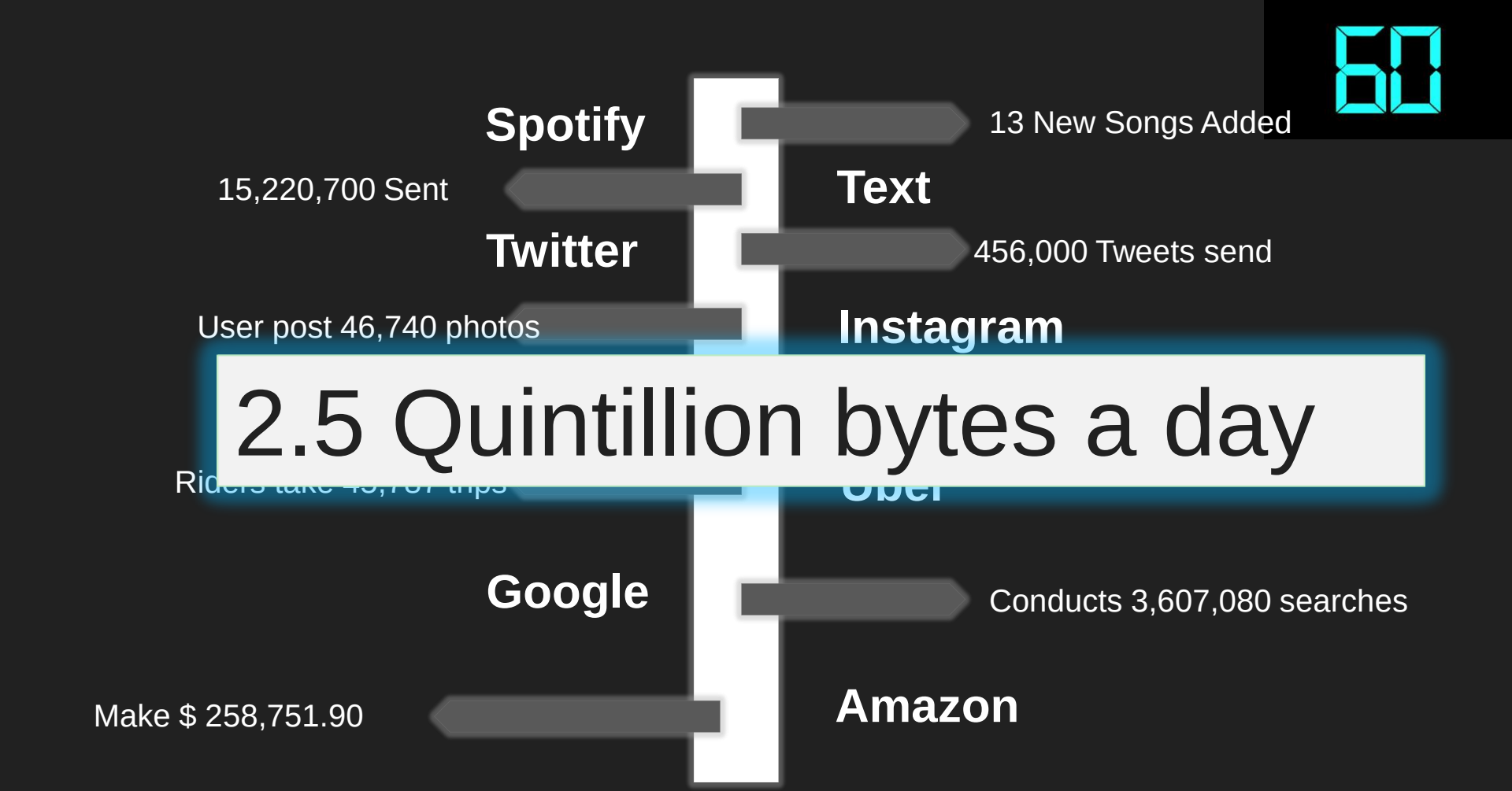
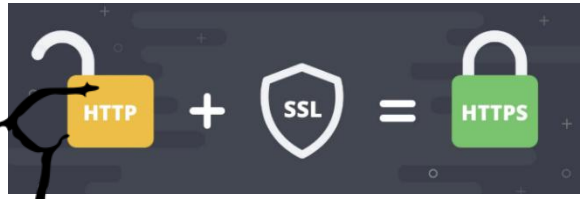
Enterprise Encryption and Authentication

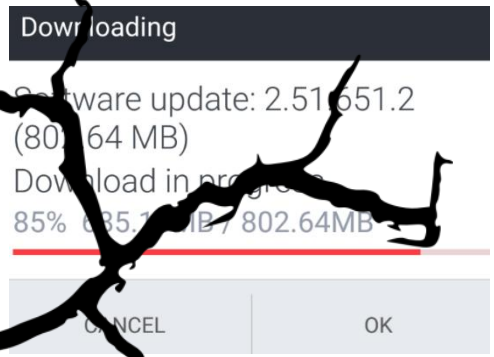
Marko Bobinac, PreSales Manager, Enterprise and Cybersecurity
26.10. 2018



https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1

Encryption=digital cement





SENETAS

TOP COMPLIANCE PRIORITIES OF 2019

*PSD2 is covered by Gemalto Banking solutions

gemalto


NO HELMET
NO PETROL
By Order
SILIGURI METROPOLITAN TRAFFI
gettyimages
DIPTENDU DUTTA
HERO
HONDA

Compliant!!!

CYBERSECURITY

HAVE A PLAN

gemalto

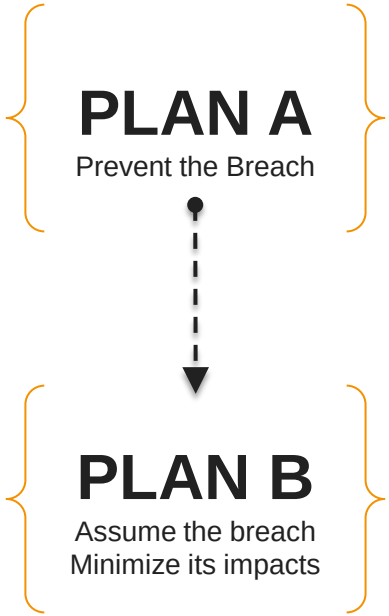
Classical Physics

- Up to 1920
- Light is electromagnetic wave
- Newton’s laws of motion
- Deterministic

Quantum Physics

- From 1920’s onwards
- Properties of smallest things in universe
- Light is a wave & particle
- Certain quantities can never be precisely measured
- Probabilistic

Cybersecurity: have a plan



ACCEPT THE BREACH

- **Perimeter security** alone **is no longer enough**.

PROTECT WHAT MATTERS, WHERE IT MATTERS

- **Data** is the **new perimeter.**

SECURE THE BREACH

- **Control who and what** can access information.
- **Apply data protection and controls** that sit with the data asset.

Do You Have a Plan B?


SECURE THE
BREACH
SECURETHEBREACH.COM
gemalto

#1: Why is Encryption Secure?

Example: AES128 = 3,4 x 10^{38} Keys

Assuming
a Super Computer can calculate ~ 1 Billion Keys / second,
we have 100 Super Computers,
we find the key in the 1%.

Finding the Key takes 10^{22} years. Universe is 10^{11} years old.

gemalto

Is “just” Encrypting data good enough?

- Ransomware
- Database encryption with weak access controls
- Full Disk encryption with user-name & Password

Path of Least Resistance: Break the Lock or Steal the Key?

gemalto

#2: Why do we need external Key Management?

No one tries to crack encryption by calculating the keys...

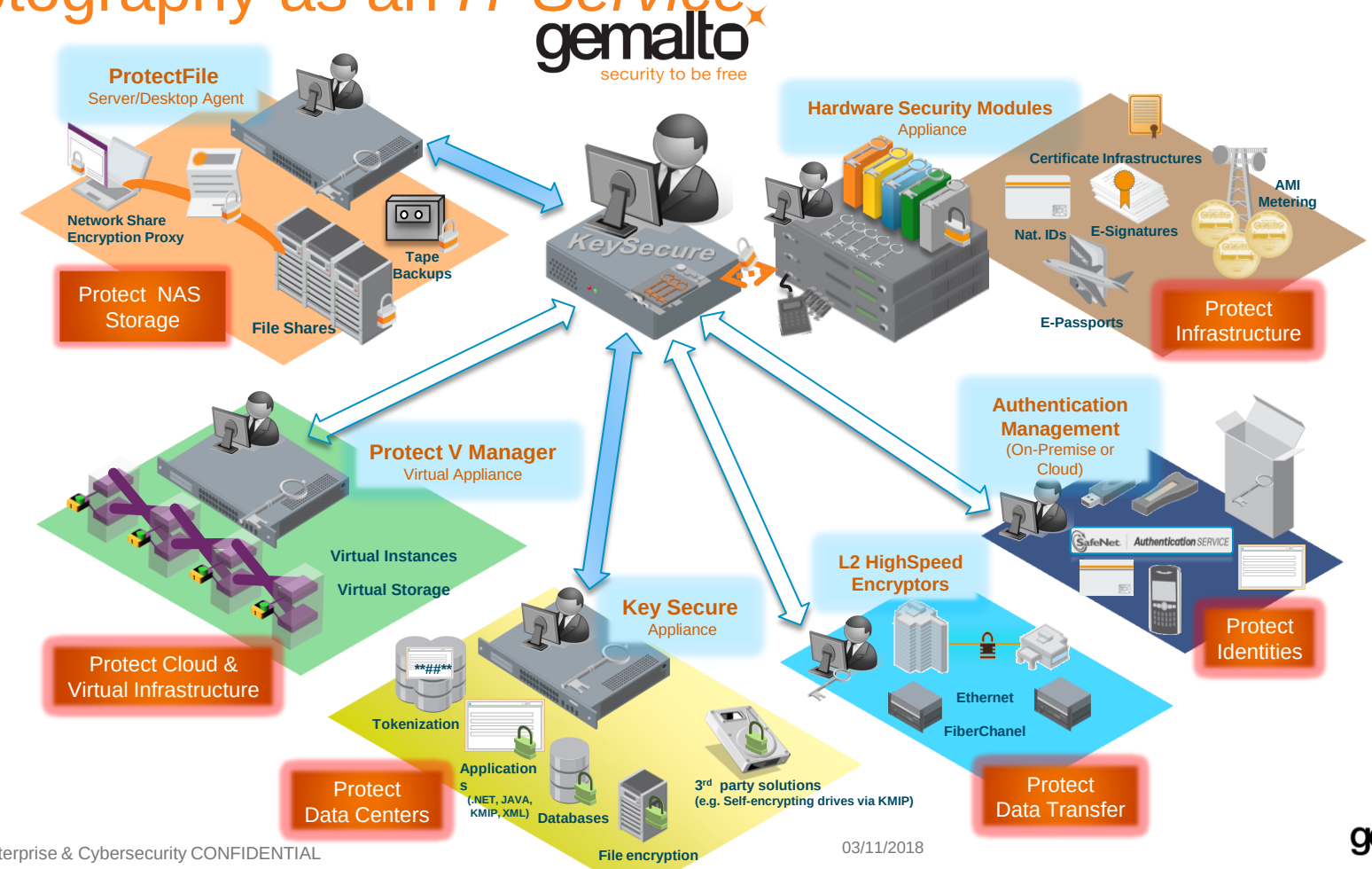
It‘s easier to use the key and decrypt the data

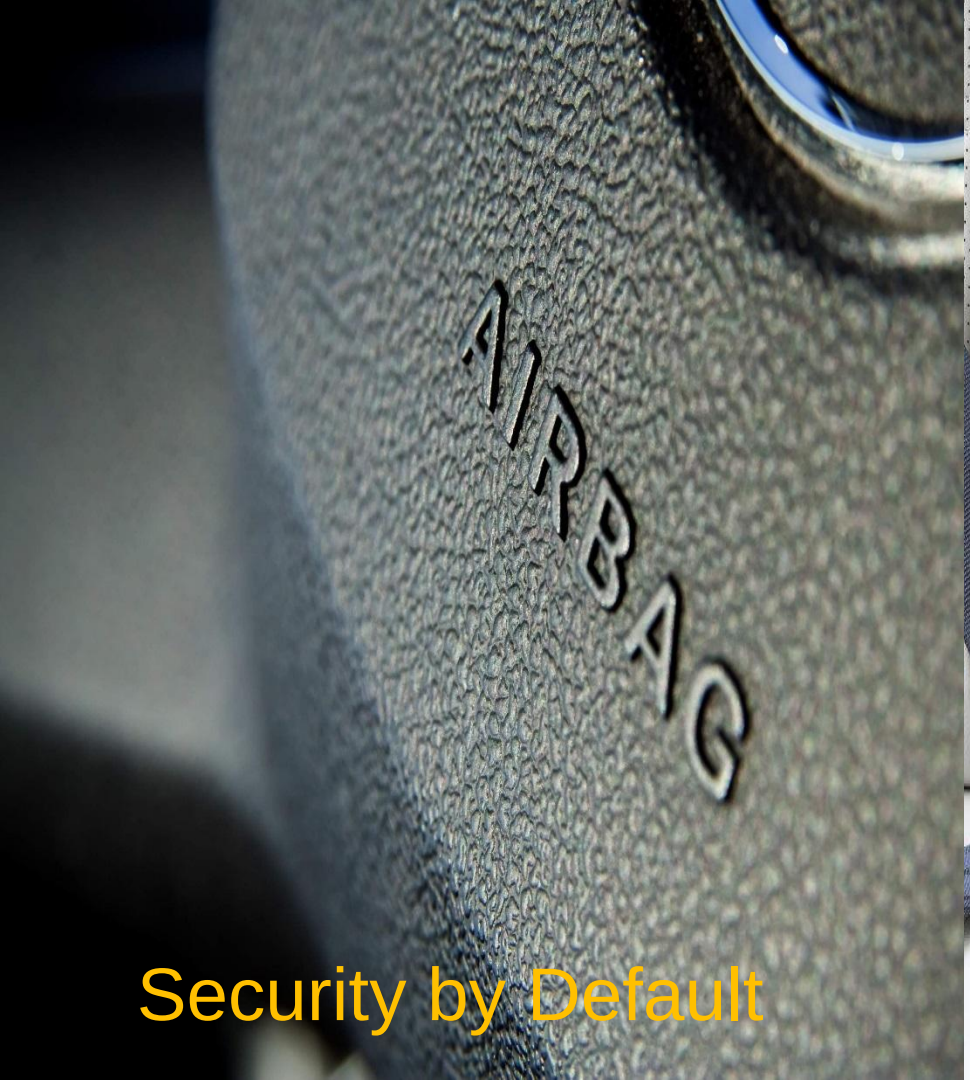
Separate Keys from Data and Store/Manage Keys securely

Attacks On Cryptography – Encrypt it the right way

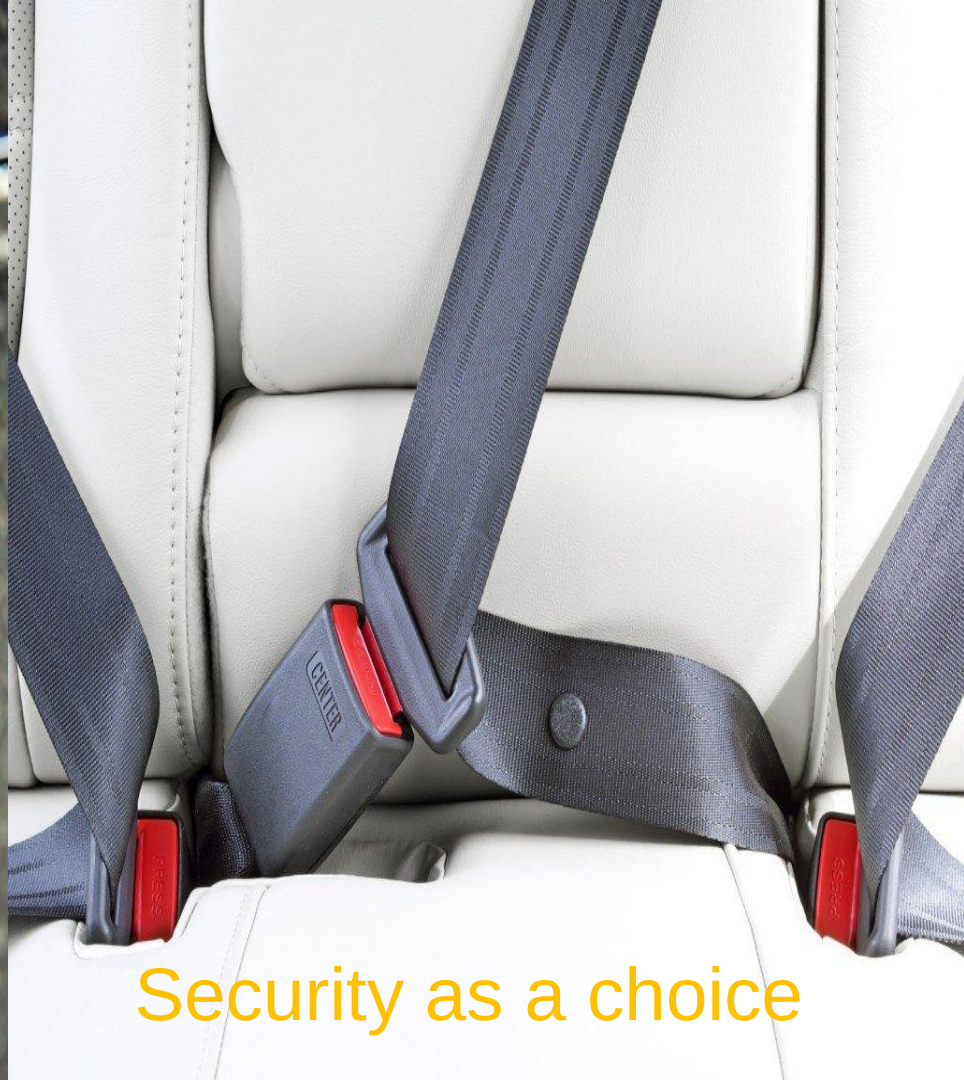
- Ciphertext-Only attack
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Differential cryptanalysis – Side Channel attack
- Linear cryptanalysis
- Implementation attacks
- Replay attack
- Algebraic
- Rainbow Table
- Frequency Analysis
- Birthday Attack
- Social engineering for key discovery
- Dictionary Attack
- Brute Force
- Reverse Engineering
- Attacking the random number generators
- Temporary Files

Cryptography as an *IT Service*





Security by Default



Security as a choice

Safe Today ≠ Safe Tomorrow

Quantum computers are not Science Fiction

Intelligent Machines

IBM Raises the Bar with a 50-Qubit Quantum Computer

Researchers have built the most sophisticated quantum computer yet, signaling progress toward a powerful new way of processing information.

by Will Knight November 10, 2017

gemalto

Quantum Computing – last few months

- Microsoft: Reveals new QC programming language in Visual Studio
- Google: Plan to scale to 49 qubits & achieve ‘Quantum Supremacy’ in the next few months
- Volkswagen: Partners with Google for Quantum automotive applications
- Intel: Delivered a 17 bit Quantum chip
- IBM: Announces a 50 qubit prototype
- China: Announces $10 Billion Quantum Computing Centre
- UNSW: Announces ‘flip-flop’ qubits promising large scale industrial manufacture

Comparison of c … security levels

1

Table 1 - Impact c … phic Algorithms

Cryptographic Algorith	… mpact from large-scale quantum computer
AES	… arger key sizes needed
SHA-2, SHA-3	… arger output needed

2

RSA	… o longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	… o longer secure
DSA (Finite Field Cryptograpl	… o longer secure

gemalto

“Hope is not a strategy”

Choose the right partner for Today and Tomorrow.

gemalto