Homework 9 Solutions
1.264, Fall 2013
Security

1. Agreement

1. Kerberos is a private key, trusted third party authentication system. It requires all the companies to have single, trusted Kerberos server. This has an internal risk: the Kerberos administrator(s) would manage all security for each ERP, not just access to the shared features. This is probably unacceptable: a customer could spy on other customers. Kerberos is almost always used within one organization, where these risks are minimal.
2. SSL is a public key, certificate-based authentication system. SSL certificates can be issued by the aircraft parts company or a third party, which is a certificate authority (CA). The aircraft parts company, if it issued its own certificates, would also use a root CA. Each of the 11 companies would decide which certificates had which privileges in its ERP system; there is no centralized security administration.
3. The tradeoffs between Kerberos and SSL are:
   a. Kerberos requires a trusted server; SSL doesn't (though it requires a certificate authority to issue the certificates)
   b. Kerberos has central management of user authentication and authorization; SSL has certificates that identify the principals, but authorization (access to apps) is handled by each ERP.
   c. SSL can be used to establish communications between parties who don't have a shared secret (private key). This isn't important in this case, since the aircraft parts company and its customers are known to each other.
   d. SSL client certificates only identify the client's email address, which is weak authentication for access that may allow financial transactions. A Kerberos username and password are controlled more closely by the Kerberos administrator.
   e. Both SSL and Kerberos encrypt the session with the ERP.
4. Usernames and passwords are probably the least acceptable.
   a. For usernames and passwords, it will be necessary for each of the 11 companies to manage their own system. Requests to add, change or delete a username will have to be handled at all 11 systems. The same username/password pair will be assigned to a user across all 11 systems. To manage this centrally would require a group that has admin access to all 11 ERPs, which is probably an unnecessary security risk, since these admins would almost certainly have access to the full ERP.

2. Define all the principals and variables in the protocol:

1. **Principals:**
    a. **Let D be driver and his/her ID**
    b. **Let T be the smartcard issued by aircraft parts company to carrier**
    c. **Let F be the freight bill number**
    d. **Let G be the gate and its smartcard reader; KT is the shared key between the gate and all smartcards**
    e. **Let C be the transportation carrier server and KC its public key**
    f. **Let M be the aircraft parts distributor server**
    g. **Let A be the access code**

Define the protocol

2. **Protocol:**
    a. **M-> C: $\{F\}_{KC}$**
    b. **C-> D: F**
    c. **T-> G: T, $\{T, N\}_{KT}$**
    d. **G-> T: $\{A\}_{KT}$**
    e. **D->G: F**

3. List three potential flaws

    a. List the flaws:

1. **Driver ID not in protocol.**
2. **Access code written to card before valid freight bill number entered.**
3. **Freight bill sent in clear.**
4. **Shared private key KT across all smart cards.**

    b. Describe one or more attacks:

If an intruder wishes to improperly enter the facility, these flaws can be used in combination:

1. **The intruder can steal a smart card from any driver of any carrier serving the distribution center. Or the intruder can use a man in the middle attack or crack the key, as in the lecture notes. Since driver ID is not in the protocol, any card will do.**
2. **The freight bill number is sent in the clear from the carrier to the driver in email, so the intruder can intercept it. The intruder can also get the number when the driver keys it in, by getting the electromagnetic radiation from the key taps, or by a hidden camera near the gate, or other means. Freight bill numbers remain valid and can be reused for some period by an attacker, so one freight bill may allow multiple entries.**
3. **The access code is written to the card before a valid freight bill number is entered. An intruder with a stolen card can get the access code from the gate first, and then get a freight bill number later, making an attack easier. The access code may remain in effect for a long period allowing multiple attacks.**

4. Use cases

Some plausible scenarios are listed below. You will have others that are equally plausible.

1. **Steal or hijack a high value shipment for direct financial gain**
    a. **Steal an access card, intercept a freight bill number as in question 3**
2. **Steal or hijack a safety critical shipment to use for blackmail or other threat.**
    a. **Same steps as above.**
3. **Break into the database to steal aircraft parts company's financial information, such as bank accounts that can be stolen from.**
    a. **Attackers try all Web pages and Web services, looking for flaws in logic. Methods include cross site script attacks, SQL injection, etc. The goal is to obtain administrator access to the database.**
4. **Break into the database to steal vendor or customer financial information, to steal from it.**
    a. **Same steps as in 3 above. Other possibilities are to compromise an employee, guess passwords, etc.**
5. **Introduce a virus in the company's systems to shut down the distribution center or cause processes to malfunction, as an extortion attempt.**
    a. **System operators with Internet access are lured to Web sites that can infect the system software.**
6. **Tamper with aircraft parts products, as an extortion attempt**
    a. **Gain physical access, as in question 3**
7. **Steal trade secrets and sell them to a competitor.**
    a. **Gain access to the company's file servers or internal network, and obtain documents with trade secrets.**

5. Biometrics

1. **Fingerprint readers are the most widely used biometric technique. Equipment is readily available. The false match rate is about 1% and the missed match rate is perhaps 4% in many cases. These are likely to be acceptable for a relatively small number of drivers, and in a system where there are other elements that control access, such as having the card and the freight bill number. Fraud is possible through "lifting" fingerprints and making copies, so a sophisticated attacker must be assumed to be able to defeat the fingerprint check.**
2. **Iris scans are more expensive, take more time (the driver would probably have to exit the truck), but have lower error rates than fingerprint readers. Fraud is possible through taking pictures of a valid driver's eyes and using the picture, possibly printed on a contact lens, so again, a sophisticated attacker must be assumed to be able to defeat the iris check.**
3. **Voice recognition is likely to be unreliable, as noted in Anderson. Recordings are an easy way to defeat them, and there are others.**
4. **These methods add security in routine operations, but probably not much against a sophisticated attack. These methods work best in attended operations, so the aircraft parts distribution center security staff may need to be assigned to the gate to obtain the benefit of biometric checks. Biometrics is unlikely to provide after-the-fact proof in court. Last, biometrics often appears to have a deterrent effect on criminals; its capabilities to identify criminals may be limited.**

1.264J / ESD.264J Database, Internet, and Systems Integration Technologies
Fall 2013