Yandex Cloud

Об одной модели нарушителя, возникающей при анализе систем полнодискового шифрования

Василий Николаев
Cryptography Services

Что обычно представляем?

- «Украли ноутбук».
  - Конфиденциальность под явной угрозой.
- Среда не скомпрометирована.
  - Если есть доступ к рабочей среде – подобрали пароль, украли разлогиненный ноутбук – game over.
- Нельзя навязать подтасованные данные.
  - Украденный диск как правило не подкидывают назад.

https://stock.adobe.com/ru/images/Thief-stealing-laptop-computer/70917639

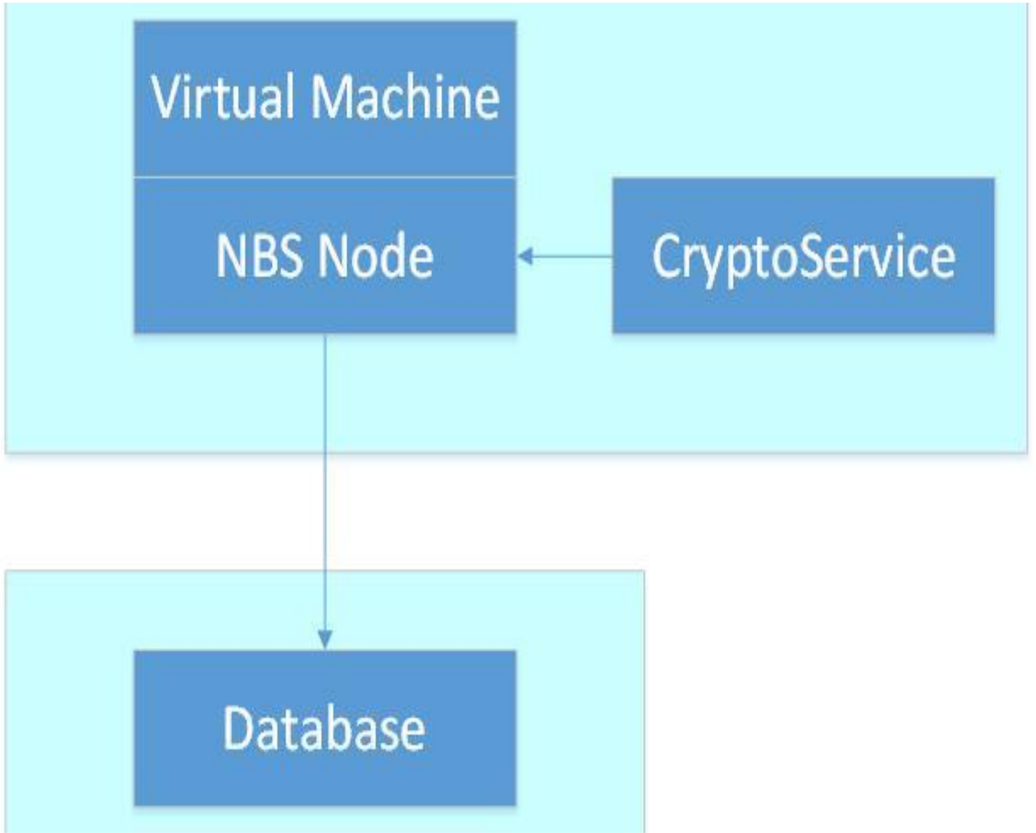
Страшный вывод

- Контроль целостности не нужен!
  - Сложно организовать.
  - «Нет адекватной модели нарушителя!»
- Используй AES-XTS и будет тебе счастье.
  - Почти все disk encryption software так и делает.
- Ну может быть и надо, но потом.

http://4pda.ru/2018/01/22/349305/?utm_source=thematic1

Network Block Storage

- Сервис дискового шифратора.
- Стандартные операции чтения/записи блока данных.
- Ключи шифрования доступны через отдельный сервис.
- Криптооперации на доверенной машине.
- Хранение данных в БД вне доверенного периметра.
- БД не доверенная!



Особенности модели

- Связь между VM и БД по незащищенному каналу.
- Физического пространства сильно больше, чем размер виртуального диска.
- Есть небольшое доверенное хранилище.

https://stock.adobe.com/images/concept-of-data-storage/46847370

Дополнения в модель нарушителя

Channel eavesdropper

Storage administrator

https://www.alamy.com/the-eavesdropper-english-the-eavesdropper-1657-oil-on-canvas-92-x-121-cm-dordrechts-museum-dordrecht-1657-92-x-121-1657-841-maes-eavesdropper-dordrecht-image185843681.html?irclickid=UQownkS6nxyNUviSyOTL63PeUkASfVw5FR%3A-yk0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1

https://stock.adobe.com/images/Hacker-seated-in-server-room-launching-cyberattack-on-laptop/466425851

Что на практике?

- GCP: AES256-XTS (но дополнительно криптозащита на уровне инфраструктуры).
- AWS: AES256-XTS (но дополнительно криптозащита на уровне инфраструктуры).

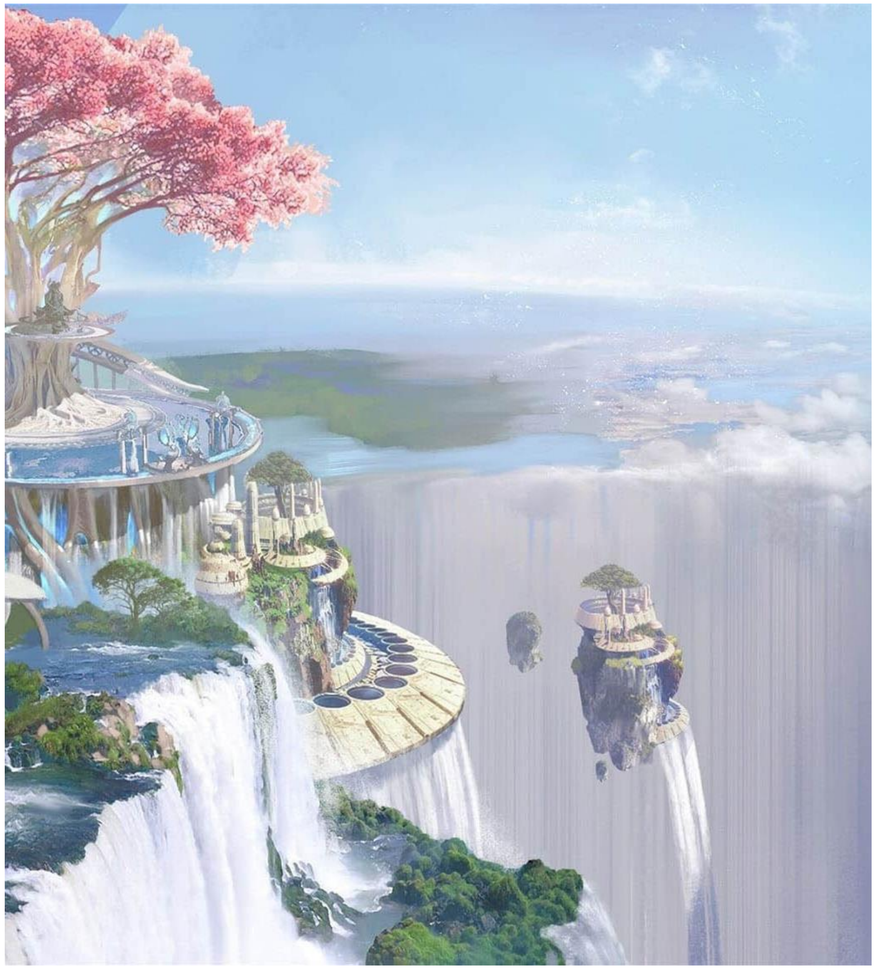
- Фактически предлагается доверять хранилищу данных.
- Контроль целостности на уровне NBS не заявлен!

https://stock.adobe.com/images/Cloud-Computing-In-Blue-And-White/448439646

Идеальный мир?

- Стандартизированное криптографическое решение для FDE с контролем целостности.

- Его реализация и повсеместное распространение.



Вопросы?

Василий Николаев
Software Developer
Cryptography Services
vasnikolaev@yandex-team.ru