Applications and Product Differentiation

- Digital rights management (enterprise as well as retail copyright management)
- Credit card and other payments information protection
- Identity management, authorization and authentication, identity theft protection
- Information protection (desktop, laptop, portable, etc.)
- Identity [theft] *protection* through *detection*.
- Digital media distribution, management and playback
- Secure file interchange with scalable distributed topologies

Securing the World's Information

Whitenoise Laboratories Inc.
Andre Brisson
VP Business Development
Co-Founder
abrisson@wnlabs.com

701 – 1736 W. 10th Ave.
Vancouver BC
Canada V6J 2A6

http://www.whitenoiselabs.com

Emerging Technology Award Finalist

2006 West Coast Security Forum

Network and application security

Content, data and privacy protection and detection

Securing the World's Information

Vision

The Whitenoise vision is to collectively make the Lower Mainland a center of excellence in digital security technologies.

DIVA™ Dynamic Identity Verification & Authentication

Whitenoise Labs

The Company has developed intellectual property in the area of protected media and content distribution, with innovative identity-preserving features and functions including unprecedented circumvention-detection capabilities. It has successfully protected this property via patent filings in over 40 countries covering two thirds of the world's population and economic activity.

Whitenoise Technology

WNL has developed a methodology for obscuring data at rest as well as in transit. Rather than mathematically related keys as is common in modern digital cryptography, the company uses a cyclic combination of prime numbers in conjunction with a reliable source of entropy to generate long "keys," referred to herein as *WNkeys*. The specific primes and the random string together constitute a "key structure." The WN algorithm, given a specific key structure, will reproduce a specific WNkey.

These extremely long WNkeys are consumed bit-by-bit in a simple operation that obscures the data of interest. For instance, each bit of content can be *x-or*'d with consecutive bits of the WNkey whose key structure is known only to the authorized end-points. This operation is far less computationally demanding than conventional cryptographic and DRM techniques, and has survived the scrutiny of acknowledged industry experts.

W***here other approaches and technologies offer a wide range of variously robust protection, WNL also offers robust detection. This is a critical differentiator.***

"Exhaustive key search is not a threat. Even if we hypothesized the existence of some magic computer that could test a trillion trillion key trials per second (very unlikely!), and even if we could place a trillion trillion such computers somewhere throughout the universe (even more unlikely!), and even if we were willing to wait a trillion trillion years (not a chance!), then the probability that we would discover the correct key would be negligible (about $1/2^{1340}$, which is unimaginably small). In this report, I tried every attack I could think of. All of them failed. This provides evidence for the hypothesis that Whitenoise is cryptographically secure."

-Professor David Wagner, Berkeley, October 2003

In addition to the data protection aspects related above, the process can also provide meaningful and highly differentiated authentication features. The critical insight here is that as content is being consumed, so is the WNkey being consumed. An aspect of the interaction between two end-points is therefore the index into the WNkey. This value is not likely to be known by third parties. Even if the WNkey was stolen, or were the corresponding key structure compromised along with knowledge of the WNL algorithm, on-going use of the WNkey to gain unauthorized access to protected data would *not* be possible without the index value corresponding to the authorized history of use between legitimate correspondents.

This continuous authentication and detection feature is called Dynamic Identity Verification and Authentication [DIVA]. The DIVA sings only for the correct audience. Not only will illegitimate users of the WNkey be denied, but the legitimate users will immediately and automatically benefit from knowledge of the attack and attempted unauthorized use: the WNkey does not need to be explicitly revoked, it will simply become unusable to its legitimate owner.