Информационные технологии. Лекция 11. Мобильная криптография

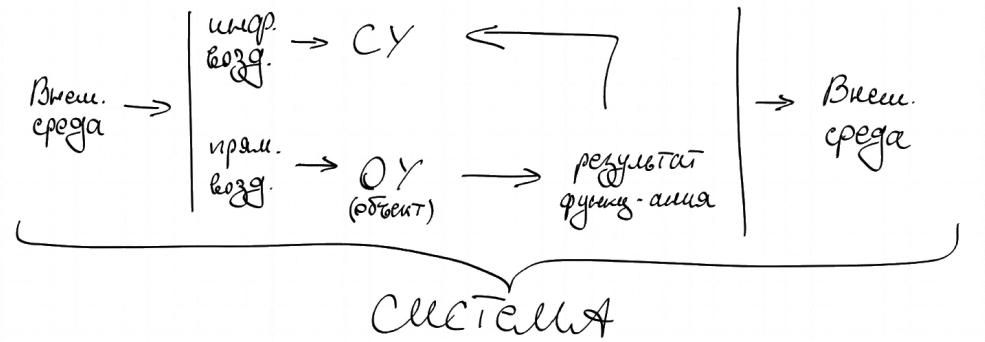
Студент группы 2305 Макурин Александр

15 мая 2023

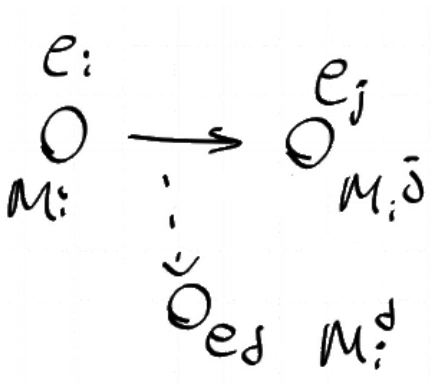
Три кита информационной безопасности:

- Целостность
- Конфиденциальность
- Доступность

Система



$e_i \xrightarrow{M} e_j$
$M_i \simeq M_j^i$ (информация с M_i на M_j) — информация дошла

1. P — св-ва M_i $P_i \neq P_i^j$
   Если хотя бы один не совпадает ⇒ нарушена целостность информации.
   $M_i = \cup m_i = \{m_i\}$
   $\{m_i\} \cap \{m_i^j\} \neq \{m_i\}$ — плохо (информация искажена в процессе передачи).
2. 

   Если $M_i^d = M_i = M_i^j$ — нарушена конфиденциальность.

Интеллектуальный агент — агент, которй может:

- взаимодействовать со средой
- обязан иметь целостность
- работать без вмешательства из вне

В контексте информационной безопасности (ИБ) каналы связи считаются гомогенными.

Модель угроз:

Предпосылки к реализации угроз → Уязвимость → Угроза → Нарушитель (элемент МАС).

МАС — мультиагентная система.

Угрозы самообучения — обучение пойдёт не туда. Примеры: Skynet; IBM Watson, которого пытались обучить доказательной медицине, подулючили к интернету, в котором модель нашла словарь ругательств и стала постоянно их использовать.

$X \to (a : X \to X_1) \to (a_1 : X_1 \to X_2) \to (a_2 : X_2 \to Y) \to Y$, где X — модель мира в момент t_i, Y — план действий T_{i+1}.

$Y = Y_д \cup Y_н$, где д — допустипый, н — недопустимый.

3 способа избавиться от недопустимых:

1. наложить ограничения на Y
2. наложить ограничения на $\{a\}$
3. наложить ограничения на X

Направления атак:

- Spoofing (СПАМ)
- DOS
- Целевые атаки
- Атаки на коммуникационные сети
- Вирусы

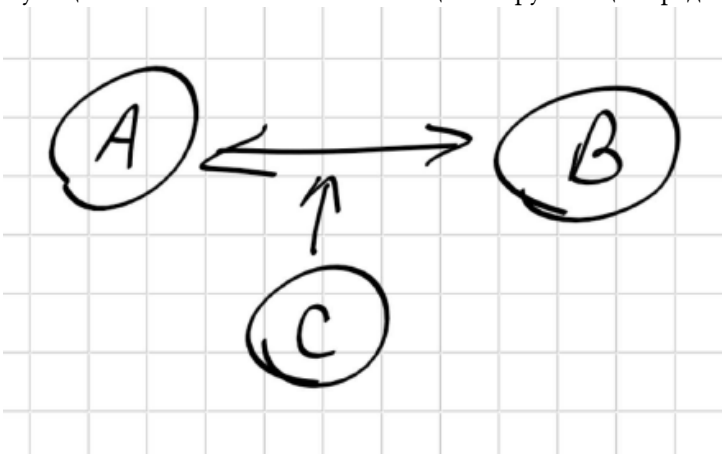
Атаки на взаимодействие элементов МАС (ведут к неверному поведению (misbehaviour)):

- on-off attack — то атакует, то нет. Невозможно выявить
- bad mouth — молчит о другом
- ballot stuffing — внесение ложной информации об окружающей среде

$Env \overset{P_{Env}}{\longleftrightarrow} e_i \xrightarrow{M} e_j$
$P_{Env} \neq P_{Env}^{e_i}$
$M^{e_i} = f(P_{Env}^{e_i})$
$M^{e_i} \neq \overline{M}(P_{Env})$
$f(P_{Env}^{e_i}) \neq f(P_{Env})$

Проблема потери пакетов на данный момент является относительно решённой.

Функциональная безопасность — защита окружающей среды и системы от самой себя.



Агент C получил доступ к сообщению от A к B и callback. C может украсть верную информацию или фальсифицировать callback.

$\widetilde{f}(x_i) = y_i$

Вопрос мобильной криптографии — найти такую f, что $f(x) = \widetilde{y_i} = E(y_i)$. Здесь $f(x)$ — отправляемая информация, которой владеет A, $\widetilde{y_i}$ — информация, получаемая B (её можно расшифровать), $E(y_i)$ — зашифрованная информация, доступ к которой может получить C.