Komunikacijska varnost v telesnih senzorskih omrežjih

Marko Kompara in Marko Hölbl

10.4.2017

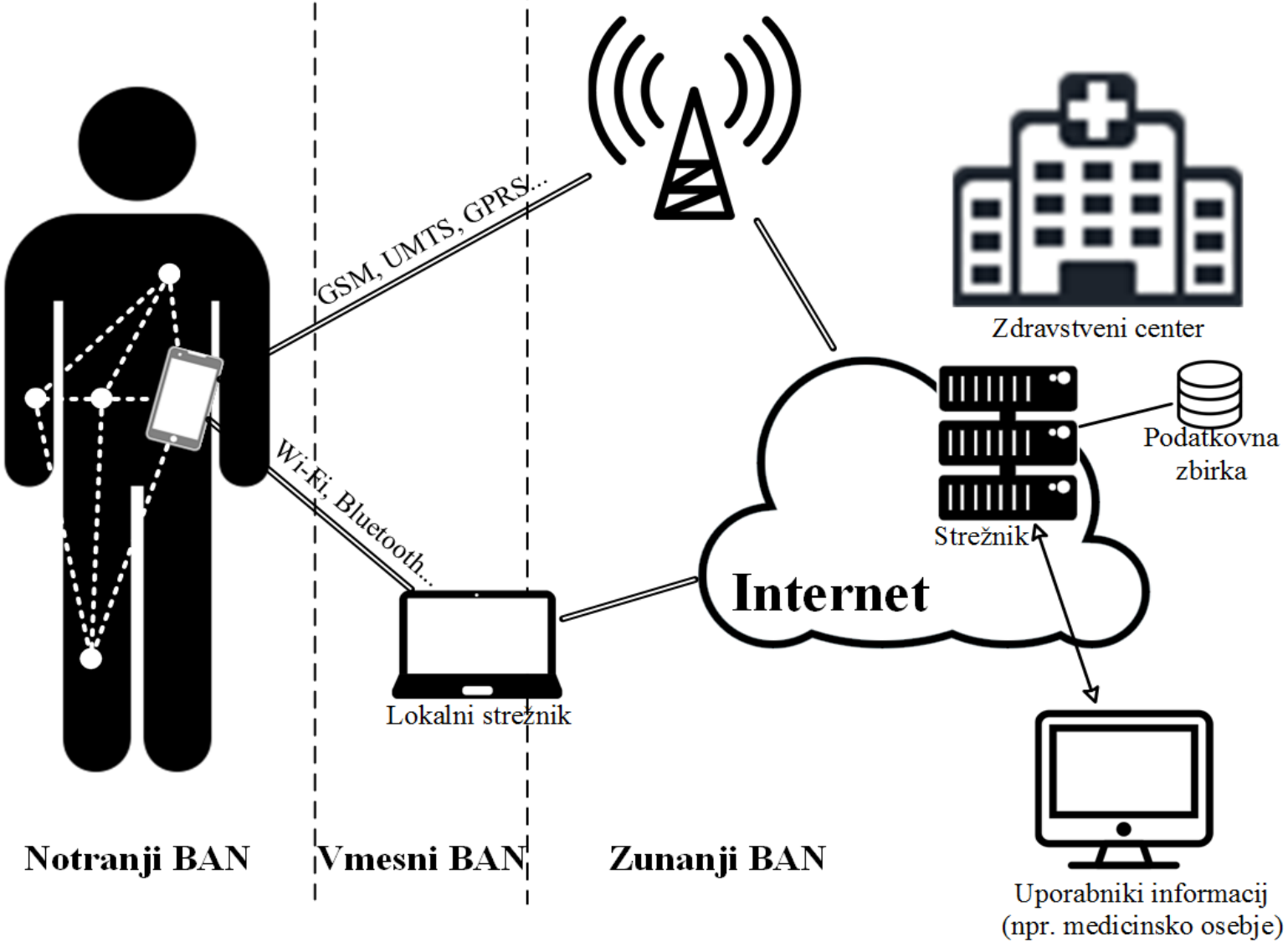
Telesno senzorsko omrežje

- Body Area Network (BAN in pa tudi BSN, WBAN, WBSN, BASN, WBASN, BANT, WMSN)
- Brezžično senzorsko omrežje (ang. Wireless Sensor Network - WSN)
- Senzorji v in na človeškem telesu, ki merijo fiziološke signale
- Osebni podatki, zanimivi za napadalce
- Velik potencial v nadaljnjem razvoju zdravstva
- Napredek v mikroelektroniki, vgrajenih sistemih in brezžični komunikaciji

Omejitve BSN omrežij

- Energijska učinkovitost
- Omejene pomnilniške kapacitete
- Nizka procesorska moč
- Omejen prenos podatkov
- Motnje
- Robustnost in odpornost na napake
- Napake v podatkih
- Bio-kompatibilnost

BSN


GSM, UMTS, GPRS...
Wi-Fi, Bluetooth...
Zdravstveni center
Podatkovna zbirka
Strežnik
Internet
Lokalni strežnik
Uporabniki informacij (npr. medicinsko osebje)
Notranji BAN
Vmesni BAN
Zunanji BAN

Dogovor o ključih v BAN

- Vzpostavitev ključa je najpomembnejši korak pri zagotavljanju zaupnosti, avtentičnost in celovitost podatkov.
- Simetrična kriptografija
- Ranljivost izmenjave ključev v brezžični komunikaciji (MITM napad)
- Tri skupine shem za izmenjavo ključev
  - Tradicionalne sheme za izmenjavo ključev
  - Dogovor o ključih na podlagi fizioloških vrednosti
  - Hibridne sheme za dogovor o ključih

Tradicionalne sheme za izmenjavo ključev

- Kriptografija javnega ključa
  - RSA in ElGamal
    - Velike zahteve po pomnilniku in procesorski moči
  - Eliptične krivulje (Elliptic Curve Cryptography - ECC)

AES	RSA	ECC
128 bit	3072 bit	256 bit
256 bit	15360 bit	521 bit

- Sheme osnovane na principu pred-distribucije šifrirnega gradiva
  - Manj procesiranja
  - Zaseda malo pomnilnika
  - Slaba prilagodljivost spremembam v omrežju
- Sheme osnovane na podlagi naključnosti kanala

Izmenjava ključev na podlagi fizioloških vrednosti

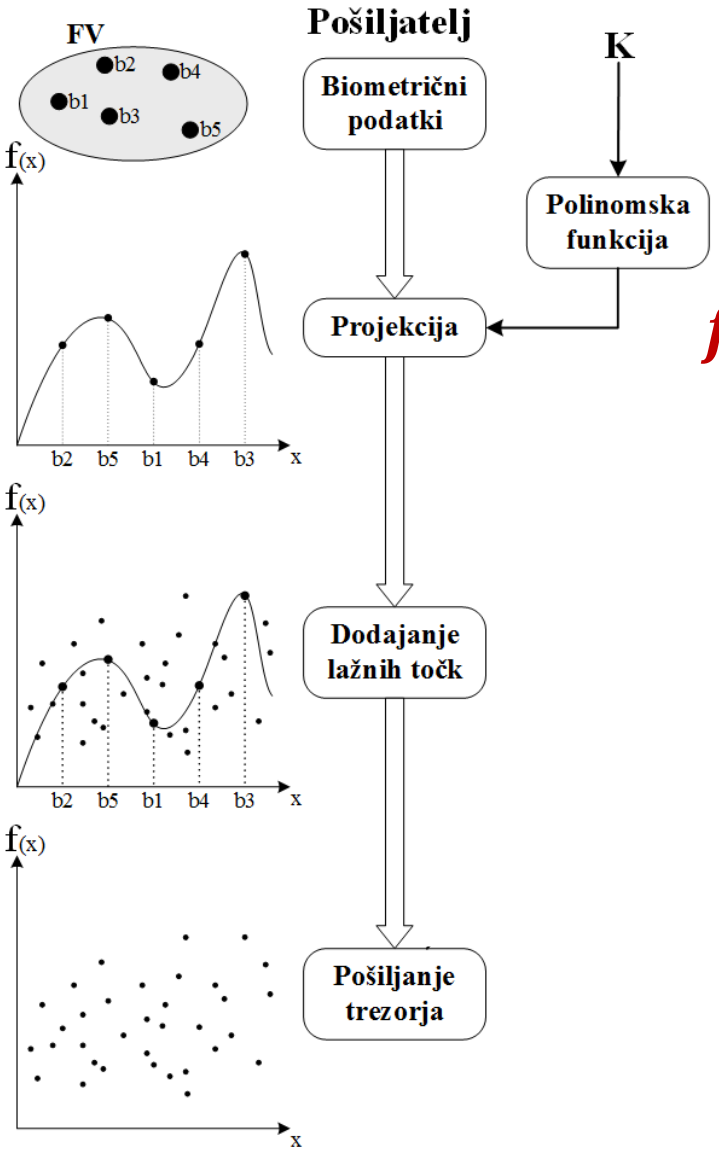
- Uporaba človeških vitalnih znakov za ustvarjanje/izmenjavo ključa
- Dva ali več senzorjev neodvisno in istočasno merita isti fiziološki signal
- Pošiljatelj in prejemnik lahko generirata enake vrednosti, ker se nahajata na istem telesu
- Krvni pritisk, Elektrokardiogram (EKG), Fotopletizmograf, Nivo kisika v krvi (SpO2), krvne ploščice,…

Izmenjava ključev na podlagi fizioloških vrednosti

- Ni pred-distribucije šifrirnega gradiva
- Ni neodvisne faze za izmenjavo ključa
- Dinamične spremembe v omrežju
- “Plug-n-play” način delovanja
- Manjša poraba pomnilnika (več procesiranja)

- Sinhrono merjenje fizioloških signalov
- Fiziološki signali z visoko entropijo
- Odstranjevanje šuma

Mehki trezor (Fuzzy Vault)



$K = 321$

$f(x) = 3x^2 + 2x + 1$

Hibridne sheme za izmenjavo ključev

- Kombinacija tradicionalnih shem in shem osnovanih na fizioloških vrednostih
  - Pred-distribucija ključa in uporaba fizioloških vrednosti
  - Uporaba fizioloških signalov za generiranje naključnih vrednosti

Zaključek

- Gartner je predvideval prodajo 274.6 milionov nosljivih naprav (2016).
- Trg vgrajenih naprav vreden preko 30 milliard € (2015).

- Dick Chaney ima onemogočen “wireless” na srčnem spodbujevalniku.
- Johnson & Johnson je našel varnostno pomanjkljivost v inzulinski črpalka.

HVALA ZA VAŠO POZORNOST!

VPRAŠANJA/PRIPOMBE/PREDLOGI