The following is a brief summary, of the Digital Rights Management talk given in class.

1 What is DRM?

DRM stands for Digital Rights Management, and deals with controlling what a consumer can/cannot do with a purchased digital item after the time of purchase. As you described, it is essentially the “Remote control” problem of remotely controlling the content after it has left your hands. You gave several examples, including digital music, digital books, and others. The problem is then one of piracy? How does one sell content online, yet still restrict what the consumer can do with said content after it leaves the sellers hands. The most interesting, and yet hardest of this family of problems is the problem of controlling digital music. Digital music is complicated by several factors, particularly the existence already of so many CD copies of songs as well as the emotional attachment so often associated with music. Furthermore, Digital Rights Management has other potential uses, including solving the online privacy problem. If one were to find a solution for DRM such could also be used to protect people’s privacy online.

Various sellers desire different protections, but an example of common protections include: no copying, limited number of reads, time limits, no forwarding, etc. Various solutions have already been tried, including the honor system (used in "donation-ware" and "The Plant" a book by Stephen King), simply giving up (HIPAA – and choose to attack the problem of accountability instead), various software solutions (some good, some bad), and finally tamper-resistant hardware solutions.

Surrounding (especially the later hardware and software attempts) there has been a lot of hype. Particularly companies touting the presence of various cryptographic algorithms in their solutions. As a student studying security, one must ask oneself however, does crypto really help? The answer, is of course ”no,” as crypto was designed to solve a different problem – one in which the final recipient could be trusted with the knowledge of the secret key. In DRM the problem then becomes, how do you keep the intended recipient from getting the key? The current solutions to this problems are generally security by obscurity, secret design, and again... if all else fails, have the marketing people hype the crypto.
2 Overview of MediaSnap

Following the brief overview of DRM, you talked a bit about the solution which your company, MediaSnap, had implemented. MediaSnap had a 2 part solution, consisting of a server, and client. The server, or "Secure Document Server" (SDS), in general held the keys which unlocked the document, the client held the document itself. The MediaSnap solution could operate in two different modes, both tethered (required a connection to the server) and un-tethered. Both were equally insecure. Basically the tethered solution kept the key on the server, only bringing it to the client briefly so as to decrypt the document. The un-tethered solution kept the key on the client... as obscured as possible. MediaSnap was unique at this time in that they were attempting an un-tethered solution. Unfortunately, as several papers have suggested obscurity is in the end impossible – someone will eventually find the key.

MediaSnap used a variety of methods to try and get around the problem, including encrypting the object code while on disk, running a kernel extension which tried to prevent a debugger, using multiple keys, utilizing very obscure code, separating the key parts, module tamper checking (hashing of in-memory object code), anti-screen capture, document watermarking, attempts at program "unique-ification" and other methods. Unfortunately, in the end none of these provide a perfect solution, similar to how cryptography can for other parts of security.

3 Other DRM Solutions

You mentioned a few other DRM solutions briefly, mostly commenting on how bad they were. Intertrust is one, characterized once as "a company whose business model appears to rely entirely on legal findings against Microsoft." Others, like SecretSeals are just complete silliness, making completely incredulous claims.

At this point you also introduced another model, the "respect model", as was used with Adobe eBooks. Basically Adobe described in great detail how to break their solution and basically asked that pdf readers simply (paraphrased) "respect the wishes of the original content owner." You also laughed briefly about MS-DRM version 2, which again violated the principles of cryptography, by rolling their own week block-cipher (MultiSwap) and using obfuscation. In short, there were no viable solutions 2 years ago, and likely none (at least not that anyone knows about) now.

4 Conclusions

You concluded then with your talk that current DRM systems are very weak. The ideal software-based solution is of-course one which at least makes it difficult for each individual user to copy the content out of the DRM system. Furthermore it must be robust (unique) enough to survive multiple attacks. In the end, I don’t believe that either is possible... but so we will see in years to come.