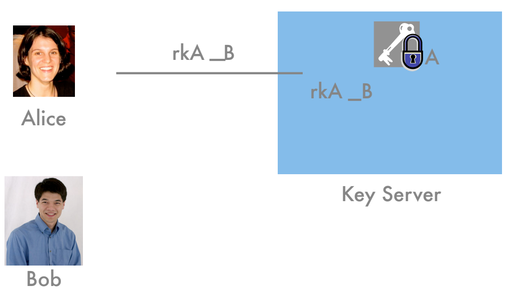
Disadvantages



- Online server is vulnerable
- Content owner must trust Key Server
- Server operator has complete access to keys

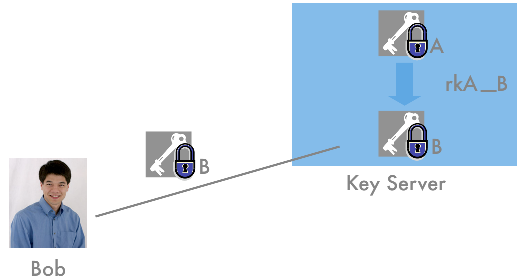
20

Sharing with New Users



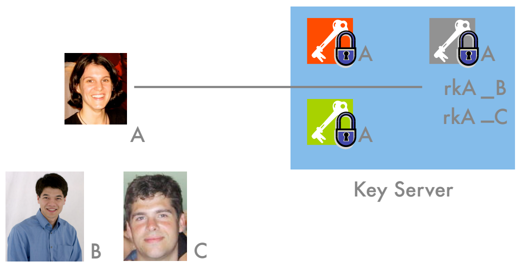
21

Proxy Key Distribution



22

Alice as Group Manager



23

Performance

- Computed on a 2.8Ghz Pentium IV
- 512-bit super-singular curve
- Miracl Library

Encryption	Re-encryption	Final Decryption
7.7ms	21.7ms	3.4ms

24

Implementation

- Built on Chefs Networked file system
  - Confidential version of SFSRO
  - 128-bit AES encryption
- Dual-purposed file and key server
- Tested performance while compiling EMACS

25

ID-based Schemes

- Encrypt under "alice@company.com"
- Specify attributes, like "Alice | | Security Clearance | | Oct 2011"
- Trusted party

26

ID-based PRE

$$(C_1, C_2) = (g^r, e(g^s, H_1(\text{"A"})^r) \cdot M)$$

$$rk_1 = h / H_1(\text{"A"})^s$$
$$rk_2 = \text{Encrypt}(\text{"B"}, h)$$

Proxy

Re-encryption:

$$C_1' = C_1 = g^r$$
$$C_2' = C_2 \cdot e(C_1, rk_1) = e(g^r, h) \cdot M$$
$$C_3' = rk_2 = \text{Encrypt}(\text{"B"}, h)$$

27

Re-encrypting multiple times

$C'_1 = C_1 = g^r$

$C'_2 = C_2 \cdot e(C_1, rk_1) = e(g^r, h) \cdot M$

$C'_3 = rk_2 =$ Encrypt(“B”, h)

Given another re-encryption key $rk_{B\text{->}C}$, we can encrypt this last ciphertext again

28

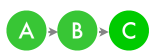
Re-encrypting multiple times

$C'_1 = C_1 = g^r$

$C'_2 = C_2 \cdot e(C_1, rk_1) = e(g^r, h) \cdot M$

$C'_3 = rk_2 =$ Encrypt(“B”, h)

$\bar{C}_1 \ \bar{C}_2 \ \bar{C}_3$



Given another re-encryption key $rk_{B\text{->}C}$, we can encrypt this last ciphertext again

29

Open Problems

- New applications and more efficient schemes
- Remove random oracles for id-based schemes and unidirectional ones
- Multi-use unidirectional schemes with no expansion
- Generalize the concept

30