Šifrování hlasu

Historie a současnost

Počátky

- „Odnepaměti“ bylo šifrování věcí textové komunikace. Jiná komunikace na dálku ani neexistovala.
  - Jediná alternativa: heliografy. Zjistit dnes něco o použitých šifrách je těžký úkol.

- První závažný konflikt průmyslových mocností, v němž byly používány polní telefony, byla rusko-japonská válka (1905).
  - Rovněž je těžké zjistit dnes detaily, mnoho archivů bylo zničeno, nebo existují jen v japonštině.
  - Válka, jejíž poznatky byly západními mocnostmi široce ignorovány, a to i přes přítomnost řady pozorovatelů.

- Běžným standardem bylo zcela nešifrované telefonické spojení mezi pozorovatelem a dělostřeleckými pozicemi.
  - Rozkazy zásadnějšího rázu se předávaly v papírové podobě, šifrované národními šiframi.

První světová válka (1914-18)

- Zabezpečení komunikace v roce 1914 bylo silně zanedbané.
  - Největší problém měla ruská armáda, kde bylo běžným standardem komunikovat po otevřeném kanále, bez použití jakýchkoliv kódů (negramotnost rekrutů).
    - Poučení dodnes: uživatel musí být připraven a schopen používat daný šifrovací prostředek.
  - Týkalo se to bohužel nejen klasického telefonu, ale i bezdrátové komunikace, která tou dobu byla úplnou novinkou.
    - Poučení dodnes: nové typy komunikace nesou nová rizika.
  - Porážka Rusů v bitvě u Tannenbergu (1914) se dá z velké části přičíst úspěšným odposlechům.

První světová válka (1914-18)

- V průběhu roku 1915 si válčící strany uvědomily, že nešifrovaný provoz „škodí zdraví“.
- První pokrok: zavedení otevřených kódů.
  - Dodnes běžná praxe: jednotlivé slovní pojmy se nahrazují jinými.
  - Knihy kódů se musely nahrazovat 2x měsíčně.
  - Vysoké riziko při ztrátě kterékoliv knihy.
    - Poučení dodnes: klíče mají platit jen po omezenou dobu.
  - Ve spěchu a při nesrozumitelném přenosu se nutnost kódování často zanedbávala.
    - Poučení dodnes: uživatelé budou obcházet nepohodlné či komplikované prostředky, i kdyby jim šlo o život.

První šifrování přenosu hlasu

- Komerční sféra: AT&T a jejich produkt “A-3”
  - V zásadě překrýval hovor šumem, který se na druhé straně odečítal.
    - Velké problémy se synchronizací.
  - Začátkem druhé světové války byl již prolomen.
    - Němci úspěšně odposlouchávali A-3 od roku 1941.
- Druhá světová válka
  - Amerika: SIGSALY.
    - Vyvinuto v AT&T jako následovník A-3.
    - První použití standardu PCM (Pulse-Code Modulation).
    - 20 ms pakety, komprese, FSK (Frequency-Shift Keying).

Systém SIGSALY

50 tun, 30 kW příkonu. Vyrobeno 16 kusů.

Poválečný vývoj

- Až do 80.let převážně specializovaná hardwarová zařízení.
  - USA: KY-3, STU-I, STU-II, STU-III.
  - Přechod k digitální reprezentaci zvuku
    - Náskok cca 40 let před světem běžného telefonování.
    - Reakce na přirozený problém - šum a výpadky.
    - Postupné zmenšování z desítek tun až po běžně vypadající telefonní přístroje.

STU-III (1987 - 2009)

Lze zapojit do běžné telefonní zásuvky a provozovat i jako normální telefonní přístroj.

Generuje jednorázové klíče pro každý hovor.

Softwarové šifrovací platformy

- Umožněny nástupem Internetu a „chytrých“ zařízení.
  - SW lze daleko snáze opravovat a vylepšovat než HW.
- SW v zásadě řeší tytéž problémy jako HW:
  - Sestavení jednorázových klíčů.
  - Efektivitu přenosu.
  - Odolnost proti výpadkům a chybám přenosu.
  - Jednoduchost použití.
- Problémy navíc:
  - Vzájemná kompatibilita.
  - Prostupnost existujícími sítěmi (např. NAT).

Typické fungování SW platforem

- Specializovaný SW běžící v operačním systému jako služba.
  - Udržuje spojení na VoIP službu.
  - „Hlídá“ příchozí hovory / zprávy.
- Při hovoru:
  - Vytváří jednorázové klíče.
  - Zajišťuje autentizaci.
  - Ošetřuje různé druhy výpadků a ztrát ve spojení.
  - Na konci hovoru likviduje klíče.

Očekávaný vývoj šifrovacího SW

- Konferenční hovory.
  - Stávající šifrovací protokoly nepostačují.
- Větší důraz na textovou komunikaci.
  - Např. nová Blackberry platforma.
- Modifikované operační systémy.
  - NSA Android.
  - Obrana proti nežádoucím aplikacím.

Děkuji za pozornost