

IT biztonság közérthetően Erdősi Péter Máté

#CleanYourVirtualDesktopDay



Miről is van szó?

- „*legföljebb* öt más egyénen keresztül, (...) kapcsolatot tud létesíteni az illetővel, csupa közvetlen - ismeretség – alapon” Karinthy Frigyes (1929)
- „A távolságot, mint üveg golyót, megkapod...” József Attila (1935. február 2.)

Karinthy Frigyes: Láncszemek

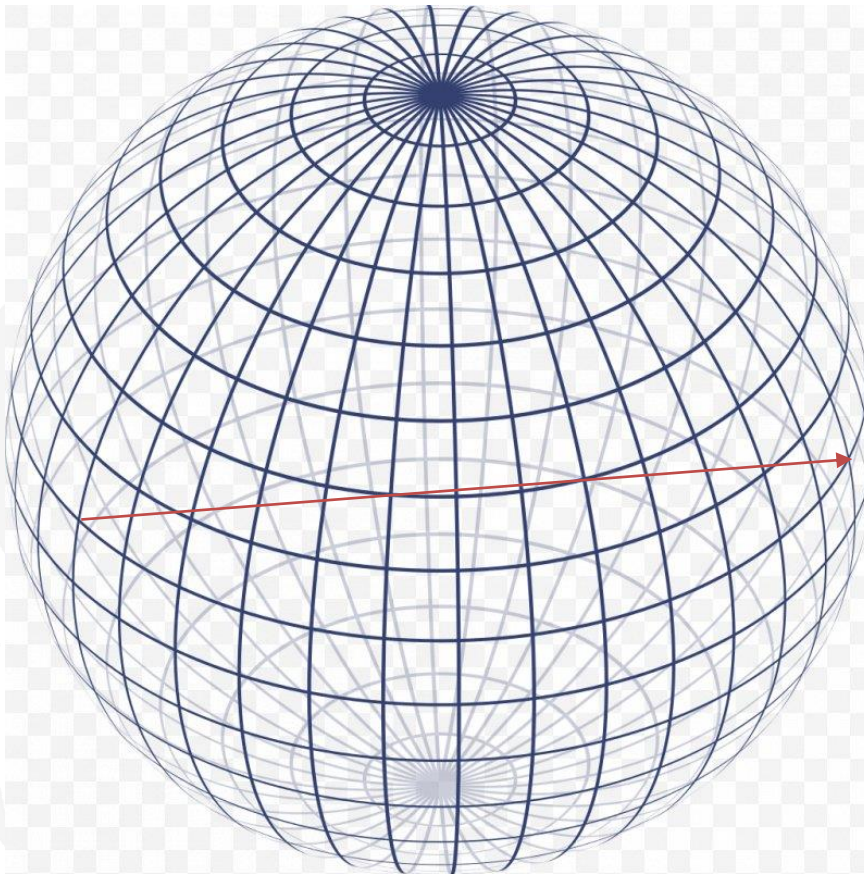
„Egyébként kedves játék alakult ki a vitából. Annak bizonyításául, hogy a Földgolyó lakossága sokkal közelebb van egymáshoz, mindenféle tekintetben, mint ahogy valaha is volt, próbát ajánlott fel a társaság egyik tagja. Tessék egy akármilyen meghatározható egyént kijelölni a Föld másfél milliárd lakója közül, bármelyik pontján a Földnek – ő fogadást ajánl, hogy legföljebb öt más egyénen keresztül, kik közül az egyik neki személyes ismerőse, kapcsolatot tud létesíteni az illetővel, csupa közvetlen – ismeretség – alapon, mint ahogy mondani szokták: „Kérlek, te ismered X. Y.-t, szólj neki, hogy szóljon Z. V.-nek, aki neki ismerőse...” stb.”

Karinthy Frigyes: Láncszemek

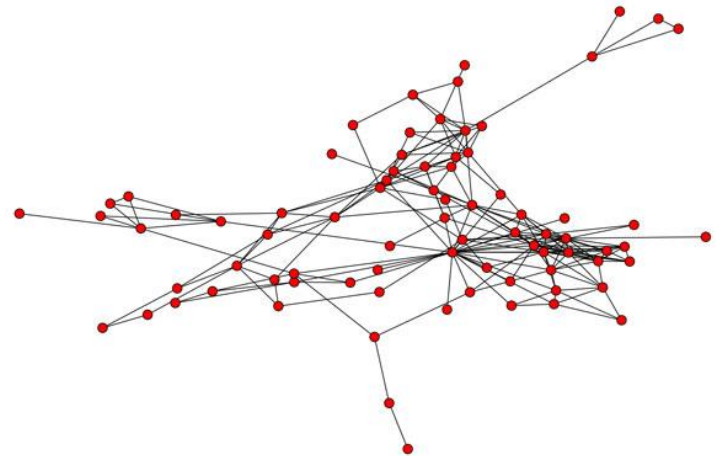
„Íme a lánc – csak két láncszem kellett hozzá a maximális öt pontból, ami természetes is, hiszen a világ nagy hírű és népszerű embereihez könnyebb kapcsolatot találni, mint a jelentéktelenséghez, lévén előbbieknek rengeteg ismerőse. „

„(...) real networks are far from being random, but display generic organizing principles shared by rather different systems.” (REVIEWS OF MODERN PHYSICS, VOLUME 74, JANUARY 2002)

Milyen messze vagyunk egymástól?



<https://en.wikipedia.org/wiki/Sphere>



<https://ituniversity.wordpress.com/tag/graph-theory/>

Miért közérthetően?

- Internetezők száma a világban:
 - 4.536.248.808 (2019. június 30-án, becsült érték)
- Földrajzi eloszlás
 - Ázsia 50,7%
 - Európa 16%
 - Afrika 11,5%
 - Latin-Amerika 10%
 - Észak-Amerika 7,2%
 - Közel-Kelet 3,9%
 - Óceánia 0,6%
 - kerekítési hiba: 0,1%

<https://www.internetworldstats.com/stats.html>

Mit tehetünk/tehetnek?

„What could be done, of course, is no index to what should be done; to make a new ice age in order to annoy others, or a new tropical, "interglacial" age in order to please everybody, is not necessarily a rational program.,,

John von Neumann: Can We Survive Technology?

Fortune, Vol. 91, No. 6, p. 106 (1955).

Mikor vagyunk biztonságban?

„A biztonság tehát egy állapot, amelynek megváltozása nem valószínű.” (...) „A megfelelő színvonalú biztonság csak úgy érhető el, ha a védelmi intézkedések kiterjednek az egész rendszerre.” (Vasvári György, 1995)



http://www.tiphaz.hu/partner/vasware/szko_2a.pdf

„Security is a process, not a product.” (Bruce Schneier, 2000) https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Lehetséges folyamatelemek

6	A védelem kialakítása	58
6.1	Felhasználók felelőssége az incidensek, biztonsági események során	61
6.2	A bizalmasság	62
6.2.1	Bizalmasság az operációs rendszerben	64
6.2.2	Merevlemezék és USB-lemezek titkosítása	65
6.2.3	Titkosítás irodai programcsomagokban	66
6.2.4	Bizalmasság tömörített állományoknál	68
6.3	Hálózat és bizalmasság	68
6.3.1	Hozzáférés-védelem, jelszavak, hitelesítés	70
6.3.2	WiFi eszköz biztonsági beállításai	77
6.3.3	Bluetooth, IrDA	81
6.3.4	E-mail	81
6.3.5	Azonnali üzenetküldés	86
6.3.6	Tűzfalak	86
6.4	Adatvédelmi megfontolások, GDPR	87
6.4.1	GDPR	88
6.4.2	Védelem böngészés közben	91
6.4.3	A látogatott oldalak biztonsága	93
6.4.4	Aktív tartalmak és a biztonság	96
6.4.5	A böngészőben tárolt adatok biztonsága	98
6.4.6	Bizalmassági eszközök közösségi oldalakon	102
6.4.7	Az adatvédelem hiányosságainak lehetséges következményei	110
6.4.8	Az adatok végleges törlése	110
6.5	A sértetlenségről	112
6.5.1	Digitális aláírás	112
6.5.2	Kivonatok (hash-ek)	114
6.6	A rendelkezésre állás megteremtése	115
6.6.1	Fájlok biztonsági mentése	119
6.6.2	Védelem az áramellátás hibái ellen	122
6.7	Komplex megközelítést igénylő fenyegetettségek és védelmi megoldások	124
6.7.1	Végpontvédelem és vírusvédelem	124
6.7.2	Biztonságos Internetbankolás	127
6.7.3	Biztonságos bankkártya használat – internetes fizetés	130
6.7.4	Elektronikus pénz és elektronikus pénztárcák	135
6.7.5	Csaló webáruházak	137
6.7.6	Hamis hírek (fake news) felismerése	141
6.7.7	Deepfake, avagy ne higgy a szemednek!	142
6.7.8	Internetes zaklatás	145
6.7.9	Utazásbiztonság – biztonság útközben	148



Megtettük ami elvárható?

Üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos - egészben, vagy elemeinek összességként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennél fogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, **amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.**

2018. évi LIV. törvény az üzleti titok védelméről, 1. § (1)

Kvantumszámítógépek

- Quantum supermacy:
 - the potential ability of quantum computing devices to solve problems that classical computers practically cannot
- Quantum advantage:
 - the potential to solve problems faster

Kvantumszámítógépek



US007246240B2

(12) **United States Patent**
Chuang et al.

(10) **Patent No.:** **US 7,246,240 B2**
(45) **Date of Patent:** **Jul. 17, 2007**

(54) **QUANTUM DIGITAL SIGNATURES**

(75) Inventors: **Isaac Chuang**, Cambridge, MA (US);
Daniel Gottesman, Berkeley, CA (US)

(73) Assignee: **Massachusetts Institute of Technology**, Cambridge, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 659 days.

6,778,669 B1 * 8/2004 Lehureau 380/256
2002/0106084 A1 * 8/2002 Azuma et al. 380/263

FOREIGN PATENT DOCUMENTS

JP 175762/2000 * 6/2000

OTHER PUBLICATIONS

25 years of Quantum Cryptography: Brussard and Crepeau, Jul. 31, 1996.*
Quantum Cryptography, Bennett, Brussard, Giles, and Ekert, Scientific American, Oct. 1992.*

Kvantumszámítógépek



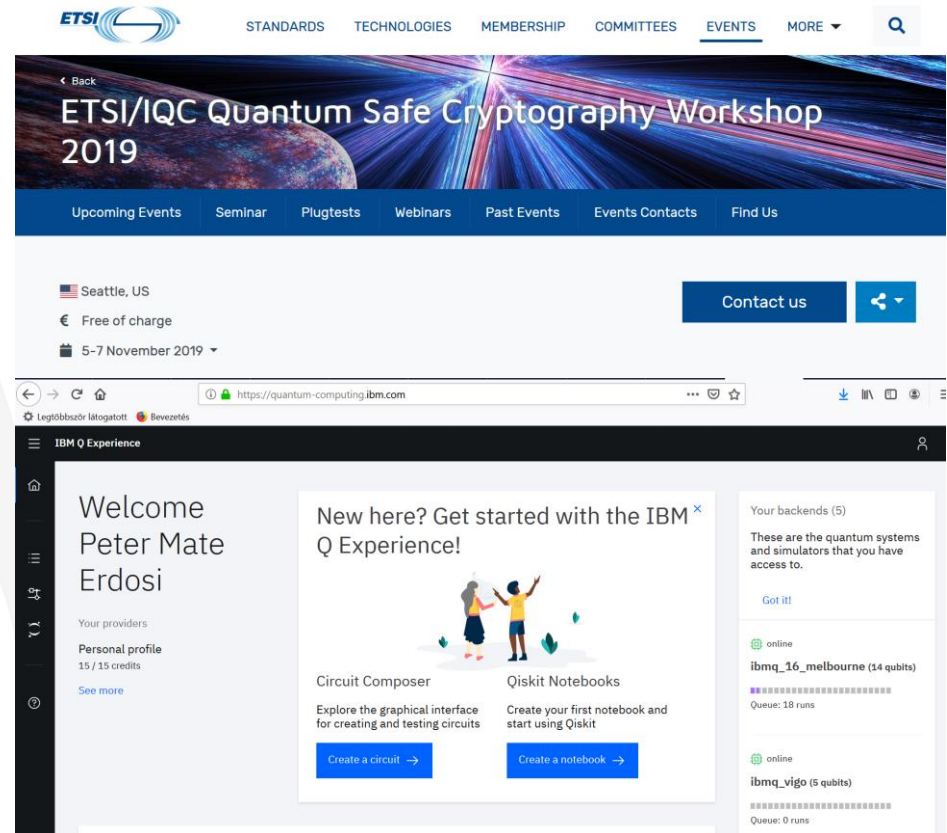
ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

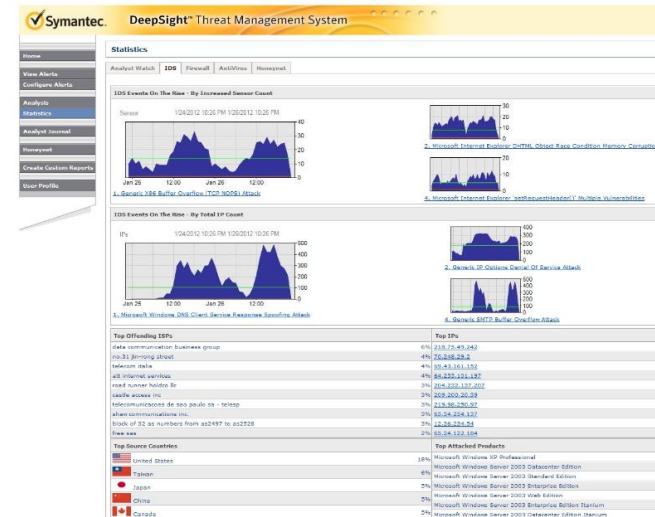
June 2015

ISBN No. 979-10-92620-03-0



<https://quantum-computing.ibm.com/>

Világbéke?



Confidence in a connected world. Symantec.

https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-deep-sight-early-warning-service_DS-21227151.en-us.pdf

Társadalmak evolúciója

- Friedrich Engels
- Yonei Masuda
- Francis Fukuyama
- James P. Huntington

Aktivitás

„Nem az a sorsunk, hogy üres esőkabátok, egy fizetési listán szereplő névtelen számok, szerepek betöltői a közgazdaságtan és a szociológia nyersanyagai vagy egy kormányjelentés statisztikái legyünk.”

Charles Handy: Üres esőkabát, 2008

Teremtsünk biztonságot!



Never give in!

(Sir Winston Leonard
Spencer Churchill,
1941 október 29.)

Köszönöm a figyelmet!



Erdősi Péter Máté, CISA
epm@idoertek.eu