ECS 235B Module 54
Analyzing Covert Channels

Analyzing Covert Channels

- Policy and operational issues determine how dangerous it is
  - What follows assumes a policy saying all covert channels are a problem
- *Amount* of information that can be transmitted affects how serious a problem a covert channel is
  - 1 bit per hour: probably harmless in most circumstances
  - 1,000,000 bits per second: probably dangerous in most circumstances
  - Begin here . . .

Measuring Capacity

- Intuitively, difference between unmodulated, modulated channel
  - Normal uncertainty in channel is 8 bits
  - Attacker modulates channel to send information, reducing uncertainty to 5 bits
  - Covert channel capacity is 3 bits
    - Modulation in effect fixes those bits

Formally

- Inputs:
  - *A* input from Alice (sender)
  - *V* input from everyone else
  - *X* output of channel
- Capacity measures uncertainty in *X* given *A*
- In other terms: maximize

$$I(A; X) = H(X) - H(X \mid A)$$

  with respect to *A*

Noninterference and Covert Channels

- If *A*, *V* are independent and *A* noninterfering with *X*, then $I(A; X) = 0$
- Why? Intuition is that *A* and *X* are independent
  - If so, then only *V* affects *X* (noninterference)
  - So information from *A* cannot affect *X* unless *A* influences *V*
  - But *A* and *V* are independent, so information from *A* does not affect *X*
- But noninterference is not necessary

Example: Noninterference Not Necessary

- System has 1 bit of state; 3 inputs I_A, I_B, I_C; one output O_X
- Each input flips state, and state's value is then output
  - System initially in state 0
- *w* sequence of inputs corresponding to output $x(w) = length(w) \bmod 2$
  - I_A not noninterfering as deleting its inputs may change output
- Define terms
  - *W* random variable corresponding to length of input sequences
  - *A* random variable corresponding to length of input sequences contributed by I_A; *V* random variable corresponding to other contributions; *A*, *V* independent
  - *X* random variable corresponding to output state

Two Cases

- $V = 0$; then as $W = (A + V) \bmod 2$, $W = A$, and so A, W not independent; neither are A, X. So if $V = 0$, $I(A, X) \neq 0$
- I_B, I_C produce inputs such that p(V=0) = p(V=1) = 0.5; then

$$p(X=x) = p(V=x, A=0) + p(V = 1 - x, A = 1)$$

Because A, V independent, this becomes

$$p(X=x) = p(V=x, A=0) + p(V = 1 - x)p(A = 1)$$

and so $p(X=x) = 0.5$. Also,

$$p(X=x \mid A=a) = p(X = (a + x) \bmod 2) = 0.5$$

establishing A, X independent; so $I(A, X) = 0$

Meaning

- Note A, X noninterfering, and I(A; X) = 0
- So covert channel capacity is 0 if either of the following hold:
  - Input is noninterfering with output; or
  - Input comes from independent sources, all possible values from at least one source are equally probable

Example (More Formally)

- If A, V independent, take $p=p(A=0)$, $q=p(V=0)$:
  - $p(A=0,V=0) = pq$
  - $p(A=1,V=0) = (1–p)q$
  - $p(A=0,V=1) = p(1–q)$
  - $p(A=1,V=1) = (1–p)(1–q)$
- So
  - $p(X=0) = p(A=0,V=0)+\mathrm{p}(A=1,V=1) = pq + (1–p)(1–q)$
  - $p(X=1) = p(A=0,V=1)+\mathrm{p}(A=1,V=0) = (1–p)q + p(1–q)$

Example (*con't*)

- Also:
  - $p(X=0|A=0) = q$
  - $p(X=0|A=1) = 1-q$
  - $p(X=1|A=0) = 1-q$
  - $\mathrm{p}(X=1|A=1) = q$
- So you can compute:
  - $H(X) = -[(1-p)q + p(1-q)] \lg [(1-p)q + p(1-q)]$
  - $H(X|A) = -q \lg q - (1-q) \lg (1-q)$
  - $I(A;X) = H(X)-H(X|A)$

Example (*con't*)

- So $I(A; X) = -[pq + (1-p)(1-q)] \lg [pq + (1-p)(1-q)] -$
  $[(1-p)q + p(1-q)] \lg [(1-p)q + p(1-q)] +$
  $q \lg q + (1-q) \lg (1-q)$
- Maximum when p = 0.5; then

$$I(A;X) = 1 + q \lg q + (1-q) \lg (1-q) = 1 - H(V)$$

- So, if $q = 0$ (meaning V is constant) then $I(A;X) = 1$
- Also, if $q = p = 0.5$, $I(A;X) = 0$

Analyzing Capacity

- Assume a noisy channel
- Examine covert channel in MLS database that uses replication to ensure availability
  - 2-phase commit protocol ensures atomicity
  - *Coordinator* process manages global execution
  - *Participant* processes do everything else

How It Works

- Coordinator sends message to each participant asking whether to abort or commit transaction
  - If any says “abort”, coordinator stops
- Coordinator gathers replies
  - If all say “commit”, sends commit messages back to participants
  - If any says “abort”, sends abort messages back to participants
  - Each participant that sent commit waits for reply; on receipt, acts accordingly

Exceptions

- Protocol times out, causing party to act as if transaction aborted, when:
  - Coordinator doesn’t receive reply from participant
  - Participant who sends a commit doesn’t receive reply from coordinator

Covert Channel Here

- Two types of components
  - One at *Low* security level, other at *High*
- Low component begins 2-phase commit
  - Both *High*, *Low* components must cooperate in the 2-phase commit protocol
- *High* sends information to *Low* by selectively aborting transactions
  - Can send abort messages
  - Can just not do anything

Note

- If transaction *always* succeeded except when *High* component sending information, channel not noisy
  - Capacity would be 1 bit per trial
  - But channel noisy as transactions may abort for reasons *other* than the sending of information

Analysis

- *X* random variable: what *High* user wants to send
  - Assume abort is 1, commit is 0
  - $p = p(X=0)$ probability *High* sends 0
- *A* random variable: what *Low* receives
  - For noiseless channel $X = A$
- n+2 users
  - Sender, receiver, *n* others that act independently of one another
  - *q* probability of transaction aborting at any of these *n* users

Basic Probabilities

- Probabilities of receiving given sending
  - $p(A=0|X=0) = (1-q)^n$
  - $p(A=1|X=0) = 1-(1-q)^n$
  - $p(A=0|X=1) = 0$
  - $p(A=1|X=1) = 1$
- So probabilities of receiving values:
  - $p(A=0) = p(1-q)^n$
  - $p(A=1) = 1-p(1-q)^n$

More Probabilities

- Given sending, what is receiving?
  - $p(X=0|A=0) = 1$
  - $p(X=1|A=0) = 0$
  - $p(X=0|A=1) = p[1-(1-q)^n] / [1-p(1-q)^n]$
  - $p(X=1|A=1) = (1-p) / [1-p(1-q)^n]$

Entropies

You can compute these:

- $H(X) = -p \lg p - (1-p) \lg (1-p)$
- $H(X|A) = -p[1-(1-q)^n] \lg p - p[1-(1-q)^n] \lg [1-(1-q)^n] +$
  $[1-p(1-q)^n] \lg [1-p(1-q)^n] - (1-p) \lg (1-p)$
- $\mathrm{I}(\mathrm{A};\mathrm{X}) = -p(1-q)^n \lg p + p[1-(1-q)^n] \lg [1-(1-q)^n] -$
  $[1-p(1-q)^n] \lg [1-p(1-q)^n]$

Capacity

- Maximize this with respect to p (probability that *High* sends 0)
  - Notation: $m = (1-q)^n$, $M = (1-m)^{(1-m)}$
  - Maximum when $p = M^{(1/m)} / (M^{(1/m)}m+1)$
- Capacity is:

$$I(A;X) = \frac{Mm \lg p + M(1-m) \lg (1-m) + \lg (Mm+1)}{(Mm+1)}$$