Design Project #2: Authenticated PalmPilot Conduits

The Problem

The 3Com PalmPilot is one of the most popular personal digital assistants (PDA) in use today. It has applications to keep track of its owner's appointments, to-do list, address book, and memos. The data is kept in databases on the PalmPilot. The device can also be connected to a desktop computer via a serial port. The model of use is that for each database application in the PalmPilot there is a corresponding application that runs on the desktop computer, with another copy of the same database. The user can work with the desktop computer version of the database, or with the palmtop version of the database; the serial port connection is used to keep the two versions of the database consistent. The serial port is also used to receive additional PalmPilot applications (which can be developed by third parties).

The ability reconcile a desktop database with the database on the PalmPilot is provided by 3Com's HotSync technology (see the HotSync section in http://www.palm.com/newspromo/history.html). HotSync allows the PalmPilot to reconcile its data with a desktop application via an application-specific *conduit*. The conduit can read and write data from and to the PalmPilot. A simple conduit might simply transfer some records from the desktop database into the PalmPilot. A more complicated application conduit might compare the two databases and add and delete records (in an application-specific way) so that the two databases contain the same records. (The PalmPilot literature often misuses the term *synchronization* to refer to *reconciliation* of information. But something called HotReconciliation technology probably would not sell as well.)

One of the challenges in developing for the PalmPilot is that it is an underpowered computer (relative to today's PCs). The PalmPilot units available these days have either 512KB (PalmPilot Personal), 1MB (PalmPilot Professional), or 2MB (Palm III) of memory and have a Motorola MC68328 DragonBall processor running at 16.6 MHz. More product information is available at the Palm Computing web site. (Palm Computing, Inc. is the 3Com subsidiary that is responsible for the PalmPilot.)

PalmPilot users are clamoring for an important new function: they want to be able to download new records, such as dates for their calendar, from sources other than the copy of the database on their desktop computer. For example, they may want to download a class schedule from the MIT web server, conference information from an information kiosk, or stock quotes from a web site. However, they want to ensure that the data that makes it onto their PalmPilot is authenticated. In addition, they want to make sure that the computer doing the download doesn't read or change any information stored on the PalmPilot without authorization.

Consider a 6.033 student with a PalmPilot and a public PC in her dorm. The student connects from the PC to a web site that claims to have the latest 6.033 quiz schedules and locations encoded as a PalmPilot memo. The student uses a conduit to add the memo to the PalmPilot. However, the student would like to be sure that the information does indeed come from the 6.033 staff.

Then, the student uses the new 6.033 automatic recitation scheduling conduit on Athena. It talks to the student's PalmPilot via the serial port on the Athena workstation to read the student's schedule and automatically figures out what recitation to assign to the student. The student wants to make sure that the recitation schedule item (with time and room number) that the software adds to her PalmPilot comes from the registrar rather than being a spoofed recitation assignment. In addition, the student would also like to make sure that the software is not able to read the schedule item that indicates that the student is planning to do a hack by putting an "I love 6.033" sign on top of the great dome. (That extracurricular schedule item should only be accessible to the people who are helping her with the hack.) Furthermore, the student does not want the 6.033 scheduling software to overwrite the "Sleep" entries in her schedule with "Study for 6.033".

Later that day, a student who has a Palm III (which has an infrared port) is walking through Harvard Square and sees an Palm III-compatible infrared transmitter that claims to be transmitting MBTA bus schedules as PalmPilot memo items. The student would like to add this information to her PDA, but would like to verify that the information does indeed come from the MBTA rather than being a trick played the local cab drivers (who want you to miss your bus and have to take a cab).

3Com has decided that it wants to add public key authentication to the PalmPilot so that the security-conscious 6.033 students can keep using and recommending their product in the scenarios described above. The company has written and is willing to issue a small patch to the PalmOS (the operating system for the PalmPilot) that allows a PalmPilot's user to put her PDA into a mode where it accepts only authenticated read and write requests. To determine the authenticity of a request, the PalmOS patch will use a new authentication library that users can install on their PalmPilots.

In authenticated mode, the PalmPilot accepts only 2 types of requests:

1. read a record (for example, a field in the address database)
2. write data to a record

Requirements

Your assignment is to design an authentication system that can be employed by 3Com. The authentication system should, at a minimum, meet the following requirements:

- provide a mechanism to authenticate the two types of requests that the PalmPilot can accept in authenticated mode
- provide a mechanism to authorize those requests
- require no changes to the PalmOS beyond the PalmOS patch described above

On the PalmPilot side, your authentication system will have to be implemented as a trusted authentication library and a security management application that users can install on their patched PalmPilots.

Once your design is deployed, 3Com and third parties will be able to modify their conduits to be able to communicate with the PalmPilot when it is in the new mode. Parties like the registrar should be able to generate authenticated content for the PalmPilot (like official alternate classroom assignments when building 34 suddenly floods).

Assume that 3Com is providing you with a fast public key algorithm for the PalmPilot (taking, say, 0.1 sec for a 1Kbyte request). The key size for the algorithm is somewhere in the 512 to 1024-bit range.

Issues

In coming up with your design, it will be helpful to consider the following issues:

Operation

- Where are keys stored? How are they used?
- How are permissions specified? Where are they kept? How are they changed?
- What does an information publisher need to do to be able to provide authenticated data?
- What does a conduit writer need to do to be able to put authenticated data on your PalmPilot? How can the conduit read data from your PalmPilot?
- How is the risk of private key compromise minimized? (Where are private keys used?)
- What sorts of security policies are available? How are those security policies specified or selected by the user and/or application author. (In some cases, the application is not in charge of this; for example, an update may need to be authorized by a bank or other party.) How does the implementation support these policies?
- How do you make sure the phone number you're downloading is newer than the old one?

Bootstrapping

- After installing your authentication library and security management application, what does a user need to do in order to use it?

Authentication

- How are the 2 types of requests encoded so that they have authentication information?
- How do you identify the author of a read or write?
- Is your authentication protocol explicit enough?
- Is your authentication protocol as simple as possible?

The above list of issues is by no means complete. It is merely intended as a starting point.

Your Team's Assignment

First, this is a team project, so form a team of 3 people where everyone has the same recitation instructor. *Please send email to your recitation instructor before Thursday, April 16 with the names and email addresses of your team members. Then get to work! Your team's report is due in recitation on Thursday, April 30.*

Your team's job is to write a detailed report that describes the design of an authentication system that meets the requirements listed above. Your design should be no more complex than necessary: your system should emphasize correctness and economy of mechanism. Your report should be long enough to be self-contained and complete, but no longer than 10 pages.

3Com has hired a team of computer systems specialists to review your proposal and make a recommendation. They know the concepts and terminology used in 6.033 (actually, the reason that 3Com hired them is that they all got A's in 6.033) and they also are all enthusiastic users of the PalmPilot. They have not thought carefully about this particular problem before reading the proposals. They know the high-level goals but probably haven't had the time to study all the technical aspects of how these goals would be achieved. However, as critics and potential users of your design, they will be eager to pound on your design to see if it breaks. It is your team's job to give them a good, coherent, self-contained, well-written proposal for a design, including an evaluation of the benefits and disadvantages. The experts will be looking for an impeccable and elegant (as simple as possible but no simpler) design. Your grade will depend on just how eager these experts are to deploy your team's system so that they can use it with their PalmPilots. You want these experts to pick *your* design.

It is crucial that you provide enough detail for the skeptical computer systems experts to evaluate the real-world feasibility of your design. Make sure your report describes the interface(s) your system presents. Describe in detail the protocol that the conduit needs to use to talk to the PalmPilot in authentication mode. Explain how your design addresses the requirements. Make sure to consider all relevant issues.

You should also describe how you initialize and configure your system for first use, how it is used in normal operation, and how you can change its authorization policies. To that end, your report should include a detailed account of two scenarios:

1. a scenario in which the data that is downloaded into the PalmPilot is authenticated
2. a scenario where access to a record on the PalmPilot via the serial port is authorized

You might use the scenarios described in the introduction or invent your own.

Don't forget to evaluate your design from a technical standpoint, explaining any assumptions you are making (and arguing that they are reasonable). Ideally, your design should be totally secure. However, if there is a problem, you are better off bringing it to the reader's attention yourself.

We suggest you pick one design for your authenticated update system and argue why it is a good design by evaluating your specific design choices. You can strengthen your report by contrasting to other possible approaches, but your report should focus on your design rather than on surveying other possible approaches.

Feel free to take a look at some authentication mechanisms (see below for some pointers) and the references included below. But, be sure to give credit to any work from which you borrow.

Finally, do not get bogged down in implementation details, but make sure that you cover all design aspects.

Useful Information

Here is some information that you might find useful. If you would like to see design papers from last year, check out the 1997 excellent reading reports. We hope to publish excellent design papers for design problem 1 later next week.

Authentication Protocols

At a minimum, check out the notes for the authentication lecture. You might also want to check some of the references listed in the notes (e.g., Schneier's "Applied Cryptography").

To see a sophisticated public-key system in action, check out SDSI. Your design does not have to be this sophisticated!

Authentication enthusiasts may want to take a look at "Authentication in Distributed Systems: Theory and Practice" by Lampson et al., ACM Trans on Computer Systems, Vol. 10, No 4, Nov. 1992, pages 265--310. This paper is cool, but not an easy read.

PalmPilot Information

- Palm Computing, Inc. - 3Com's PalmPilot site
- Calvin's PalmPilot FAQ - It has a large collection of links
- Pilot Software Development - A software development page for the PalmPilot
- Hardware Stuff - describes the PalmPilot hardware
- Wade's Pilot Programming page - programming tips
- News release - about Certicom providing elliptic curve cryptography for future PalmPilots
- HotSync FAQ - the 3Com FAQ about HotSync.
- Developer FAQs - More development stuff.
- Microsoft's MSCHAP - Using authentication stuff (MSCHAP) with HotSync.
- Pilot UNIX source code - real code!

If you have additional suggestions for this list, please email to them to us.

Handing in Your Report (Read carefully - there is a surprise here)

Your team's report is due in recitation on Thursday, April 30. On that Thursday in recitation, you are expected to turn in your design project 2 reports. Your group should hand in two copies at your designated recitation. One copy should contain a title page with the names of the group members. This copy is going to be graded by your recitation instructor. You will receive one grade for the paper and all the members of a group will receive the same grade for the paper.

The other copy, which you will turn in at the same time as the first copy, should have a title page but without the names of the group members. Include a 6-digit code on the cover page instead and put the same code on the cover page of the "signed" report.

This second anonymous copy is going to be given to another team in your section on the same day, and that team will prepare a 5-minute presentation on it for next Tuesday's recitation. You will thus get an opportunity to do what is called a "peer review", and because the paper you review will not identify its authors, you will be doing a "blind review". Of course, if you do some sleuthing you can probably figure out whose paper you are reading, but that would not be in the spirit of blind reviewing, so restrain yourself.

Because of the constraints given by this schedule we cannot give extensions and all papers should be turned in on Thursday in recitation. (Tip: Start working on this project immediately.) Teams that consist of two people from one section and one from another should turn in the paper in the section to which two members belong (as described earlier, both sections must be with the same recitation instructor).

In preparation for Tuesday's section on May 5, your design team should prepare a 5-minute presentation on the paper of your classmates you received on Thursday. In addition to the presentation, each team should hand in a single one-page reading report on the paper that you reviewed as a group. This one-page report should include the names of all the team members/evaluators as well as the 6-digit "secret" code. The one-page reports should be attached to the anonymous copy of the paper you were evaluating.
