

Outline for February 29, 2012

Reading: §14.6, 16.1–16.2

1. Identity
 - a. State and cookies
 - b. Anonymity (remailers, onion routing)
2. Information flow
3. Entropy
 - a. Random variables
 - b. Joint probability
 - c. Conditional probability
 - d. Entropy (or uncertainty in bits)
 - e. Joint entropy
 - f. Conditional entropy
4. Entropy-based analysis
 - a. Flow of information from x to y
 - b. Implicit flow of information
5. Non-lattice policies
 - a. Transitivity
 - b. Information flow policy
 - c. Confinement flow model
6. Transitive non-lattice policies
 - a. Quasi-ordered sets
7. Non-transitive policies
 - a. Dual mappings
 - b. Theorem: a dual mapping from a reflexive information flow policy into an ordered set is order-preserving