О ПОДХОДАХ К ОБЕСПЕЧЕНИЮ ДОСТАТОЧНОГО УРОВНЯ СТОЙКОСТИ В ЧАСТИ КОНФИДЕНЦИАЛЬНОСТИ ПРИ МАЛОЭНТРОПИЙНЫХ ПРЕДВАРИТЕЛЬНО РАСПРЕДЕЛЕННЫХ СЕКРЕТАХ

- Варфоломеев Александр Алексеевич,
- канд. физ.-мат. н., доцент, МГТУ, МИФИ, РУДН, г. Москва, a.varfolomeev@mail.ru

Малоэнтропийные секреты, короткие ключи, слабые ключи, пароли

- **Короткие ключи.**
- Симметричные шифры:
  - 56 бит (ПП № 313);
  - 80 бит (ISO/IEC 29192-2:2012 - Lightweight cryptography - Part 2: Block ciphers.)
- Асимметричные шифры:
  - 512 бит или 112 бит (ПП № 313);
- Если H(PW) = 56 бит, то
- Длина PW при H(PW) = 56 равна 37 букв английского языка (1, 5 бит на букву). Не запомнить.
- **Малоэнтропийные секреты (ключи).**
  - Low-entropy password - 4 цифры – PIN. H(PIN) = 13,288 бит.
  - 118 бит (PSK -pre-shared key, де-факто стандарт для ряда приложений IPsec).

- ISO/IEC 11770-4:2017(en) Information technology — Security techniques — Key management — Part 4: Mechanisms based on **weak secrets**

РусКрипто 2018.

Варфоломеев А.А.

ОБ АСИММЕТРИЧНО ВЫПОЛНИМЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ (ШИФРАХ)

Асимметричность трудоемкости выполняемых работ законными участниками взаимодействия, например, при зашифровании открытого текста отправителем и при расшифровании соответствующего шифрованного текста получателем.

- Рекомендации для использования в симметричных системах с короткими ключами (короткие ключи - 56 бит, 512 бит, 112 бит).
  - Случайный выбор добавления к короткому ключу отправителем.
  - AON преобразование (All-Or-Nothing Transform)
  - OAEP (Optimal Asymmetric Encryption Padding).
  - Режим шифрования (5.3 Режим гаммирования с обратной связью по выходу (s<n) или
  - 5.5 Режим гаммирования с обратной связью по шифртексту (s<n)).
  - Сокрытие части шифрованного текста для его перебора получателем.

Пример.

- 56 бит ключ симметричного алгоритма шифрования.
- 20 бит опробование на PC в течении 1 мин получателем (V= 10^9 оп/сек).
- открытый текст – 370 Кбайт.
- Режим шифрования - Режим гаммирования с обратной связью по шифртексту.
- Трудоемкость метода полного опробования увеличивается с порядка 2^56 до порядка 2^97 операций.

РусКрипто 2018.

Варфоломеев А.А.

ОБ АСИММЕТРИЧНО ВЫПОЛНИМЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ (ШИФРАХ)

12 слайд из презентации 2018 года.

Другие технологии повышения стойкости.

- EKE – Encrypted Key Exchange (Bellovin S., Merritt M.) 1992г.
- SESPAKE – Security Evaluated Standardized Password Authenticated Key Exchange (Алексеев Е., Ахметзянова Л., Ошкин И., Смышляев С.) 2016г.
- Р 50.1.115-2016 (Протокол выработки общего ключа с аутентификацией на основе пароля).
- И др.

AKE - Authenticated key exchange – Обмен ключами с аутентификацией

- 1. Использование цифровых подписей и сертификатов открытых ключей - Public Key Infrastructure (PKI)-based authentication.
- 2. Использование парольных слов или фраз - Password-based AKE (PAKE).
- PAKE - двусторонний протокол установления (выработки) высокоэнтропийного сессионного ключа на основе обладания сторонами лишь общего пароля (малоэнтропийный ключ).
- Часто – «Клиент – сервер» модель.
- 2PAKE – A,B.
- 3PAKE – A,B, trusted server.

Примеры PAKE

- PAK (2000)
- PPK (2000)
- J-PAKE - Password Authenticated Key Exchange by Juggling (2017)
- Secure Pre-Shared Key (PSK) authentication for Internet Key Exchange (IKE) protocol (RFC 6617 – 2012).
- SRP - Secure Remote Password protocol (RFC 2945 – 1998).
- O-PAKE –Oblivious PAKE (2013-127)
- IBPAKE – Identity-based PAKE (2015-1099)
- DE-PAKE – Device Enhanced PAKE (2015-1099).
- Threshold - PAKE (2014-650).
- SESPAKE (2015 – 1237, RFC 8133).
- **Патентованные.**
  - EKE – (1995. US Patent 5,440,635)
  - SPEKE – Simple Password Exponential Key Exchange (US Patent 6,226,383. 2001).
  - AugPAKE
  - OPAQUE
- **Стандарты**
- ISO/IEC 11770-4:2017(en) Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets.

Некоторые обзоры по PAKE

- 2012. David Pointcheval. Password-based Authenticated Key Exchange. International Conference on Practice and Theory of Public-Key Cryptography (PKC 2012).

- 2015. Stanislav V. Smyshlyaev, Igor B. Oshkin, Evgeniy K. Alekseev, Liliya R. Ahmetzyanova On the Security of One Password Authenticated Key Exchange Protocol (2015-1237).
  - One-Encryption Key-Exchange (OEKE/AuthA);
  - Password Authenticated Key Exchange (PAK);
  - Password Authenticated Connection Establishment (PACE);
  - DragonFly;
  - Strong Password-Only Authenticated Key Exchange (SPEKE);
  - Simple Password-Based Encrypted Key Exchange (SPAKE2);
  - Password Authenticated Key Exchange by Juggling (J-PAKE);
  - Augmented Password Authenticated Key Exchange (AugPAKE);

Типы протоколов установки ключей (Key establishment protocols)(1)

- Протоколы транспортировки ключей (Key transport)
- Протоколы согласования ключей (Key agreement)

Типы протоколов согласования ключей (Key agreement protocols)(2)

- **Balanced password-authenticated key agreement**. Сбалансированное согласование ключей с аутентификацией по паролю: два объекта использовали один и тот же слабый секретный ключ; и ни один из двух объектов не может предопределить значения общих секретных ключей.
- **Augmented password-authenticated key agreement**. Расширенное согласование ключей с аутентификацией по паролю: A имеет слабый секрет, а B имеет проверочные данные, полученные из значения односторонней функции от слабого секрета A. Это увеличивает цену для противника, чтобы получить слабый секрет A от B (verifier-based PAKE или V-PAKE). SRP, PAK-Z, AMP, AugPAK, OPAQUE, AugmentedEKE, B-SPEKE.
- **Password-authenticated key retrieval (PAKR)**. A имеет слабый секрет, а B имеет сильный секрет, связанный со слабым секретом A. (IEEE 1363.2)

PAKE для пост-квантового мира

- 2017-360 Provably Secure Three-party Password Authenticated Key Exchange Protocol Based On Ring Learning With Error.(3PAKE protocol from lattices).
- 2017-1192 Efficient Implementation of Password-Based Authenticated Key Exchange from RLWE and Post-Quantum TLS.
- 2017-1196 Post-Quantum Secure Remote Password Protocol from RLWE Problem.
- Provably secure password authenticated key exchange based on rlwe for the post-quantum world. CT-RSA 2017. 183–204.
- Two-round pake from approximate sph and instantiations from lattices. ASIACRYPT 2017, pages 37–67.
- 2018-886 An Isogeny-Based Password-Authenticated Key Establishment Protocol. **Oleg Taraskin, Vladimir Soukharev, David Jao, Jason LeGrow**.

Bellovin S., Merritt M. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks (1)*

- Рассматривать парольное слово PW как 56 битовый ключ.
  - Транспортировка высокоэнтропийного ключа k от B к A
- 1. A: [A, E(PW; PKa)] → B ,
  - E(PW; PKa) – симм. шифр. на ключе PW, PKa – открытый ключ A.
- 2. B: E(PW; E_PKa(k)) → A , k – высокоэнтропийный ключ.
  - Подтверждение ключа k – «Запрос-ответ»
- 3. A: PW, Pka, E(PW; E_PKa(k)) -> k, E(k; R_a) → B.
- 4. B: k, E(k; R_a) -> R_a, E(k; R_a II R_b) →A.
- 5. A: k, E(k; R_a II R_b) -> R_a II R_b , R_a =?, E(k; R_b) → B
- 6. B: k, E(k; R_b) -> R_b =?

Bellovin S., Merritt M. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks (2)*

- Рассматривать парольное слово PW как 56 битовый ключ.
  - Транспортировка высокоэнтропийного ключа k от B к A
- 1. A: [A, E(PW; PKa)] → B ,
  - E(PW; PKa) – симм. шифр. на ключе PW, PKa – открытый ключ A
- 2. B: E(PW; E_PKa(k)) → A , k – высокоэнтропийный ключ.
  - Подтверждение ключа k – «Запрос-ответ»
- 3. A: PW, Pka, E(PW; E_PKa(k)) -> k, E(k; R_a) → B.
- 4. B: k, E(k; R_a) -> R_a, E(k; h(R_a) II R_b) →A. h- хэш-функция
- 5. A: k, E(k; R_a II R_b) -> R_a II R_b , R_a =?, E(k; h(R_b)) → B
- 6. B: k, E(k; R_b) -> R_b =?

Трудоемкость вскрытия

- T = O(2^56 * L_(1/3)[1,9018, 512]) ,
- если «либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит»
- Или
- T = O(2^56 * 2^56) - если «на методе вычисления дискретных логарифмов в иной группе размера, не превышающего 112 бит»

Bellovin S., Merritt M. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks (3)*

- 1. A: [A, E(PW; PKa)] → B ,
  - E(PW; PKa) – симм. шифр. на ключе PW, PKa – открытый ключ A
- 2. B: E(PW; E_PKa(k)) → A , k – высокоэнтропийный ключ.
  - **1 вариант усиления.** Если увеличить PW до PW-R:
- 1. A: [A, E(PW-Ra; PKa)] → B , У B нет критерия на ОТ для PKa.
  - Заменим
- 1. A: [A, E(PW-Ra; Pka II h(Pka)] → B , аналог шифрования структурного открытого текста. Методы усиления – СМ. выше.
- 2. B работает больше A. B перебирает Ra и ищет Pka.
- Далее E(PW; E_PKa(k)) → A.
- Но критерий на открытый текст получает и противник.

Bellovin S., Merritt M. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks (4)*

- 1. A: [A, E(PW; PKa)] → B ,
  - E(PW; PKa) – симм. шифр. на ключе PW, PKa – открытый ключ A
- 2. B: E(PW; E_PKa(k)) → A , k – высокоэнтропийный ключ.
  - **2 вариант усиления.** Если увеличить число открытых ключей:
- 1. A: [A, E(PW; PKa1, PKa2, …, PKaN)] → B.
- 2. B: Выбирает один ключ PKaJ пользователя A.
- E(PW; E_PKaJ(k II h(k))→ A , k – высокоэнтропийный ключ. Стойкое шифрование на открытом ключе - E_PKaJ(k II h(k) .
- 3. A работает больше B. A перебирает свои открытые ключи PKa1, PKa2, …, PKaN, ищет PKaJ и ключ к. Критерий – нахождение ключа к с правильным прикрепленным значением h(k).

Bellovin S., Merritt M. *Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks (5)*

- 1. A: [A, E(PW, PKa)] → B ,
  - E(PW; PKa) – симм. шифр. на ключе PW, PKa – открытый ключ A
- 2. B: E(PW; E_PKa(k)) → A , k – высокоэнтропийный ключ.
  - **3 вариант усиления – комбинация 1 и 2 вариантов**.
- 1. A: [A, E(PW – Ra; PKa1, PKa2, …, PKaN, h(*))] → B.
- 2. B: B перебирает Ra и ищет истинный набор открытых ключей. Выбирает один ключ PKaJ пользователя A.
- E(PW-Rb; E_PKaJ(k II h(k))→ A , k – высокоэнтропийный ключ. Стойкое шифрование на открытом ключе.
- 3. A: перебирает свои открытые ключи PKa1, PKa2, …, PKaN и Rb, ищет PKaJ и ключ к. Критерий – нахождение ключа к с правильным прикрепленным значением h(k).

Система шифрования с открытым ключом Эль Гамаля (1)

- Параметры: p – большое простое число (не более 512 бит).
- Z*_p = (g) – мультипл. группа кольца вычетов целых чисел по модулю p. g – генератор.
- A,B
- PKb – открытый ключ пользователя B, y_b = g^x_b (mod p).
- x_b – долговременный закрытый ключ пользователя B.
- Зашифрование ОТ M. A: K = y_b^k (mod p), k – разовый закрытый ключ.
- C1 = g^k (mod p), C2 = K*M (mod p).
- Расшифрование. B: K = C1^x_b (mod p), M = C2 / K (mod p).
- G. Атака решением DLP. C1 - > k.
- Для усложнения - разбить C1 = C1_l II C1_r и C1_r не передавать.
- B перебирает C1_r. Зная x_b находит K и M. Противник x_b не знает, но может найти из y_b = g^x_b (mod p) решая DLP.
- Для усложнения B создает N открытых ключей: y1_b, y2_b, … , yN_b.

Система шифрования с открытым ключом Эль Гамаля (2)

- Зашифрование открытого текста M.
- A: Случайно выбирает открытый ключ yJ_b, из {y1_b, y2_b, … , yN_b}.

- K = yJ_b^k (mod p), k – разовый закрытый ключ.
- Шифртекст: C1 = g^k (mod p), C2 = K*M (mod p).
- C1 = C1_l II C1_r и часть C1_r и не передавать.

- Расшифрование.
- B: перебирает неизвестную часть C1_r и yi_b для i из {1, … N}.
- K = (C1_l II C1_r)^xi_b (mod p), M = C2 / K (mod p). Критерий – структурность ОТ (например, добавить h(M)).
- Опробование каждого варианта полиномиально (1 возведение в степень).

- G. Не знает часть C1 и не знает, какой был использован открытый ключ.
- Модель предполагаемого G.
- Не может регулярно решать DLP для параметров 512 (112) бит.

Система шифрования с открытым ключом Эль Гамаля (3)

- **Особенности применения в протоколе ЕКЕ**
  - Подлинность открытых ключей подтверждается не УЦ, а PW.
  - **3 вариант усиления – комбинация 1 и 2 вариантов**.
- 1. A: [A, E(PW – Ra; PKa1, PKa2, …, PKaN, h(*))] → B.
- 2. B: B перебирает Ra и ищет истинный набор открытых ключей. Выбирает один ключ PKaJ пользователя A.
- E(PW-Rb; E_PKaJ(k II h(k))→ A , k – высокоэнтропийный ключ. Стойкое шифрование на открытом ключе.
- 3. A: перебирает свои открытые ключи PKa1, PKa2, …, PKaN и Rb, ищет PKaJ и ключ к. Критерий – нахождение ключа к с правильным прикрепленным значением h(k).
- Можно добавить для усиления сокрытие части шифртекста для ее перебора участниками (и противником).

Сложность применения PAKE в России – нет стандарта на асимметричный шифр.

- ISO/IEC 29192-1:2012 Information technology - Security techniques - Lightweight cryptography - Part 1: General.
- ISO/IEC 29192-2:2012 - Lightweight cryptography - Part 2: Block ciphers.
- ISO/IEC 29192-3:2012 - Lightweight cryptography - Part 3: Stream ciphers.
- ISO/IEC 29192-4:2013 - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques.
- ISO/IEC 29192-5:2016 - Lightweight cryptography - Part 5: Hash-functions.
- **Present cipher** - The block size is 64 bits & the key size can be 80 bit or 128 bit.

Заключение

- Малоэнтропийные ключи – хуже коротких.
- Технология асимметричного выполнения шифров может быть применена для увеличения стойкости протоколов PAKE.
- Необходимо больше гармонизировать международные криптографические стандарты по аналогии со стандартами в области ИБ (ГОСТ Р ИСО/МЭК 27001 и др.).