CS 4235: Introduction to Information Security December 6, 2011

Problem Set 5: Cryptography and Anonymity

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three **optional** questions, each with several parts (plus a fourth fun activity). Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup **December 14, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **Crypto Hacks (25 Points).** Alice and Bob are good friends. To save time, they agree to simply find one good pair of primes, p and q and therefore use the same public modulus, $n = pq$. To save confusion over who signed which message, they select different exponents e_a and e_b. Show that, in this system, it's possible to decrypt a message M sent to both of them if $\gcd(e_a, e_b) = 1$. That is, given,

$$\begin{aligned} C_a &= M^{e_a}(mod n) \\ C_b &= M^{e_b}(mod n) \end{aligned}$$

   an adversary can compute M.

2. **Internet Transparency (40 Points).** Various projects are now trying to monitor the availability of various Web sites, informations and services. Two such systems are Herdict (`http://herdict.org/`), and Google's Transparency Report (`http://google.com/transparencyreport/traffic/`. Herdict relies on manual reports of downtime and unavailability, whereas Google's transparency report uses anomalies in traffic volumes to discover reachability problems from various regions for a particular service.

   - **10 points.** What are the possible sources of inaccuracy of each approach? How would you verify the accuracy of information reported from each of these systems?
   - **30 points.** Design and build a simple system that takes reports from the Herdict Web site and automatically measures their reachability properties from a variety of different locations. For this purpose, you may need access to a set of distributed servers. The PlanetLab testbed (`http://planet-lab.org/`) is a good resource for this. I can provide you an account if you need one.

3. **Anonymity (35 Points).** Download and install Tor.

   - **(15 Points).** Identify the locations of the various entry and exit nodes that you can use in Tor. What is the distribution of entry and exit nodes across Internet service providers and countries? Provide a table of the top 10 countries and ISPs (autonomous systems) that host Tor entry and exit nodes.

- **(20 Points).** The Tor Metrics page has some interesting examples of statistics of Tor usage in different countries during times when countries attempted to block Tor. For example, see `http://goo.gl/6Pcfn` for an example of when Iran blocked Tor. Find at least two other examples of cases where Tor appears to have been blocked in a country. *Include a graph from the Tor metrics page and a description of what you think is going on.* How would you have stopped these events?