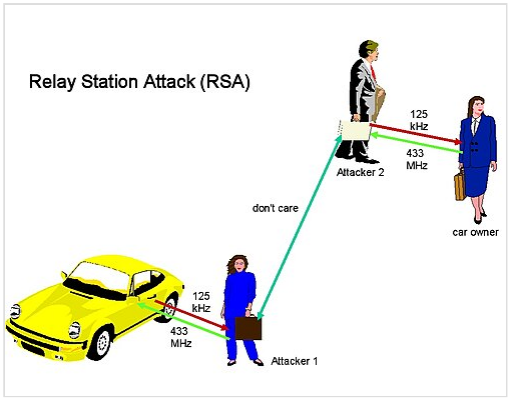
Ретрансляционная атака

Релейная атака (также известная как атака двух злоумышленников) [1] в компьютерной безопасности — это метод взлома, связанный с атаками посредника и ретрансляцией. В классической атаке посредника злоумышленник перехватывает и манипулирует сообщениями между двумя сторонами, инициированными одной из них. В классической релейной атаке злоумышленник инициирует связь с обеими сторонами, а затем просто пересылает сообщения между ними, не манипулируя ими и даже не обязательно читая их.



Атака с использованием ретрансляционной станции. Две ретрансляционные станции соединяют транспондер владельца с приемопередатчиком автомобиля на большом расстоянии.

Пример атаки

Пегги работает в здании с высоким уровнем безопасности, куда она попадает с помощью смарт-карты в сумочке. Когда она подходит к двери здания, система обнаруживает наличие смарт-карты и инициирует обмен сообщениями, которые представляют собой доказательство с нулевым разглашением того, что карта принадлежит Пегги. После этого Пегги может войти.

Мэллори хочет проникнуть в здание.

1. Мэллори подходит к зданию с устройством, имитирующим смарт-карту, и здание в ответ инициирует обмен сообщениями.
2. Мэллори пересылает сообщение своей сообщнице Эвелин, которая следит за Пегги, пока та выполняет поручения в другой части города.
3. Эвелин передаёт сообщение на смарт-карту Пегги, ждёт ответа и передаёт его Мэллори, которая, в свою очередь, передаёт его зданию. Таким образом Мэллори и Эвелин передают сообщения между зданием и смарт-картой Пегги до тех пор, пока здание не убедится, что оно взаимодействует со смарт-картой Пегги.
4. The building opens and Mallory enters.

References

1. Jeong, Hyera; So, Jaewoo (2018-03-01). "Channel correlation-based relay attack avoidance in vehicle keyless-entry systems" (https://onlinelibrary.wiley.com/doi/10.1049/el.2017.4360). *Electronics Letters*. **54** (6): 395–397. Bibcode:2018ElL....54..395J (https://ui.adsabs.harvard.edu/abs/2018ElL....54..395J). doi:10.1049/el.2017.4360 (https://doi.org/10.1049%2Fel.2017.4360). ISSN 0013-5194 (https://search.worldcat.org/issn/0013-5194). S2CID 115601361 (https://api.semanticscholar.org/CorpusID:115601361).

External links

- Academic Survey on Relay Attacks (http://www.rfidblog.org.uk/index.html#relay2009)
- Detailed Practical Example of Relay Attack on RFID system (http://www.rfidblog.org.uk/index.html#relay)
- Relay Attack Demonstration (https://www.youtube.com/watch?v=VxeqiBG18xA) (and related Software (https://github.com/nfcgate/nfcgate) and Paper (http://tuprints.ulb.tu-darmstadt.de/5414/1/NFCGate%20-%20Maass%20et%20al.pdf))

- Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones (http://eprint.iacr.org/2011/618)
