MINUTES OF THE FIRST MEETING OF THE MARSIK SOFTWARE WORKING PARTY

Date: 7th November 1985

Present: (CH), (SMT2), (CHP), (CHR), (SMT2), (CHR1) and (SMT3).

Distribution: ADD, SM, SMT, SMT2, SMC, CH, CHP, CHR

Background:

During the meeting of the MARSIK Project Committee in October 1985, it was decided that the Working Party should produce two papers relating to further developments of Project MARSIK. The paper to be completed first was to be coordinated by SMT3, and its purpose was to assess the need for networking, and to make recommendations on the suitability of the available software products.

SMT3 called this first meeting of the Working Party to determine CH requirements for networking, and to discuss some related issues.

Summary of Proceedings:

It was agreed that CHR would produce a proposal for a short term strategy for cryptanalytic processing conversion, to be endorsed by CH. It was stated that this strategy would require a fast link between BACKER and MARSIK.

It was agreed that CHP, CHR and SMT3 would cooperate in a study to estimate the operational load that this link would have to handle.

Some general problems connected with the use of a link for cryptanalytic processing were raised. For example, the value of running interactive programs over a link was queried.

There followed some general discussion of the pro's and con's of

.

The discussion then turned towards longer term issues, in particular the decommissioning of BACKER. Some of the more interesting points made were:
* SMT2 estimated that if the four programs which used the most CPU time were converted, the load on BACKER would be reduced to one which would occupy only 8Ø% of a CYBER 83Ø.
* CHR1 estimated that this conversion would take about two man-years.
* A query which arose was "what would be the effect of doubling the amount of automatic processing on the CYBER ?" In particular, would this increase the CYBER load beyond the capacity of a CYBER 83Ø ? This was left as a subject for further investigation.

MINUTES OF THE SECOND MEETING OF THE MARSIK SOFTWARE WORKING PARTY

Date: 20th December 1985

Present:
(SMC), (CH), (SMT2), (SMC),
(CHR), (CHP), (CHR), (SMT2),
(CHR1), (SMT3) and (SMT2).

Distribution: ADD, SM, SMT, SMT2, SMC, CH, CHP, CHR

Background:

On the return to DSD of and this month, it was decided that a Working Party meeting should be held in order to hear of their impressions of NSA cryptanalytic computing (including their future plans), and to provide a forum for discussion with them on DSD planning for the use of MARSIK. The following agenda was drawn up in advance:

1. Opening Remarks
2. Minutes of last Meeting
3. Comments on Trip to NSA by ; NSA Plans for FOLKLORE etc.
4. Plans for Networking at DSD
5. on MARSIK
6. The Signals to NSA and GCHQ
7. Any other Business

Summary of Proceedings:

The opening remarks were made by CH, principally to explain the function of the Working Party meetings, and included reading the terms of reference.

The minutes of the last meeting were read by CHR, who reported on the work which followed. A CHR minute was published on the sixth of December which outlined the interim plan for incorporating MARSIK into CH crypt production. This paper also gave an estimate of the load on the BACKER - MARSIK link which is an important feature of this plan. The question raised in the last meeting about how a large increase in automatic processing would affect CPU time used by CH was investigated by . He found that relevant automatic processing used so little of the total CPU time that doubling it would not significantly increase the total.

and then spoke about their trip, and about NSA crypt processing generally. The following is a brief summary of what was said.

(a) They had problems getting access to relevant systems.

(b) The decision has been made that the FOLKLORE operating system will be phased out, but there were signs that it could be around for another 10 years or so. It appears that the replacement will be UNIX

(c) Conversion

(d) Compatibility:

(e) A very fast FORTRAN compiler NFT is being written by CRAY. It will be the successor product of CFT.

(f) are anxious that we should see their demonstrated.

(g) We should be getting the software for FOLKLORE.

(h) FOLKLORE is very slow at advancing job steps.

On the question of network software.

It was agreed that the short term plan outlined in the CHR paper (referred to above) was sensible, and SMC stated that they would provide the which is an integral part of the plan.

The most lively discussion of the meeting took place at the end when the issue of the CH signal to AUSLO was raised. The delay in the response was put down to two main causes. First, there was an unaccountable delay between the time the signal was sent and the time word was received . Second, apparently felt that a simple answer to each of the questions would convey a false impression. Nothing was heard from .