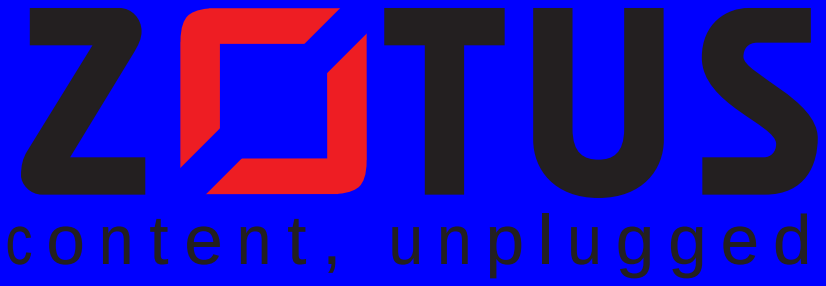


Secret-free DRM and efficient delivery method

Presented by Yves Legris (yves@zotus.com)

Contact: Vladan Djakovic, CEO
415.934.0373 voice, 415.934.1276 fx, vladan@zotus.com
601 Van Ness Ave suite E-841, San Francisco, CA 94102

The Agenda

ZOTUS
content, unplugged

1. The Two Proven Mistakes in DRM
2. The Fundamental Solution for the Above
3. Application Samples

Prepared for CPTWG. Jan 11 2007

The Proven Mistake #1 - Secret-based DRM

ZOTUS
content, unplugged

- We shall create a tamper-proof end-user agent that will enforce our policies, based on some secret it knows but end-users don't, so they can't "emulate it on a PC".
- We shall sell this agent to millions of end users, and they will not figure how to extract that secret, ever. And even if they do, we can today predict the ways in which they can do it in the future, and we can prepare the agent today to deal with that.
- This time we shall do it right.

The Proven Mistake #2 - Streaming

ZOTUS
content, unplugged

- Forget DRM. The content will be streamed from the central server to the end user once the end user is authenticated in real time. This way we can ensure the compliance. The cost of serving ($0.25/GB) will be calculated into the price.
- Realistic consumer bandwidth, 0.5 to 1 Mbit/sec, 6-15 times less than the DVD quality, will be accepted as “DVD quality”. Later we call it High Definition.
- The above is an acceptable substitute for DVDs to consumers.

What if ...

ZOTUS
content, unplugged

- End user agents had no secrets in them whatsoever?

  Nothing to emulate on a PC. Nothing to transmit via Internet.

- Content could be superdistributed, unprotected and unsupervised, to anyone, paying customer or not, in full quality via cheapest available means (P2P, broadcast, truckloads of free DVDs) ?

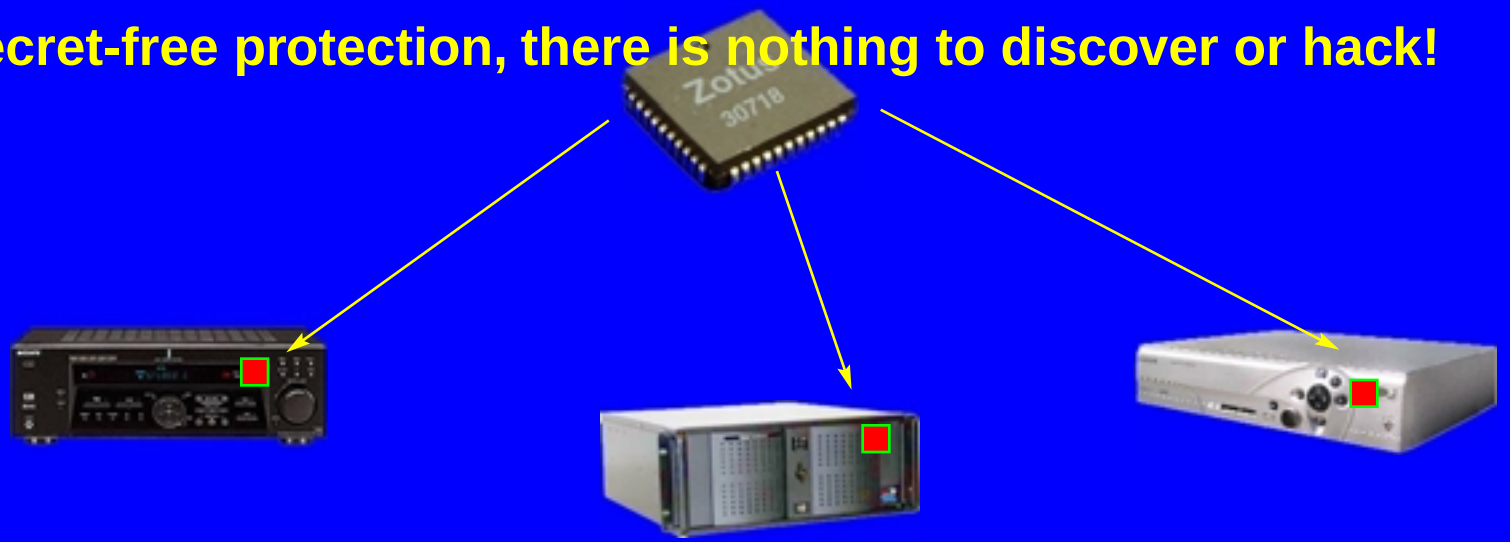
  Multi-gigabyte movies and games at near-zero delivery cost.

- ... and yet only the authorized end users could play the content?

  Simple as owning legit DVD.

Enter Zotus

- Conditional access method completely encapsulated in a low cost ASIC core (silicon chip.)
- Security not contingent on the environment, software, operating systems or communication protocols. Completely transparent and works within the existing infrastructure.
- Strong identity for untethered players.
- Superdistribution without BOBE (Break Once, Break Everywhere.)
- Secret-free protection, there is nothing to discover or hack!



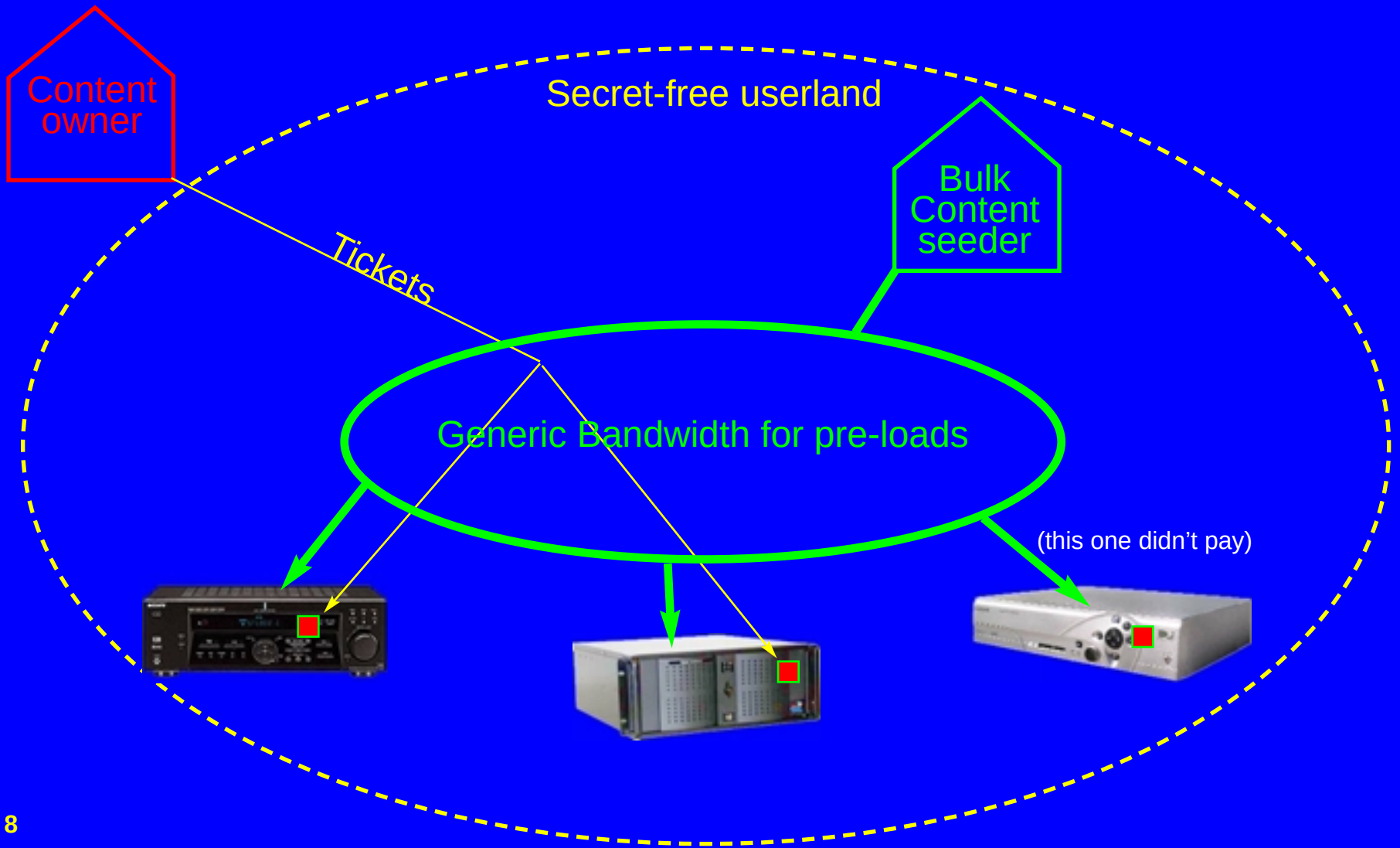
How it works ?

ZOTUS
content, unplugged

- Each playback device has Z-core with unique identity. No secrets on chip - everyone knows everything about each Z-core.
- Each content is prepared the same for everyone. Everyone knows exactly how.
- A ‘ticket’ (256-byte string) is issued to each playback device for each authorized content. The ticket itself has no secrets, can be freely copied but cannot be forged.
- Yet, without a ‘ticket’ specific to the playback device and to the content, which only the content owner can mint, the content is unusable.

No secrets in userland!

- No secret keys.
- No secret algorithms.
- No secure communication.
- Nothing to find out.



Breaking protection means building hardware per user

- Requires $10K+ investment per user to foil ... or 500 high-end PCs. This is a sample point on the cost/barrier curve.
- Reviewed and inspected. Uses proven crypto components decades old. No home-brew crypto.
- Breaking Zotus is always harder than analog recapture.

Legitimate

VS.

$10K+ FPGA board

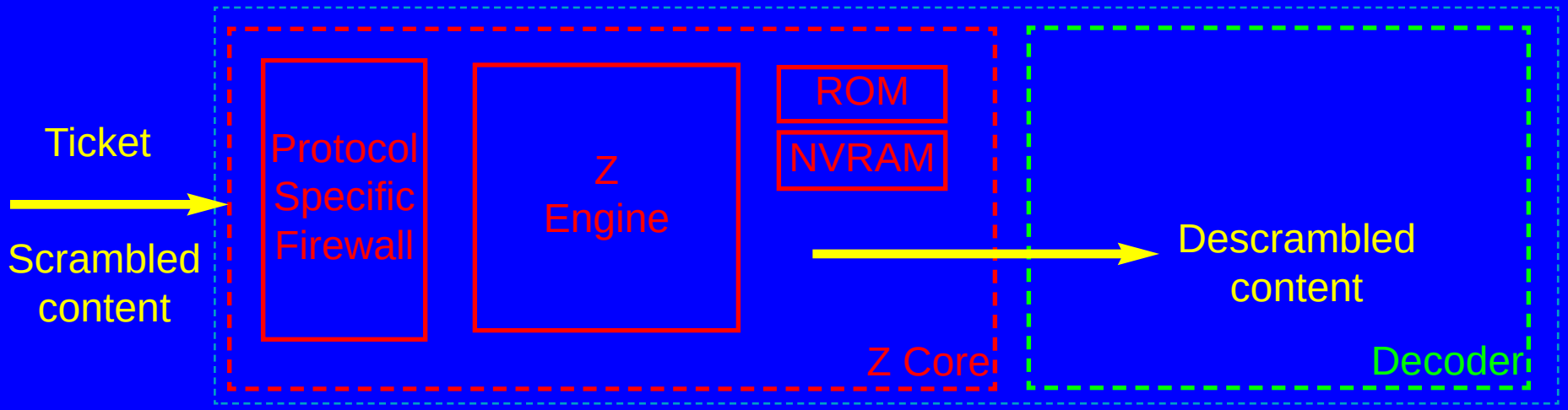
Illegitimate

500+ PCs

Prepared for CPTWG, Jan 11 2007

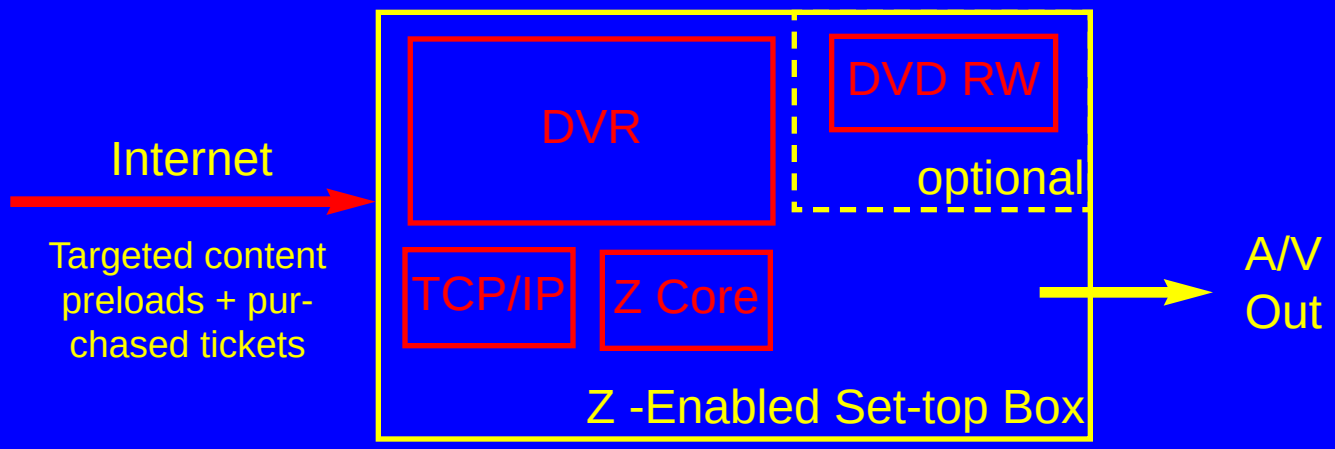
The Z Core

- The core has nearly 1 M gates for the stated circumvention barrier.
- The semiconductor process is not critical - synthesis on 0.18µ standard library shows 100 MHz performance with 6.4 Gbit/sec max throughput.
- Customized bits sit either on the external flash component wired under the same epoxy, or on the same silicon if the foundry has efficient NVRAM cells.



Sample Design - STB

- DVR + IP protocol stack + Z core + glue logic.
- Supervised P2P transport enables individually targeted DVD quality (4-6Gb per movie) preloads.
- Uses public networks because it does not require secure transport.
- Timed rental or purchase.



Q & A

ZOTUS

content, unplugged