

Secure Operating System Design and Implementation

Time

Jon A. Solworth

Dept. of Computer Science
University of Illinois at Chicago

February 1, 2011

Part I

Time overview

Overview

- Time is used in many parts of the system
 - For scheduling
 - For encryption (nonces)
 - For reliability (round trip time)
 - To tell what order events occurred in (e.g., file writes)
- Time within computers should satisfy properties
 - monotonically increasing
 - no gaps
 - accurate
- Unfortunately, accuracy trades off with the other time properties

Time anomalies

- Leap years
- Daylight savings time
- Gaps (change from Julian to Gregorian calendar different in different places)
- Leap seconds (extra seconds when earth gets out of whack)
- Bad ideas
 - Base fundamental time on decisions affected by humans
 - Base fundamental time on earth-specific issues (i.e., rotation rate of earth)

Time systems

- **Temps Atomique International** is an average of atomic clock
- atomic clocks are physics, not subject to the vagaries of man time
- time is measured at sea level (geode)
- because time is influenced by gravity (gravitational time dilation), as predicted by general relativity
- TAI does not have leap seconds (i.e., it is defined with respect to atomic decay rates)
- UTC does have leap seconds (currently 34 seconds different from TAI)
- look at <http://cr.ypt.proto/utctai.html> for more information

Time sources

- Atomic clock
- Crystal oscillator
- NTP: network time protocol
- Radio wave 60 kHz, 1 bit/second (in the US, from Fort Collins, Colorado)
- GPS: an accurate time source is inherent to GPS triangulation
- Cellular tower

Part II

Ethos time

Ethos time based on TAI

- Ethos time based on TAI
- With the guarantee that its non-decreasing
 - So that the difference of a later time from an earlier time is always positive and
 - and so that nonces never repeat
- We also have a best guess accurate time
- But unless its set from a trusted and reliable source, who knows
- So reliable time is subject to attack unless substantial expense is made to prevent it