CSE 590YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #5

Due in class: February 12

Fun with CRLs: In this problem we're going to make some estimates on the size of certificate revocation lists (CRLs) we would have to pass around if everyone in the US used X.509 certs for signed e-mail. We're going to base our numbers on the current VeriSign CRL for SSL server certificates; you can find all of VeriSign's CRLs at http://crl.verisign.com/; the one we're interested in is the RSASecureServer.crl file. This CRL is (as of today) valid from 2/5/2002 to 2/15/2002, is 800KB in size, and has just over 23,100 entries in it. Assume that all of the certs listed on the CRL were issued within the past 12 months. VeriSign claims to have over 765,000 sites with "Secure Server IDs", so assume that's the universe from which 23,100 certs have been revoked.

1. VeriSign also sells "personal use" certificates that are appropriate for SSL client authentication and e-mail use. If VeriSign sold one "personal use" cert per person in the US, how big would the corresponding CRL be in bytes, assuming the same proportion of "personal use" certs are revoked as are SSL server certs.

2. Since it is not reasonable to make people download that big a CRL every 10 days, suggest some approaches VeriSign could use to reduce the size of the CRLs users would have to download. Describe what changes or additional information, if any, you would need to add to VeriSign-issued certs or CRLs to make your scheme work.

Fun with OCSP: Since a CRL serving everyone in the US seems unworkable, let's take a look at an on-line solution. Let's assume VeriSign runs an OCSP responder that hands out signed OCSP responses whenever someone queries about the current state of a certificate.

3. If the average size of an OCSP request/response message pair is 3KB, how often would a user have to request an OCSP response from the VeriSign OCSP responder in order to generate the same about of bandwidth usage as that user would generate downloading the CRL you computed in Problem 1. How does your answer change for OCSP if you implement the performance improvements for CRLs you outlined in your answer to Problem 2.

Linking independent CA hierarchies with cross-certification or bridge CAs: *Cross-certification* is the process of linking together two independent CA hierarchies through the issuance of mutual cross certificates. For example, if Microsoft and Boeing each have independent CA hierarchies terminating in a Company Root Authority, they could cross-certify each other by having the Microsoft Root issue a certificate for the Boeing Root and the Boeing Root issue a Certificate for the Microsoft Root.

4. How does cross-certification scale as the number of to-be-interconnected Roots grows? How does the introduction of a Bridge CA help solve the scaling problem? Is cross-certification without a bridge CA semantically equal to cross-certification with a bridge CA? Why or why not?

A web of Trust: An alternative to a hierarchical certificate structure is a decentralized "web of trust" in which individuals use their personal private keys to certify public keys of their friends, colleagues, etc. Thus, if Alice and Bob are acquainted and Bob and Carol are acquainted, Alice can send a signed message to Carol and provide Bob's certificate on Alice's public key. If Carol trusts Bob's attestation, she can verify the signature as coming from "the person Bob knows as Alice" and act accordingly.

While a web of trust can work well within an environment of personal contacts, it is not well-suited to the situation of, "I saw your add on e-Bay and would like to chat."

5. Suppose that each of 1 billion web users has certified (and been certified by) 10 acquaintances. For simplicity, make the unrealistic assumption that each individual's 10 acquaintances are randomly and independently chosen from among the community of 1 billion users. Estimate the probability that two randomly chosen individuals can be "linked" by a chain of 2 certificates. Repeat for each of 3, 4, 5, and 6 certificates. (For these estimates, you may assume that second order effects due to repetitions are negligible.) Describe a search technique for finding a chain of certificates between two individuals that normally works by examining fewer than 1 million certificates and requires no more than a few million steps.