Lecture 29 case study solutions
1.264 Fall 2013

A manufacturer, Andrews Co., proposes to exchange information with another manufacturer, BBI, over the Web. Because Andrews Co. uses a home-grown ERP (enterprise resource planning) system on a non-standard operating system, they must develop custom security rather than using an off-the-shelf solution. Andrews Co. proposes the following:
Step 1. Andrews Co. assumes that BBI has a certificate with a public key, and that BBI sends Andrews Co. the public key whenever it changes (which will be infrequent).
Step 2. Andrews Co. and BBI will secure only a subset of transactions. Shipment notification and order status will be sent in the clear (i.e unsecure). Purchase orders and payment information will be secure. All of these transactions use SOAP (HTTP and XML). All have sequential transaction numbers.
Step 3. Secure transactions will go to one IP address, and insecure transactions will go to another IP address. Both Andrews Co. and BBI will set up two IP addresses just for these transactions.
Step 4. Andrews Co. will create a new 56 bit symmetric key periodically during the day, roughly every hour, but it may be less frequent if there are no transactions to be sent.
Step 5. Andrews Co. will send BBI the new symmetric key as the first message of the day, encrypted with BBI's public key.
Step 6. Any secure transaction between BBI and Andrews Co. will be encrypted with the symmetric key Andrews Co. generates during the day.

a. Write down the protocol for the secure transactions using the notation used in the Anderson book and in class. For example, X -> Y: {K_Z. X, Y}. Use K_X for X's public key, K_{XY} for a symmetric key. Define any other symbols that you use. Please use "A" for Andrews Co. and "B" for BBI.

Solution:
B-> A: K_B (and possibly A, B, T)

A-> B: {K_{AB}}K_B (and possibly A, B, T)

B-> A: {N, M_{BA}}K_{AB}

A-> B: {N, M_{AB}}K_{AB}

Where N is the sequential number in each transaction (it may be embedded in M).

b. List, if possible, 3 attacks you can devise that would break the security of this connection. Describe each briefly and why it would or could succeed. The attacker has not broken into either Andrews Co. or BBI's servers or clients.

Attacker C could spoof (use) Andrew's IP address and send a different symmetric key to BBI if some time has elapsed since the last one, encrypted with BBI's public key. C could then send and receive bogus messages.

Attacker C could break the 56 bit key by brute force in seconds or minutes.

Attacker C could spoof (pretend to be) BBI and send a bogus public key to Andrew. When Andrew sends the symmetric key, C can decrypt it with the corresponding private key. C can send the altered symmetric key on to BBI encrypted with BBI's public key, and BBI will not know. Attacker C then also spoofs Andrew's IP address to BBI and can decrypt, using the altered symmetric key (that BBI is using) messages from BBI to Andrew. This is a man in the middle attack.