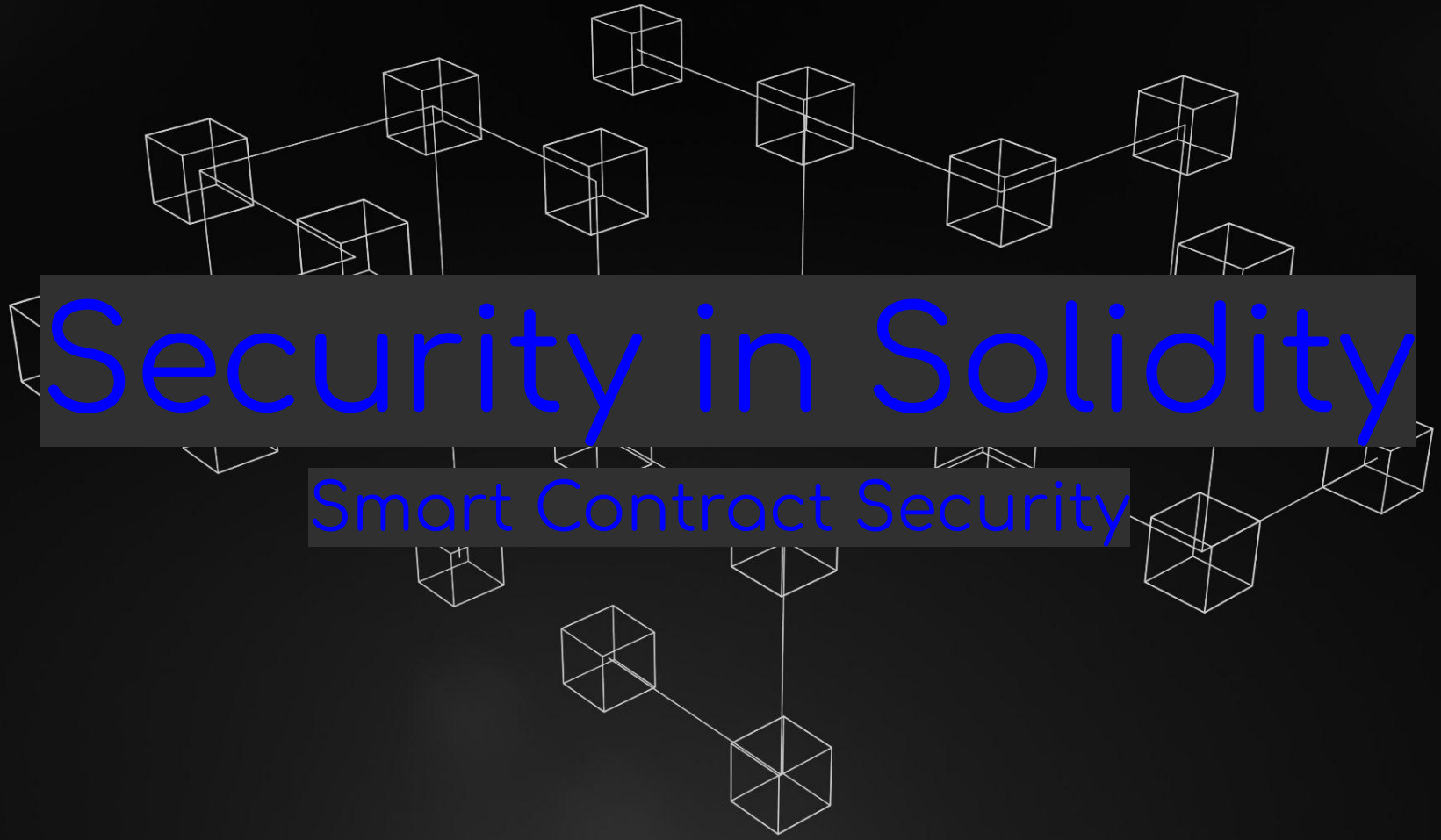
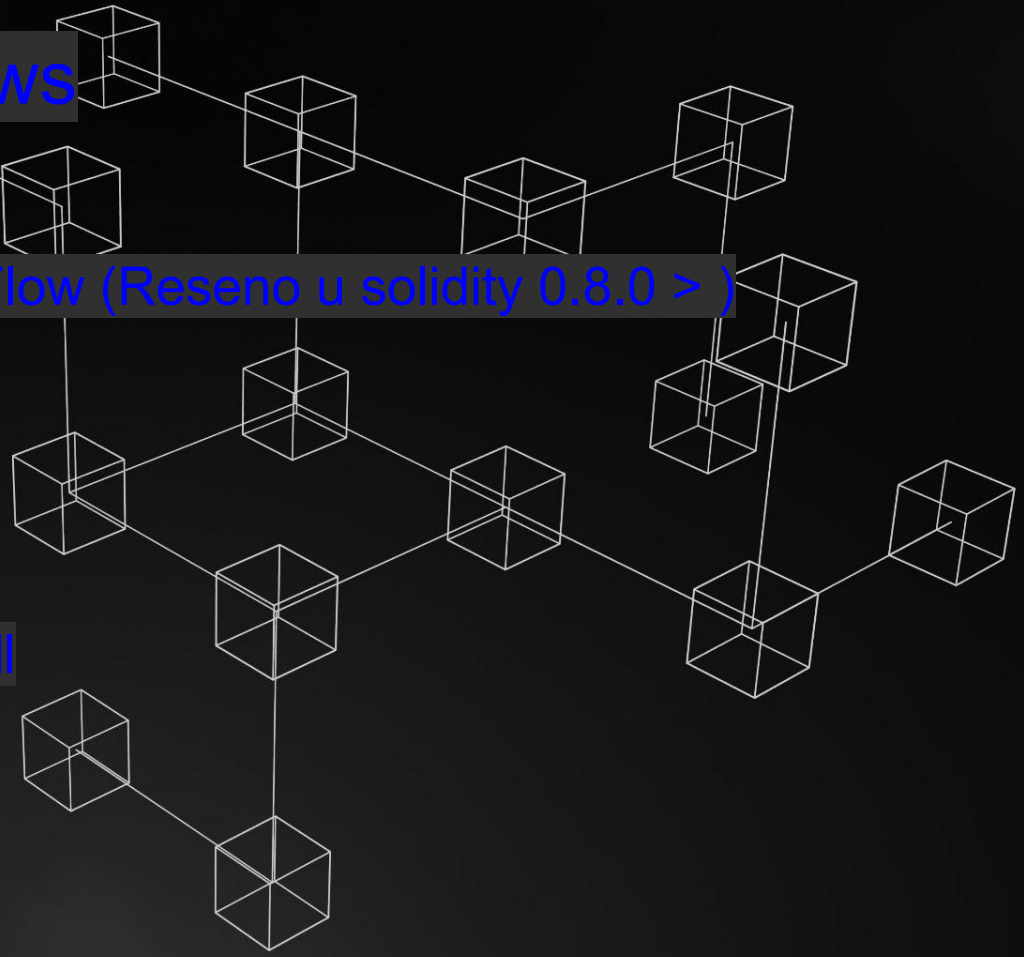


Security in Solidity

Smart Contract Security

Solidity Security Flaws



- Reentrancy Attack
- Integer Overflow/UnderFlow (Reseno u solidity 0.8.0 >)
- DoS (Denial of Service)
- Broken Access Controls
- Front Running
- Insecure Randomness
- Visibility and delegatecall
- ….

Reentrancy Attacks

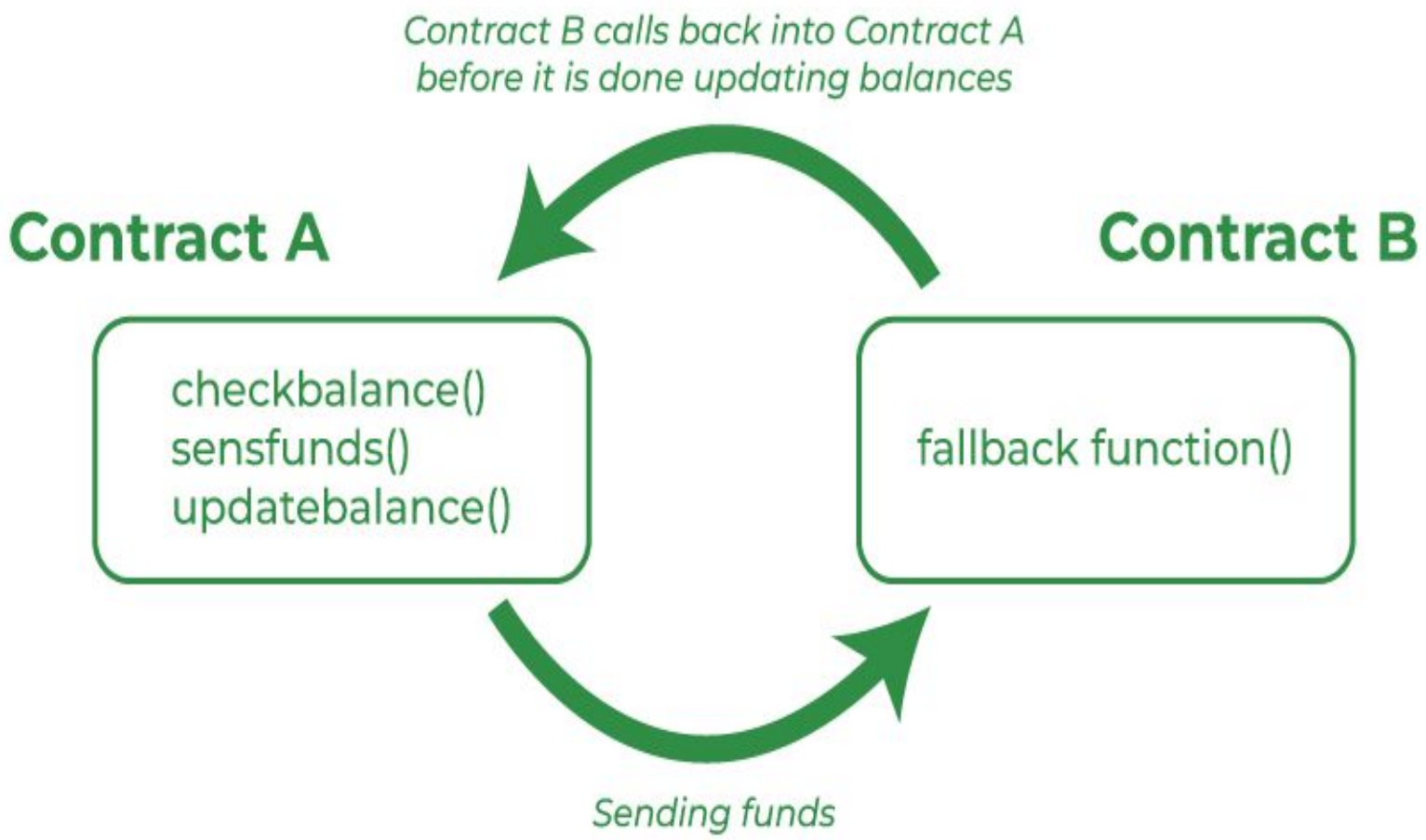
Reentrancy napad je vrsta napada u kojem pametni ugovor pokusava da izvrsi vise akcija odjednom na drugom ugovoru pre nesto sto zavrsi svoje izvrsenje.

Primer:

Recimo podizanje novca.

Pri podizanju novca sa racuna proverava se koliko novca imate na racunu, i imate li dovoljno novca da podignete zeljenu svotu onda izbaci novac i oduzme tu svotu sa vaseg racuna.

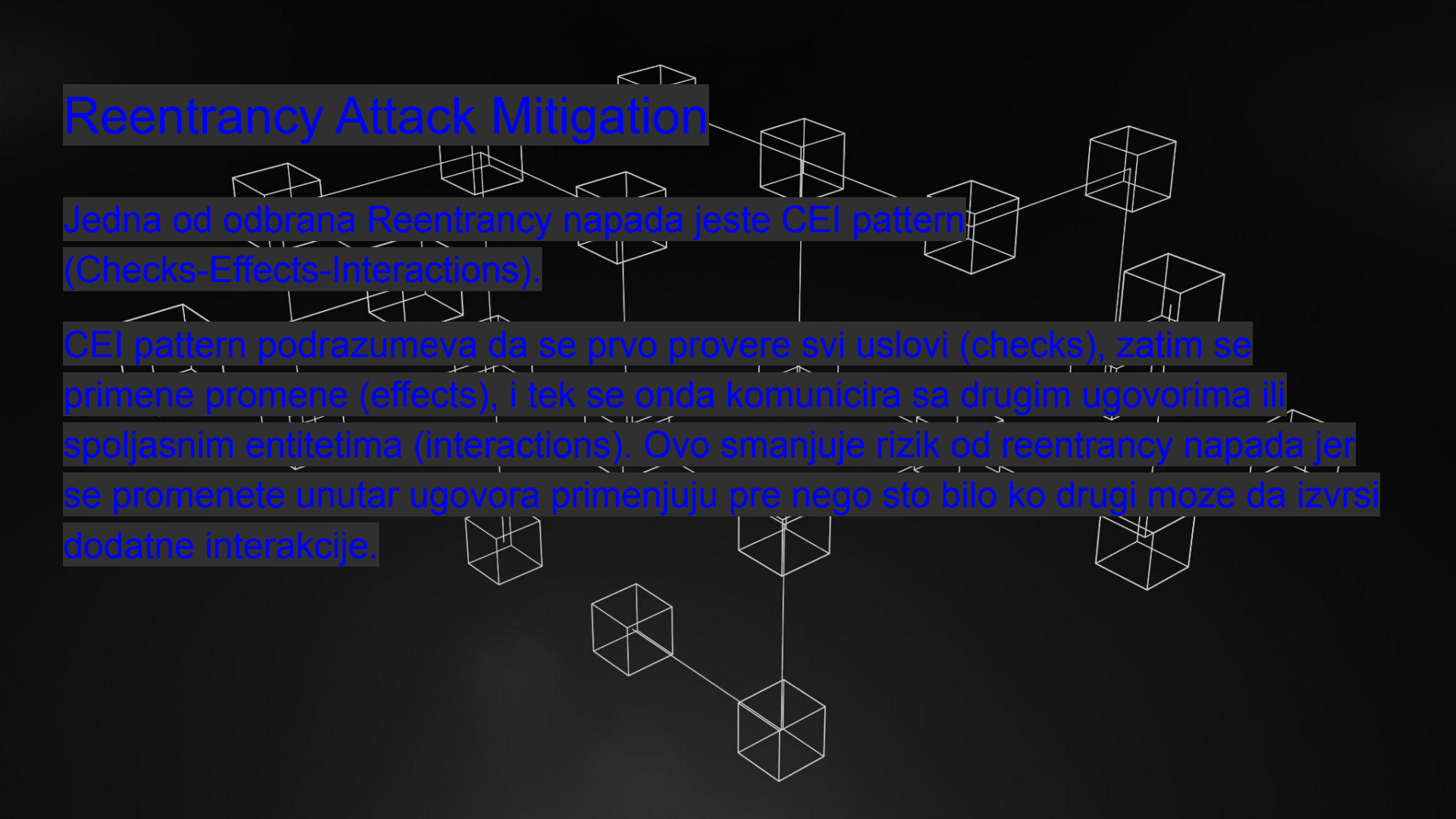
Recimo da se podizanje novca izvrsi pre nego sto bankomat oduzme tu svotu sa vaseg racuna, vi podignete tu svotu opet i sve tako u krug jer bankomat jos uvek nije azurirao novo stanje vaseg racuna.


Contract B calls back into Contract A
before it is done updating balances
Contract A
Contract B
checkbalance()
sensfunds()
updatebalance()
fallback function()
Sending funds

Reentrancy Attack Mitigation

Jedna od odbrana Reentrancy napada jeste CEI pattern (Checks-Effects-Interactions).

CEI pattern podrazumeva da se prvo provere svi uslovi (checks), zatim se primene promene (effects), i tek se onda komunicira sa drugim ugovorima ili spoljasnim entitetima (interactions). Ovo smanjuje rizik od reentrancy napada jer se promenete unutar ugovora primenjuju pre nego sto bilo ko drugi moze da izvrsi dodatne interakcije.



Broken Access Control

Broken Access Control je vrsta bezbednosnog propusta gde se nepravilno upravlja pravima pristupa, omugucavajuci neovlascenim korisnicima da dobiju pristup odredjenim funkcijama ili informacijama.

Primer:

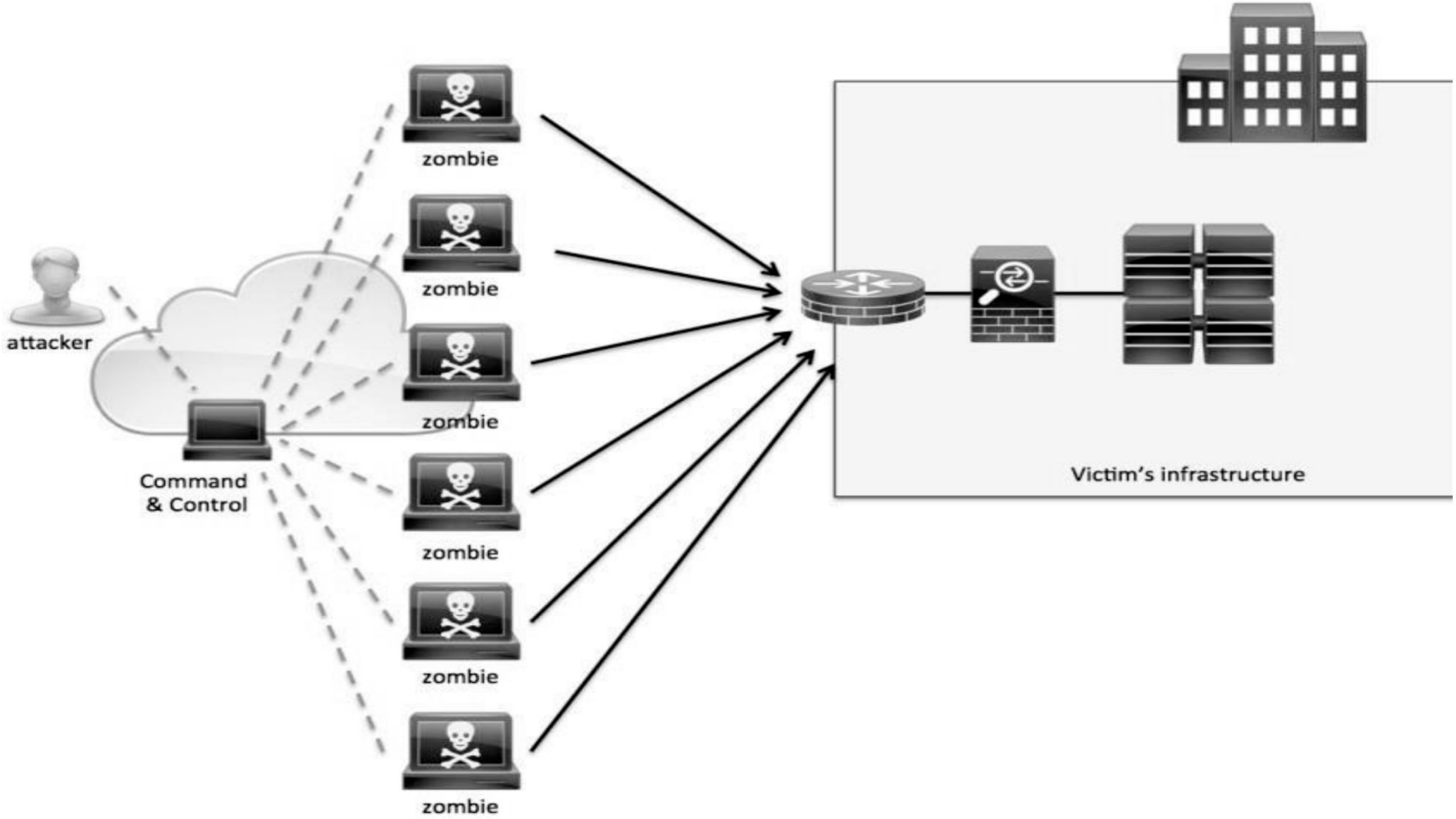
Pretpostavimo da imamo ugovor koji upravlja databazom korisnika. U ugovoru imamo funkciju koja omugucava bilo kome da promeni status korisnika iz npr. obicnog korisnika u Admina jer nema nikakvu zastitu pristupanja te funkcije.

DOS (Denial Of Service)

DOS (Denial of Service) je vrsta napada koja onemugacava normalno funkcionisanje servisa ili mreze tako da postane nedostupna za korisnike. Ovo se desava kada dodje do preplavljivanja sistema velikim brojem zahteva ili potrosnjom resursa cime dolazi do preopterecenja.

Primer DOS-a na blockchainu:

Pretpostavimo da imamo pametni ugovor koji pruza neku funkciju da obavi neki vazan zadatak. Umesto da je ta funkcija brza i efikasna progamer ju je napisao tako da traje veoma dugo. Kada napadac neprestano poziva tu funkciju ona traje dugo i koristi puno resursa. Ako neko neprestano salje zahteve za ovom funkcijom, ona ce se neprestano izvrsavati i zauzimati sve resurse blockchain mreze sto dovodi do DOS-a.


zombie
zombie
zombie
zombie
zombie
zombie
attacker
Command
& Control
Victim's infrastructure

DOS Mitigation

Odbrana od DOS napada u kontekstu pametnih ugovora je preduzimanje ralizitih mera kako bi se umanjili efekti i sprecilo nezeljeno uskracivanje usluga.

- Postavljanje ogranicenja na resurse koji ugovor moze da koristi tokom izvrsavanja.
- Koriscenje Rate Limitinga kao ogranicenje brzine slanja transakcija sa jednom racuna ili adrese
- Pazljivo planiranje trosenje gasa i izbegavanje skupih operacija.
- Koriscenje provarjdera protiv DOS napada

Hvala na paznji :)

Emin Skrijelj

Openzepplin contracts
Openzeppelin security docs