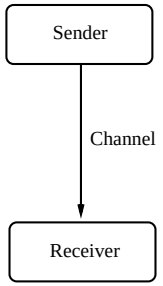
Foundations of Computer Security

Lecture 28: Information Theory

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

What is Information?

The fundamental paradigm of information theory is represented here: A sender conveys information to a receiver across a communication channel.



Information is any content to be conveyed. It is sent in the form of one or more *messages*.

Information theory attempts to quantify the *content* of messages and the *capacity* of channels on which information may flow.

Some Questions

Information theory asks questions such as the following:

1. How much information is encoded in a particular message?
2. How efficiently can a given alphabet/language be transmitted?
3. What is the maximum capacity of a given transmission medium?
4. How is that capacity or efficiency reduced by interference/noise?

These questions all have very precise and deep answers, that are beyond our scope here. We'll only scratch the surface.

Why Do We Care?

Information theory is very important in computer science. It affects all communication, hardware design, protocol design, cryptography, fault-tolerance, etc.

For example, in our current context it is useful to know how much information can be transmitted over a specific covert channel. This is the "bandwidth" of the channel.

A useful way of measuring bandwidth is *bits per second*.

Quantifying Information: Thought Experiment

How do you quantify the information content of a response to a "yes" or "no" question?

What does that even mean? Maybe it means the following:

1. Sender has either a "yes" or a "no."
2. Receiver knows that Sender has one of those two possibilities, but not which.
3. Sender wants to transmit enough data, but no more, to resolve entirely Receiver's uncertainty.
4. How much data must Sender transmit?

In those terms the answer is pretty clear: One bit of data. *But what must be true for Receiver to interpret the answer?*

Thought Experiment Lessons

This suggests:

1. In some cases, *it is possible* to quantify the information content of a message.
2. Maybe an appropriate unit of information content is *bits*.
3. Sender and receiver must have some shared knowledge, included an agreed encoding scheme.

Lessons

- Information is any content that can be conveyed from a sender to a receiver across a communication channel.
- Information theory attempts to quantify the amount of information in a message and the capacity of the channel.
- Communication requires some shared knowledge.

Next lecture: Information Content