From: Frank Gill [Frank_Gill@ccm.jf.intel.com]
Sent: Monday, February 12, 1996 8:51 AM
To: Craig_Kinnie@ccm.jf.intel.com; Mike_Maerz@ccm.jf.intel.com; Jim_B_Johnson@ccm.jf.intel.com; Sandra_Morris@ccm.jf.intel.com; Patrick_P_Gelsinger@ccm.jf.intel.com; mcg@ibeam.intel.com
Subject: MS Meeting Notes

---------- Forwarded with Changes ----------
From: Parvinder S Kohli at JFCCM9
Date: 2/8/96 10:47AM
To: Frank Gill at JFCCM11
*To: Steve McGeady at SMTPGATE
*To: Craig Kinnie at JFCCM7
*To: Avram Miller at RNBCCM1
*To: Mike Richmond
*cc: Dave Landsman at FMCCM11
*cc: Robert Sullivan at SFG_NW1
*cc: George Cox at SMTPGATE
*cc: David Aucsmith at JFCCM10
*cc: Dave J Riss at SMTPGATE
*cc: Denise J Ecklund at SMTPGATE
*cc: Milind Khare
*cc: Melissa Laird at JFCCM7
Subject: MS Meeting Notes

To all: here is PS's trip report on security that i mentioned this morning at ms meeting. frank

We met with Microsoft yesterday; they brought Marshal Brumer and the Program Manager from the Personal Systems Division, in addition to the old gang. Dave Landsman already put out meeting minutes; this note is to convey the "between the lines" messages, to get a strategy discussion going.

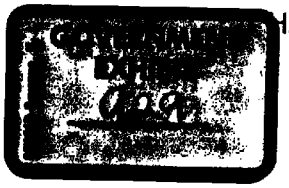
This was NOT the meeting we had planned for where we would get together and hammer out technical details for a consistent architectural direction; they did not bring the right technical people.

1. MS pulled the usual "we have been doing this all along" trick. They presented foils which essentially mirror our architecture; they introduced, for the first time, WinTrust and WinCert, direct analogues for the Integrity and Certificate Management aspects of CDSA. These two were the distinguising features of CDSA, as the crypto work was largely the same from both companies. Their comment: "it is amazing how two companies working independently arrived at the same architecture".

2. Advanced Techology Group, where the crypto and cert work has been going on, is now the PNBU (Public Networks Business Unit). PNBU is both a P&L (it will sell products) and develop technologies for use by other MS dividions (Personal Systems Div and Business Systems Div). THERE IS NO DISTINCTION OR FIREWALL BETWEEN API WORK AND INTERNAL USES OF THE APIs. In fact, when the WinTrust APIs are first exposed to the public in March, Internet Explorer will already have implemented them. It is clear that the work MS is doing in the crypto space is to get them competitive advantage in the browser wars, and later in the NT space. They WILL NOT sacrifice product schedules to achieve a broader, enabling architecture. Conclusion: MS will only address those aspects of security that their product needs demand, along a timeline that is driven by product release schedules.

3. They delivered two very strong messages to us (via Marshal); this seems to be the management direction they have received:
-if we do joint work, the end result is a MS API, NOT an Intel/MS spec. They were very sensitive to this. They are willing to take input, but will retain veto power.

477MSCID00064
Intel Business Information
Highly Confidential



-MS will not support a public forum a la WinSEC, only MS Open Design Review Process

4. The good news: they seem to have adopted our architecture as their own and claim that they will release it on a schedule that is maybe a 6 month delay from where we would have introduced our work. At least so they promise.

5. In order to get them to the next step of getting in a room and having a technical discussion at an API level and to further expose what engineering work they have in the cert space (we suspect there is very little there), we agreed to 3 above, with the caveat that if we do not see a willingness by MS to truly merge the collective works where they make sense, we will continue on our original plan of engaging the ISVs and creating an open forum and process to evolve the spec and implementation. They wanted us to shoot Winsec already, but we told them that we were committed to the open review process.

The Decision:
It is clear that we have two choices:
1. Work with MS and get them to include as much of our work as is possible into their CryptoAPI, WinTrust and WinCert efforts and use our resources to accelerate the integration effort. I think we will run into a considerable amount of NIH and it is unclear that we will meet our objective of widely deploying to the industry in '96

2. Strike out on our own. Change WinSEC to PCSec, do a Windows implementation and get leading ISVs to use it and get engaged with Netscape and Sunsoft for cross-platform implementations.

I am calling a meeting with Steve, Mike and Craig for next week to discuss this.

psk

Intel Business Information
Highly Confidential