Foundations of Computer Security

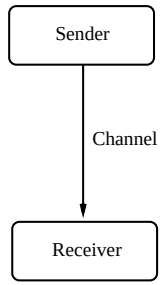
Lecture 29: Information Content

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Quantifying Information

How much information
is contained in each of the following
messages? How would you decide?

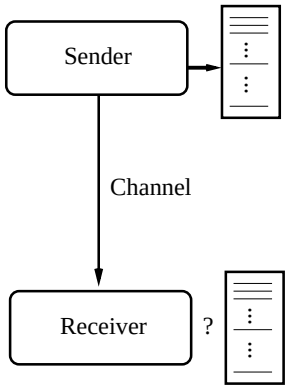
- An n-bit binary number.
- A single decimal digit.
- A two digit decimal number.
- "The attack is at dawn."



Quantifying Information

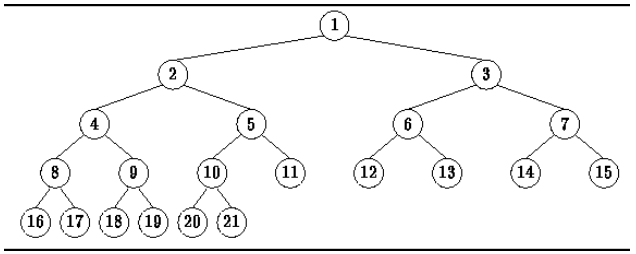
Suppose Sender and Receiver
have agreed that Sender will transmit
one of exactly 16 messages. *How many bits of information must be transmitted to convey the message? Why?*

Msg	code	Msg	code
M_0	0000	M_8	1000
M_1	0001	M_9	1001
M_2	0010	M_{10}	1010
M_3	0011	M_{11}	1011
M_4	0100	M_{12}	1100
M_5	0101	M_{13}	1101
M_6	0110	M_{14}	1110
M_7	0111	M_{15}	1111



Binary Tree Representation

Suppose we represent all possible *choices* in any decision as the leaves of a "complete" binary tree. The longest path is $\lceil \log_2(k) \rceil$, if there are k leaves on the tree.



Each choice (bit) reduces the search space by half.

Encoding

That suggests that the information content of any message from a space of K messages should be something like: $\lceil \log_2(K) \rceil$.

But to get a very efficient transmission:

- Sender and Receiver must know in advance the space of possible transmissions.
- They must have agreed on an encoding.

How Much Information?

How much information is contained in the message: "The attack is at dawn"?

Answer: It depends on the Receiver's level of uncertainty.

- If the *only* uncertainty were whether at dawn or dusk: one bit.
- If the attack could have come anytime during the day: ? bits.
- If the day was uncertain...: ? bits.

"The word 'information' relates not so much to what you do say, as to what you could say. ... That is, information is the measure of your freedom of choice when you select a message." –Warren Weaver

Lessons

- The information content of a message is the amount of uncertainty it resolves.
- In an ideal situation, each bit transmitted can reduce the uncertainty by half.
- Very few circumstances are ideal in the required sense.

Next lecture: Exploring Encodings