Saranapuolen kautta sisään

- Useat nykyaikaiset salaukset ovat hyviä, eikä niitä pystytä ratkomaan kryptoanalyysin keinoin. Hyökkäykset ovat teoreettisia.
- Uuden tyyppisiä hyökkäyksiä:
  - mikropiirien suojausten murtaminen
  - differentiaalinen virheanalyysi
  - ajoitushyökkäys.
- Perinteiset hyökkäykset ovat perustuneet vain kerättyihin salakielisiin ja selväkielisiin sanomiin.

  Uudet hyökkäykset vaativat salaisen avaimen sisältävään laitteen fyysistä tutkimista tai manipulointia.
- Uhka älykorteille ja muille luotetuille laitteille, jotka annetaan hyökkääjän haltuun.

Mikropiirien suojausten murtaminen

- Hyökkäyksiä kehitetty kautta aikojen ammattimaisesti lähinnä maksu-TV-kortteja vastaan.

  Usein hyökkääjä tarvitsee useita kortteja rikottavaksi (joko vahinkojen tai suojausmekanismien takia).
- Hyökkäyksiä:
  - Virransyötön häiriöt tai fyysinen kosketus nollaavat pysyvän muistin bittejä helpommin kuin nostavat. Nollataan suurin (satunnaisesti valittu) osa avaimen biteistä ja selvitetään kokeilemalla jäljelle jääneet.
  - Muistipaikkoja voidaan rikkoa laserilla. Etsitään standardirakenteita mikroskoopilla ja rikotaan sopivat muistipaikat salausalgoritmin muuttamiseksi.
  - Lyhyet jännitepiikit ja liian nopeat kellotaajuudet voivat sekoittaa mikropiirin prosessorin. Ratkaisu: piirille oma kello ja teholähde.
  - Satunnaislukugeneraattorien häiritseminen tai vahingoittaminen.
  - Piirin suojauskerrosten poistaminen ja jännitemittaukset tai sähkömagneettisen kentän havainnointi.
- Yksinkertaiset hyökkäykset tepsivät halpoihin massavalmisteisiin kortteihin.

  Suojautumiseen on keinoja, mutta ne maksavat. Hyökkäykset kehittyvät, joten kortit on uusittava usein.

Differentiaalinen virheanalyysi

(*differential fault analysis*)

- Menetelmä julkisen avaimen salausten ratkaisemiseksi: Demillo ja Lipton 1996

  Salaisen avaimen salausten ratkaiseminen: Biham ja Shamir 1996, Anderson ja Kuhn 1996
- Hyökkäyksen tavoitteena on selvittää suojatulla mikropiirillä oleva salausavain.

  Säteilytetään mikropiiriä ionisoivalla säteilyllä tai mikroaalloilla, jotka aiheuttavat satunnaisia yhden bitin virheitä mikropiirin rekistereissä.

  Verrataan virheellisten salausten tuloksia ja päätellään avain.
- **DES**: Salataan sama selväkielinen sanoma virheettömästi ja useaan kertaan säiteilytyksessä. Verrataan salakielisiä sanomia.

  Jos vain muutama salakielen bitti muuttuu, tiedetään virheen tapahtuneen ennen tiettyä kierroksen 15 tai 16 S-boksia. Säteilytyksessä kääntynyt bitti on yksi kuudesta S-boksiin menevästä.

  Päätellään kuten differentiaalisen kryptoanalyysin 2R-hyökkäyksessä: Tunnetaan S-boksiin menevät arvot, jotka eroavat yhden bitin, ja boksista tulevien arvojen differenssi. Saadaan 6 avainbittiä. Pian koko viimeinen aliavain tunnetaan.

- Säteilyn aiheuttamat virheet eivät aina ole näin ideaalisia. Kerätään tilastoa mahdollisista avainbiteistä. DES-aliavaimen selvittämiseksi tarvitaan noin 200 toistoa.
- Viimeisen aliavaimen selvittyä on mahdollista ratkaista sitä edellinen aliavain jne. Näin voidaan ratkaista myös moninkertainen salaus.
- On mahdollista selvittää tuntemattomien salakirjoitusten rakennetta (S-boksien koot ja sisältö).
- Suojautumiseen käytetään virhetarkistuksia:
  - pariteettibitit
  - kaksi rinnakkaista prosessorin lohkoa, joiden tuloksia vertaillaan
  - tarkistuslaskelmat modulo jokin pieni luku.
- Keskeinen periaate: suojatun piirin murtamisen pitää olla kalliimpaa kuin siitä saatava hyöty.

  Yhdellä piirillä olevan tiedon paljastuminen ei saa haitata muita käyttäjiä. Ei yhteisiä salaisuuksia kaikille piireille!
- Hyökkäysten teoria tunnetaan, mutta käytännön toteutuksia ei julkistettu.

Ajoitushyökkäys

(*timing attack*)

- Paul Kocher 1995 (uudenlaisten hyökkäysten aallon aloittaja)
- Koskee **julkisen avaimen** algoritmeja, ei salaisen!
- Mitataan vasteaikoja älykortilta tai verkon yli.

  Kerätään ajoista tilastoa.

  Päätellään yhsityisen avaimen avaimen suuruus (tai muu ominaisuus) laskentaan kuluneen ajan perusteella. Eri algoritmeille kehitetty tarkkoja tilastollisia kaavoja.
- Hyökkäykseltä suojaudutaan antamalla vastaus vakioajassa tai lisäämällä laskenta-aikoihin satunnaisia viiveitä.