OmniQ

Section 1201 Roundtable Class 3
UCLA

Johann George

My Background

- Co-founded, managed and/or advised 7 startups to successful exits.
- Co-authored several patents: 12 issued so far.
- Wrote Coherent, the first Unix-compliant operating system to run on x86 hardware; was indirectly used to develop Linux.
- Entered University of Waterloo at age 13.

OmniQ: Recap

- Transfer data from DVD or Blu-Ray to another electronic medium without making a copy
- Data is re-encrypted using multiple 2048 bit keys
- At all times, continue to respect the intent of CSS and AACS: do not permit copies to be made
- Requesting exemption to permit reading and decryption of media while strengthening intent of copy protection

Encryption

- Video data is broken up into chunks, likely a megabyte in size, each of which is encrypted with its own 2048 bit key.
- Better protection than CSS (Content Scrambling System) which uses 40 bit keys or AACS (Advanced Access Content System) which uses 128 bit keys.
- Unlike CSS and AACS, which use a single key for all the data, each megabyte chunk is encrypted with its own 2048 bit key.
- Encryption algorithm is a stream cipher similar to CSS and AACS.
- Each time data is moved, new keys are generated limiting the lifetime of each key.

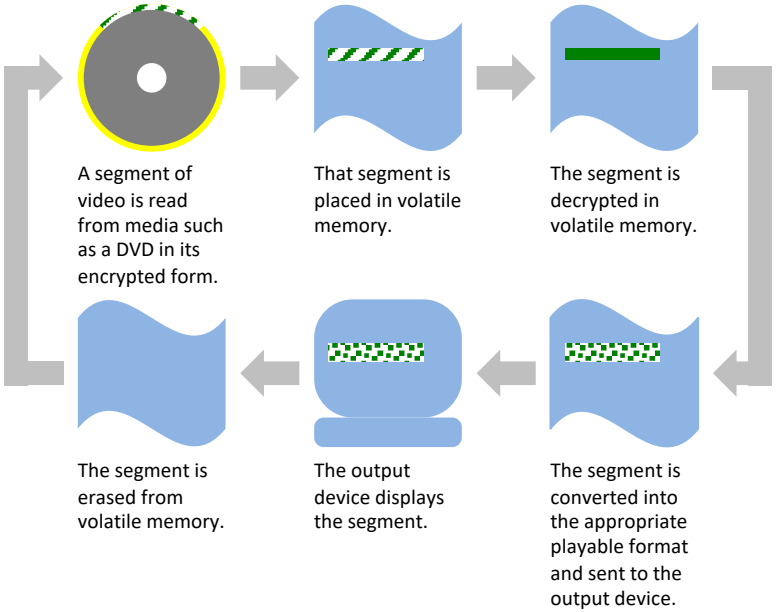
Transitory Duration

- Each megabyte chunk of data exists in volatile memory for less than a second.
- When moving data across a network, it needs to remain in volatile memory for as long as is needed to send it to the recipient and erase it from the sender.
- With average latencies in the U.S. of 50 ms and average transfer speeds of 50 Mbit/sec, a megabyte of data is transferred in about 250 ms.
- It can take another 50 ms to let the sender know that that data has been received and about 50 ms for the sender to erase the data bringing the total to 350 ms or well under ½ second.
- In cases where transfer speeds are slower, smaller chunks may be sent.

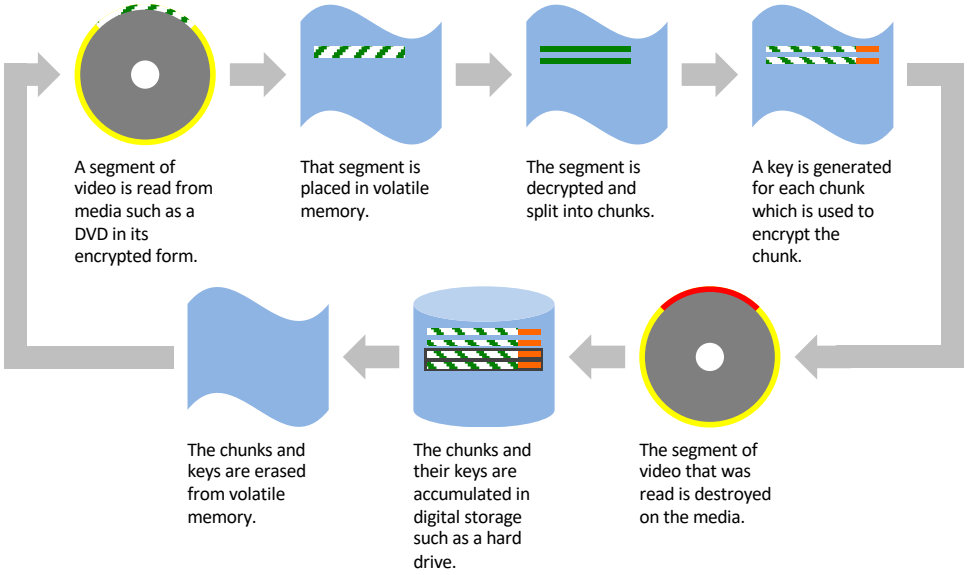
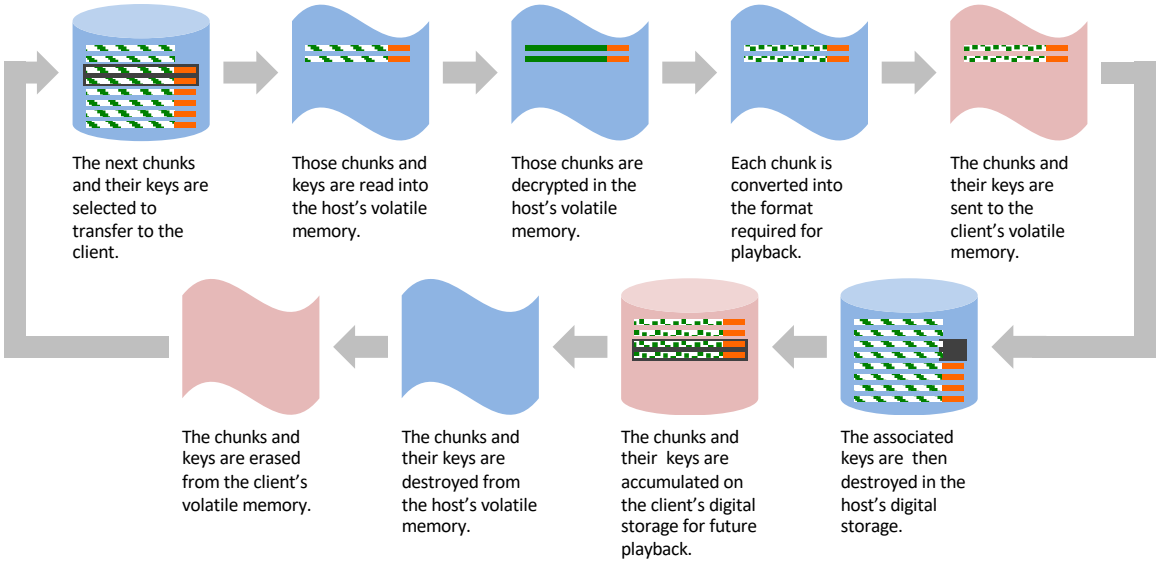
Supplemental

OmniQ

How A Media Player Works



Moving Video Data To Digital Storage With Encryption



Moving Video Data Across A Network