Homework #7

Problem 1: Show a man-in-the-middle attack

① $A \rightarrow S : A, B, N_a$
② $S \rightarrow A : A, B, \{A, N_a, K_{ab}\}K_a, \{B, N_a, K_{ab}\}K_b$
③ $A \rightarrow B : A, B, \{B, N_a, K_{ab}\}K_b$

Solution

Prerequisites:

① Let A, B, M be registered users with trusted server S:
- A = Alice
- B = Bob
- M = Man-in-Middle
- S = Server

② Assume M can intercept and modify communication between A, B, S; but cannot decrypt tickets with secret keys between $A \rightarrow S$ and $B \rightarrow S$.

Phase 1: M obtains a shared key with A, while A thinks it has shared key with B.

① A requests shared key with B:

$A \rightarrow S : \{A, B, N_a\}$

② M intercepts request, modifies, then forwards to S:

$A \rightarrow M : \{A, B, N_a\}$

$M \rightarrow S : \{A, M, N_a\}$

(next page)

③ S responds to M with shared key:

$S \rightarrow M : A, M, \{A, N_a, K_{am}\}K_a, \{M, N_a, K_{am}\}K_m$

④ M modifies identity to A, then forwards to A:

$M \rightarrow A : A, B, \{A, N_a, K_{am}\}K_a, \{M, N_a, K_{am}\}K_m$

Note 1: A can verify $\{A, N_a, K_{am}\}K_a$ is accurate.

Note 2: A cannot verify $\{M, N_a, K_{am}\}K_m$ to know identity has been changed to M.

Note 3: M now has shared key with A (K_{am}) while A thinks it has shared key with B.

Phase 2: M obtains shared key with B, while B thinks it has shared key with A.

① B requests shared key with A:

$B \rightarrow S : \{B, A, N_b\}$

② M intercepts request, modifies, then forwards to S:

$B \rightarrow M : \{B, A, N_b\}$

$M \rightarrow S : \{B, M, N_b\}$

③ S responds to M with shared key:

$S \rightarrow M : B, M, \{B, N_b, K_{bm}\}K_b, \{M, N_b, K_{bm}\}K_m$

(next page)

④ M modifies identity to B, then forwards to B:

$M \rightarrow B : B, A, \{B, N_b, K_{bm}\}K_b, \{M, N_b, K_{bm}\}K_m$

Note 1: B can verify $\{B, N_b, K_{bm}\}K_b$ is accurate.

Note 2: B cannot verify $\{M, N_b, K_{bm}\}K_m$ to know identity has been changed to M.

Note 3: M now has shared key with B (K_{bm}) while B thinks it has shared key with A.

Phase 3: M mounts a man-in-the-middle attack when A attempts to communicate with B.

① A sends ticket to B:

$A \rightarrow B : A, B, \{M, N_a, K_{am}\}K_m$

* where ticket $\{M, N_a, K_{am}\}K_m$ was issued to A in phase 1, step 4.

② M intercepts ticket and proceeds with Needham-Schroeder verification process below:

$M \rightarrow A : \{N_m\}K_{am}$

$A \rightarrow M : \{N_m - 1\}K_{am}$

(next page)

③ M sends ticket to B :

$$M \rightarrow B : M, B, \{B, N_b, K_{bm}\}K_b$$

* where ticket $\{B, N_b, K_{bm}\}K_b$ was issued to B in phase 2, step 4.

④ B completes Needham-Schroeder verification process below:

$$B \rightarrow M : \{N_b\}K_{bm}$$

$$M \rightarrow B : \{N_b - 1\}K_{bm}$$

Conclusions :

① M has a shared key with A (K_{am}) established from phase 1, step 4. However, A believes key is established with B.

② M has a shared key with B (K_{bm}) established from phase 2, step 4. However, B believes key is established with A.

③ M can use shared keys to establish communication with A (A thinking its B), or with B (B thinking its A).

Problem 2 :

a) How can Crypto lock achieve properties ? What key-related material, if any, should be part of the malware binary ? How would encryption and decryption work ?

Proposed Solution :

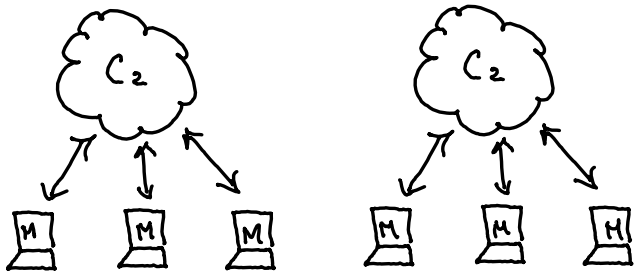

Exhibit 1 : All infected computers will communicate with a command and control node (C2) for a unique encryption key. Encryption keys are generated by C2, and are used by malware to encrypt files on computer. There will be multiple C2 nodes geographically dicbursed across US, EU, APAC to eliminate single point of failure, and reduce key generation load for each C2 node. Once infected computer gets encryption key, it no longer communicates with C2 node, and begins encrypting files on computer.

(next page)

- key generation
- key distribution
- key storage

Exhibit 2: Each C2 node implements the RSA crypto-system that generates unique public / private key pairs for each infected computer, distributes public key to computer, and stores the public / private key pairs in database. An attacker can easily query the database for private key using public key from victim. As this is the RSA crypto-system, C2 nodes will generate "e", "d", "N" following equations $C = m^e \bmod N$ and $M = C^d \bmod N$. key distribution established via short lived web-socket between computer and C2 node.

- locate C2 node
- encrypt / decrypt files

Exhibit 3: Malware is installed on computer via user clicking on link within phishing email. Once installed, malware will locate closest C2 (algorithm built into malware), request for encryption key, encrypt all files with encryption key, then display pop-up with public key (so attacker can provide decryption key) and payment instructions (email address for pre-paid gift card). Each C2 has its own email alias for redundancy, and reduced loss if compromised.

(next page)

Summary: My CryptoLocker system will utilize multiple geographically disbursed C2 nodes that implement the well established RSA crypto-system in order to generate, distribute and store unique public/private keys for every infected computer (1024 bits). Infected computers will receive "e" and "N" while C2 stores "d" key material. Using a well vetted crypto-system ensures rapid deployment and reliability, while unique asymmetric keys allows public keys to be distributed over internet and unique private keys required for decryption. An attacker can retrieve decryption key with public key displayed (provided by victim. A victim can decrypt files after emailing gift cards to attacker, and entering decryption key at malware prompt.

b) Name one advantage and one disadvantage of your design (author's point of view).

Advantage: The system utilizes RSA, which is a thoroughly vetted and widely used crypto-system. This makes the implementation easier and the system more reliable than custom crypto-system.

Disadvantage: All infected computers must communicate with a C2 node for an encryption key, a C2 can be overwhelmed with many requests and thus, be brought down by a denial of service attack it caused on itself. The remediation is adding more C2 nodes and throttling mechanisms, however, there is a tradeoff of more cost and complexity.

References

Student Discussions

- CB Bangalore
- Satya Srinivas
- Nick Keith
- Jyotsna Sharma
- Aaron Crouch
- Matthew Holmes

} Office hours

Tools and Resources

- Hoffstein textbook
- Stallings textbook
- Async video (module 9)
- Google searches
- Youtube
- Wikipedia
- Stack Exchange