Круглый стол «Плюсы и минусы биометрической идентификации»

Новая биометрия для новой экономики

Зав. каф. Защиты информации МФТИ, д.т.н., в.н.с., Валерий Аркадьевич КОНЯВСКИЙ
konyavskiy@gospochta.ru
Зам. зав. лаб. Прикладных исследований МФТИ-Сбербанк, н.с., Сергей Алексеевич ТРЕНИН
s.trenin@gmail.com

Москва
2018

Среда открытой цифровой экономики

- Корпоративные системы:
  - Доверенные СВТ;
  - Нет проблемы обеспечить всех участников сертифицированными идентификаторами и выполнять операции по аутентификации в доверенной среде.
- Открытые системы:
  - ***Недоверенные СВТ – важнейшая характеристика среды идентификации в цифровой экономике;***
  - Обращаясь за госуслугами, телемедицинскими консультациями, услугами банков, услугами в секторе B2C граждане всегда будут пользоваться смартфонами, о доверенности которых говорить не приходится.

Задача биометрической аутентификации (криминалистика)

H_0: **«Идентифицируемый объект – тот, за кого он себя выдает (за кого его принимает субъект)».**

- Обычный объект – это труп, подозреваемый или преступник;
- Цель анализа – доказать факт совершившегося доступа объекта – к орудию и/или месту преступления, установление личности потерпевшего и так далее;
- Объект обычно не заинтересован в правильной идентификации;
- Используемые технические средства – доверенные;
- Цель противодействия (бездействия) – отклонить нулевую гипотезу при том, что она верна;
- Противодействие (со стороны субъекта, или сообщников, или трудности, связанные с недостатком данных) направлено для достижения ошибки «*false positive*» - ошибки первого рода.

Задача биометрической аутентификации (цифровая экономика)

H_0: **«Идентифицируемый объект – тот, за кого он себя выдает (за кого его принимает субъект)».**

- Объект идентификации - живой и добропорядочный участник экономической деятельности;
- Пример его потребности – получить доступ к некоторым ресурсам;
- Объект заинтересован в правильной идентификации;
- Технические средства – произвольные. Это обычные планшеты и смартфоны, ничем не защищенные от внедрения вредоносного ПО;
- Цель противодействия – выдать себя за другого. Вынудить субъекта принять нулевую гипотезу при том, что она ложна;
- Противодействие (со стороны хакеров) направлено на достижение ошибки «*false negative»* – ошибки второго рода.

Сравнение задач аутентификации

Сфера применения	Объект идентификации	Заинтересованность объекта в подтверждении гипотезы	Желательный результат
Криминалистика	Добропорядочный гражданин (подозреваемый)	Нет	Верный
	Преступник	Нет	Ошибка 1 рода
Цифровая экономика	Добропорядочный гражданин	Да	Верный
	Преступник	Да	Ошибка 2 рода

Таблица 1. Субъект идентифицирует объект. Сравнительные характеристики целей объекта.

Сравнение задач аутентификации

Характеристики процесса для субъекта	Криминалистика	Цифровая экономика
Гипотеза	Объект – тот, за кого его принимает субъект	
Доверенность среды идентификации и контролируемость инструмента	Да	Нет
Значимость того, жив ли объект	Нет	Да
Значимость согласия объекта на идентификацию	Нет	Да
Значимость согласия объекта с результатами	Нет	Да

Таблица 2. Субъект идентифицирует объект. Сравнительные характеристики процесса с точки зрения субъекта

Замечания

- успешный опыт применения биометрии связан с применением в области подобной криминалистической идентификации – предполагается, что в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией – доверенные;
- при таком глубоком различии процессов представляется странным использование одинаковых инструментов. Отметим, что инструмент лишь обрабатывает данные, он их не порождает. И для каждой цели нужно выбирать те данные, которые содержат необходимую информацию. В нашем случае – нужно рассмотреть **особенности идентификационных признаков –** достаточно ли в них информации для решения поставленных задач.

Замечания

- статичные биометрические характеристики применяются в криминалистике для идентификации и аутентификации в силу своей инвариантности к внешним факторам, полной или частичной;
- исследования по применению биометрических механизмов явно или неявно основываются на предположении о доверенности технических средств обработки;
- в случае цифровой экономики это предположение явно неверно, и именно поэтому необходимо изменить подход к биометрическим характеристикам как к инвариантам;
- простота подделки статических биометрических модальностей сегодня осознана.

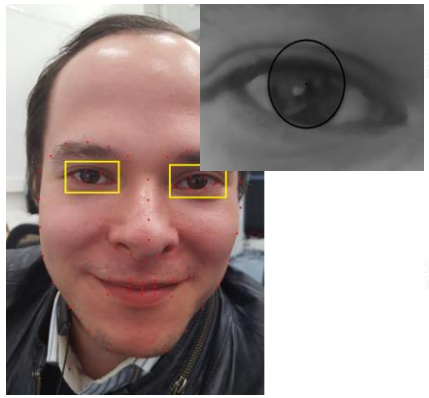
Новая биометрия. Замысел защиты.

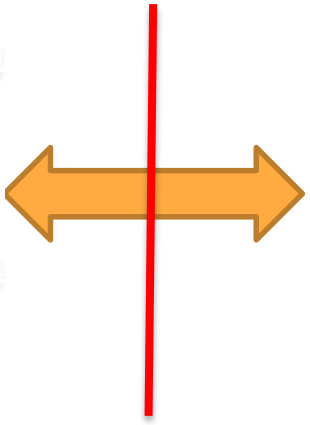
- для устранения уязвимостей, связанных с простотой подмены измерений на недоверенных устройствах, необходимо от статических показателей перейти к динамическим типа «стимул-реакция» со сложной динамикой связи;
- динамическим звеном, чрезвычайно сложным на сегодняшний день для моделирования, являются нервная и вегетативная системы человека и связанные с этим особенности физиологии движений;
- в частности, индивидуальными оказываются непроизвольные реакции на внешние стимулы (в частности, аудио и видео раздражители);
- реакция на стимулы может быть зафиксирована датчиками клиентского устройства, обработана с помощью методов искусственного интеллекта, например, искусственных нейронных сетей, что позволит определить источник потоков данных и повысить достоверность идентификации.

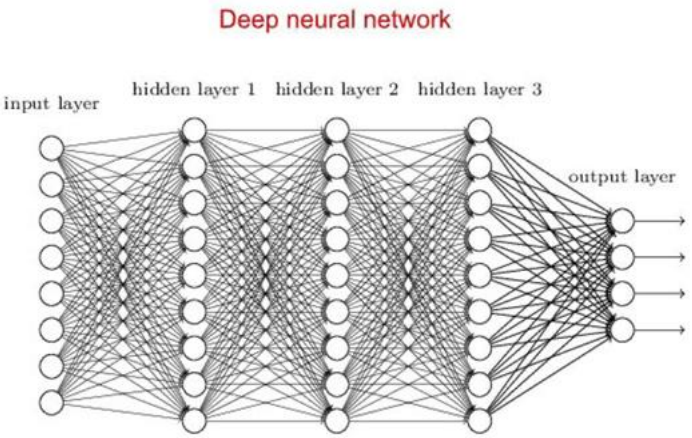
Концептуальная архитектура системы новой биометрической аутентификации

Недоверенное клиентское устройство

Доверенный центр обработки данных







1. Пользователь хочет аутентифицироваться в мобильном приложении

2. Для него генерируется стимул и зафиксированные реакции пересылаются в центр обработки данных

3. Система на основе нейросети подтверждает личность пользователя

Сложно построить модель функционирования нервной системы.
На сегодняшний день таких моделей просто нет! Это дает возможность использовать рефлекторную дугу для одновременного решения проблем аутентификации на недоверенном устройстве и виталентности.

Случайные стимулы гарантируют невозможность простого копирования реакций

Прямая задача (определить идентификатор человека) может быть решена, в то время как, сложность обратной задачи (идентификатору построить модель реакции человека) – эквивалентна сложности обращения сети

Спасибо!

Зав. каф. Защиты информации МФТИ, д.т.н., в.н.с., Валерий Аркадьевич КОНЯВСКИЙ
konyavskiy@gospochta.ru
Зам. зав. лаб. Прикладных исследований МФТИ-Сбербанк, н.с., Сергей Алексеевич ТРЕНИН
s.trenin@gmail.com

Москва
2018