CSS / DeCSS

Frederick Reitberger
fredc@reitberger.org

Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

What is CSS?

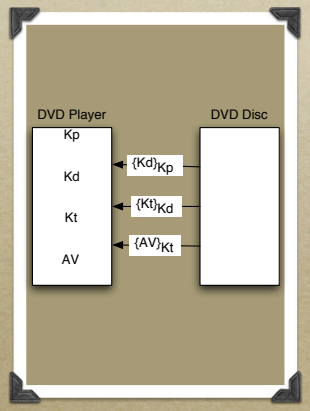
- *Content Scrambling System*
- *Used on DVD's*
- *Encrypts the Video and Audio Streams*

CSS

- *40-bit Encryption*
- *Each Licensed Player has its own key*
- *Each DVD knows 400 valid keys*

CSS

- *The Licensed Player key is used to decrypt a Disc Key*
- *The Disc Key will decrypt a Title Key*
- *The Title Key will decrypt the AV data for that title*



Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

Original Intents of CSS

- *Copy Protection*
- *Region Enforcing*
- *Non-Skippable FBI Warnings*

Other Consequences

- *Linux DVD Lockout*
- *Non-Skippable Advertisements*
- *What happens if someone moves from one DVD region to another region?*

Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

Weaknesses of CSS

- *Bit-wise Copies*
  - *Cheap DVD Burners (< $100)*
- *Only 40-bit encryption*
  - *Weak to brute-force*

CSS Weaknesses

- *Licensed DVD players must encrypt their player keys*
- *Multiple player keys reduce the key space*

Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

What is DeCSS?

- *A response to the above*
- *C Source Code to implement CSS decryption*
- *Originally intended for an Open Source Linux DVD player*

DeCSS

- *XingDVD failed to encrypt its player key*
- *Linux hackers reverse-engineered XingDVD and were able to retrieve a player key*
- *After one key was found, many more were discovered with brute force methods*

Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

Legal Issues

- *Legality of DeCSS*
- *Is DeCSS protected by the First Amendment as Free Speech?*
- *Fair Use and Copyright Issues*
- *7-9 GB per DVD - Where to store this data?*

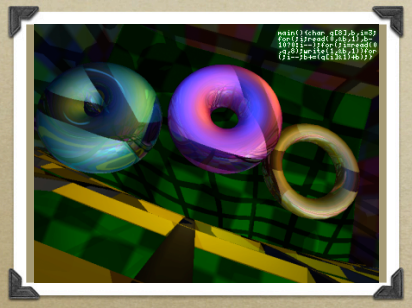
Legal Issues

- *Lawsuits filed against authors and anyone linking to sites with DeCSS*
- *DeCSS Obfuscation and Mirroring*
- *Illegal Prime Numbers*

Illegal Prime Number

```
4
8565078965 7397829309 8418946942 8613770744 2087351357
9240196520 7366869851 3401047237 4469687974 3992611751
0973777701 0274475280 4905883138 4037549709 9879096539
5522701171 2157025974 6669932402 2683459661 9606034851
7424977358 4685188556 7457025712 5474999648 2194184655
7100841190 8625971694 7970799152 0048667099 7592359606
1320725973 7979936188 6063169144 7358830024 5336972781
8139147979 5551339994 9394882899 8469178361 0018259789
0103160196 1835034344 8956870538 4520853804 5842415654
8248893338 0474758711 2833959896 8522325446 0840897111
9771276941 2079586244 0547161321 0050064598 2017696177
1809478113 6220027234 4827224932 3259547234 6880029277
7649790614 8129840428 3457201463 4896854716 9082354737
8356619721 8622496943 1622716663 9390554302 4156473292
4855248991 2257394665 4862714048 2117138124 3882177176
0298412552 4464744505 5834628144 8833563190 2725319590
4392838737 6407391689 1257924055 0156208897 8716337599
9107887084 9081590975 4801928576 8451988596 3053238234
9055809203 2999603234 4711407760 1984716353 1161713078
5760848622 3637028357 0104961259 5681846785 9653331007
7017991614 6744725492 7283348691 6000647585 9174627812
1269007351 8309241530 1063028932 9566584366 2000800476
7789679843 8209079761 9859493646 3093805863 3672146969
5975027968 7712057249 9666698056 1453382074 1203159337
7030994915 2746918356 5937621022 2006812679 8273445760
9380203044 7912277498 0917955938 3871210005 8876668925
8448700470 7725524970 6044465212 7130404321 1826101035
9118647666 2963858495 0874484973 7347686142 0880529443
```

Steganography



Outline

- *What is CSS?*
- *Original Intents of CSS*
- *Weaknesses of CSS*
- *What is DeCSS?*
- *Legal Issues*
- *Timeline*

Timeline

- *September 1996 - DVD Format Specification*
- *1997-1998 - Growth of DVD Market*
- *1998 - Methods to Copy DVDs put to use*
- *October/November 1999 - DeCSS announced on LiViD mailing list*

Timeline

- *December 1999 - MPAA Seeks Temporary Restraint Order*
- *January 2000 - Trial Begins*
- *July 2000 - Ruling in Favor of MPAA*
- *November 2003 - Author of DeCSS creates tool to remove DRM from AAC files*

References

- *http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/plain-english.html*
- *http://www.wired.com/news/technology/0,1282,32263,00.html*
- *http://en.wikipedia.org/wiki/DeCSS*
- *http://www.cs.nmsu.edu/~joshagam/css/*
- *http://www.opendvd.org/*