From: Rich Lappenbusch
Sent: Monday, September 11, 2000 5:56 PM
To: DMD Strategy
Subject: 9/13 Pre-Reading and Agenda

DMD Strategy Team Meeting
9/13/2000
25/1069
3:30-5PM
Chaired by RichLap
\\churchill\strat\DMDStrategy\

Agenda Item #1: Personal Protected Content Sharing Service
Sandeep Sahasrabudhe for 40 minutes

P2P services, which share content, have exploded onto the Internet landscape recently, e.g. Napster, Aimster. As of now, these services allow their users to flout intellectual property rights and as a consequence have run into lawsuits. We have an opportunity to learn from the popularity of these services and launch a competing service of our own which could allow us to win on many fronts. The proposed service will allow end-users to share DRM-protected content with other users of the service. Typically an end-user will volunteer their protected content to the service and be able to download other protected content from other users. The downloaded content will come with an n-play license depending on the business model of the content producer. The n+1th playback will take the user to the content producer's site (or retailer's site depending on the business models) for purchase/advertisement etc. I believe that we have all the necessary technology to launch such a service and a supporting business model, which will enable us to win on multiple levels. For more information including why end-users might want to be a part of the service: <http://sandeeps/upnp/ppcs.doc>

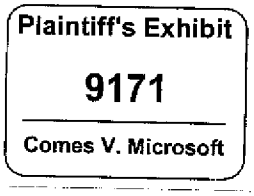
Decision needed:
Shall we required a P2P task force to build the concept up with input from a wider set of contributors?

Agenda Item #2: SVP and DRM for Down-Level Windows
Donna Liu for 40 minutes

SVP (secure video path) was an enhancement to DRM end-to-end security initially proposed for whistler, where the aims were to protect compressed video better by protecting the communications between the SDK and codecs, and to protect uncompressed video to the extent possible technically and of marketable value to customers. The latter was questionable, even with suggested changes to NT memory manager, due to VRAM easily accessible.

We now propose that we drop this deliverable from whistler and instead make it a feature of DRM as part of WMP9. We broaden the solution to include general plug-ins, and remove the dependency on memory manager changes. This solution provides better solution for compressed content, while the real solution to VRAM lies in hardware.

Decision needed:
We should decide whether to go for the revised proposal, taking into consideration if we need to tie the solution to the latest and greatest OS to make the OS platform more attractive for content owner to target. More broadly, we need to formulate strategies with regard to making DRM features available to down-level versions of Windows. Is it likely to help or hurt OS/DRM if we tie our features to latest and greatest OS when we don't



MS-CC-Bu 000000166342
HIGHLY CONFIDENTIAL

have to technically speaking?

Supporting Documents:

Given that the SVP work and the secure plug-in discussions are on a converging path, that we have found ways to decouple SVP from system changes, and that we have a shipping vehicle (WMP9/SDK9) six months after Whistler that will put the feature in the hands of consumers around the same time as Whistler itself, we have re-visited our plan for SVP, which will now include secure plug-in as well.

We had the following goals for SVP before

1) Protect compressed content
2) Protect uncompressed content where it makes sense
3) Have a phased approach that will showcase security advancement in latest os and our influence with IHVs to make PC more secure

With the proposal in this mail, we can achieve the additional goals:

4) Address secure plug-in as a generalized case of SVP. The content no longer has to tunnel through user mode. The user can enjoy the special effects etc. available on his PC.

5) Make the solution available on the installed base that content providers care very much about.

Modified Plan:

Near-Term: (WMP9)

We do a reasonable job protecting against intra-process and inter-process attacks in user mode through the following tactics:

- We will compile a list of modules loaded into the process. We will authenticate them through code signature not only on disk but in memory, not only once but periodically. We will watch out for performance impact, which may limit how often we could afford to check. The tactic will help catch hacker code loaded into the process and attempt from another process to patch the code. For authentication, we will need secure crypto code from crypto team and we already have an estimate from the crypto team that this dependency will be met in time for WMP9.

- We will include in DRM license agreement requirements for new apps not to enable frame stepping and capturing exposed in the new VMR in Whistler for DRM protected content. Hacker code will have to face touch synchronization on systems where double/triple/quadruple buffering is in the works. We'll re-visit the license agreement when write-only VRAM is available.

Charlie and PratulD will own putting in place the process (including license agreement additions) for code signatures on third party components.

Long-Term: (Blackcomb)

- Make inter-process attacks harder if possible

  We'll continue to work with NT team to see if there is any software-only solution they can facilitate to make the inter-process attacks (where another process can read from process memory, and so on) harder.

- Evangelize for IHVs to have write-only VRAM

  The component at the end of the graph will write to VRAM, after all the processing is done in user mode. No code in user or kernel mode can read from it. This is the only viable solution for kernel mode attack.

This proposal has been circulated through those on the Cc: line and bought off by them. I would like your approval to make it our plan of record. If more details than what we can communicate over the mail are necessary, I will set up a meeting for next week.

MS-CC-Bu 000000166343
HIGHLY CONFIDENTIAL