Přežije 5G v době post-kvantové?

Konference e-governmentu - Mikulov 2026
7. - 9. 9. 2026

O2 Czech Republic a.s.
Michal Hozák

Více ze života

Co nás dnes čeká?

1. Zhodnocení bezpečnostní hrozby kvantovými počítači
2. Současná bezpečnostní protiopatření
3. Kompaktní mobilní varianta MPN pro government

Obecné principy kvantového počítače

V kvantových počítačích je superpozice stav někde mezi 1 a 0 se schopností qubitu zkolabovat do stavu 1 nebo 0 dle určené pravděpodobnosti.

Qubit v superpozici lze naklánět tak, aby pravděpodobnost mezi 1 a 0 byla stejná nebo různá. Výsledek se ukáže, když dojde k měření a tím ke kolapsu do stavu 1 nebo 0.

$$\left|\circlearrowleftrightarrow\right\rangle = \frac{1}{2}\left|0\right\rangle + \frac{1}{2}\left|1\right\rangle$$

V kvantových počítačích je kvantové provázání motorem, který umožňuje paralelní zpracování dat v masivním měřítku.

Zatímco klasické počítače procesují informace jednu po druhé, kvantové provázání spojuje qubity (kvantové bity) do jednoho společného systému. Díky tomu roste výpočetní síla počítače s každým dalším přidaným qubitem exponenciálně, nikoliv lineárně.

Je „kvantová“ hrozba reálná?

Kvantové počítače přicházejí a s nimi hrozba, která může zásadně ohrozit bezpečnost celé digitální infrastruktury, včetně 5G sítí.

Co jsou kvantové počítače?

Místo klasických bitů (0 nebo 1) pracují s **qubity**, které díky principu superpozice a kvantového provázání provádějí některé výpočty exponenciálně rychleji než jakýkoli klasický procesor.

Shorův algoritmus *dokáže prolomit asymetrické šifrování RSA nebo ECC během* ***několika hodin*** *— klasickému počítači by stejný úkol trval miliony let*

Groverův algoritmus zrychlí brute-force útok na symetrické šifry. Efektivně sníží bezpečnost „na polovinu“.
128bit → efektivně ~64bit

Proč může být 5G v ohrožení?

Asymetrické šifrování v 5G slouží k ověření identity, digitálním podpisům a sdílení bezpečnostních klíčů (handshake).

Odhalení identity uživatelů (SUCI)

Kompromitace protokolu AKA – protokol zajišťuje, že se telefon a síť operátora poznají a dohodnou se na klíči pro šifrování dat. Hrozí např. vytvoření falešné základnové stanice a odposlech.

Hrozba Harwest Now, Decrypt Later – Již nyní můžeme ukládat zašifrovaná data s předpokladem, že k prolomení dojde, až kvantové počítače dosáhnou požadovaného výkonu.

Napadení CORE - Komunikace mezi jednotlivými komponentami např. pomocí TLS nebo IPsec opět spoléhá na asymetrické klíče. Prolomení by znamenalo kolaps jádra 5G.

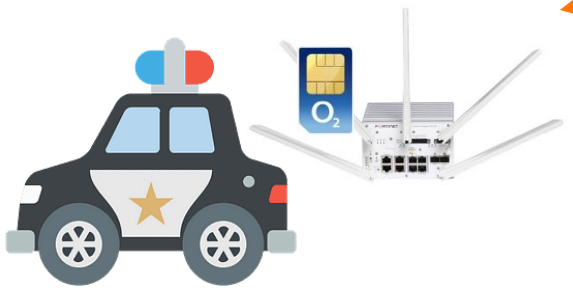
Současné protiopatření kvantové hrozby

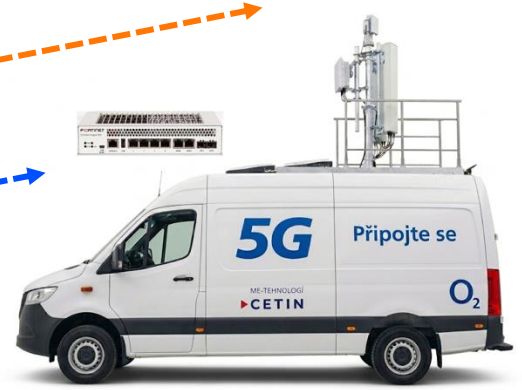
1 **TUAK –** sada algoritmů pro autentizaci a generování klíčů (využívá algoritmus Keccak SHA3 – 256bit klíč).

-Původní Milenage z 4G založený na AES 128 nebude v budoucnu kvantově odolný

signalizace sítě – kvantovou odolnost zajišťuje přímo 5G CORE

uživatelská data – kvantovou odolnost zajišťuje FortiGate





O2 5G privátní síť umí být odolná proti aktuálním kvantovým hrozbám.

2 **ML-KEM** (asymetrická postkvantová šifra) – pomůže přenést „tajný klíč“. Následně je již použit symetrický AES-256.

-Kromě ML-KEM jsou k dispozici i další PQC algoritmy jako jsou například HQC, BIKE nebo Frodo.

Disclaimer: Vzhledem k tomu, že nelze s jistotou říci kdy a kam se technologie kvantových počítačů a jejich algoritmů dostane, nelze tak ani tyto metody pokládat za definitivně kvantově odolné.

Mobilní varianty MPN pro government

5G privátní síť včetně CORE, s možností lokálního provozu

Cíl: vytvořit rychle zabezpečenou 5G „bublinu“ pro jednotku / stanoviště / obec

1

Vestavba do vozidla – „mobilní uzel“ s rádiem + CORE.

2

Přenosný box – připraveno k instalaci během pár minut, převoz i v osobním voze.

Varianta integrovaná ve vozidle

- Nasazení bez instalace – „zapni a použij“
- Vhodné pro mobilní velitelské pracoviště / retranslaci / testovací polygon
- Pokrytí okolí vozidla pro připojení koncových zařízení jednotky
- Možnost napojení na další spojení (WAN/backhaul) podle dostupnosti
- Větší dosah než u přenosné varianty

Varianta přenosný box

2

- Přenositelné řešení pro rychlé vytvoření privátní sítě v nové lokalitě
- Kompaktní 5G CORE připravený pro rychlé nasazení v terénu
- Lokální řízení uživatelů, služeb a politik (bez nutnosti internetové konektivity)

- Příprava na připojení napájení a antén – minimum kroků v terénu
- Vhodné pro dočasné stanoviště, cvičení, krizové situace, ochranu objektu
- Možno využít i jako rozšíření pokrytí veřejné O2 sítě

Děkuji za pozornost,

přijměte pozvání k našemu stánku.

Backup

O_2

Kontroverzní IMSI Catcher

IMSI je unikátní číslo uložené na SIM kartě, která identifikuje uživatele v síti.

IMSI Catcher je zařízení, které předstírá, že je legální vysílač mobilního operátora.

1 Sledování přítomnosti a identifikace uživatele

Silnější signál IMSI Catcheru donutí telefon se zkusit přihlásit k němu (Attach request)
Stanice si vyžádá IMSI v nešifrované podobě ještě před zahájením autentizace. (Identity Request)

2 Vynucený přechod na 2G síť

Falešná základnová stanice odmítne přihlášení telefonu s chybovým kódem např: „EPS service not allowed“ nebo zaruší 4G frekvence.
Telefon vyhodnotí situaci přepnutím do staré 2G sítě ve které chybí vzájemná autentizace a podvržená základnová stanice získá přístup k volání SMS i datům.

3 Fyzická lokalizace

Jakmile IMSI Catcher přiměje cíl ke komunikaci, donutí telefon k opakovaným odpovědím- (uplink). Catcher měří sílu signálu, úhle příchodu signálu případně časové zpoždění. Směrovou anténou je pak určena poloha telefonu.

4 Odepření služeb (DoS)

Cyklické odmítání pokusů o připojení, případně neustálá smyčka- navazování spojení způsobí postiženým telefonům ztrátu možnosti telefonovat i datovat.

Jak se bránit?

- Je nutné mít SIM s podporou SUCI.
- Vypněte si 2G na zařízení/ modemu – pokud je to možné.

1 Na radiovém rozhraní se už nikdy nevysílá nezašifrovaný identifikátor volajícího.

2 Identita se šifruje přímo na SIM a je dynamická, tedy vysílaný identifikátor je pokaždé jiný.

3 Pokaždé se generuje nový jednorázový klíč, při vysílání se jeví jako náhodný řetězec bajtů.

4 Pokud IMSI Catcher v 5G síti pošle výzvu k identifikaci, dostane pokaždé jinou hodnotu. Nemá šanci zjistit komu SIM patří, ani spojit dva požadavky s jedním zařízením.