

Outline for October 6, 2003

Reading: Chapters 3.2, 4.1–4.4, 4.6

Discussion Problem

Ever wonder why people need to write program specifications and requirements carefully? The answer is that those specifications seem to live forever. Here's an example:

The United States Standard railroad gauge (distance between the rails) is 4 feet, 8.5 inches. That's an exceedingly odd number. Why was that gauge used? Because that's the way they built them in England, and the United States railroads were built by English expatriates. Why did the English people build them like that? Because the first rail lines were built by the same people who built the pre-railroad tramways, and that's the gauge they used.

So, why did "they" use that gauge? Because the people who built the tramways used the same jigs and tools that they used for building wagons, which used that wheel spacing. Okay! Why did the wagons use that odd wheel spacing? Well, if they tried to use any other spacing the wagons would break on some of the old, long distance roads, because that's the spacing of the old wheel ruts.

So who built these old rutted roads? The first long distance roads in Europe were built by Imperial Rome for the benefit of their legions. The roads have been used ever since. And the ruts? The initial ruts, which everyone else had to match for fear of destroying their wagons, were first made by Roman war chariots. Since the chariots were made for or by Imperial Rome, they were all alike in the matter of wheel spacing.

Thus, we have the answer to the original questions. The United States standard railroad gauge of 4 feet, 8.5 inches derives from the original specification for an Imperial Roman army war chariot. Specifications and bureaucracies live forever. So, the next time you are handed a specification and wonder what horse's rear came up with it, you may be exactly right, because the Imperial Roman chariots were made to be just wide enough to accommodate the back-ends of two war horses.

— source unknown, but circulated on USENET and other message systems

Outline for the Day

1. HRU Result (*con't*)
 - a. Determining security of a generic system with generic rights is undecidable
 - b. Meaning: can't derive a generic algorithm; must look at (sets of) individual cases
2. Policy
 - a. Sets of authorized, unauthorized states
 - b. Secure systems in terms of states
 - c. Mechanism vs. policy
3. Types of Policies
 - a. Military/government vs. confidentiality
 - b. Commercial vs. integrity
4. Types of Access Control
 - a. Mandatory access control
 - b. Discretionary access control
 - c. Originator-controlled access control
5. High-Level Policy Languages
 - a. Characterization
 - b. Example: DTEL
6. Low-Level Policy Languages
 - a. Characterization
 - b. Example: Tripwire configuration file