

Ежегодная международная научно-практическая конференция

# «РусКрипто'2022»

## **О возможностях нарушителя при атаках на некоторый класс протоколов аутентифицированной выработки общего ключа**

**Алексеев Е.К., к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро**

**Ахметзянова Л.Р., зам. начальника отдела криптографических исследований, КриптоПро**

**Божко А.А., инженер-аналитик, КриптоПро**

**Куценко К.О., инженер-аналитик, КриптоПро**

**Кяжин С.Н., к.ф.-м.н., ведущий инженер-аналитик, КриптоПро**

# Моделирование в криптографии

**Цель криптоанализа:** предсказать будущее! (в части того, будет ли взломана криптосистема в ближайшие  $N$  лет)

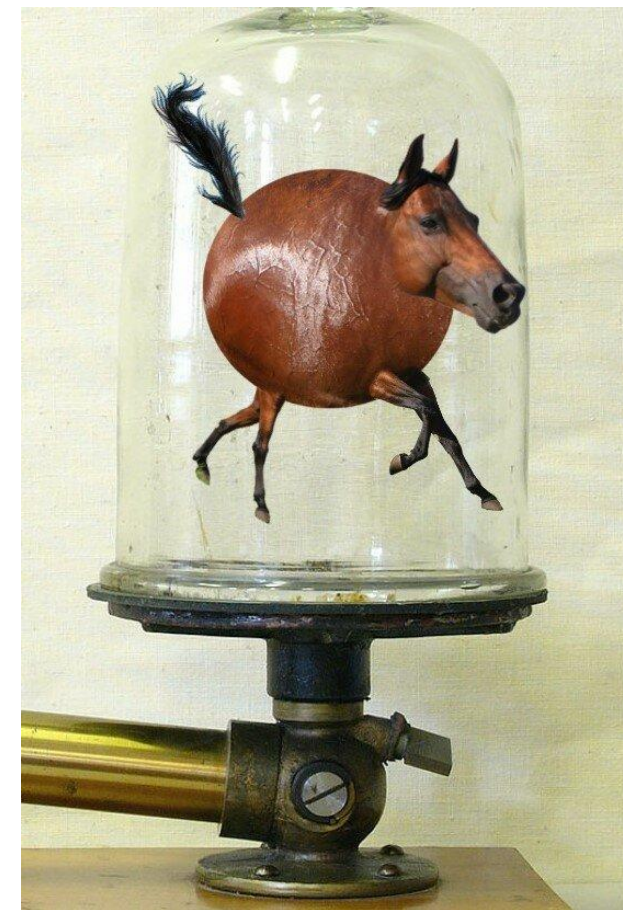
**Два этапа:**

- 1) Моделирование исследуемой криптосистемы
- 2) Оценка стойкости в математической модели

Результаты в формальной модели абсолютны.

Моделирование же основывается на экспертном опыте.

В работе – структурированный обзор с учетом актуальных практических примеров использования.



# Что такое модель безопасности?

Wenbo Mao «Modern Cryptography: Theory and Practice»:

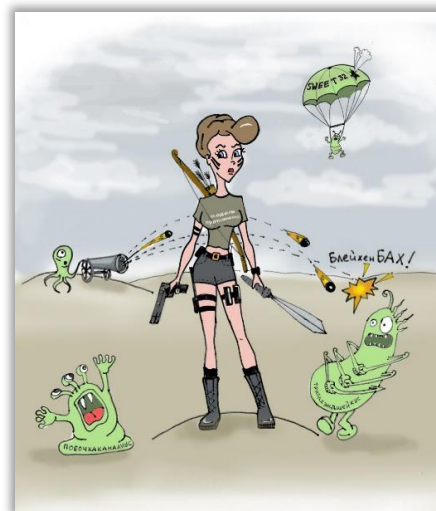
«Nowadays, however, cryptography has a modernized role in addition to keeping secrecy of information: ensuring fair play of "games" by a much enlarged population of "game players."»

Три компоненты:

- Возможности нарушителя (тип атаки)
- Угрозы
- Ресурсы

# Почему важно и сложно сделать правильную модель?


- Алексеев Е.К., Ахметзянова Л.Р., Карпунин Г.А., Смышляев С.В.  
«Что плохого можно сделать, неправильно используя криптоалгоритмы», Лекция на CTCrypt 2019.
- Алексеев Е.К., Ахметзянова Л.Р., Божко А.А., Грибоедова Е.С.  
«Теоретическая криптография в реальных условиях». Блог КриптоПро, 2019.
- Degabriele J.P., Paterson K.G., Watson G.J.  
«Provable Security in the Real World». IEEE Security and Privacy Magazine, 2011.
- Грибоедова Е.С., Царегородцев К.Д.  
«Еще раз о важности построения модели противника на примере протокола аутентификации 5G-AKA»,  
**ЧЕРЕЗ ПОЛ ЧАСА ЗДЕСЬ ЖЕ, НЕ ПРОПУСТИТЕ!**



The Science of Security

## Provable Security in the Real World

Provable security plays an important role in the design and analysis of systems using cryptography. However, protocols can be vulnerable to attacks outside the scope of the existing formal analyses.



If we define *science* as an objective approach to analysis and pursuit of knowledge on the basis of rigorous logical arguments, then, cryptogra- symmetric encryption schemes used in Internet Protocol security (IPsec), Secure Sockets Layer (SSL)

# Какие АКЕ-протоколы рассматриваем?

АКЕ – «Authenticated Key Establishment»

Рассматриваем только АКЕ-протоколы  
для 2 участников

- Вход: 2 идентификатора  $A, B$
- Выход участника  $A$ :  $S_A = \{A, P_A\}, K_A, R_A$
- Выход участника  $B$ :  $S_B = \{B, P_B\}, K_B, R_B$

Цель протокола:

- $K_A = K_B$  – выработанный ключ
- $R_A \neq R_B$  – роли (инициатор, респондер)
- $S_A = S_B$



# Начальные условия для нарушителя

Нарушителю известны:

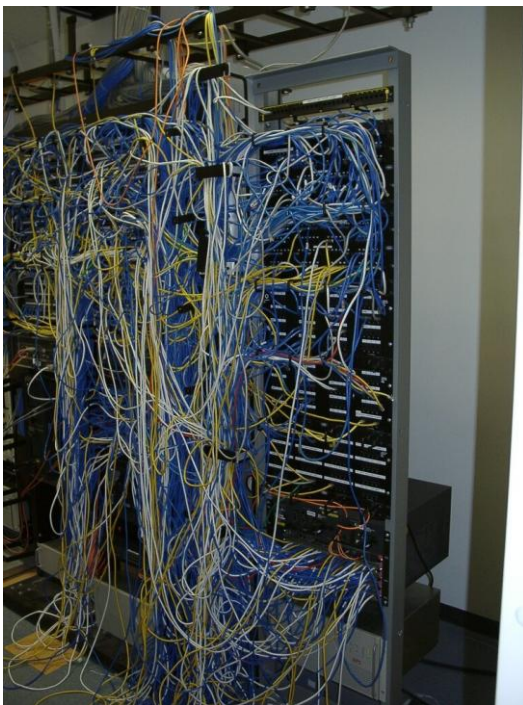
- идентификаторы, флаги ролей и ключевые наборы (кроме **секретных ключей**) всех участников сети
- для начатых сессий – «место» отправленного сообщения в протокол

## Что мы будем говорить о возможностях?

- **Причины рассмотрения**
- **Примеры атак, использующих возможность:**
  - Наименование протокола
  - [AA00] - ссылка на работу, в которой приведена атака (список литературы – в конце презентации),  
\* - обозначение авторской атаки

# Типы возможностей нарушителя

Каналы связи



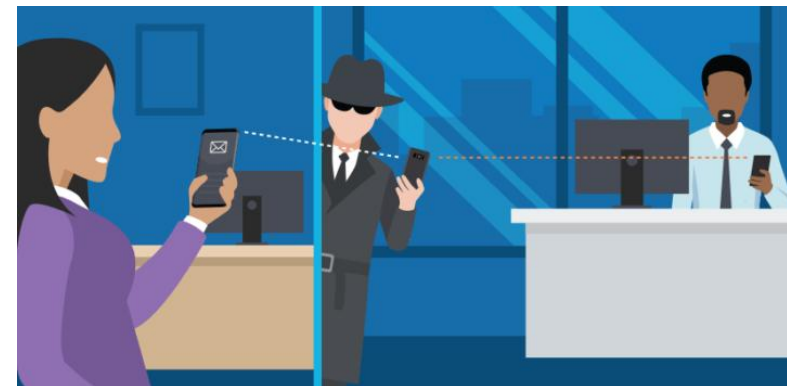
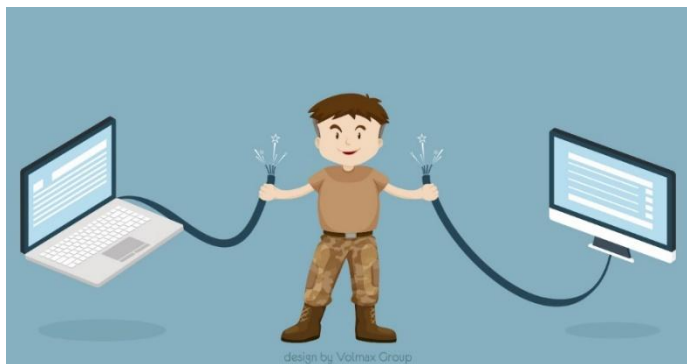
Регистрация узлов



Узлы сети



# Активный нарушитель в канале

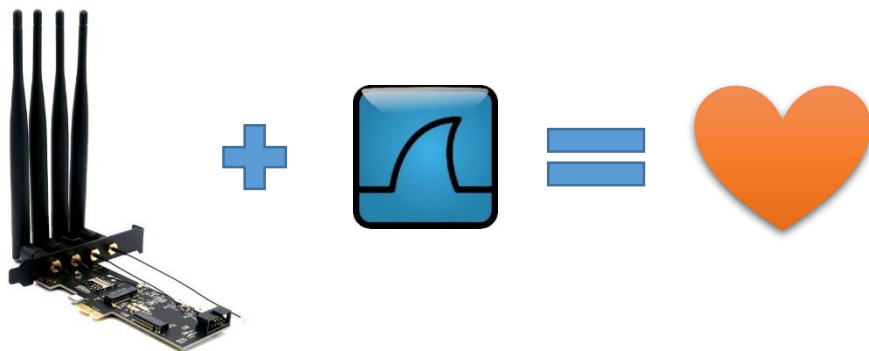


## Примеры атак:

- TLS 1.3 PSK – [DG19]
- HMQV – [MU08]
- MTI/A0 – [MQV95]



# Пассивное прослушивание



## Причины рассмотрения:

- «Работает – не трожь!» – развертывание сети на основе уже существующего аутентифицированного канала (IKE+AH)
- Недостаточная квалификация нарушителя

## Примеры атак:

- ISO 11770 (3-11) – [CH14]
- Yacobi (MTI/A0) – [B94]

# Инициирование взаимодействия

## Причины рассмотрения:

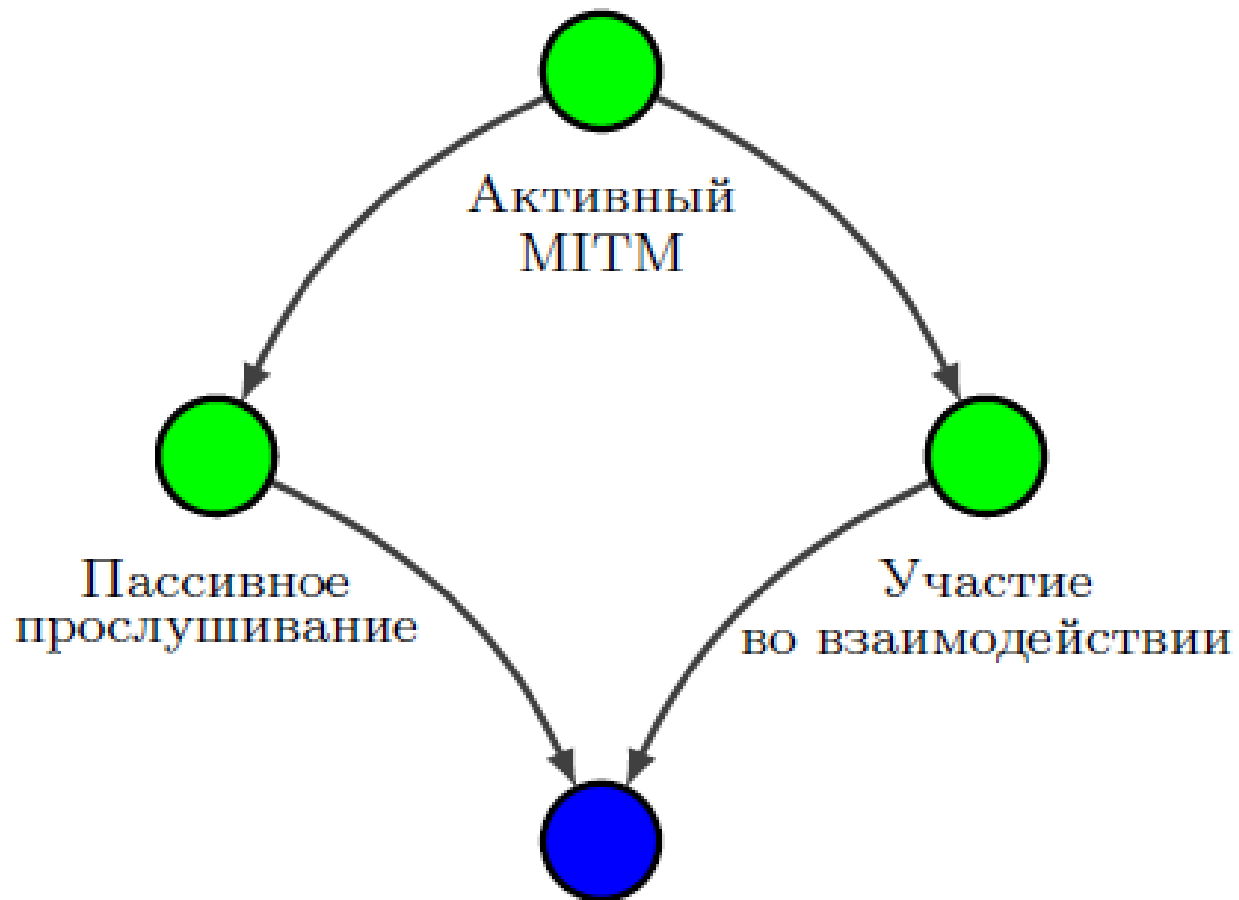
- Публичные сети

## Примеры атак:

- NMQV – [TC11]
- Yacobi (MTI/A0) – [B94]
- MTI/A0 – [\*]



# Каналы связи: краткий итог



# Регистрация узлов

- Возможность быть легитимным узлом
- Динамический состав узлов сети
- Выбор ID
- Выбор аутентифицирующей информации
- Регистрация без проверки знания закрытого ключа
- Регистрация без проверки уникальности открытого ключа



# Возможность быть легитимным узлом



## Причины рассмотрения:

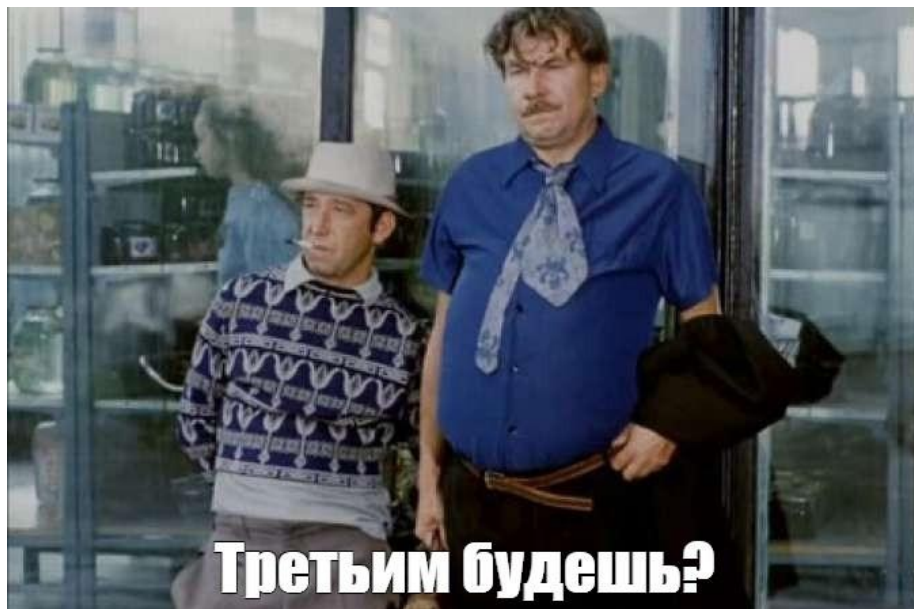
- Внутренний нарушитель
- Возможность компрометации устройств

## Примеры атак:

- Yacobi (MTI/A0) – [B94]
- STS-MAC – [MQV95, BM99]
- HMQV – [MU08]



# Динамический состав узлов



## Причины рассмотрения:

- «Фича» – масштабируемость сети
- Независимость системы регистрации (PKI)

## Примеры атак:

- HMQV – [MU08]
- STS-MAC – [BM99]

# Выбор ID

**Создание почтового ящика**

Имя: RusCrypto      Фамилия: 2022

Дата рождения: 24 Март 2022

Пол:  Мужской  Женский

Имя ящика:  @mail.ru

Укажите желаемое имя ящика

Пароль:  [Сгенерировать надёжный пароль](#)

Укажите резервную почту

Укажите желаемое имя ящика

- ruscrypto@inbox.ru
- ruscrypto.2022@bk.ru
- 2ruscrypto@bk.ru
- ruscrypto@internet.ru
- 2022.ruscrypto@bk.ru
- ruscrypto2@bk.ru
- ruscrypto.2022@inbox.ru
- 2ruscrypto@inbox.ru

## Причины рассмотрения:

- «Фича» системы регистрации

## Примеры атак:

- НМҚV – [MU08]

# Выбор пары (ключевой)



## Причины рассмотрения:

- Стандартная практика получения сертификатов в УЦ

## Примеры атак:

- STS-ENC – [MQV95]
- STS-MAC – [BM99]
- HMQV – [MU08]

# Регистрация без проверки знания закрытого ключа



## Причины рассмотрения:

- Сложность внедрения криптографических протоколов в систему регистрации
- Желание не использовать закрытый ключ вне целевого АКЕ-протокола

## Примеры атак:

- НMQV – [MU08]
- STS-MAC – [MQV95]
- MTI/A0 – [MQV95]

# Регистрация без проверки уникальности открытого ключа



## Причины рассмотрения:

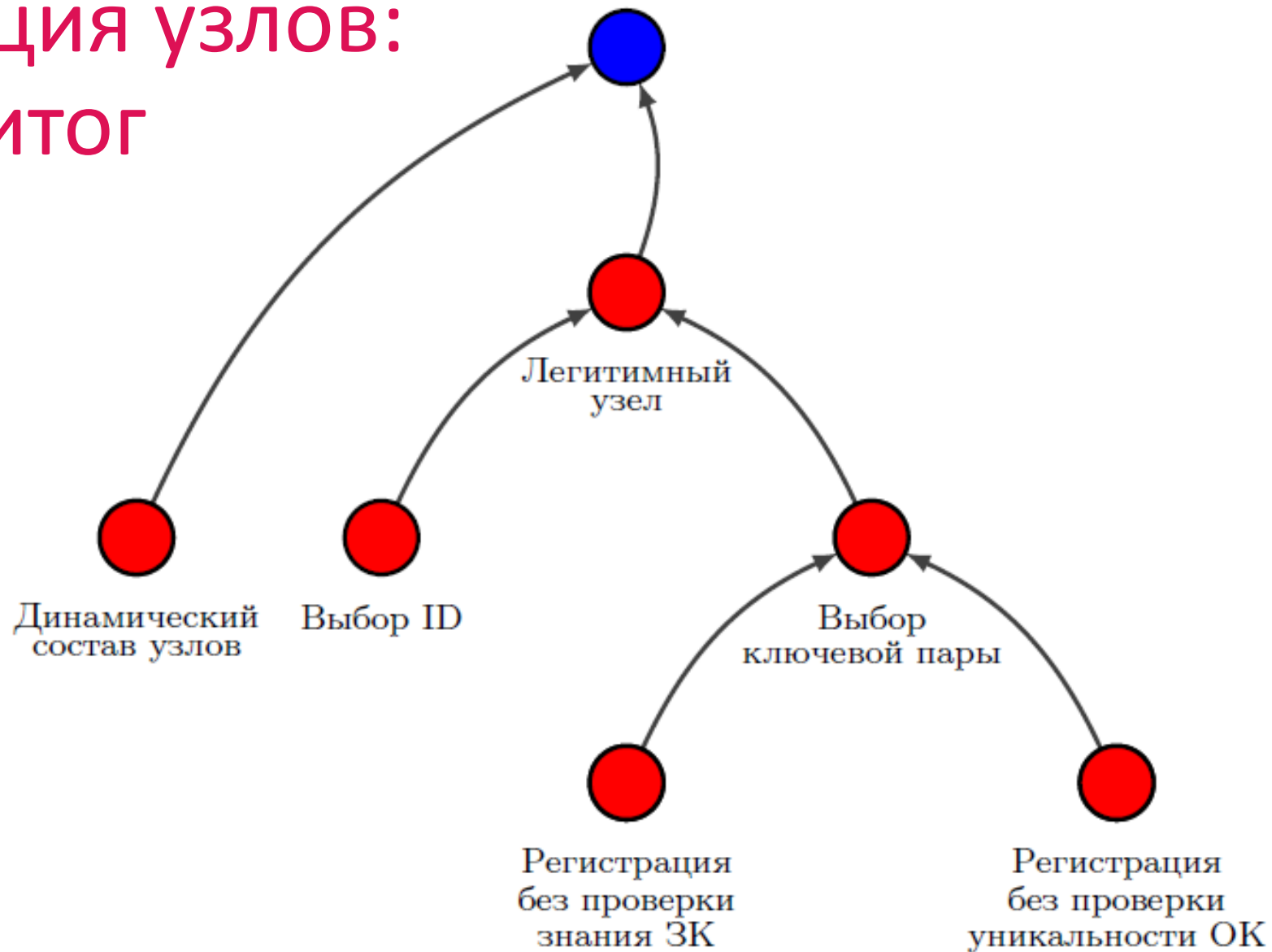
- Использование внешней по отношению к сети системы регистрации
- Часто встречающаяся недоработка

## Примеры атак:

- HMQV – [MU08]
- STS-MAC – [MQV95]
- STS-ENC – [MQV95]



# Регистрация узлов: краткий итог



# Узлы сети

- Возможности, не связанные с внутренним состоянием узлов
- Повтор и навязывание внутреннего состояния
- Вскрытие внутреннего состояния



# Возможности, не связанные с внутр. состоянием

- Параллельные сессии
- Знание/незнание идентификатора ответчика в момент начала выполнения протокола (pre-/post-specified peer model)
- Роли аутентифицирующих параметров
- Навязывание взаимодействия

# Параллельные сессии

## Причины рассмотрения:

- Возможность работы нескольких процессов (потоков) в приложении

## Примеры атак:

- TLS 1.3 PSK – [DG19]



obretu.ru

# Отложенная идентификация ответчика (post-specified model)

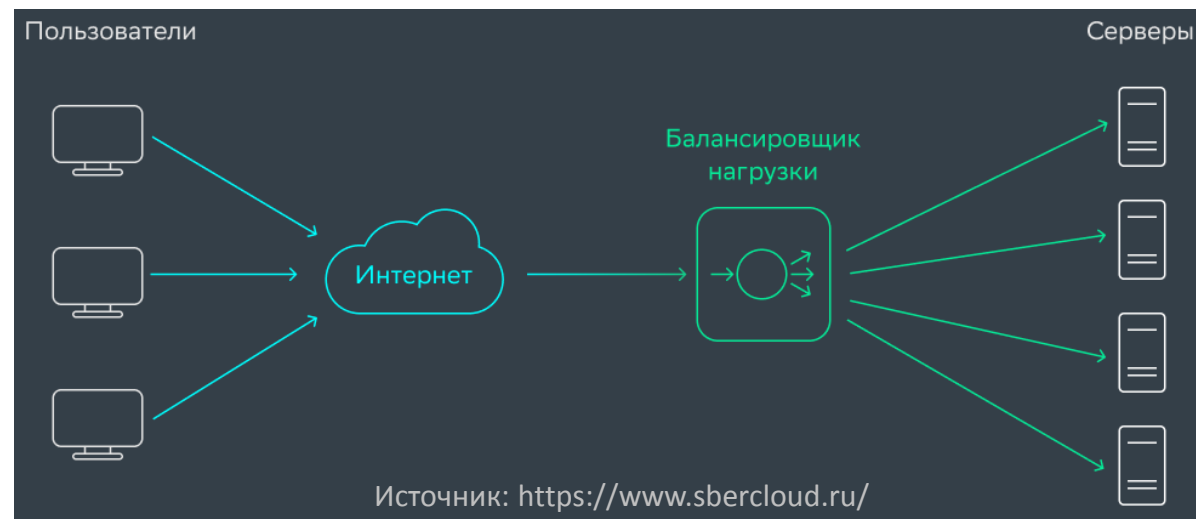
*Инициатору в начале неизвестен  
идентификатор респондера*

## Причины рассмотрения:

- Возможность реализации multicast
- Параллельное выполнение одинаковых функций несколькими узлами сети

## Примеры атак:

- НМQV – [MU08]
- МТI/A0 – [\*]





# Роли аутентифицирующих параметров

*Одинаковые ключи для ролей инициатора и респондера*

## Причины рассмотрения:

- «Выпуск новых ключей – это дорого»
- «Это же в 2 раза больше ключевой информации хранить»

## Примеры атак:

- TLS 1.3 PSK – [DG19]



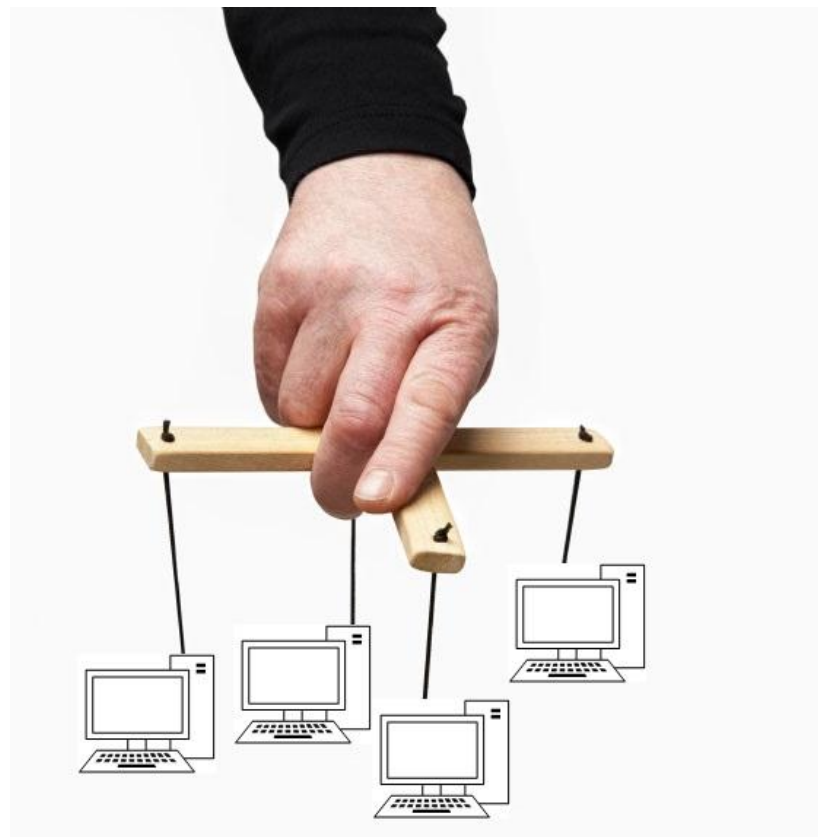
# Навязывание взаимодействия

## Причины рассмотрения:

- Желание учесть все сценарии влияния нарушителя на пользователя

## Примеры атак:

- HMQV – [TC11]
- TLS 1.2 – [RY10]
- MTI/AO – [\*]



# Внутреннее состояние узлов



Долговременные секреты



Промежуточные значения

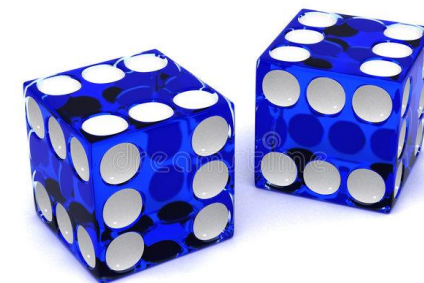


Сессионный ключ

# Вскрытие внутреннего состояния

## Причины рассмотрения:

- Небезопасное использование (swap и hibernate-файлы)
- Небезопасное хранение
- Плохая (предсказуемая) случайность
- Использование сессионных ключей в нестойких протоколах защиты канала связи
- Атаки по побочным каналам



# Вскрытие внутреннего состояния

	Промежуточные значения							
	Долговременные		Предвычисляемые		Вычисляемые		Сессионные ключи	
	До	После	До	После	До	После	До	После
Открытые	Всегда известны		НMQV-C [SS17]	В канале		В канале	Не рассматривается	
Закрытые	НMQV [TC11]	ISO 11770 [CH14]	НMQV [TC11]	DHKE [K05]	Naxos [C08]	НMQV [*]	Не применимо	Yacobi [B94]



# Повтор и навязывание внутреннего состояния

## Причины рассмотрения:

- Повторение случайности при копировании виртуальных машин
- Слабодовверенное окружение
- Использование недоверенного УЦ
- Небезопасное хранение



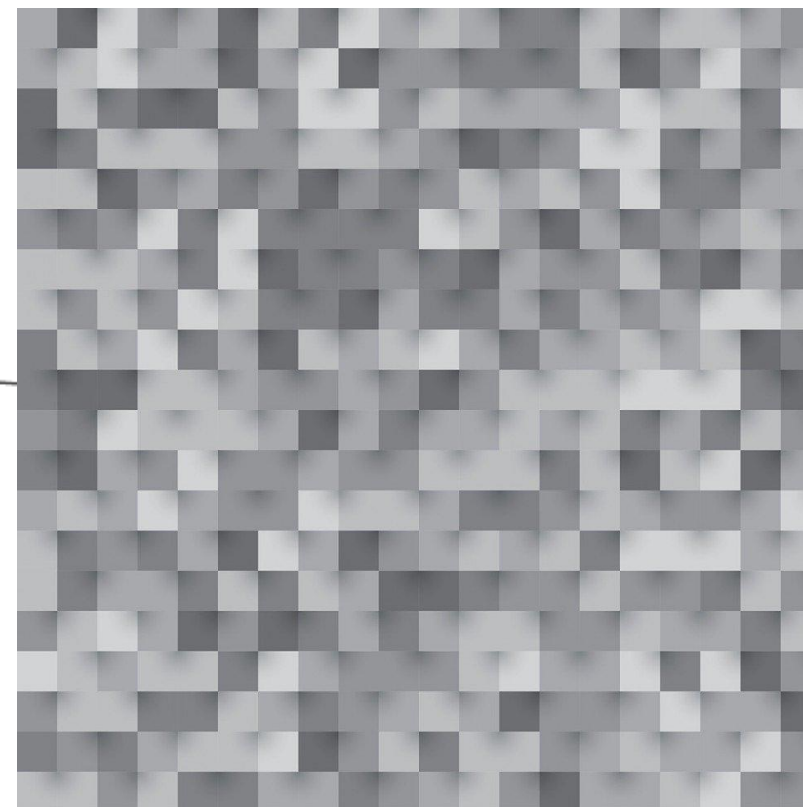
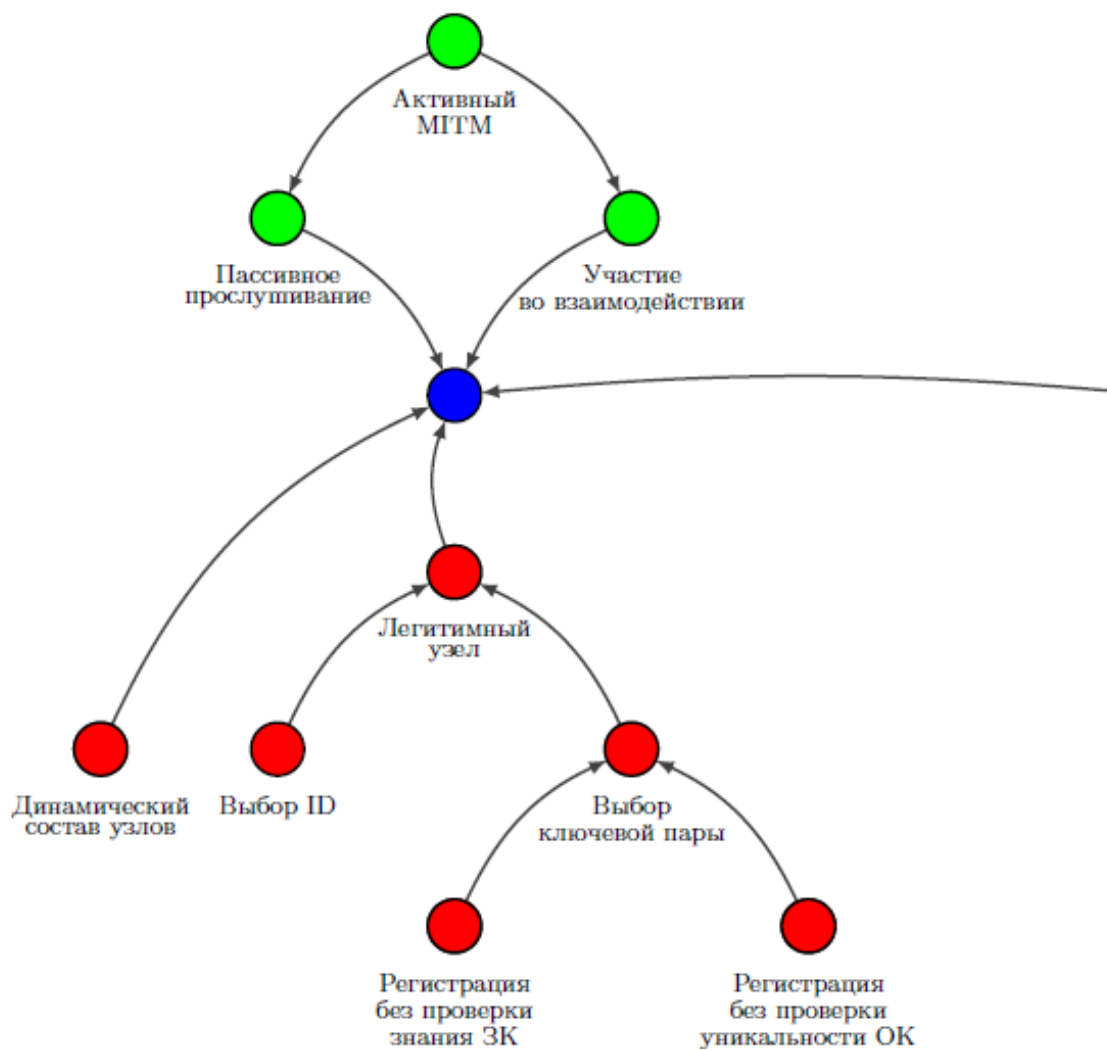


# Повтор и навязывание внутреннего состояния

			Промежуточные значения			
	Долговременные		Предвычисляемые		Вычисляемые	
	Повтор	Навязывание	Повтор	Навязывание	Повтор	Навязывание
Открытые	Не рассматривается		ISO 9798 (mod.) [K03]			
Закрытые	MTI/A0 [*]		ISO 9798 [K03]			

Для протоколов подписи рассматривается в [AABS21]

# ИТОГ



# Все ли возможности рассмотрены?

- Появление оракулов из-за использования долговременного ключа в других протоколах («атаки с выбранным протоколом»)
- Возможность взлома базовых примитивов
- Возможности, связанные с некорректной реализацией (EAP-PSK)
- Навязывание несогласованной ключей пары до/после регистрации легитимного узла

# Что дальше?

- Более подробную версию доклада планируется представить на семинаре «Математические методы криптографического анализа» ВМК МГУ (подписывайтесь на рассылку и следите за анонсами: [mmca2013@mail.ru](mailto:mmca2013@mail.ru))
- А что с угрозами?

**«*Defining Trivial Attacks for Security Protocols is Not Trivial*»**  
(ePrint Archive 2017/818)



# Вопросы ???

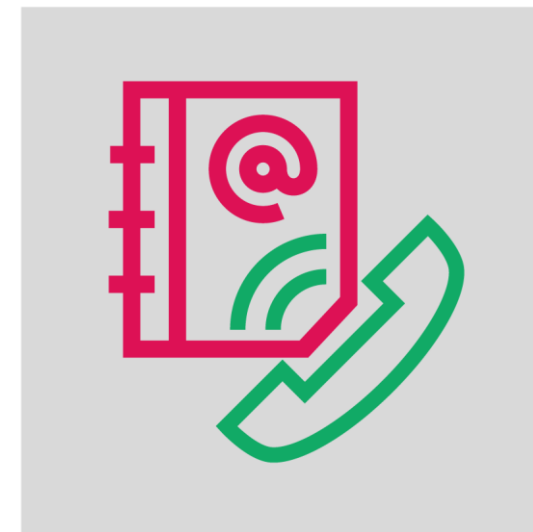
# Контактная информация

Электронная почта:

[alekseev@cryptopro.ru](mailto:alekseev@cryptopro.ru)

Сайт:

[www.cryptopro.ru](http://www.cryptopro.ru)





# Список литературы

- [AABS21] Алексеев Е.К., Ахметзянова Л.Р., Божко А.А., Смышляев С.В. Безопасная реализация электронной подписи с использованием слабодоверенного вычислителя // Математические вопросы криптографии, 12:4, 5--23. 2021.
- [DG19] Drucker N., Gueron S. Selfie: reflections on TLS 1.3 with PSK // IACR Cryptology ePrint Archive, 2019/347.
- [SS17] Seye P., Sarr A. Enhanced Modelling of Authenticated Key Exchange Security // Security and Trust Management, pp. 36--52, 2017.
- [CH14] Cremers C., Horvat M. Improving the ISO/IEC 11770 Standard for Key Management Techniques // Lecture Notes in Computer Science, 8893: 215--235. 2014.
- [TC11] Tang Q., Chen L. Extended KCI attack against two-party key establishment protocols // Information Processing Letters. 111: 15, 744--747. 2011.
- [RY10] Ristenpart T., Yilek S. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography // Proceedings of Network and Distributed Security Symposium. 2010.
- [MU08] Menezes A., Ustaoglu B. Comparing the pre- and post-specified peer models for key agreement // Lecture Notes in Computer Science, 5107: 53--68. 2008.

# Список литературы

- [C08] Cremers C. Session-state Reveal is stronger than Ephemeral Key Reveal: Attacking the NAXOS Authenticated Key Exchange protocol // Lecture Notes in Computer Science, 5536: 20--33. 2009.
- [K05] Krawczyk H. HMQV: A High-Performance Secure Diffie-Hellman Protocol // Lecture Notes in Computer Science, 3621: 546--566. 2005.
- [K03] Krawczyk H. SIGMA: The 'SIGn-and-MAC' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols // Lecture Notes in Computer Science, 2729: 400--425. 2003.
- [BM99] Blake-Wilson S., Menezes A. Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol // Lecture Notes in Computer Science. 1560: 154--170. 1999.
- [MQV95] Menezes A.J., Qu M., Vanstone S.A. Some new key agreement protocols providing implicit authentication // Workshop on Selected Areas in Cryptography (SAC'95), pp. 22--32, 1995.
- [B94] Burmester M. On the risk of opening distributed keys // Lecture Notes in Computer Science. 839: 308--317. 1994.

# Что такое АКЕ-протокол?

В общем случае у каждого участника при выполнении протокола имеется:

- $ID$  – идентификатор участника
- $f_I, f_R$  – флаги ролей, которые может исполнять участник
- $Cred_I$  – ключевой набор для исполнения роли инициатора
  - $Cred_I^0 = (pk_I^0, sk_I^0)$  – ключевая пара участника в роли инициатора
  - $Cred_I^j = (ID^j, pk^j, k^j)$  – идентификатор, открытый ключ, симметричный ключ, используемый для взаимодействия с  $j$ -м участником в роли инициатора,  $j \in \{1, \dots, n\}$
- $Cred_R$  – ключевой набор для исполнения роли респондера
  - $Cred_R^0 = (pk_R^0, sk_R^0)$  – ключевая пара участника в роли респондера
  - $Cred_R^j = (ID^j, pk_R^j, k_R^j)$  – идентификатор, открытый ключ, симметричный ключ, используемый для взаимодействия с  $j$ -м участником в роли респондера,  $j \in \{1, \dots, n\}$