# Что плохого можно сделать, неправильно используя криптоалгоритмы?

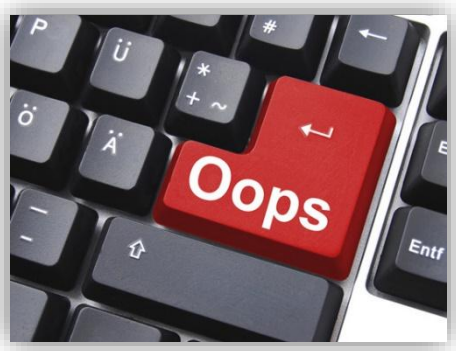
Алексеев Евгений Константинович,
к.ф-.м.н., начальник отдела криптографических исследований

КРИПТОПРО

CTCrypt’2019

# Теория vs Практика


Перенос на практику




- Многочисленные теоретические исследования
- Одобрение научного сообщества
- Создание стандартов

- Нарушение штатного функционирования системы
- Компрометация критичных данных
- Подделка электронных подписей

Где, что и почему пошло не так?

КРИПТОПРО

# Теория vs Практика

- Не бывает просто стойких или просто безопасных криптосистем

- E. Rescorla (rfc 3552):

  Most people speak of security as if it were a single monolithic property of a protocol or system, however, upon reflection, one realizes that it is clearly not true. Rather, security is a series of related but somewhat independent properties. Not all of these properties are required for every application.

- В ходе анализа криптосистемы «живут» в модельных условиях, которые составляют так называемую **модель противника**

КРИПТОПРО

# Модель противника

## Атака

Возможности противника по взаимодействию с системой

**Модель противника**

## Ресурсы противника

Предположения о вычислительных и информационных ресурсах противника

## Угроза

Задача противника по нарушению свойств безопасности

КРИПТОПРО

# Модель противника

- Модель для симметричных систем шифрования:
  - ✓ Интуитивное свойство – противник не получает никакой информации о защищаемых данных
  - ✓ Формализации – модели на основе задачи определения бита (LOR, ROR и т.п.)
  - ✓ Типы атак – с адаптивным выбором открытых текстов, с выбором открытых и шифрованных текстов

- Модель для протоколов установления защищенного канала:
  - ✓ Противник полностью контролирует каналы передачи данных (может изменять, удалять, добавлять сообщения в канал)
  - ✓ Может обладать или не обладать возможностью вскрывать долговременные ключи легитимных сторон

# Жизненный цикл криптосистем

**Реальная система**
(решаемые задачи безопасности)

Моделирование

**Модельная система**
(включает модели противника)

КРИПТОПРО

# Жизненный цикл криптосистем

**Реальная система**
(решаемые задачи безопасности)

Моделирование

**Модельная система**
(включает модели противника)

Синтез и анализ

**Криптографические алгоритмы и протоколы**

КРИПТОПРО

# Жизненный цикл криптосистем

**Реальная система** (решаемые задачи безопасности)

Моделирование

**Модельная система** (включает модели противника)

Синтез и анализ

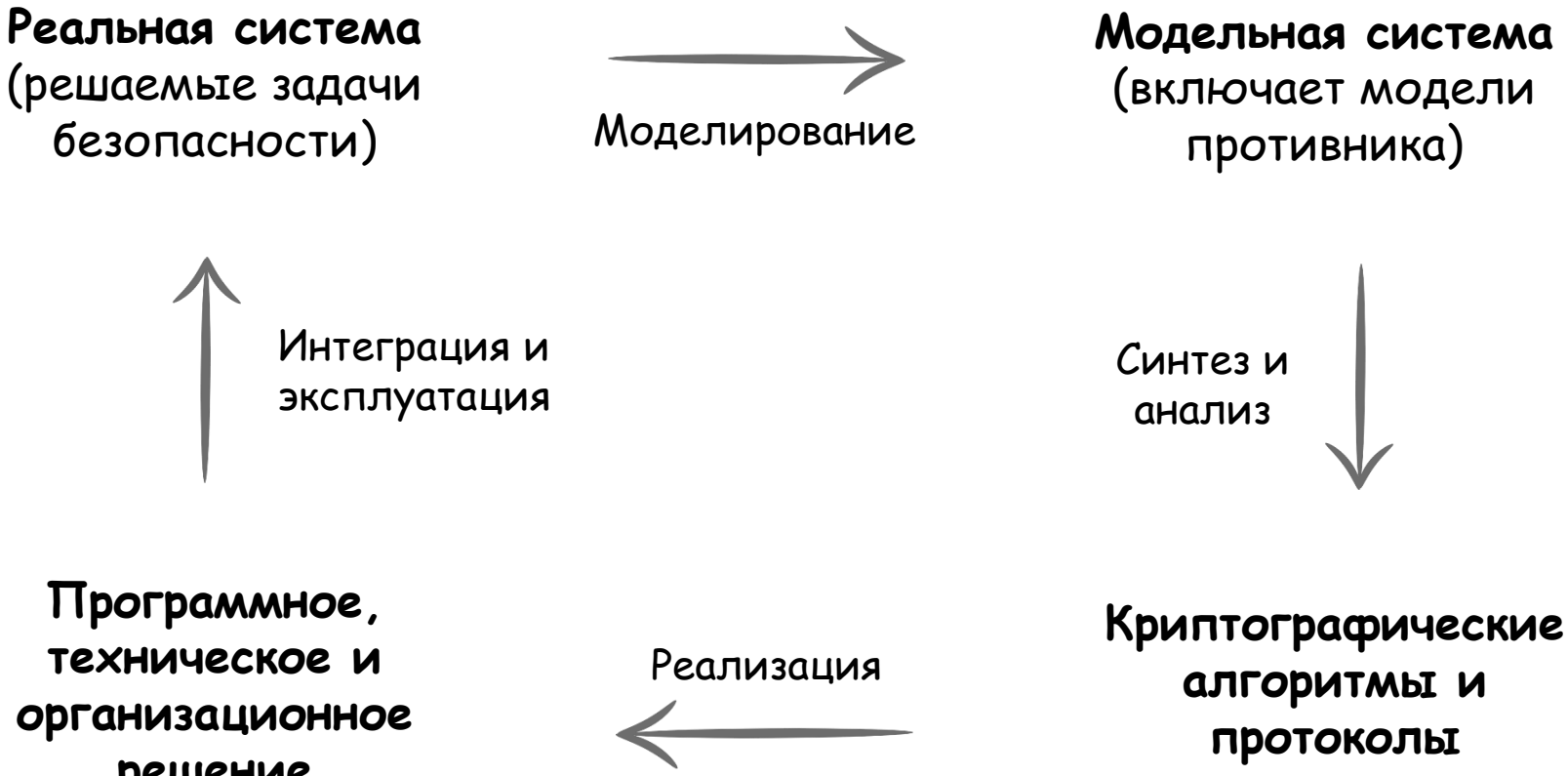
**Криптографические алгоритмы и протоколы**

Реализация

**Программное, техническое и организационное решение**

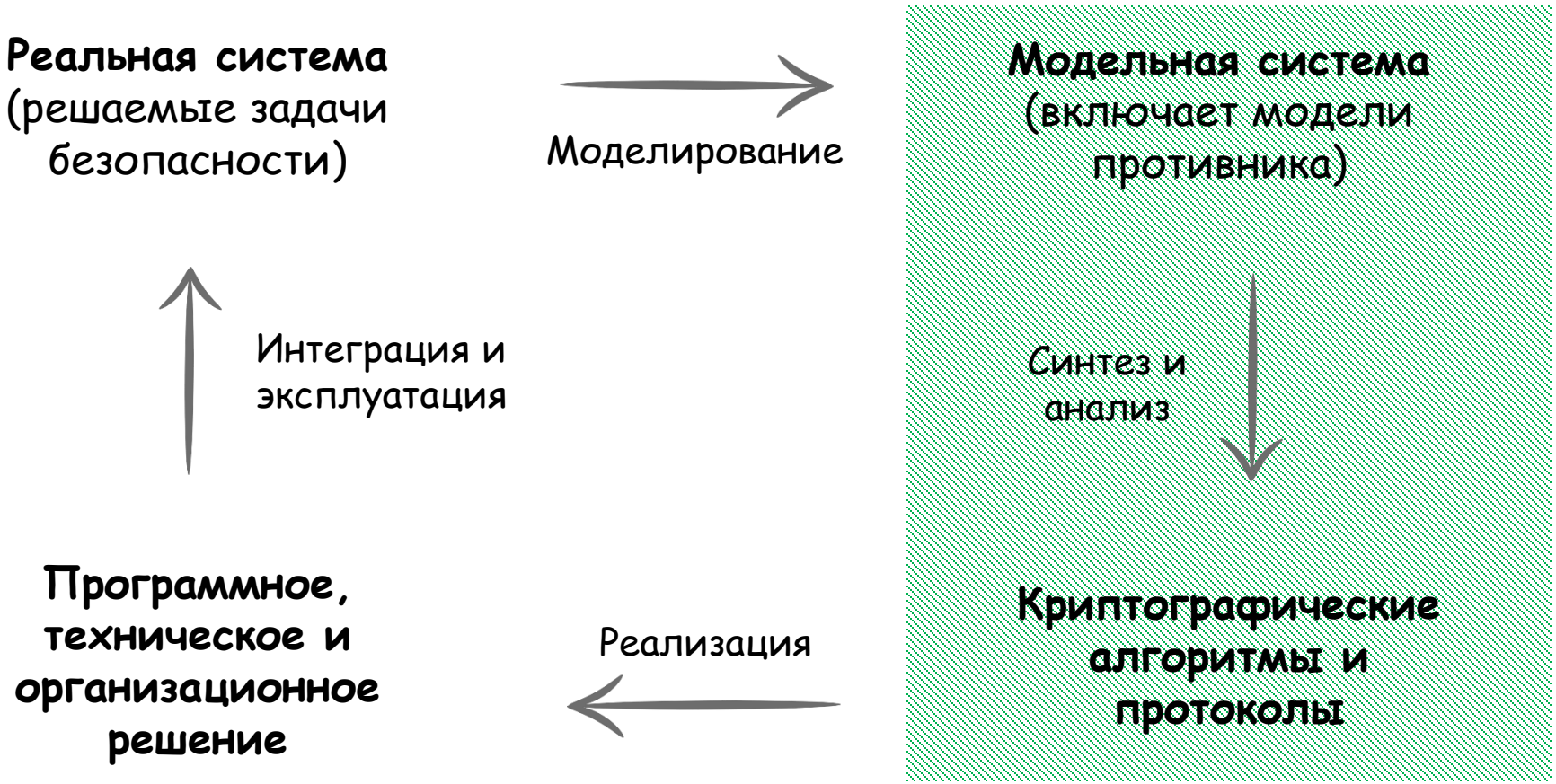
КРИПТОПРО

# Жизненный цикл криптосистем




КРИПТОПРО

# Жизненный цикл криптосистем

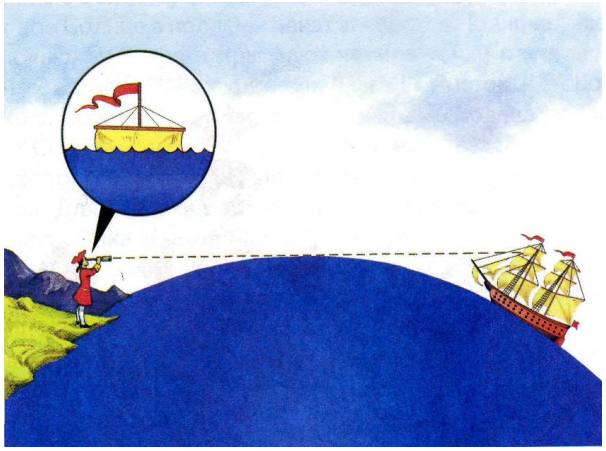



КРИПТОПРО

# Проблемы моделирования

Реальность:

Плоская земля



?

КРИПТОПРО

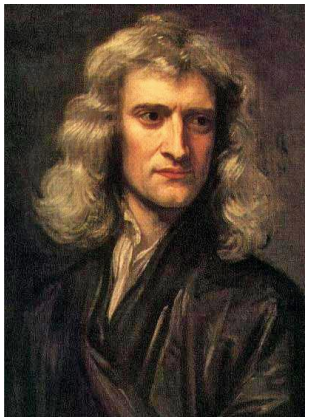
# Проблемы моделирования

Реальность:

Плоская земля

Шар

Проблемы с явлениями, связанными с суточным вращением Земли



?

КРИПТОПРО

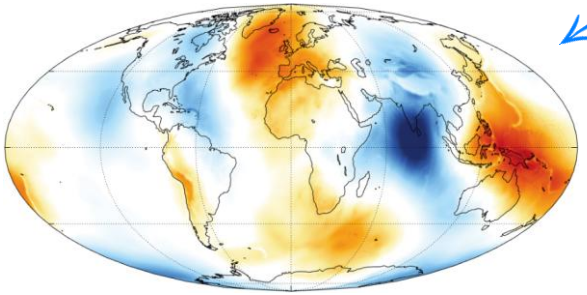
# Проблемы моделирования

Реальность:

Плоская земля

Шар

Эллипсоид вращения



Вопросы из геодезии и навигации

?

КРИПТОПРО

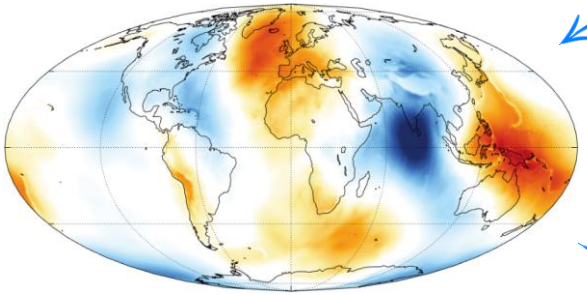
# Проблемы моделирования

Реальность:

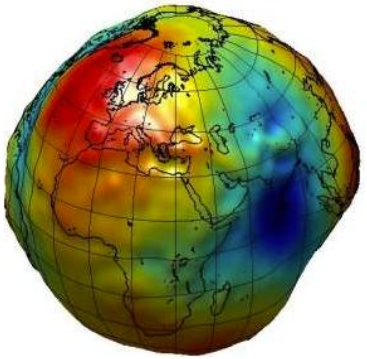
Плоская земля

Шар

Эллипсоид вращения



Геоид



КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

# Несоответствие атаки

Возможные причины несоответствия:

1. На этапе моделирования некоторые возможности противника были сочтены несущественными или попросту не были замечены
2. На этапе реализации у криптосистемы появились особенности и свойства, которых не должно было быть

Примеры:

1. Атаки с дополнительной информацией на TLS.Record
2. Атака на ePSK в TLS 1.3
3. Дополнительная фрагментация
4. Bug-атака на эллиптические кривые

КРИПТОПРО

# Несоответствие атаки (атаки на TLS.Record)

- 2001 год. В работе Кравчика «The Order of Encryption and Authentication for Protecting Communications (Or: How Secure Is SSL?)» доказана стойкость схемы Authenticate-then-Encrypt, которая используется для защиты данных в протоколе TLS.Record.

- 2002 год. В работе «Password Interception in a SSL/TLS Channel» (Canvel B., Hiltgen A., Vaudenay S., Vuagnoux M.) описана атака на реализацию протокола TLS.Record в OpenSSL.

- Причина: не учли, что что противник на практике получает информацию о том, где конкретно произошла ошибка при расшифровании – при проверке корректности дополнительных данных (padding) или при проверке имитовставки.

- 2008 год. Модель противника была расширена с учетом данной особенности: «Immunising CBC Mode against Padding Oracle Attacks: A Formal Security Treatment» (K.G. Paterson и G.J. Watson)

КРИПТОПРО

# Несоответствие атаки (ePSK TLS 1.3)

- 2016 год. В работе «A Unilateral-to-Mutual Authentication Compiler for Key Exchange (with Applications to Client Authentication in TLS 1.3)» (Krawczyk H.) приведено следующее замечание:

«*We exclude the case where the attacker has the same PSK key shared with both C and S in which case a transcript replication attack is unavoidable.*»

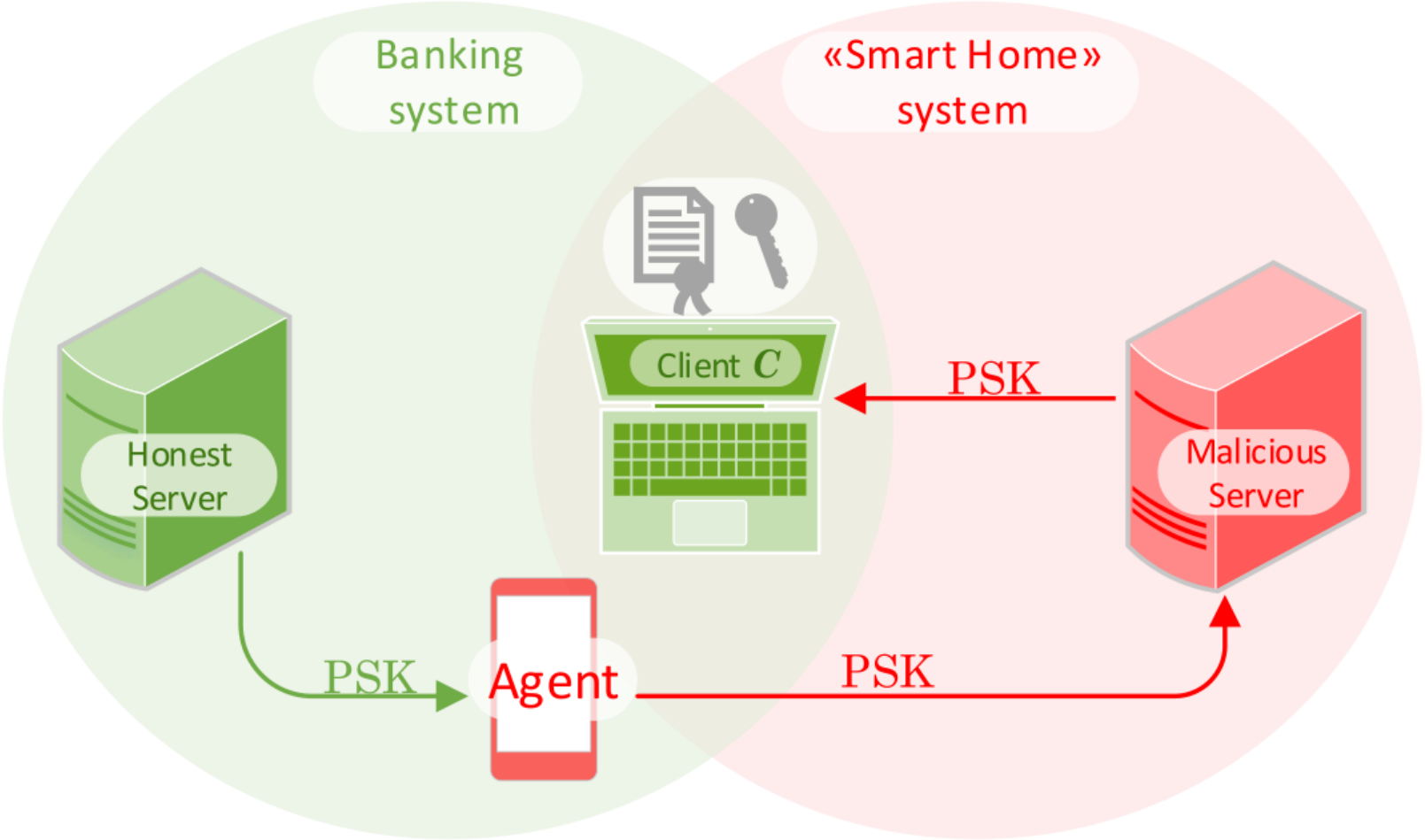
- 2018 год. Протокол TLS 1.3 принят без каких-либо примечаний или контрмер, направленных на устранение данной уязвимости.

- Возможность разделения одного и того же внешнего PSK более чем двумя сторонами признано практически неосуществимым.

- Обратное обосновано в работе «Continuing to reflect on TLS 1.3 with external PSK» (Akhmetzyanova L., Alekseev E., Smyshlyaeva E., Sokolov A.), 2019 год.

КРИПТОПРО

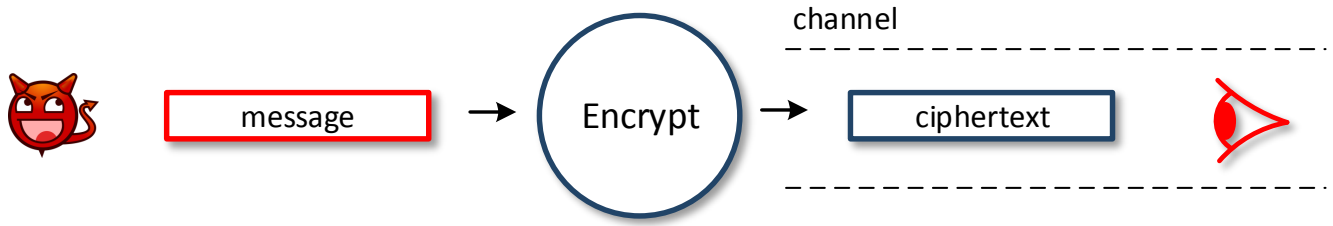
# Несоответствие атаки (ePSK TLS 1.3)



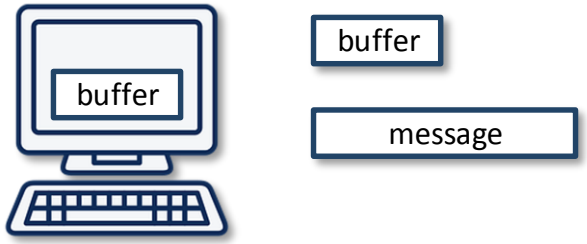

КРИПТОПРО

# Несоответствие атаки (вынужденная фрагментация)

- Модельный мир:

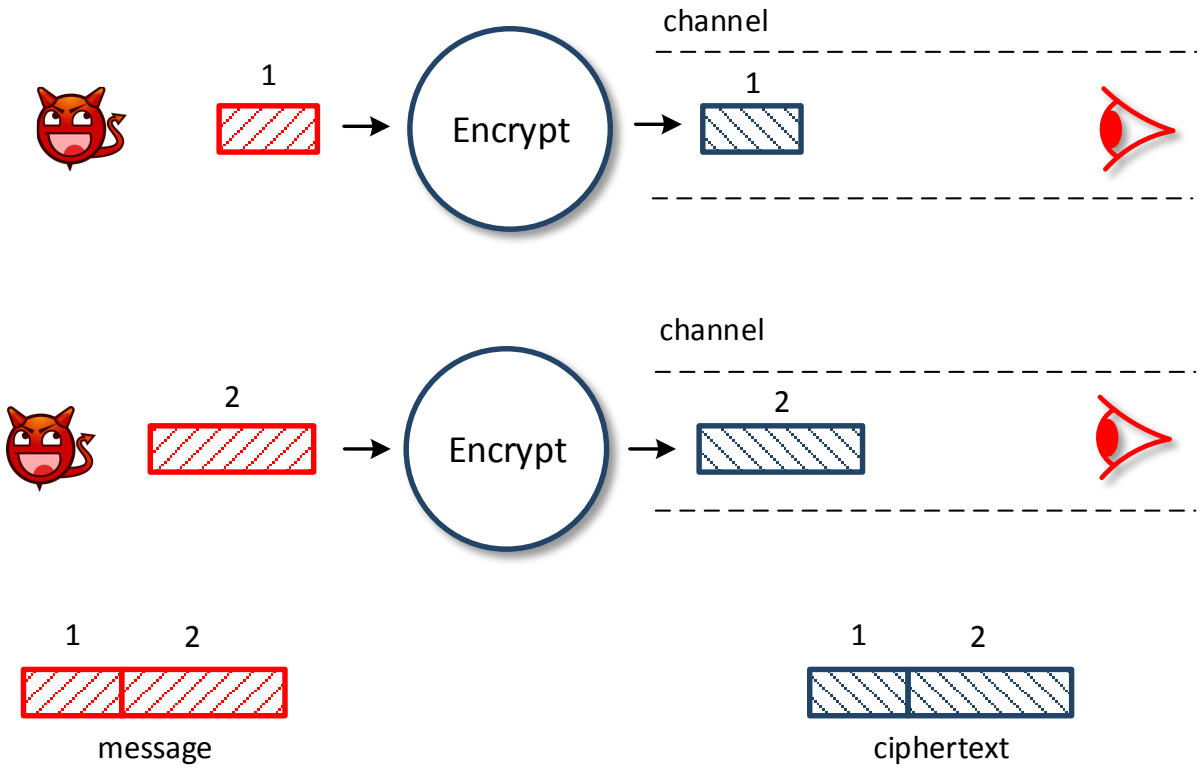



- Реальность:




КРИПТОПРО

# Несоответствие атаки (вынужденная фрагментация)




- 2002 год. «Authenticated Encryption in SSH: Provably Fixing the SSH Binary Packet Protocol» (Bellare M., Kohno T., Namprempre C.).
- 2006 год. «Modes of Encryption Secure against Blockwise-Adaptive Chosen-Plaintext Attack» (G. Bard).

КРИПТОПРО

# Несоответствие атаки (Bug-атаки)

- 2011 год. «Practical realisation and elimination of an ECC-related software bug attack» (B. B. Brumley, M. Barbosa, D. Page, F. Vercauteren)

- На основе ошибки в реализации арифметики в одной из версий OpenSSL был предложен метод восстановления закрытого ключа TLS-сервера:

**Abstract.** We analyse and exploit implementation features in OpenSSL version 0.9.8*g* which permit an attack against ECDH-based functionality. The attack, although more general, can recover the entire (static) private key from an associated SSL server via 633 adaptive queries when the NIST curve P-256 is used. One can view it as a software-oriented ana-

КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

# Несоответствие угрозы

При моделировании некоторые возможные ситуации не были расценены, как негативные. То есть не были учтены все аспекты обеспечиваемого свойства безопасности.

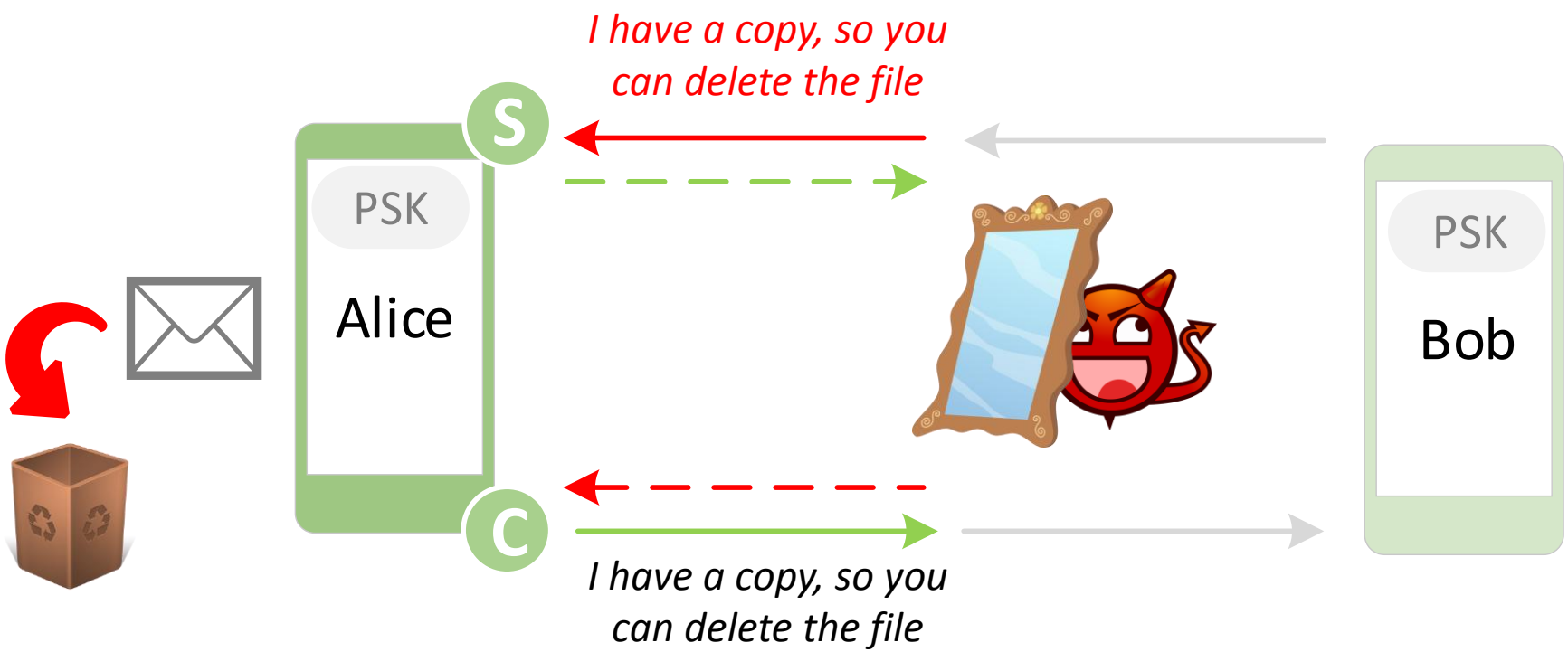
Примеры:

- Атака Selfie на TLS 1.3
- Защита голосовых сообщений с помощью DTLS

КРИПТОПРО

# Несоответствие угрозы (Selfie TLS 1.3)

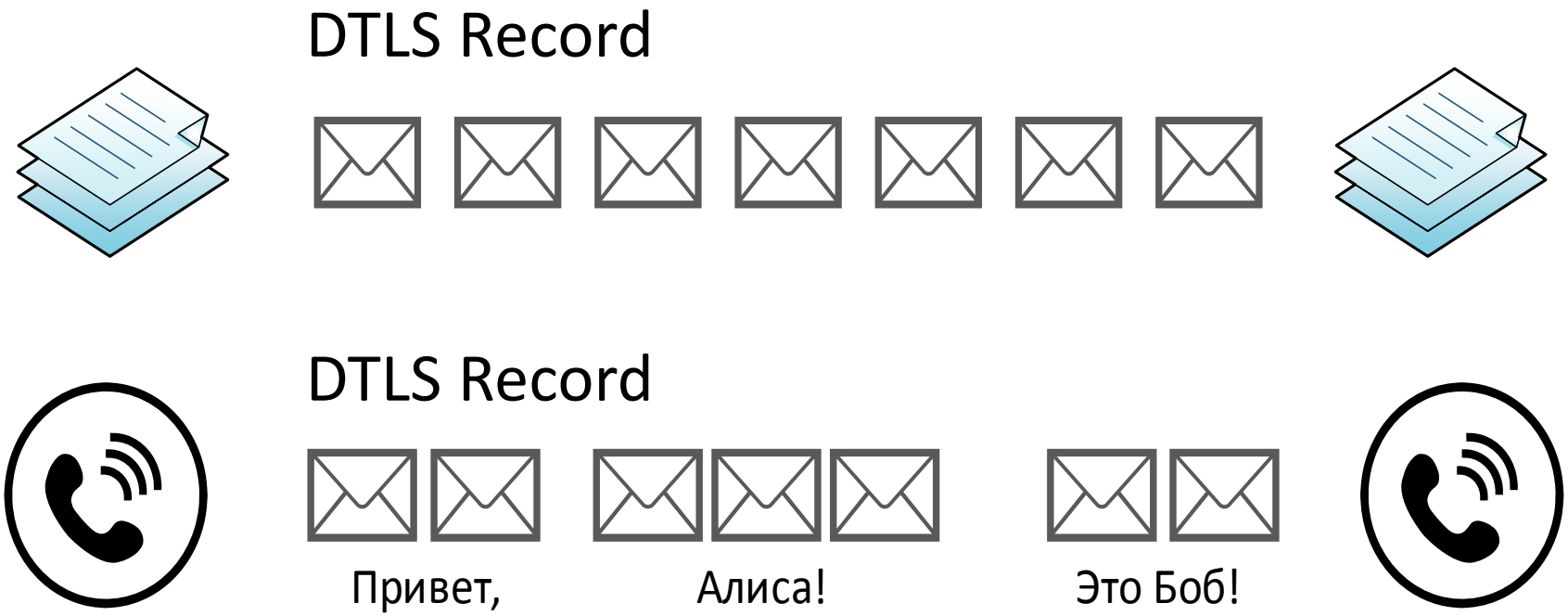
**Угроза**: клиент устанавливает соединения сам с собой




КРИПТОПРО

# Несоответствие угрозы (Voice Encryption)

**Угроза**: нарушение конфиденциальности на уровне потока сообщений (размеры сообщений)




КРИПТОПРО

# Несоответствие угрозы (Voice Encryption)

- 2011 год. «Phonotactic reconstruction of encrypted VoIP conversations: Hookt on fon-iks» (White A., Matthews A., Kevin Z. Snow K., and Monrose F.)

***Abstract*—In this work, we unveil new privacy threats against Voice-over-IP (VoIP) communications. Although prior work has shown that the interaction of variable bit-rate codecs and length-preserving stream ciphers leaks information, we show that the threat is more serious than previously thought. In particular, we derive approximate transcripts of encrypted VoIP conversations by segmenting an observed packet stream into subsequences representing individual phonemes and classifying those subsequences by the phonemes they encode. Drawing on insights from the computational linguistics and speech recognition communities, we apply novel techniques for unmasking parts of the conversation. We believe our ability to do so underscores the importance of designing secure (yet efficient) ways to protect the confidentiality of VoIP conversations.**

- Расширение модели: Boundary Hiding (BH-CPA). «Security of Symmetric Encryption in the Presence of Ciphertext Fragmentation» (Boldyreva A., Degabriele J.P., Paterson K.G., Stam M.), 2015 год.

КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

# Несоответствие предположений о ресурсах

На практике ресурсы, доступные противнику, оказались существенно больше, чем это предполагалось в модели.

Примеры:

- Sweet32
- Отсутствие счетчиков в PAKE-протоколах

КРИПТОПРО

# Несоответствие ресурсов (Sweet32)

- 2000 год. Оценка стойкости приведена в классической работе «A Concrete Security Treatment of Symmetric Encryption» (M. Bellare, A. Desai, E. Jokipii, P. Rogaway).

**Theorem 17** [**Security of** CBC **using a pseudorandom permutation**] *Suppose $F$ is a PRP family with length $l$. Then, for any $t, q_e$ and $\mu_e = ql$,*

$$\mathbf{Adv}^{\text{lor-cpa}}_{\text{CBC}[F]}(\cdot, t, q_e, \mu_e) \leq 2 \cdot \mathbf{Adv}^{\text{prp}}_{F}(t, q) + q^2 2^{-l-1} + \left(\frac{\mu_e^2}{l^2} - \frac{\mu_e}{l}\right) \cdot 2^{-l} \; . \blacksquare$$

- В то время данная оценка даже для 64-битных шифров представлялась совершенно недостижимой, поэтому не была принята в расчет.

- 2016 год. В работе «On the Practical (In-)Security of 64-bit Block Ciphers» (K. Bhargavan, G. Leurent) продемонстрирована возможность восстановления секретного значения cookie при использовании 64-битного шифра 3DES.

- Для атаки необходимо около 800 ГБ трафика (в среднем 30 часов работы)

КРИПТОПРО

# Несоответствие ресурсов (безоружный PAKE)

- PAKE-протоколы – протоколы выработки общего ключа с аутентификацией на основе пароля.
- Matthew Green (blog): «*PAKE is actually one of the most useful technologies that (almost) never gets used. It should be deployed everywhere, and yet it isn't.*»
- Основная цель PAKE-протоколов – защита от offline-перебора, т.е. от перебора в условиях, когда противник может задействовать довольно большие вычислительные мощности.
- При этом PAKE-протоколы беззащитны против online-перебора, когда противник просто пытается раз за разом установить соединения с использованием разных паролей

КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

# Ковбойский подход

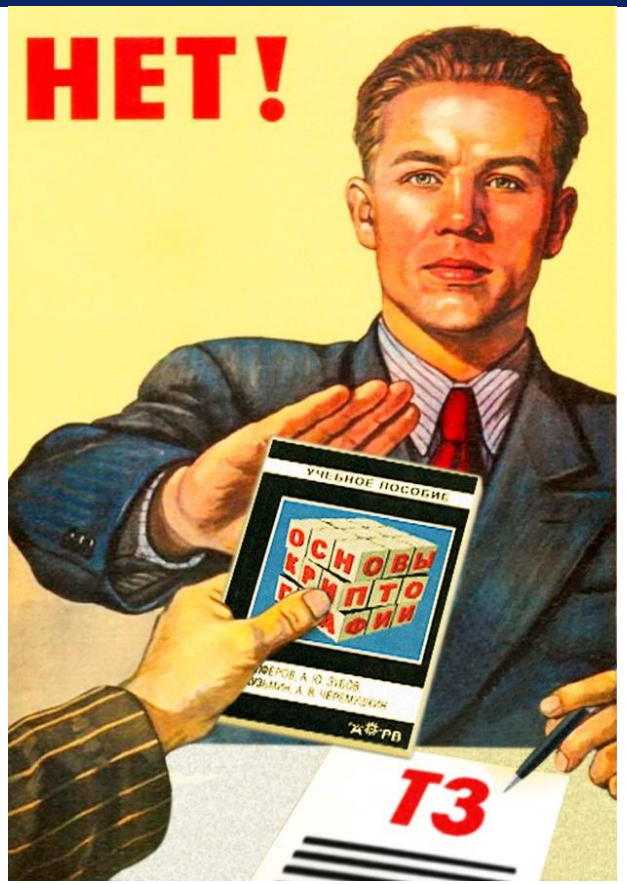
**Реальная система**
(решаемые задачи безопасности)

Интеграция и эксплуатация

Интуиция

**Программное, техническое и организационное решение**

Реализация




**Криптографические алгоритмы и протоколы**

КРИПТОПРО

# Хэширование конфиденциальных данных

Часто встречающийся тезис: «Чем больше данных, от которых зависит шифртекст, тем лучше, т.к. зависимости будут сложнее, а криптосистема более стойкой».

Пример системы шифрования:

**Вход:** сообщение m

1. Сгенерировать инициализирующий вектор IV=H(m)
2. Зашифровать сообщение m в режиме CBC с помощью шифра Кузнечик и выбранного IV

**Выход:** шифртекст $C=IV||CBC_K(IV,m)$

КРИПТОПРО

# Хэширование конфиденциальных данных

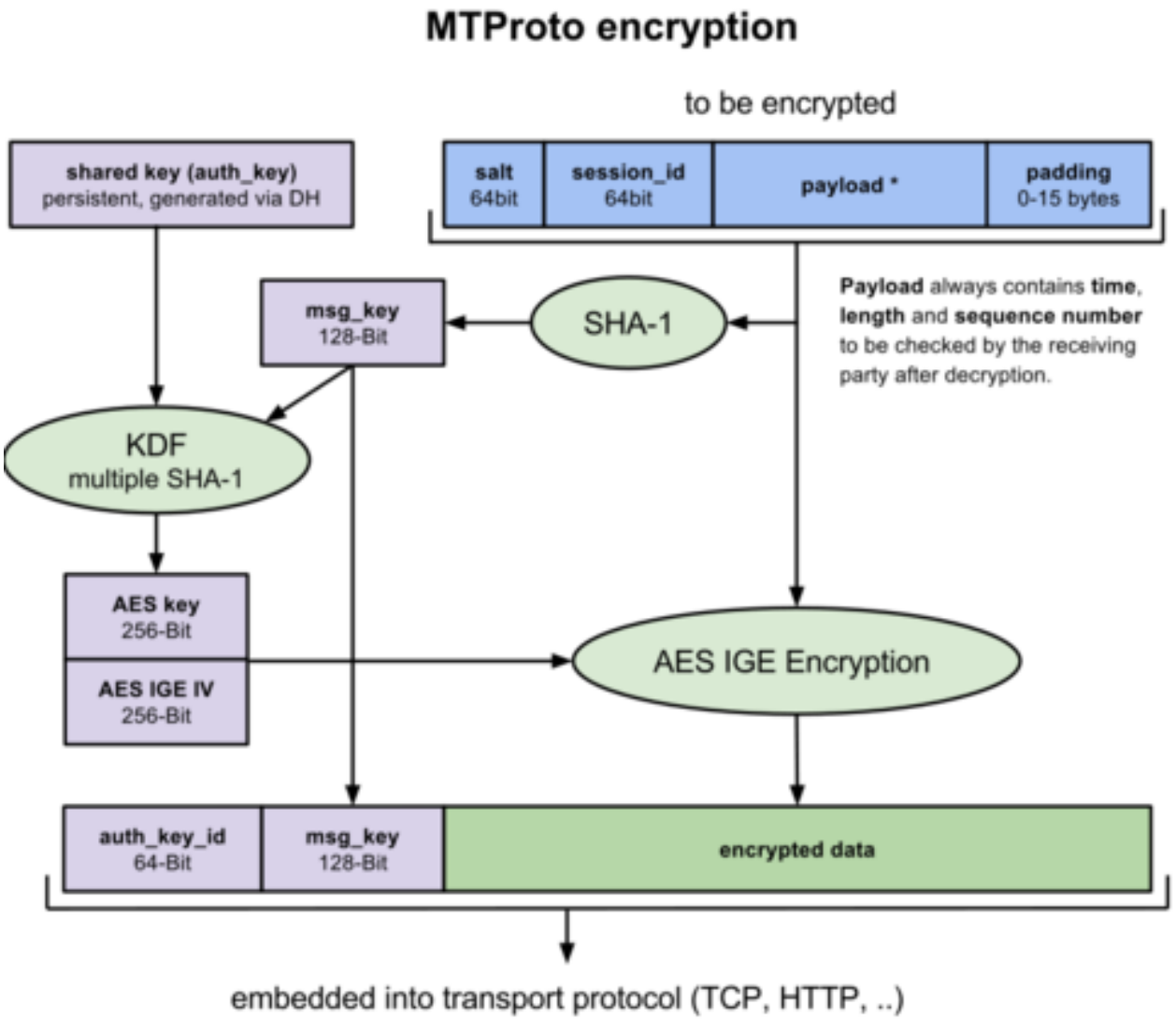
Несмотря на то, что стойкая хэш-функция должна быть «труднообратимой», это свойство не действует, когда про хэшируемые данные известно почти все.

Нарушение конфиденциальности при использовании описанной криптосистемы:

- m = “7622” – PIN-код от банковской карты
- Противник восстанавливает m не по $CBC_K(IV,m)$, а по IV=H(m) обычным перебором (всего-то 10000 вариантов)

КРИПТОПРО

# Хэширование конфиденциальных данных




**NB:** After decryption, **msg_key** MUST be equal to SHA-1 of data thus obtained.

КРИПТОПРО

# Подпись конфиденциальных данных

Электронная подпись, как и хэш, сохраняет информацию о подписываемых данных: при наличии открытого ключа подписанный текст, если он короткий или о нем почти все известно, можно восстановить обычным перебором.

**Пример**: схема шифрования Sign-&-Encrypt

- **Input**: m
- $S = Sign_{PK}(m)$ – обеспечение целостности
- $C = Enc_K(m)$ – обеспечение конфиденциальности
- **Output**: C||S

# Подпись конфиденциальных данных

Электронная подпись, как и хэш, сохраняет информацию о подписываемых данных: при наличии открытого ключа подписанный текст, если он короткий или о нем почти все известно, можно восстановить обычным перебором.

**Пример**: схема шифрования Sign-&-Encrypt

- **Input**: m
- $S = Sign_{PK}(m)$ – обеспечение целостности
- $C = Enc_K(m)$ – обеспечение конфиденциальности
- **Output**: C||S

**Уязвимость**: m восстанавливается не по C, а по S.

КРИПТОПРО

Причины возникновения уязвимостей на практике:

1. Несоответствие типа атаки
2. Несоответствие модели угрозы
3. Несоответствие предположений о ресурсах

Вне конкурса:

- Использование «кустарной» или «hand-made» криптографии
- Ошибки при реализации

КРИПТОПРО

# Реализация протокола TLS от компании Apple

```
static OSStatus SSLVerifySignedServerKeyExchange(...)
{
    OSStatus        err;
    ...
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...
fail:
    ...
    return err;
}
```

*SSLHashSHA1.final* не выполнится

Процедура проверки сертификата не выполняется

КРИПТОПРО

# Спасибо за внимание!
# Вопросы?

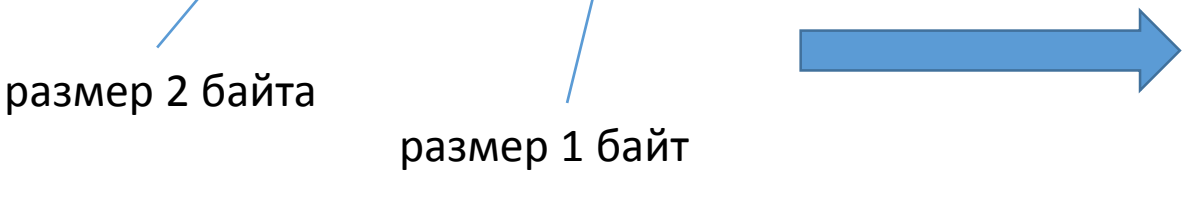
Авторы доклада:

Алексеев Е.К. (alekseev@cryptopro.ru)
Ахметзянова Л.Р. (lah@cryptopro.ru)
Карпунин Г.А. (karpunin@cryptopro.ru)
Смышляев С.В. (svs@cryptopro.ru)

КРИПТОПРО

# Неправильное приведение типов

```
...
#define MODE_KEEPKEY 0x0400
...
static void
aes_setup(boolean key_expanded, boolean generate_iv, boolean reset_iv)
...
typedef unsigned char boolean;
...
aes_setup(mode & MODE_KEEPKEY, mode & MODE_GENIV, mode & MODE_RESETIV);
...
```




Ключ становится равным вектору инициализации, который уже послан в канал!!!

КРИПТОПРО

# Underhanded C Contest 2007

```c
#define TOBYTE(x) (x) & 255
#define SWAP(x,y) do { x^=y; y^=x; x^=y; } while (0)

static unsigned char A[256];
static int i=0, j=0;

void init(char *passphrase) {
  int passlen = strlen(passphrase);
  for (i=0; i<256; i++)
    A[i] = i;
  for (i=0; i<256; i++) {
    j = TOBYTE(j + A[TOBYTE(i)] + passphrase[j % passlen]);
    SWAP(A[TOBYTE(i)], A[j]);
  }
  i = 0; j = 0;
}

unsigned char encrypt_one_byte(unsigned char c) {
    int k;
    i = TOBYTE(i+1);
    j = TOBYTE(j + A[i]);
    SWAP(A[i], A[j]);
    k = TOBYTE(A[i] + A[j]);
    return c ^ A[k];
}
```

Решили сэкономить и не вводить третью переменную для обмена

А что произойдёт, если *x* = *y*?

Через несколько итераций

Все элементы массива A равны 0

В канал посылается открытый текст

КРИПТОПРО