TIS
INCIDENT REPORT

Project:	Incident Number/Reference: 004

DESCRIPTION *(data and sequence of actions leading to fault, details of actual and expected response)*

in S.P1229.41.2 Formal Specification v1.0 it states that *now* represents time. If *now* represents the real time then we cannot guarantee that polling will result in *currentTime* = *now.* The Formal specification needs to be more explicit about what *now* represents and what assumptions we make on time.

Found in test:

Supporting documentation attached YES/~~NO~~ *Continued* ~~YES/~~NO

Found during: *(use actual project stages)* ~~Reqs /Sys spec/Security Spec/~~Proof of Spec/~~Formal Design/INFORMED Design~~/ Proof of Design/~~Code/Code Proof/Integration/Sys test/Acceptance~~

Date: 6/6/2003	Signature of Originator:

EVALUATION *(include list of items affected, details of work required, other similar faults, tests to be re-run)*

In section 4.1 we should state that *now* represents an external time source, and that we require it to deliver an increasing time, and if it doesn't, our system does not guarantee to work.

Continued YES/NO

Classification: ~~Critical / Major~~ / Minor ~~/ Interfaces / Test / No Fault~~

Introduced during: *(use actual project stages)* ~~Reqs/~~Sys spec/~~Security Spec/Formal Design/INFORMED Design/ Code/Integration/Sys test/Acceptance~~

Date: 6/6/2003	Signature of Evaluator:

RESPONSE *(detail how incident is to be resolved, identify cause of problem, related faults and change requests)*

Update Formal Specification as described in evaluation

Continued ~~YES/~~NO

Date: 26/6/2003	Signature of Project Manager:

IMPLEMENTATION *(if applicable)*

Assigned to: janet	Signature of Project Manager:

Item modified	Date/Version	Signature of Checker	Signature of Integrator
S.P1229.41.2	1.1	David Coop	N/A *Continued* YES/NO

Janet Barnes

From: David Cooper
Sent: 06 June 2003 09:25
To: Janet Barnes
Cc: Tokeneer-Internal
Subject: RE: time increases

So, we should be able to tell what to do by reading our spec. After all, this is supposed to be our repository of decisions, and the thing that tells us what it means for our system to be secure. (Sarcasm off).

Well, our spec says "The only assumption we make of the real world is that time increases." So we have been up-front about what we assume of the real world, and we could reasonably point to this if Bill makes time decrease and say that that is outside our assumptions, and the client has signed off the spec. But possibly more usefully we could ask the Reveal system-boundary question, and ask what *now* and *currentTime* are meant to represent. If *now* is the real time in the real world, then we are justified in saying that it increases --- the real world really does behave like that. But then we are not justified in writing
currentTime' = now
in *PollTime*, because we can't guarantee to read the actual, real time correctly.

But if *now* is the time represented by some external trusted time source, we could reasonably expect to be able to read it correctly, but can we trust that it always increases? We can if we say it.

So, after that ramble, I think we should tweak the spec to say that *now* represents an external time source, and that we require it to deliver an increasing time, and if it doesn't, our system does not guarantee to work.

David

> -----Original Message-----
> **From:** Janet Barnes
> **Sent:** 05 June 2003 18:15
> **To:** David Cooper
> **Subject:** RE: time increases
>
> David
>
> To be honest I stated this intending it to be a property of a trusted time source.
>
> At present we are assuming a trusted time source and we don't check that the property holds of times that we read in. We could of course but then as you then suggest there is a question of what we do.
>
> Is this an example of another critical system fault for which we should shut the system down. SPRE will be able to tamper with the system clock so I guess we need to cover it or claim it is outside of scope because we a assuming a trusted time source.
>
> Janet.
>
>> -----Original Message-----
>> **From:** David Cooper
>> **Sent:** 05 June 2003 15:23
>> **To:** Janet Barnes
>> **Subject:** time increases
>>
>> Janet,
>>
>> Our spec says that time increases. As time is read from an "external" source (the clock), do you check that this assumption holds? And if the check shows that it fails (i.e. the external source doesn't match what we expect), what do we do?
>>
>> David

David Cooper
Praxis Critical Systems www.praxis-cs.co.uk
20 Manvers Street Direct: 01225 823889
Bath Tel: 01225 466991