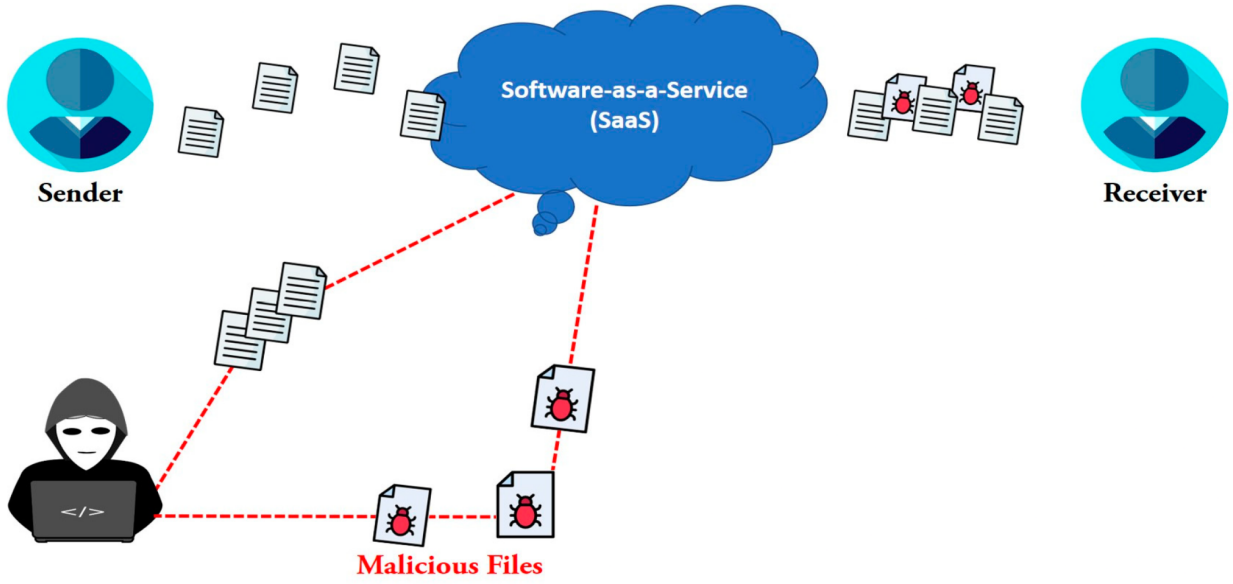
Replay Attack - Think like Attacker

Sam napad se sastoji iz nekoliko faza koje ce biti opisane u daljem tekstu.

Uprosteno:

Napac prikuplja pakete koji se razmenjuju putem mreze i nakog odredjenog vremena vrsi ponovno slanje i tako vrsi narusavanje samog SCADA sistema ili konzistentnosti podataka na SCADA HMI-u.

Detaljnjije:



1. Sam napadac treba prvo da izvrsi prikupljanje paketa koji se razmenjuju izmedju dva elementa SCADA sistema u nasem slucaju Master-a(SCADA HMI) i Slave-a(Simulator Postrojenja).
2. Nakon ovoga sledi samo analiziranje paketa i upoznavanje sa protokolom.U okviru ovog koraka napadac se upoznaje sa samim protokolom u ovom slucaju Modbus i gleda njegove nedostatke i nacine kako da iskoristi te nedostatke kako bi narusio samo funkcionisanje sistema.
3. U ovom koraku napadac vrsi samo napadanje gde bi retransmitovao stare podatke kroz mrezu.

Primer napada:

-U SCADA sistemu se odvija konstantna akvizicija podataka i zadavanje komandi na osnovu odredjenih vrednosti koje su prikupljene.Sam cilj ovog napada je da mi napravimo bazu sa validnim paketima i nakon odredjenog vremena da ponovimo slanje validnih paketa kako bi se sistem zbunio.

Primer:

SCADA HMI - vrsi akviziciju podataka(salje upite) na postrojenje kako bi dobio azurno stanje,server mu vraca odgovore o samom stanju sistema.Mi kao napadac vrsimo prikupljanje tih odgovora kako bi poslali lose vrednosti SCADA HMI-u,samim tim dolazi do zbunjivanja operatera a i samog sistema.

Npr. meri se temperatura vode u sistemu,mi kao operater posmatramo akviziciju i u jednom momentu nam dolaze stare vrednosti(koje mogu biti sa malim odstupanjem od sistema ali moze isto tako da budu velike),ovo zbunjuje samog operatera ali isto i tako sistem za automatizaciju.Ako bi temperatura bila 30 stepeni a mi kao napadac smo poslali staru vrednost od 28 stepeni,a nas sam sistem treba da izvrsi odredjenu automatizaciju zato sto se na 30 stepeni npr. pali low alarm i voda treba da se zagreje dodatno. Sa ovim smo usporili sam sistem koji nece odmah odreagovati u skladu sa automatizacijom vec ce proci odredjeni vremenski period dok sistem odreaguje prilikom cega ce temperatura vode mozda dodatno da padne.

U slucaju automatskog upravljanja ovaj scenario nike moguc zato sto se svaka komanda za automatskim upravljanjem cuva lokalno na scada stanici i ako ne stigne odgovor sa istom porukom koja je poslata prethodno sistem nece odreagovati,recice da je u pitanju greska tj da nije izvrseno automatsko upravljanje.