РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ НЕФТИ И ГАЗА
ИМЕНИ И.М.ГУБКИНА

Идентификация личности - ключевая проблема облачной подписи

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ РОССИИ
А.П. БАРАНОВ
baranov.ap@yandex.ru

П.А. БАРАНОВ, к.т.н.

baranov.ap@yandex.ru

Облачная технология ЭП

1. Классическая технология: ключ ЭП и криптопровайдер «на борту» пользователя
2. Облачная технология: ключ и криптопровайдер отсутствуют «на борту», где только формируется сообщение и подтверждается после возврата из облака
3. В Windows криптопровайдер вместе с ОС «на борту», а где на самом деле ключ, знает только АНБ США
4. SSL в Windows работает, как и везде, через УЦ или АНБ США
5. Отечественный пользователь не может так безбрежно использовать отечественный ключ и криптопровайдера, как у Microsoft, поскольку нет Windows или Linux с предустановленным отечественным криптопровайдером, хотя бы и имени ФСБ России. Крипто API от Windows у нас известен не полностью

baranov.ap@yandex.ru

УЦ в облачном виде

1. КЭП, выданная в УЦ, имеет много общего с паспортом, удостоверяющем личность и выданном в паспортном столе МВД
2. По всем тенденциям однажды выданный КлЭП может обновляться далее каждый год без личной явки
3. КЭП позволяет удаленно осуществлять большое число юридически значимых действий без физической идентификации личности заявителя
4. КЭП, подтвержденная в УЦ, позволяет делать ряд объемных финансовых и хозяйственных действий
5. УЦ при выдаче КлЭП обязан хотя бы один раз удостоверить заявляемый юридический статус биологическому объекту
6. «Старые» УЦ становятся партнерскими филиалами перелицензированных УЦ с прежними традициями

baranov.ap@yandex.ru

Облачный ЭДО и его взаимодействие с УЦ

1. ЭДО – является посредником между пользователем и УЦ, хранящим ключ подписи пользователя
2. Кто определяет соответствие биологического объекта заявленному юридическому статусу пользователя? Система ЭДО или УЦ?
3. Кому будут предъявляться юридические и финансовые претензии: коммерческому ЭДО или государственному УЦ?
4. Подтверждение для ЭДО личности заявителя (пользователя) основано лишь на факте отзыва на запрос подтверждения, пришедшего на номер абонента
5. Определение номера запросчика и его отображение на смартфоне есть процесс верхнего уровня ПО, а Центр авторизации сотовой связи, работает на нижнем уровне связи в модели ISO. На этом работают пранкеры

baranov.ap@yandex.ru

ЭДО и подтверждение физической сущности. Соревнование защиты и нападения

1. Стандартный тезис оценки надежности криптосхем – ее известность, как алгоритмическая, так и на уровне образцов реализации в ПО или железе
2. Наряду с «доказуемой» стойкостью в условиях моделирования ситуаций, применяется оценка стойкости в круге известных методов нападения
3. Обоснование стойкости конкретной криптосхемы многолетний научно-технический процесс
4. Подтверждение принадлежности биометрических данных конкретной физической сущности (личности) также является схемой обеспечения безопасности, для которой надо определить ее стойкость т.е. надежность
5. Следовательно, надо четко формулировать модели для логического доказательства или очертить круг методов нападения в которых алгоритм определения соответствия стойкий с доказанными значениями ошибок

baranov.ap@yandex.ru

Биометрия и ошибки

1. Начиная с 10 IPhone, есть для домашних экспериментов алгоритм распознавания лица владельца вместо пароля. Отличное поле для исследования одной из лучших разработок
2. Несмотря на всякие околонаучные рассуждения разработчиков систем распознавания, есть только два связанных параметра:

$$\alpha = P\{\text{принять } H_1 | H_0\} \text{ и}$$

$$\beta = P\{\text{принять } H_0 | H_1\}$$

3. Часто, но не всегда: чем меньше (больше) α, тем больше (меньше) ß. IPhone настроен так, чтобы α была большей, а ß - меньшей
4. Насколько близки должны быть лица или физические сущности, чтобы они гарантировали те или иные ошибки α и ß и их соотношения?
5. Где результаты серьезных научно-технических экспертиз свободных, непредвзятых, объективных экспертов?

ХРАНЕНИЕ – ДВИЖЕНИЕ ВО ВРЕМЕНИ

- 1. 4 основных формы движения информации: передача, использование, хранение и переработка.
- 2. Информационная безопасность (ИБ) хранения соответствует также классическому подходу: конфиденциальность, целостность, доступность.
- 3. Накопление в базах данных или озерах данных – способы обеспечения ИБ: шифрование (конфиденциальность); электронная подпись (целостность); расшифрование (полное или частичное) на ключе хранения при каждом обращении (доступность)
- 4. Применение биометрических данных в массовой географически распределенной системе высокой степени риска и ее ИБ: передача по сети шифрованной информации не на ключе хранения, а на ключе взаимодействия с конечным потребителем. Не хранение биометрии на месте, а гарантированное уничтожение после применения (конфиденциальность); проверка целостности- самая простая процедура; непрерывная высокоскоростная связь с ЦОДом хранения(доступность)

baranov.ap@yandex.ru

Проблема хранения базы биометрических образов и передачи от оператора в Центр авторизации

1. Идея накопления миллионов биометрических образов лиц (не только пальцев) граждан безумна! Проблема защищаемых на определенное время по Закону физических лиц
2. При любом хранении информации существуют значительная вероятность ее утечки, что демонстрируется на примерах утечек Гостайны, шпионах и Сбербанком
3. Соревнование экспертных систем распознавания и подделки лица личности - борьба щита и кинжала
4. В отличие от скомпрометированного ключа электронной подписи биометрический образ физической личности заменить нельзя! Разве что пластической операцией или маской
5. Утечка биометрии требует абсолютного изъятия из удаленного оборота конкретных личностей и фиксации этих личностей в юридически значимых списках
6. При массовой идентификации (проход в метро), где будут храниться биометрические образы для сравнения на станциях или в Центре авторизации?

baranov.ap@yandex.ru

Заключение

1. Аналогия Центра хранения биометрии имеется в виде Центра авторизации сотовой связи с ключами SIM карт
2. Разница в последствиях компрометации ключей и биометрии, заключается в возможности, в последнем случае, несанкционированного применения КЭП и невозможности изменения биометрии личности
3. За рубежом распознавание личности по биометрии лица используется в малозначимых процедурах. США отключили применение биометрии в удаленных банковских операциях и ожидают накопления опыта в других странах
4. В России – полигон новых опасных технологий с невосполнимыми потерями для граждан в случае утечки их биометрии, которую изменить нельзя при предъявлении себя, но которую можно подсунуть вместо объекта

Спасибо за внимание

baranov.ap@yandex.ru