TOMÁŠ ROSA

ODPOSLECH POHLEDEM KRYPTOLOGA

LUŠTĚNÍ VERSUS ODPOSLECH

ZÁLEŽÍ NA KONTEXTU A OČEKÁVÁNÍCH

- Odposlech zde chápejme jako spolehlivou provozní službu
- Odposlouchávámе díky cílenému způsobu konstrukce
- Luštění patří spíše do oblasti vojenské a zpravodajské, jeho principy a kontext jsou zásadně odlišné, než co by například obecný kriminalista očekával
- Luštíme díky neplánovaným slabinám

KRYPTOGRAFICKÁ SÍLA ALGORITMŮ

PROČ JI NEUMÍME ŠKÁLOVAT?

- Model výpočetní síly útočníka není technologicky dostatečně přesný
- Pracujeme s představou technicky extrémně dobře vybaveného protivníka a zanedbatelnou pravděpodobností jeho úspěchu
- Cokoliv jiného je pro nás nezvládnutelný terén
- Nelze očekávat, že toto se změní
- Naopak, s příchodem kvantových počítačů musí model síly útočníka pokrýt i jeho nové principiální schopnosti, a to opět extrémním způsobem

SKRYTÁ OSLABENÍ

ZADNÍ VRÁTKA DO PEKLA

- Neumíme-li škálovat sílu algoritmů obecně, může nás napadnout oslabit je jen pro někoho
- Pro někoho, kdo má výhodu v lepší znalosti řešení použitého matematického problému
- Svého druhu se jedná o klíč, jenže tento druh klíče neumíme ochránit
- Neumíme odhadnout, jak složité je pro někoho dalšího tento klíč najít a zneužít
- Neumíme spolehlivě poznat, že k tomu došlo, a do komunikace vstoupila další strana
- Z výhody se tak stává významná nevýhoda, ani původní odposlouchávající strana se už nemůže na svůj zdroj spolehnout

ODPOSLECH NUTNO PŘIZNAT

JEHO PODMÍNKY JSOU DÁNY UŽ NA ZAČÁTKU KOMUNIKACE

- Monitorující strana se sama stává součástí protokolu
- Její možnosti jsou dány znalostí klíčů
- Toto je jediná výhoda, jejíž rozsah a účinnost umíme pro všechny strany spolehlivě garantovat
- Prakticky by to ovšem dnes znamenalo přestavět současnou komunikační infrastrukturu
- Zbrždění, možná i kolaps, probíhající digitalizace společnosti je pravděpodobné