

Умные протоколы для умных устройств

Криптография для киберфизических систем

Татьяна Липина,
Кирилл Царегородцев

Компания «Актив»

О чем доклад

- Абстрактное описание системы.
- Специфика киберфизических систем (КФС) с точки зрения криптографии.
- Особенности учета специфики КФС в моделях безопасности.
- Особенности криптографических протоколов, использующихся в КФС.

Криптография $\neq$ информационная безопасность

«За бортом»: другие аспекты информационной (и иной) безопасности, которые особо актуальны в больших неравномерно защищенных распределенных системах.

- Атаки на вещи умного дома: анализ незашифрованного трафика, запись видеопотока, запись разговоров, накопление данных¹ (угроза нарушения приватности, физическая безопасность).
- Mirai и аналоги: построение ботнета, DDoS-атаки.
- Stuxnet и аналоги (Industroyer, Duqu, ...): атаки на объекты инфраструктуры, вывод их из строя, промышленный шпионаж.

¹Gu и др., «Iotspy: Uncovering human privacy leakage in iot networks via mining wireless context»; Paula Albuquerque и др., «Privacy in smart toys: Risks and proposed solutions»; Ulsmåg, Lin и Lee, «Investigating the Privacy Risk of Using Robot Vacuum Cleaners in Smart Environments».

Киберфизическая система (КФС)²

Интеллектуальная система, включающая в себя спроектированные взаимодействующие сети физических и вычислительных компонентов.

Будем выделять четыре типа сущностей³:

- сенсоры (датчики),
- актуаторы,
- контроллеры,
- управляющая система⁴.

² НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ. Термины и определения.

³ Cardenas, «The Cyber Security Body of Knowledge v1.1.0, Cyber-Physical Systems Security».

⁴ не всегда может быть выделена в явном виде

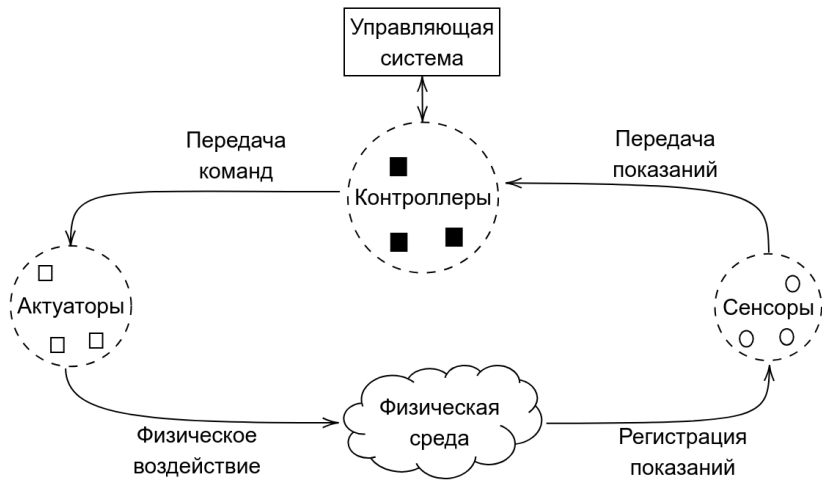


Рис. 1: Абстрактное представление киберфизической системы

Примеры киберфизических систем

- Электрические сети (smart grid).
- Интеллектуальные системы водоснабжения.
- Манипуляционные роботы на предприятиях (умные заводы).
- Умные дома.
- Беспилотный транспорт.
- Системы видеонаблюдения, веб-камеры.
- Системы контроля и управления доступом (СКУД).
- Медицинские КФС (умные кардиостимуляторы, системы мониторинга).

- Низкоресурсная криптография.
- Граничные/периферийные вычисления.
- Аппаратная безопасность (hardware security⁵).
- Совместные конфиденциальные вычисления (MPC).
- Механизмы консенсуса.
- Искусственный интеллект и анализ данных.

⁵Verbauwhede, «The Cyber Security Body of Knowledge v1.1.0, Hardware Security».

Криптографические свойства безопасности для КФС

Базовые свойства

- Целостность данных.
- Аутентификация пользователя.
- Конфиденциальность данных.
- Защита от атак повторного воспроизведения (replay).
- Защита от чтения назад.
- Анонимность.

Эксплуатационные свойства

- Защищенность от атак по побочным каналам.
- Низкоресурсность.
- Низкое время отклика.
- Минимальное расширение сообщения при зашифровании.

Примеры специфических криптографических свойств

- Согласованность внутреннего состояния системы и физической среды⁶.
- Защищенность относительно противника с доступом к квантовому компьютеру⁷.
- Защищенность относительно атак со связанными ключами⁸.
- Личностное шифрование (IBE), гомоморфное шифрование (FHE)⁹.
- Стойкость в моделях MRAE, RUP и т.д.

⁶Jin, «Cryptographic Solutions for Cyber-Physical System Security».

⁷Canteaut и др., *Saturnin: a suite of lightweight symmetric algorithms for post-quantum security*.

⁸McKay и др., *Report on lightweight cryptography*.

⁹Mahato и Chakraborty, «Securing edge computing using cryptographic schemes: a review».

Специфика киберфизических систем

- **Распределенность:** множество взаимодействующих субъектов, не всегда можно выделить единый «центр» (механизмы распределенного реестра/консенсуса).
- **Неоднородность среды:** различные физические среды передачи сигналов, специфика передачи данных между устройствами, различные форматы сообщений (множество протоколов).
- **Требования к задержкам (системы реального времени):** ограничения на время ответа устройства (используемые криптографические механизмы).
- **Низкоресурсность:** жесткие ограничения по потребляемой энергии, площади и стоимости реализации (используемые криптографические механизмы).

Специфика киберфизических систем

- **Требования к минимальности накладных расходов при передаче данных** (минимальные присоединенные данные, малая полезная нагрузка, короткие счетчики).
- **Сложность обновления:** устройства КФС могут находиться в труднодоступных местах; будучи единожды введенными в эксплуатацию, они могут работать на протяжении десятков лет (нагрузка на ключ, постквантовая стойкость, протоколы безопасного обновления ПО устройства).
- **Обратная совместимость:** необходимость учитывать старые версии протоколов (downgrade-атаки).
- **Высокая стоимость ошибки,** вплоть до фатальных исходов.

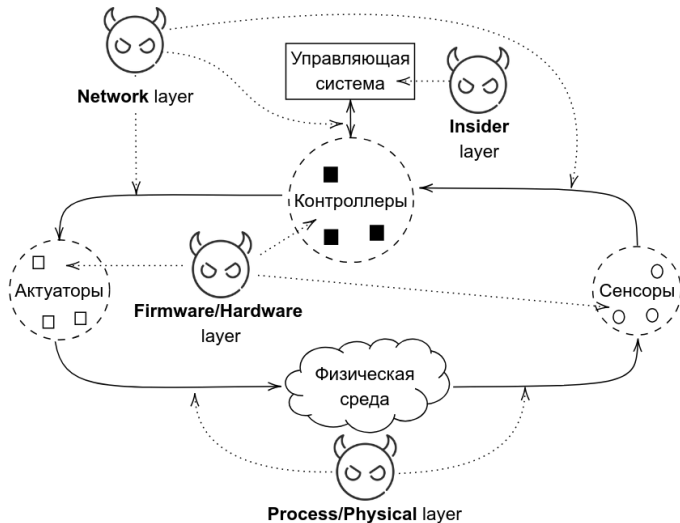


Рис. 2: Возможности противника в рамках абстрактной схемы, см. также Jin, «Cryptographic Solutions for Cyber-Physical System Security»

О возможностях противника: Network/Channel layer

- Уровень, описывающий возможности противника по перехвату/модификации/задержки сообщений между сущностями в ходе передачи по каналам связи.
- Возможности могут зависеть от типа канала между сущностями.
- Опции: пассивный/активный противник.

О возможностях противника: Physical/Process layer

- Особенный уровень, выделяемый для киберфизических систем¹⁰.
- Возможность навязать на считывание какие-либо показания, например, с помощью зашумления, попыток навязывания ложных физических данных для считывания сенсором¹¹.
- Опции: чтение, ограниченная запись, неограниченная запись.
- Особенности: не всегда защищается криптографическими средствами, однако иногда требуется «привязка» физических замеров к криптографическим преобразованиям¹².

¹⁰ Jin, «Cryptographic Solutions for Cyber-Physical System Security».

¹¹ Ahmed и др., «Noiseprint: Attack detection using sensor and process noise fingerprint in cyber physical systems»; Liu, Ning и Reiter, «False data injection attacks against state estimation in electric power grids»; Shoukry и др., «Pycra: Physical challenge-response authentication for active sensors under spoofing attacks».

¹² Avoine и др., «Security of distance-bounding: A survey».

О возможностях противника: Firmware/Hardware layer

- Возможности противника напрямую зависят от аппаратных методов защиты¹³.
- Доступ к RAM: если ключевое хранилище (контроллер) расположено в незащищенном корпусе, то возможны компрометация сеансовых ключей и других промежуточных значений, навязывание несогласованных ключевых пар¹⁴.
- Физический доступ к устройству: атаки по побочным каналам (замеры времени, напряжения и т.д.), атаки по ошибкам вычислений при физическом воздействии (повышение температуры, подача импульсов).
- Доступ к EEPROM: если используются контроллеры без аппаратных мер защиты, то возможна компрометация долговременных ключей, состояния ПДСЧ, повтор значений (replay-атаки) и так далее.
- Для атак требуется оборудование, чем лучше защищено ключевое хранилище, тем дороже оно будет стоить.

¹³Verbauwhede, «The Cyber Security Body of Knowledge v1.1.0, Hardware Security».

¹⁴Алексеев, Кяжин и Смышляев, «Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей».

О возможностях противника: Insider layer

- Выделяется отдельно, поскольку, как правило, управляющая система защищена лучше, чем периферийные устройства.
- Аналогично возможностям противника при атаках на уровне микропрограмм/физических периферийных устройств.
- Может иметь физический доступ к элементам управляющей системы.
- Может аутентифицироваться в управляющую систему.

О классификации протоколов: ожидания

Протоколы могут быть классифицированы по следующим категориям:

- **Тип протокола:** протокол защиты канала, аутентификации, аутентифицированной выработки ключа и так далее.
- **Постулируемые свойства** (например, в рамках терминологии¹⁵ или¹⁶).
- **Предварительные предположения:** предраспределенные («прошитые») секретные ключи PSK, инфраструктура PKI, безопасно распределенные секретные/открытые ключи на этапе регистрации (RPK/RSK) и т.д.
- **Используемые механизмы:** блочные шифры, псевдослучайные функции, вычисления в группе, билинейные спаривания и т.д.
- **Область использования и ограничения:** почему протокол используется в этой области и какие фундаментальные ограничения.

¹⁵Нестеренко и Семенов, «Методика оценки безопасности криптографических протоколов».

¹⁶Черемушкин, «Криптографические протоколы: основные свойства и уязвимости».

О классификации протоколов: реальность

- Огромное количество протоколов на каждый случай жизни — первична инженерная задумка, криптография как опциональная добавка.
- Специфика построения документов и стандартов — криптография не выделяется как нечто отдельное.
- Некоторые протоколы допускают большое множество криптонаборов, обеспечивающих совершенно разные свойства.
- Ad-hoc криптография без доказательств — приводит к тому, что в протоколах часто имеются уязвимости (незащищенные поля, возможности для понижения версий протоколов, неудачные решения в плане комбинации изначально «хороших» механизмов).
- Не всегда легко выделить «обоснование дизайна» протокола (зачем делали X, если есть хороший Y)?

Один пример: протокол OPC UA

- Протокол предназначен для безопасной выработки сеансовых ключей с последующей защитой канала связи между управляющей системой (SCADA) и контроллерами.
- У протокола есть несколько профилей, задающих политики безопасности.
- Протокол подразумевает двухэтапную процедуру: сначала вырабатывается сеансовый ключ и устанавливается защищенный канал, после чего в рамках защищенного канала можно открыть/восстановить сессии для передачи информации.
- Сторона может участвовать в нескольких сессиях в разных сеансах одновременно.
- Сессии открываются с помощью паролей или сертификатов.

Протокол OPC UA

- Сессии могут быть открыты с разными параметрами (только целостность, шифрование + целостность, без защиты).
- Держатель сессии может быть анонимен (опционально).
- Параметры протокола выбираются в ходе его работы (политики безопасности).
- Сессии могут «перебрасываться» между каналами.
- Ключи каналов связи могут обновляться при передаче специального сообщения в канале.

A comprehensive formal security analysis of OPC UA

The relevant security aspects of the specification <...> span 5 documents (out of more than 20), totaling 528 pages. We have extracted what we believe to be a specification suitable for a protocol security analysis.

Начальные предположения

- PSK: предварительно распределенный («прошитый») секретный ключ.
- PKI: инфраструктура открытых ключей.
- RSK: безопасно переданный на этапе инициализации секретный ключ.
- RPK: безопасно переданный на этапе инициализации открытый ключ.
- PWD: предварительно распределенный низкоэнтропийный секрет (пароль).

О криптографических свойствах

Тип протокола	Усл. обозн.	Свойства безопасности
Имитозащита без шифрования	MAC	Целостность
Аутентиф. шифрование (с присоед. данными)	AENC (AEAD)	Конфиденц., целостн. (+ цел. присоед. данных)
Аутентификация	Auth	Аутентификация ¹⁷
Защита канала	Ch	Конф., цел. на уровне канала (контроль выпадения пакетов) ¹⁸

¹⁷привязка к общему секретному ключу или подпись на ключе, соответствующем открытому

¹⁸стратегия по обработке ситуаций с выпавшими пакетами может быть различна

О криптографических свойствах

Тип протокола	Усл. обозн.	Свойства безопасности
Аутентифицированная выработка ключа	АКЕ	см., например, ¹⁹
Аутентифицированная выработка ключа на основе пароля	РАКЕ	см., например, ²⁰
Безопасный канал связи	АССЕ	АКЕ + Ch

¹⁹Нестеренко и Семенов, «Методика оценки безопасности криптографических протоколов».

²⁰Алексеев и Смышляев, «О безопасности протокола SESPake».

Примеры криптографических протоколов в КФС

Протокол	Тип	Область применения
DLMS	PSK: Ch [+ Auth], PKI: ACCE	обмен данными между приборами учёта и системами сбора данных, клиент-серверная модель
DTLS, Lithe, E-Lithe	PSK: Ch [+ Auth], PKI: ACCE	видеозвонки, ip-телефония, сценарии, требующие безопасность, но допускающие издержки переупорядочивания пакетов, потери датаграмм, а также избыточного размера данных, больших, чем датаграммный размер пакета
Wireguard	RPK: ACCE	защита видеопотока, объединение серверов, доступ в инфраструктуру

Примеры криптографических протоколов в КФС

Протокол	Тип	Область применения
NB-Fi	PSK: AENC	передача малого объема данных с низким энергопотреблением на большие расстояния (телеметрия, M2M, IoT)
ZigBee SKKE	PSK,RSK: AKE	Беспроводные сенсорные сети, умные дома
OSGP ²¹	PSK: Ch	Умные сети электроснабжения
LoRaWAN RU	PSK: ENC, PSK: ENC+MAC	создание широкополосных сетей с низким энергопотреблением на большие расстояния, предназначенный для передачи данных между устройствами

²¹ Jovanovic и Neves, «Practical cryptanalysis of the open smart grid protocol».

Примеры криптографических протоколов в КФС

Протокол	Тип	Область применения
Modbus	PKI : ACCE	Промышленный протокол обмена данными между устройствами (управление системами отопления, вентиляцией, электроэнергией)
IPkir	PSK: Ch+Auth	Создание виртуальных частных сетей
CRISP	PSK: Ch+Auth	Индустриальные системы: учет ресурсов, автоматизация транспортных узлов и т.д.
EC-JPAKE	PWD: PAKE	Используется в протоколах, использующих пароли

Некоторые выводы

- Специфика КФС отражается как на уровне модели безопасности (возможности противника, рассматриваемые задачи по нарушению свойств безопасности), так и на уровне конкретных криптографических механизмов и протоколов.
- Жесткие ограничения пропускной способности канала, требования минимальных задержек и низкоресурсность приводит к появлению огромного количества инженерных решений ad-hoc, в которые затем каким-либо образом встраивается криптография (или не встраивается вообще...)
- При внедрении какого-либо протокола целесообразно проверить, нет ли какого-то уже существующего криптографического протокола, обеспечивающего те же свойства и может ли он быть встроен в протокол связи.

Спасибо за внимание!



info@rutoken.ru



www.rutoken.ru
www.aktiv-company.ru



+7 495 925-77-90



Список литературы I

-  Ahmed, Chuadhry Mujeeb и др. «Noiseprint: Attack detection using sensor and process noise fingerprint in cyber physical systems». В: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 2018, с. 483—497.
-  Avoine, Gildas и др. «Security of distance-bounding: A survey». В: *ACM Computing Surveys (CSUR)* 51.5 (2018), с. 1—33.
-  Canteaut, Anne и др. *Saturnin: a suite of lightweight symmetric algorithms for post-quantum security*. Тех. отч. INRIA, 2019.
-  Cardenas, Alvaro. «The Cyber Security Body of Knowledge v1.1.0, Cyber-Physical Systems Security». В: KA Version 1.0.1. University of Bristol, 2021. Гл. Cyber-Physical Systems Security. URL: <https://www.cybok.org/>.
-  Gu, Tianbo и др. «Iotspy: Uncovering human privacy leakage in iot networks via mining wireless context». В: *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE. 2020, с. 1—7.

Список литературы II

-  Jin, Chenglu. «Cryptographic Solutions for Cyber-Physical System Security». Дис. ... док. 2019.
-  Jovanovic, Philipp и Samuel Neves. «Practical cryptanalysis of the open smart grid protocol». В: *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers 22*. Springer. 2015, с. 297—316.
-  Liu, Yao, Peng Ning и Michael K Reiter. «False data injection attacks against state estimation in electric power grids». В: *ACM Transactions on Information and System Security (TISSEC)* 14.1 (2011), с. 1—33.
-  Mahato, Ganesh Kumar и Swarnendu Kumar Chakraborty. «Securing edge computing using cryptographic schemes: a review». В: *Multimedia Tools and Applications* 83.12 (2024), с. 34825—34848.
-  McKay, Kerry и др. *Report on lightweight cryptography*. Тех. отч. National Institute of Standards и Technology, 2016.

Список литературы III

-  Paula Albuquerque, Otávio de и др. «Privacy in smart toys: Risks and proposed solutions». В: *Electronic Commerce Research and Applications* 39 (2020), с. 100922.
-  Shoukry, Yasser и др. «Pycra: Physical challenge-response authentication for active sensors under spoofing attacks». В: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015, с. 1004—1015.
-  Ulsmåg, Benjamin, Jia-Chun Lin и Ming-Chang Lee. «Investigating the Privacy Risk of Using Robot Vacuum Cleaners in Smart Environments». В: *International Conference on Information and Communications Security*. Springer. 2024, с. 312—330.
-  Verbaauwhede, Ingrid. «The Cyber Security Body of Knowledge v1.1.0, Hardware Security». В: KA Version 1.0.1. University of Bristol, 2021. Гл. Hardware Security. URL: <https://www.cybok.org/>.

Список литературы IV

-  Алексеев, Евгений Константинович, Сергей Николаевич Кяжин и Станислав Витальевич Смышляев. «Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей». В: *Прикладная дискретная математика* 66 (2024), с. 60—77.
-  Алексеев, Евгений Константинович и Станислав Витальевич Смышляев. «О безопасности протокола SESPake». В: *Прикладная дискретная математика* 50 (2020), с. 5—41.
-  НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ. Термины и определения. 2025.
-  Нестеренко, Алексей Юрьевич и Александр Михайлович Семенов. «Методика оценки безопасности криптографических протоколов». В: *Прикладная дискретная математика* 56 (2022), с. 33—82.

Список литературы V



Черемушкин, Александр Васильевич. «Криптографические протоколы: основные свойства и уязвимости». В: *Прикладная дискретная математика. Приложение 2* (2009), с. 115—150.