Teorija kodiranja in kriptografija 2013/2014

Varnost kripotsistemov

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 8. 4. 2014

Vsebina

- Stopnje varnosti kriptosistemov
- Lastnost popolne tajnosti
- Semantična varnost

Cilji nasprotnika

Napadalec je prestregel en kriptogram.
Njegovi cilji so lahko

- odkriti dekodirni ključ,
- dešifrirati kriptogram, oziroma del kriptograma, z določeno (nezanemarljivo) verjetnostjo; lahko tudi samo ugotoviti iz kriptograma neko informacijo v zvezi z besedilom,
- z verjetnostjo več kot 1/2 razlikovati med kriptogramomoma dveh različnih besedil oziroma med kriptogramom danega besedila in naključnim nizom.

Stopnje varnosti

Glede na računsko zahtevnost vdora v sistem ločimo naslednje stopnje varnosti:

1. **brezpogojna varnost** (unconditional security): vdor v sistem ni mogoč, tudi če imamo neomejene računske vire;
2. **absolutna računska varnost** (computational security): vdor v sistem je mogoč, a zahteva enormno količino računskih virov;
3. **relativna računska varnost** (provable security);
4. **šibka računska varnost**: za problem vdora v sistem niso znani učinkoviti algoritmi, ga pa lahko učinkovito prevedemo na neki znan domnevno težek problem.

Relativna računska varnost

Nek znan domnevno težek problem R (referenčni problem) lahko učinkovito prevedemo na problem vdora v sistem (torej: če lahko učinkovito vdremo v sistem, lahko učinkovito rešimo R).

To pomeni, da je vdiranje v sistem vsaj tako težko kot rešiti R.

Nekaj znanih težkih problemov:

- Faktorizacija celih števil
- Problem diskretnega logaritma
- Problem diskretnega logaritma na eliptični krivulji

Sistemi s popolno tajnostjo

To so zgledi brezpogojno varnih kriptosistemov.

Intuitivno:
kriptosistem ima lastnost popolne tajnosti, če kriptogram sam (brez ključa) ne daje nobene informacije o besedilu.

Lastnost popolne tajnosti - definicija

Naj bo $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ simetrični kriptosistem.

Kriptosistem $\mathcal{S}$ opremimo z verjetnostno porazdelitvijo na množici $\mathcal{B} \times \mathcal{K}$.

Osnovni poskus: izbira besedila $b \in \mathcal{B}$ in ključa $k \in \mathcal{K}$.

- B slučajna spremenljivka z zalogo vrednosti $\mathcal{B}$,
- K slučajna spremenljivka z zalogo vrednosti $\mathcal{K}$ in
- C slučajna spremenljivka z zalogo vrednosti $\mathcal{C}$;
  C je določena z B in K.

Predpostavke:

- B in K sta neodvisni:

$$P[B = b \cap K = k] = P[B = b] \cdot P[K = k].$$

- za vsak $b \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ velja še

$$P[B = b] > 0 \quad \text{oziroma} \quad P[C = c] > 0.$$

Potem ima kriptosistem $\mathcal{S}$ z dano verjetnostno porazdelitvijo na množici $\mathcal{B} \times \mathcal{K}$ **lastnost popolne tajnosti** natanko tedaj, ko za vsak $b \in \mathcal{B}$ in $c \in \mathcal{C}$ velja

$$P[B = b | C = c] = P[B = b].$$

Slučajna spremenljivka C

Vrednosti C: za dana $b \in \mathcal{B}$ in $k \in \mathcal{K}$ slučajna spremenljivka C zavzame vrednost

$$c = E_k(b).$$

Verjetnost dogodka $C = c$ dobimo s pomočjo formule za popolno verjetnost:

$$P[C = c] = \sum_{B \in \mathcal{B}} P[C = c | B = b] \cdot P[B = b],$$

kjer je

$$P[C = c | B = b] = \sum_{k \in \mathcal{K} : E_k(b) = c} P[K = k].$$

Trditev

Če ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti, potem

- *za vsak $b \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ obstaja $k \in \mathcal{K}$:*

$$E_k(b) = c$$

- *in velja*

$$|\mathcal{B}| \leq |\mathcal{C}| \leq |\mathcal{K}|.$$

Izrek (Shannon)

Naj velja $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{K}|$. Potem ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti natanko tedaj, ko

- *za vsak $b \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ obstaja natanko en $k \in \mathcal{K}$: $E_k(b) = c$ in*
- *slučajna spremenljivka K je enakomerno porazdeljena*

Vernamova šifra

Vernamova šifra ali enkratni ščit, *angl. one-time pad*

$\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$,
ključ k iz $\{0,1\}^n$ izberemo naključno.

Kodiranje:

$$E_k(b) = b \oplus k.$$

Dekodiranje:

$$D_k(c) = c \oplus k.$$

To je pravzaprav Vigenèrjeva šifra, le da je ključ enako dolg kot besedilo.

...Vernamova šifra

- Šifro je patentiral Gilbert Vernam leta 1919.
- Joseph Mauborgne je predlagal, da je ključ naključen in se uporabi samo enkrat.
- Claude Shannon je v 1940' letih pokazal, da je takšna šifra nezlomljiva.

Trditev

Če ključ izbiramo slučajno in vsakega z enako verjetnostjo, ima Vernamova šifra lastnost popolne tajnosti.

Pomen LPT

Lastnost popolne tajnosti pomeni brezpogojno varnost pri napadih z golim kriptogramom.

Tudi če imamo dovolj računskih virov, da preizkusimo vse možne ključe, dobimo le vsa možna besedila dane dožine in ne vemo, katero je pravo. Še več, ne dobimo prav nobene informacije o besedilu.

Slabosti: zelo dolg ključ, kar povzroča težave pri generiranju in distribuciji, predvsem pa napeljuje k ponovni uporabi istih ključev, kar je huda napaka (glej prosojnice tokovne šifre).

Semantična varnost

Napadalec, ki ima omejene vire, ne more izračunati nobene informacije o besedilu iz kriptograma v polinomskem času.