Digital Rights Management issues for Real-Time and Safety/Mission Critical Software

FSMLabs White Paper
Victor Yodaiken
(c) Finite State Machine Labs Inc.
yodaiken@fsmlabs.com

1 Problem

Digital Rights Management Passport (DRMP) technology (TCPA from Intel and Palladium from Microsoft and similar) is intended to make it hard to copy downloaded music or pirated software. Preventing teenagers from making copies of Eminem songs may seem harmless, but Internet Age technology is all about convergence. When a technology gets pervasively embedded in microprocessors, computer boards, and software, it will alter the performance of power turbines, jet engines, medical instruments, cell phones and missile guidance systems. Unfortunately, DRMP technology is incompatible with security and with the kinds of reliability needed in safety critical or mission critical applications. Ross Anderson has written an excellent comprehensive analysis of DRMP [1]. Here I want to look at some concrete consequences that are important in defense and manufacturing.

Despite marketing, DRMP is a licensing technology, not a security technology[2]. The combination of hardware and software being championed and fought over by the entertainment companies , Microsoft, and Intel, enforces something like an identity card or passport system on software. The idea is that DRM agents will be incorporated into software, processors[3], and other computer hardware and the DRM agents will examine files containing programs and data (such as digitized music) to make sure the file is attached to a valid digital passport. The passports prove that the file is being used within its license terms. Before you can play a movie on your PC, the DRM agent in the processor will demand the passport on the video player and the video player software will demand the passport of the video file. Before you run a word processor, some DRM agent will make sure you have a valid license and have not violated any of the fine print of the shrink-wrap license and that the file you are opening is something you have a license to read. Programs that do not incorporate certified DRM agents will not be able to get passports, so there will be a world-wide web of DRM agents working together.

[1] http:www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[2] TCPA denies this. You can find their arguments at http://www.trustedcomputing.org/tcpaasp4/index.asp

[3] Intel has announced that it will begin incorporating "trusted computing" agents into its next generation Pentium 4 processors.

2 Safety

The DRMP system is based on the premise that unlicensed use of software or data should make computers stop working. You could also argue that bridges should be designed to fall down if someone is detected crossing without paying the toll.

> *Heart patient Mr. Smith's life is in the hands of the sophisticated critical care life-support equipment that breaths for him, keeps his heart beating, delivers drugs in measured doses, and watches all his vital signs. A nurse plugs a digital thermometer into the life-support machine, not knowing that the thermometer was dropped and broken. The DRM agent in the core system tries to validate the passport on the new component, fails, declares that someone is stealing digital content, and shuts the main processor down. Too bad for Mr. Smith.*

DRMP advocates will say that I'm an alarmist and that there will be ways to turn off the DRMP system or mitigate the effects. This is hard to credit. Try browsing the Internet without enabling cookies and Java to see how easy it is for pervasive options to become non-optional. DRMP only works if two conditions are both true (1) it is physically impossible to turn the agent off and (2) DRM agents are omnipresent, creating an inescapable web of DRM. If there is a way to turn the DRM agent off in a processor, some teenager will discover it and distribute disabling software over the network.[4]. Let's figure out what would be needed to allow medical instrument makers to turn off DRMP.

1. Very expensive non-standard hardware. The cost savings of commodity chips will not be available.

2. Very expensive specially designed software. After all, poor Mr. Smith is dead just the same if the life support is shut down by the operating system, the data base, or the email program instead of the processor.

3. Very expensive specially designed networking. Undoubtedly, the life support machine must connect to the network to allow remote access, and to connect to medical records. If the database system refuses to provide the latest medical orders to the life-support machine because the life-support machine does not provide a valid passport, Mr. Smith is still in trouble.

4. A very expensive specially designed medical Internet. Mr. Smith's doctor's may want to access the National Library of Medicine database from their computers and use that information to adjust Mr. Smith's drug protocols. Oops, the NLM computer system asks for a passport!

In summary: it would be incredibly expensive and it still would not work.

DRMP advocates will say the DRM agents can just refuse to work with the thermometer and not shut the system down. But to make a safety critical system fail, you only need to cause a temporary delay. The DRM agent can endanger Mr. Smith by preempting the

[4]TPCA says that the hardware device that stores and handles encryption can be turned off locally. However, what this will mean in practice is that any DRM sofware will detect failure and refuse to operate.

operation of the heart-lung machine for few seconds while it rejects the passport. What happens if the thermometer data stops being tracked or if a more critical component is rejected? An emergency code is called, the defibrillator is plugged in and the first thing that the life support system does is to run a DRM agent to examine the passport! Most of us would agree that licensing should not be the first priority of safety critical or mission critical computer systems. But DRMP is based on the assumption that nothing is more important than licensing.

You cannot engineer a system to meet two conflicting imperatives at the same time. If nothing is more important than licenses, safety will suffer. If safety comes first, it will be easier to defeat licensing.

> *A detachment of special forces is pinned down by enemy fire. The bad guys have found a bug in the special forces target tracking software that allows them to confuse it, maybe by putting out heat sources that are right on the threshold of what is flagged as a target by the software. The good guys fix their program in the field, correct the bug and reinstall. The DRM agent rejects the new software and prints a little message: You have tried to run unlicensed software on this processor.*

DRMP assumes that users of computer systems are consumers who buy packaged software and content from a certified producer. But computers are not CD players. Users may need to modify software or create new software on the fly. This is as true of manufacturing companies as it is of investment banks and military units. Fix a minor software problem that is holding up production on your assembly line and, before you start running, get a new passport for the modified software. Field upgrade a jet engine control program and, until you can get a new passport made, your jet engine can be used as a paper weight. Just replacing a peripheral device can cause a DRMP system to refuse to run software. The passport for the operating system will no longer match the passport for the hardware and the DRM agent will not be able to distinguish this case from unlicensed reuse of the operating system in a new computer. So when you replace the network cards in your mission critical database cluster or manufacturing line control system the machine will be unusable until you get passwords reauthorized. This process may require the cooperation of multiple vendors.

3 Security

DRMP means that users no longer own computer systems, they have a status that is more similar to that of a tenant at will. . If you own a house, you can replace a door without asking permission from the landlord. Tenants, on the other hand, must ask permission for every modification. If you own a house, you decide who gets keys. Tenants may be required to put up with unannounced visits from the landlord. A tenant in such conditions has no possibility of security. The landlord has the keys and may use them at any time and may give copies to others, without notifying the tenant. If there is a door that won't lock, the tenant must request the landlord for permission to replace the lock. If the landlord is sloppy with key control, the tenant will pay the price.

Traditionally, "security" means "nobody else can take control of my computer or damage or access my data" but to DRMP, "security" means "no use of software or data not permitted by the passport system"[5]. DRMP is incompatible with security for four reasons.

1. DRM agents have ultimate control of the computer system. They cross all security boundaries, have access to all data and can control computation at all levels. If a DRMP based system is used in a secure setting, the "owner" of the system must trust set of complex control programs from multiple third parties that are specifically designed to prevent the owner from managing them.

2. DRMP is a hugely complex system that is an invitation for exploits, some of which are obvious and some of which will likely be quite surprising. How hard will it be to convince a DRM agent that your data base system passport is incorrect? What happens when a virus sends messages to the other systems in a cluster telling them that each of the others has been DRM compromised? The old last resort of reinstalling to remove infections may fail on a DRMP system once the hardware is convinced that something underhanded is going on or once the stored passports have been corrupted.

3. DRMP is going to ultimately require that DRM agents have access to the network so that they can query the central passport registry. Hackers will break the encryption for the agents and use these routes to break into your intra-net, disrupt operations, and steal information. While standard networking technology allows owners of computer systems to improve security by controlling their own firewalls, there is no assurance that DRMP will permit you to use your computer system if it cannot freely send queries back to the central registry. Since consumers have no control over DRM agents, once a virus has penetrated a DRM agent, the user will have no recourse but to wait for a fix from the central passport licensing bureau.

4. Any security failures in the central passport registry, industrial or state espionage, disgruntled employees, or stupidity or sloppiness, affects all systems infected with DRM agents utilizing the registry.

> *The computer aided manufacturing software in your factory is purchased from company ABC. After a year or two of operation, you've had it with the lousy performance of ABC's software. You purchase software from XYZ only to find that ABCs software has placed ABC passports in all of your manufacturing data. When the DRM agent checks to see if XYZ software can access that data, it sees the ABC software forbids use with XYZ software. The DRM agent is not interested in arguments that you own the data, it just checks passports. So you call up the central passport agency beg them for keys to change the passports. Much delay, legal wrangling, and unhappiness follow. When you resolve it, you find that ABC has sent copies of all your data to a competitor. ABC claims that its passwords in the files prove its ownership.*

[5]While Palladium does provide an ability to force security levels on data, far simpler and more reliable schemes for that are available.

The scenario above is unrealistic in one respect: the very existence of XYZ software as an alternative is unrealistic. Why? Because DRMP creates many barriers to entry. You can't just write new software and put it on the market. The new software needs to have a passport and incorporate an authorized DRM agent. If you want to market a new product that competes with an important Microsoft product, you may need to get Microsoft to license your use of their certified DRMP agent, certify your software is DRMP compliant, and issue you passports. How probable is it that such a situation will lead to a vibrant and competitive marketplace?

4 The solution: due diligence

All participants in the debate have interests at stake, and I am no exception. Semiconductor companies are hypnotized by the prospects of chip sales in entertainment. The "entertainment" industry wants to get paid for each listen or view and some software companies want to be able to go from selling products to charging rents. Civil libertarians hate the loss of privacy implicit in DRM and Free software people know that DRM may end up killing free software. My interest is pretty clear. Our company, FSMLabs, sells real-time control software that is used in many mission critical applications. Our business relies on a mix of commercial developer-seat/runtime licenses and open source licenses. Unauthorized copies of the commercial licensed products and unauthorized incorporation of the open source products into non-open source systems is not something we appreciate. If DRMP would stop piracy, we'd support it. But DRMP will stop competition more effectively than it will stop piracy and it will also put our customers at risk. We have made an enormous investment in developing reliable high performance software and making it securable. The field is still immature, the complexities are great and reliability is not easy to achieve. DRMP means that we are unable to control the behavior of our programs, and we shudder to think of what might happen if a DRM agent in some microprocessor silently destroyed the timing on a control system using our software.

Unlike some technical controversies, the facts of the DRMP debate can be easily determined non-experts. The trade press has seen through the "security" claims and a little reading will provide a great deal of information[6]. But the definitive determination is to ask vendors to share the risks of DRMP. Will vendors of DRMP infected software and hardware warrant that DRM agents or their hardware assistants will not cause or contribute to any safety or security failures? Will they provide a warranty that DRM agents cannot interfere with your fair use rights or your rights to use your own data or rights to use purchased digital data? It's easy to *say* that DRM passports are reliable and non-intrusive and that articles such as this one are alarmist. Accepting liability is something else. Will your vendor indemnify you against any losses due to DRMP? If the answer to the question on indemnification is, "no", the risks to purchasers are obvious. The potential gains are not obvious.

[6] http://www.extremetech.com/article2/0,3973,263367,00.asp