

HW #7: Threat Modeling

CS 392/681: Computer Security
Fall 2006

[100pts] DUE 11/13/2006 (midnight)

Problem 1 [10+15pts]

In the class, we studied RSA signing using hash functions (such as MD-5 or SHA_1). This involves hashing the message first and then signing the hash value using RSA. However, note that the hash value is 160-bit or 128-bit long, but the RSA message space is much larger, i.e., 1024-bit long. What in essence should happen is that the messages should be mapped to a 1024-bit long value and that value should then be signed using RSA. Although the approach of hashing message using MD-5 or SHA-1 and then signing it, is not shown to be insecure, it is not shown to be insecure either.

We have a secure version of RSA signing which called Full Domain Hash (FDH) RSA is signing. FDH is a hash function that maps a message to 1024-bit output. This output is then signed using RSA. Download the paper explaining the details regarding FDH RSA at <http://www.cs.ucsd.edu/~mihir/papers/exactsigs.pdf>, read through it and answer the following questions:

1. Explain how RSA FDH signing and verification works (you can cut/paste the “picture/figure” in the paper when you write your answer)
2. Refer back to the HW #4 Problem 3, where you experimented with the timing of RSA signing/verification using the code at <http://www.funet.fi/pub/crypt/cryptography/asymmetric/rsa/rsaref2.tar.gz>

First check if this code uses FDH RSA (let me know if it does not). Look at the source code that implements FDH function. Then, time the cost of performing FDH hash on a message of length 2048-bits.

Problem 2 [50pts]

I hope you all have heard about the RFID technology. In this exercise, your task is to prepare an attack/threat tree related to the security and privacy of RFID communication. Your primary reference is this presentation: <http://lasecwww.epfl.ch/~gavoine/download/slides/Avoine-2006-smartuniversity-slides.pdf>, which lists various threats (and also possible solutions, you don't need to refer

to the solutions for the sake of this exercise). You are also recommended and free to use any other resources (they are there aplenty online) to prepare your attack tree. Try to cover all possible attacks, from the physical layer to the application layer, and with respect to both security and privacy, and try to cover all steps in a particular attack. If your tree becomes huge, you can split it up among separate trees. The tree can be hand-drawn, but it should be clear and easily understandable (that's the whole purpose of attack trees – to document the attacks nicely)

You are also free to work in teams of no more than two people (for this exercise only!)

Your work would be useful for my present/future research in this area – by looking at a well-documented and complete attack tree, I can have a very clear understanding of all possible threats. Thanks to you in advance ☺

Problem 3 [25pts]

As you all know, we had the following problem at Poly a couple of weeks back:

[Quoting support]

“Recently, the spam filter (Postini) for the staff/faculty email accounts went down. Because of this, all emails sent/receive from staff/faculty were rerouted to the Barracuda filter, which is the main spam filter for the students. We believe Barracuda was overwhelmed and that's why the students email were bounced off. Please try to resend it again and let us know if the problem persist.”

Note that this is an example of a threat that is caused due to a natural fault -- more of a reliability/robustness issue rather than of security, inter-related nevertheless. Note also that this problem has occurred only once in the last 5 years.

Due to this problem, 100 faculty members each had to spend 10 hours extra (mainly in re-sending the dropped emails). Moreover, 500 students each had to spend 2 hours extra (in making sure that they don't lose important mails from a number of faculty members). Assume that an average faculty at Poly earns \$100,000 a year for working 40 hours per week, and that a student earns \$15 per hour.

One way to resolve the problem is for Poly to buy a few servers (in addition to Postini and Barracuda) that distribute/replicate the spam filter operation to achieve better fault-tolerance. The more the number of servers, the robust the system is. The overall cost of one such server is \$3,000 per year.

I am going to raise this issue during the next faculty meeting (I can, but I don't want to ☺; actually, Poly won't care because they are not paying us extra for our over-time ☺). How many servers should I recommend buying? Explain your answer in details. You can assume that there are 48 weeks per year.