

General Data Protection Regulation and cryptographic solutions

Bavo Van den Heuvel

CIPP/E – CIPM – CIPT

ISO27001 Lead Auditor – Forensic Computer Auditor

Data Protection Officer

Barcelona, July 7 2015

bavo@cranium.be

copyrighted material!!



Commercial Engineer - University of Antwerp 1996

Ca 20 years IT-security, +10 years Data Protection Officer

Owner of CRANIUM BVBA: mainly working as Data Protection Officer (DPO) for large government agencies:

<http://www.cranium.be>

Also co-founder and trainer at Data Protection Institute BVBA where future DPO's from public and private sector are trained to be ready for the new General Data Protection Regulation (GDPR): <https://www.dp-institute.eu>

About me

2

CRANIUM: applied privacy and beyond...

copyrighted material!!



1. Crypto basics
2. Re-identification Risk
3. Encryption prevents Data Breach?
4. Lost Laptop contains no data?
5. Data Protection benefits of HTTPS
6. My strong password and the keylogger
7. The un-encrypted cloud

TOC

CRANIUM: applied privacy and beyond...

3

- Symmetric keys
- Asymmetric keys
- Hash
- Digital signature
- File encryption



Educational pictures in this chapter: with kind permission of Sophos unless otherwise stated

1. Crypto Basics

CRANIUM: applied privacy and beyond...

4

copyrighted material!!



CRANIUM
APPLIED PRIVACY

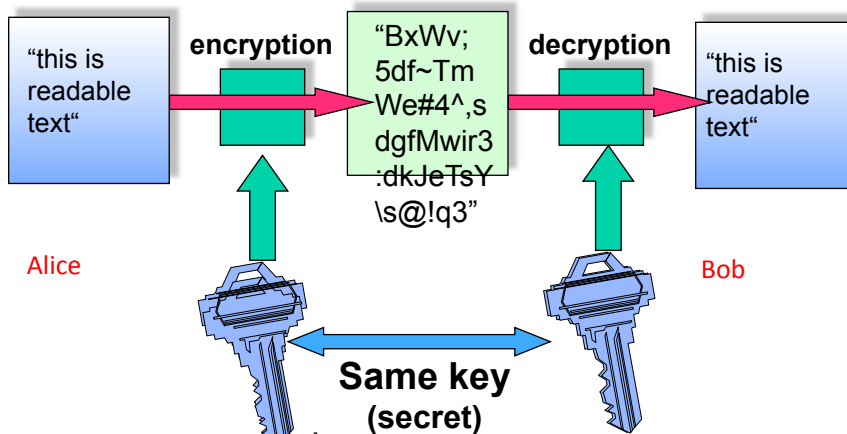
Symmetric keys

5

CRANIUM: applied privacy and beyond...

copyrighted material!!

Same key for encryption and decryption



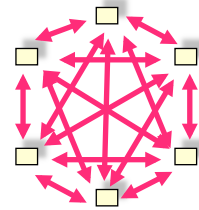
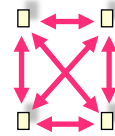
CRANIUM
APPLIED PRIVACY

Symmetric keys

6

CRANIUM: applied privacy and beyond...

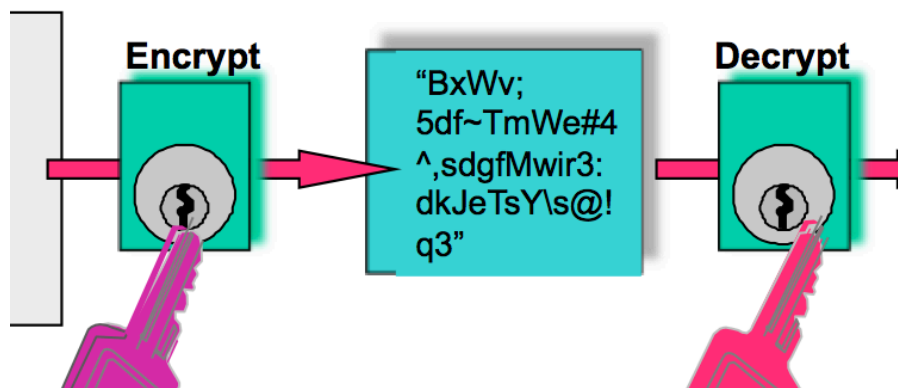
- Simple key-generation
- Known algorithms: DES, triple-DES, AES
- Very fast processing:
 - 4000 times faster then asymmetric key
 - Slightly slower then hashing
- Biggest challenge: key-distribution:
 - Alice and Bob: one key
 - Alice, Bob, Charlie: three keys
 - For n partners: $n * (n-1)/2$



Typical of symmetric key

7

CRANIUM: applied privacy and beyond...



Asymmetric keypair

8

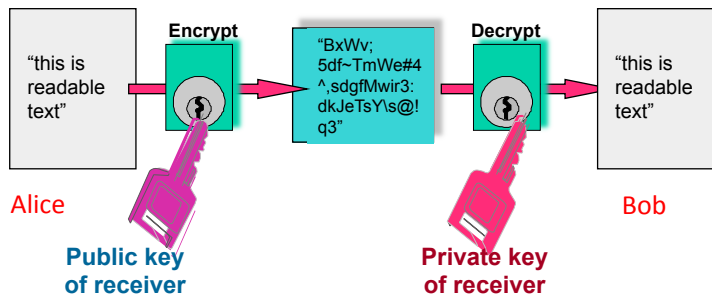
CRANIUM: applied privacy and beyond...

- Each user receives his own keypair (generated):
 - One private key: to be kept private
 - One public key: to be shared in public
- These keys belong to each other:
 - If you encrypt with your private key, a receiver can only decrypt with your corresponding public key
 - If you encrypt with the public key of a receiver, the receiver can only decrypt with his corresponding private key
- Example of known algorithm: RSA
- Encryption with an asymmetric key is 4000 times slower than encryption with a comparable symmetric key

Typical of asymmetric keypair

9

CRANIUM: applied privacy and beyond...



Advantage: only receiver can decrypt

Disadvantage: there is no information about the sender, performance

Asymmetric keys: usage 1/2

10

CRANIUM: applied privacy and beyond...

copyrighted material!!

Alice

Bob

Encrypt

Decrypt

Private key of sender

Public key of sender

Advantage: receiver knows sender

Disadvantage: everybody can decipher the ciphertext, performance

CRANIUM
APPLIED PRIVACY

Asymmetric keys: usage 2/2

11

CRANIUM: applied privacy and beyond...

copyrighted material!!

md5crack

md4, md5, sha1 calculator

Calculate Md4/5 and sha-1 Hash

Enter the password/text you want to be encrypted, then select the algorithm option you want below.

Input: Ashish

Calculate: MD4 MD5 SHA-1

Result: 633a612ae9cb31748e12a8369dcf2801

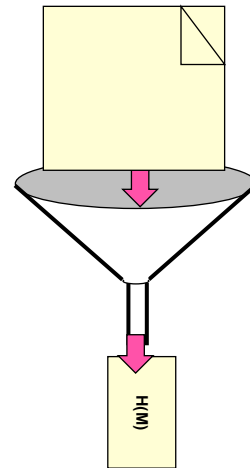
CRANIUM
APPLIED PRIVACY

Hash (function)

12

CRANIUM: applied privacy and beyond...



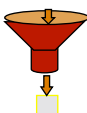
- One-way function
- Generates fixed length output, independent of size of input:
 - 5 MB docx => MD5: 128 bit string
 - 500 MB X-ray image => MD5: 128 bit string
- Given the hash one can not "recalculate" the input string on which it was calculated
- Input changes one bit => output (hash) changes too
- Based on its hash, a file can be uniquely identified: it is a unique fingerprint for that file
- Known hash functions: MD5 gives 128 bit length, SHA-1: 160 bit, ...
- The calculation of a hash is very fast, even faster than the encryption with a symmetric key



Hashfunction

13

CRANIUM: applied privacy and beyond...

Typ	Algorithms	MByte/sec @ P90MHz
 Symmetric algorithms	DES	0,4 (1,9 in HW)
	Triple-DES	0,16 (0,7 in HW)
	IDEA	1,0
	RC5 (64 Bits)	2,7
	AES	4,3
 PublicKey	RSA (512 Bits)	0,001
 Hash	MD5	14,2
	SHA-1	6,1
	RIPEMD-160	5,0

Speed (Pentium 90 MHz!)

14

CRANIUM: applied privacy and beyond...

copyrighted material!!

- Encrypting with your **private key** the **hash** of the document you want to send, and sending this together with the document, can give the receiver the **guarantee** about your **identity** and the **integrity** of the document

Alice

Source: http://alicecrawley.com/wp-content/uploads/2014/12/Alice-signature-sml_transparent_bgnd.png

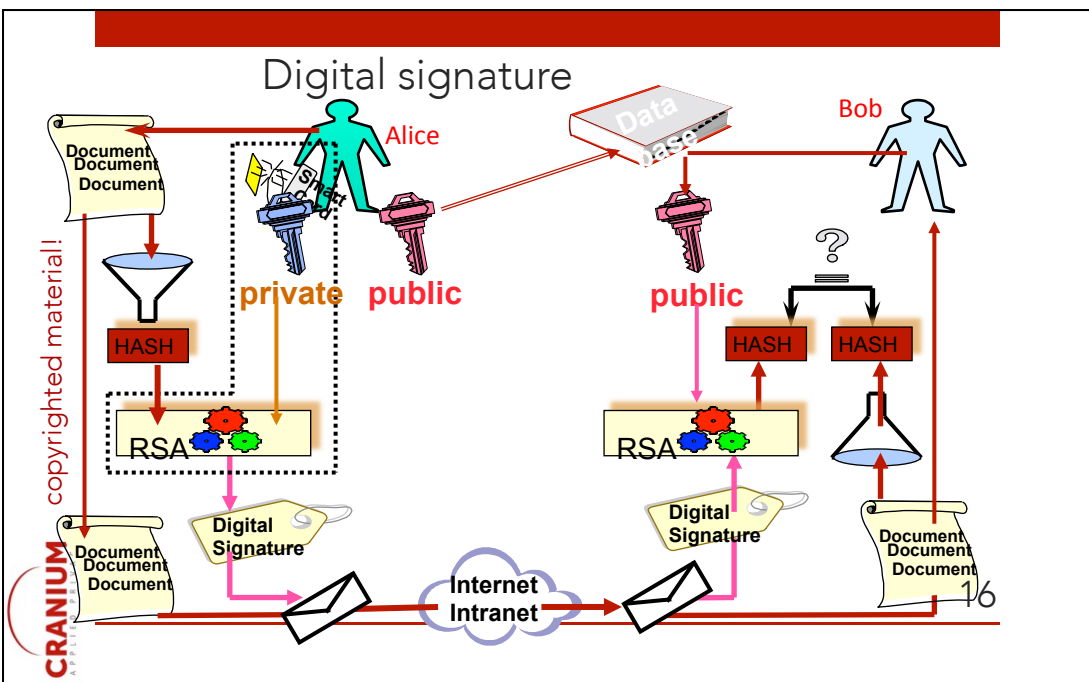


Digital Signature: idea

15

CRANIUM: applied privacy and beyond...

copyrighted material!!



- Guarantees you:
 - The sender can be identified (important for the receiver)
 - Outsiders can not adapt the message without you knowing (important for sender and receiver)
 - The sender can not deny he send the message (important for receiver) = non-repudiation
 - NB: some extra measures are necessary: a right time-base and a trusted delivery channel
- Does not give you:
 - Confidentiality! The message stays readable for everybody, the digital signature is a seperate file that is linked to the message

Digital signature: typical

17

 CRANIUM: applied privacy and beyond...

You sign with a certain identity that you want to add to the message: you as a person, or your company, or a certain application server

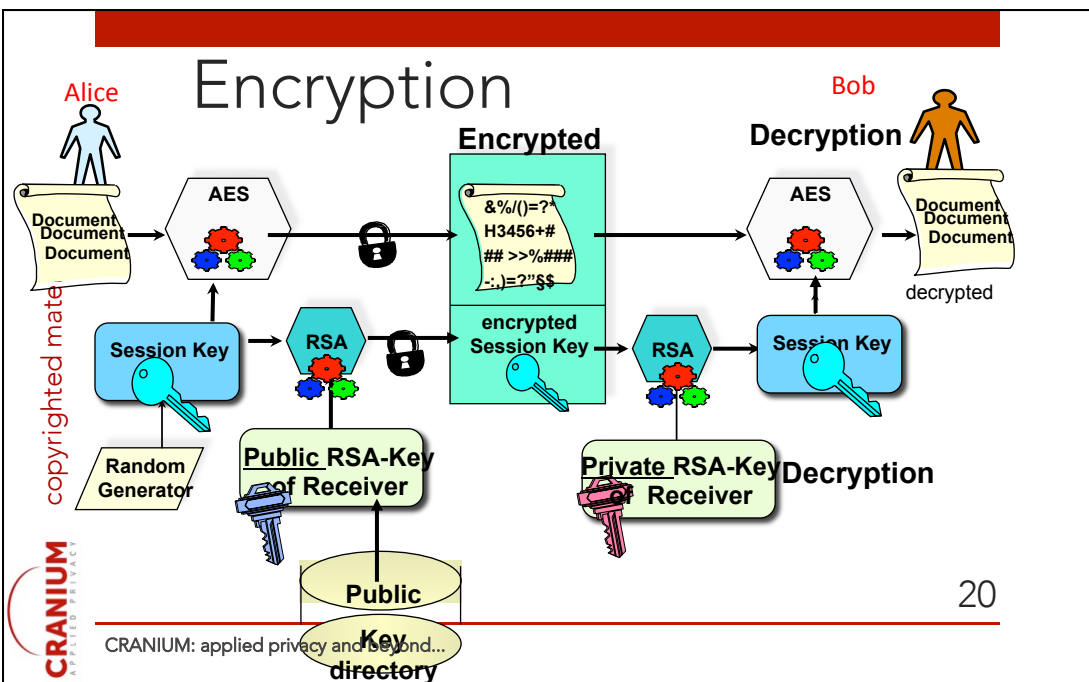
- Contracts
- Software: e.g. Windows updates
- Time stamp: e.g. for a timely tax declaration
- File integrity
- Web site identity (e.g. TLS)
- Web service security: signing a SOAP message (or parts of it)
- ...

Digital Signature

18

 CRANIUM: applied privacy and beyond...

- Encrypting a document with a random **symmetric key** and sending this encrypted document together with the symmetric key encrypted by the chosen receiver's **public key**, can give you guarantee that **only** your chosen receiver can decipher and read this message



- Gives you:
 - Certain guarantee that only selected receivers can decipher your message, hence giving confidentiality
- But:
 - Receiver does not know who was sender (emailaddress or ip-address do not give enough certainty)
 - No integrity guaranteed: in case the message was tampered with, the right receiver will not be able to decipher the message or gets meaningless results



Encryption: typical

21

CRANIUM: applied privacy and beyond...

You encrypt for certain receivers: e.g. based on X.509v3 certificates, or because you hand over to them the passphrase by a "second secure channel"

- File encryption e.g. Win-zip or 7-zip
- Encryption on file system
- Encryption of (part of) database (e.g. Health data)
- Encryption of communication: Threema, Signal, Zenmate, Jitsi, some VPNs, SSL/TLS
- BYOD: encryption of (all) data on the device
- Web service security: encrypting a SOAP message (or parts of it)
- ...



Encryption

22

CRANIUM: applied privacy and beyond...

- Are they anonymous?
- Metadata:
 - Sex
 - Clothes
 - Color
 - Pose
 - Environment
 - Exif data
 - GPS data
 - ...



2. Re-identification Risk 23

CRANIUM: applied privacy and beyond...

95/46 EC: art 17

- Security of processing: implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

GDPR: (still draft): new: pseudonymous data, art 10:
Processing not allowing identification

• Risk:

- Re-identification through rainbow tables
- Re-identification through big data analytics: metadata
- Re-identification through social engineering

CRANIUM: applied privacy and beyond...

24



Source: http://en.wikipedia.org/wiki/Transportation_in_New_York_City#/media/File:Yellow_Cabs_in_New_York.JPG

Example of re-identification:

- Taxi: new york, hash, open data => detailed whereabouts
- <https://medium.com/@vijayp/of-taxis-and-rainbows-f6bc289679a1>

Solutions:

- Salt and hash
- Small Cell Risk Analysis
- Anonymization: k-anonymity

More:

- ICO
<https://ico.org.uk/media/1061/anonymisation-code.pdf>
- WP29:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- CNIL: 1.10 in
<http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf>

25

CRANIUM: applied privacy and beyond...

What if:

- Off the shelf usb-stick is lost
- AES 128 bit software encrypted

But:

- Password: 1234
- Amount of trials before deletion: ∞

3. Encryption prevents Data Breach? 26

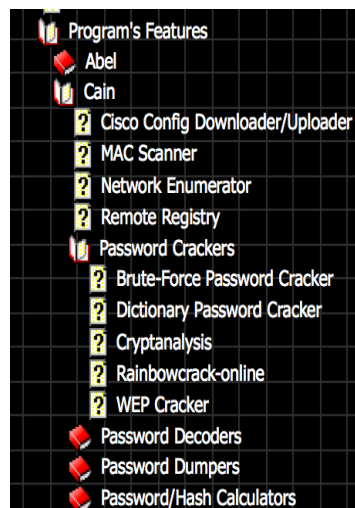
CRANIUM: applied privacy and beyond...

- 95/46: art 17 implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access
- GDPR: draft: Art 31,32 data breach notification
- Risk: lost USB stick but encrypted
 - Weak algorithm:
 - RC4, DES
 - No password policy
 - No audit trail of content
 - Brute force attack possible

27

CRANIUM: applied privacy and beyond...

Example of crack software



Solutions:

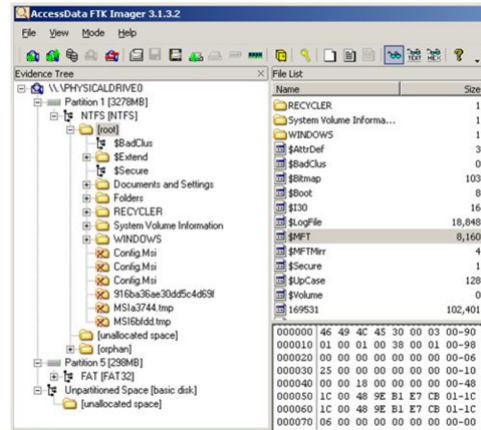
- "Good": BYOD usb stick, policy that asks to encrypt with winzip (even when you ask strong password you can not check user or know the content on the lost stick), but then again an attacker can keep on guessing
- Better: iLocker: pinpad on stick, AES encrypted, 7-15 long: auto delete after 10 guesses
- Best: centrally managed solution: only company accepted sticks, policy enforced password, logs of what data on what stick



28

CRANIUM: applied privacy and beyond...

- People only "work on files server"
- Computer trash was emptied
- Most data is still recoverable from "free space"



4. Lost Laptop contains no data? 29

CRANIUM: applied privacy and beyond...

June 15 and 16 2015 Justice and Home Affairs Council:

- 95/46 art 17: (...) Having regard to the state of the art and the cost of their implementation, such measures shall ensure level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- GDPR: art 23 *Data protection by design and by default*, art 30 *Security of processing*, art 32 *Respect to Ris*, art 33 *data protection impact assessment*
- **Right to erasure and "to be forgotten"**: data controllers must erase personal data without undue delay where:
 - the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - the data subject withdraws consent for the processing of personal data;
 - the data subject objects to the processing of personal data;
 - the data were unlawfully processed;
 - a law requires the controller to erase the data.

In relation to information society services, individuals may also obtain the erasure of their data without undue delay, within the limits of:

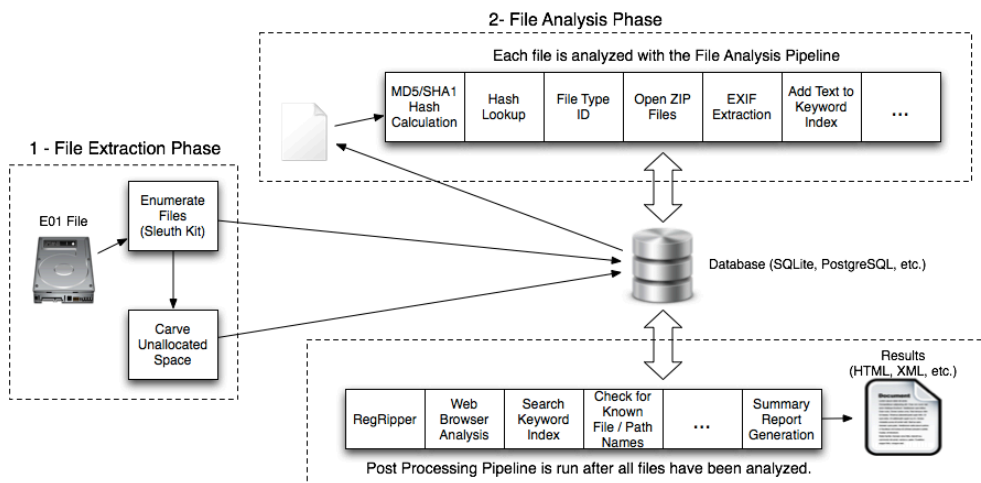
- freedom of expression and information,
- legal obligations applicable to the controller,
- public interest,
- scientific, statistical and historical archiving and
- the establishment, exercise or defence of legal claims. 30

CRANIUM: applied privacy and beyond...

- Risk:
 - Lost laptop: empty space contains lots of data
 - Partial encryption asks for discipline
 - Working from file server: temporary files on harddisk
 - End of life: storage media in: computer, multifunctionals, CCTV-recorders, smartphones, tablets, PABX,...

31

CRANIUM: applied privacy and beyond...



- Example of recovery software Source: http://www.sleuthkit.org/sleuthkit/docs/framework-docs/basics_page.html

32

CRANIUM: applied privacy and beyond...

Example: simple tool, no admin rights necessary:

<http://portableapps.com/apps/utilities/wise-data-recovery-portable>

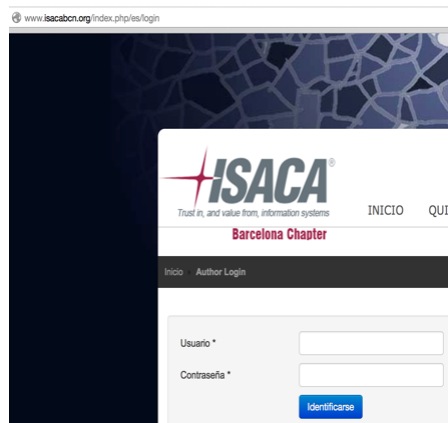
Solutions:

- Sector level encryption (is also good solution for end of life): file vault on OS X, correct bitlocker on Windows, other tools: Diskcryptor

=> always have a fall back in case of lost key: challenge/response or (virtual) vault

33

CRANIUM: applied privacy and beyond...



5. Data Protection benefits of HTTPS 34

CRANIUM: applied privacy and beyond...

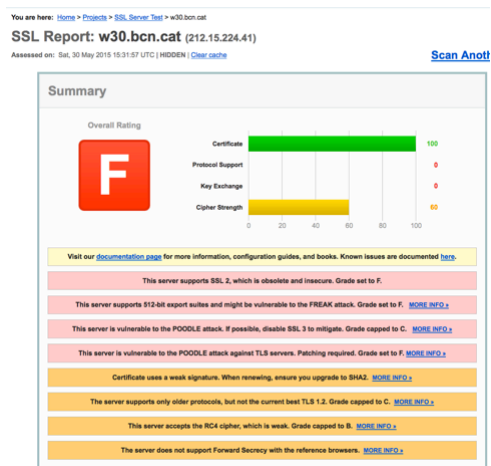
- 95/46: art 17 (...) implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

• Risk:

- Credentials can be sniffed
- User does not know he is on right site
- All communication is readable between browser and endpoint
- Weak cipher suite can be exploited
- Low score on sslabs.com can attract hackers

35

CRANIUM: applied privacy and beyond...



36

CRANIUM: applied privacy and beyond...

copyrighted material!!

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [dp-institute.eu](#)

SSL Report: dp-institute.eu (176.62.167.166)

Assessed on: Sat, 30 May 2015 15:36:27 UTC | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating

A

Category	Score
Certificate	100
Protocol Support	95
Key Exchange	90
Cipher Strength	90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

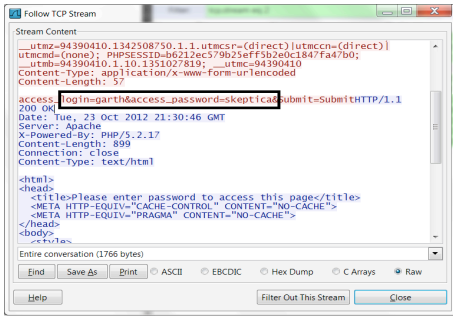
This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

CRANIUM: applied privacy and beyond...

37

copyrighted material!!

Example: sniffing credentials



http://skepticaesoterica.com/wp-content/uploads/2012/10/unsecure-wireshark-sniffing.png

Solutions:

- Update ciphersuite: <https://www.ssllabs.com/downloads/SSL-TLS-Deployment-Best-Practices.pdf>
- Add https to any website, preferably extended validity cert: <https://18f.gsa.gov/2014/11/13/why-we-use-https-in-every-gov-website-we-make/>
- User: do not trust untrusted certificates (fake websites, intercepting appliances)

CRANIUM: applied privacy and beyond...

38

copyrighted material!!



<http://core0.staticworld.net/images/article/2014/11/yubikey-nano-in-earring-100533119-large.jpg>



6. My strong password and the keylogger 39

CRANIUM: applied privacy and beyond...

copyrighted material!!

	L	a-z	L	a-z en 0-9 en A-Z	L	ASCII set
1		26		62		255
2		676		3.844		65.025
3		17.576		238.328		16.581.375
4		456.976		14.776.336		4.228.250.625
5		11.881.376		916.132.832		1.078.203.909.375
6		308.915.776		56.800.235.584		274.941.996.890.625
7		8.031.810.176		3.521.614.606.208		70.110.209.207.109.400
8		208.827.064.576		218.340.105.584.896		17.878.103.347.812.900.000
9		5.429.503.678.976		13.537.086.546.263.600		4.198.916.253.692.290.000.000
10		141.167.095.653.376		839.299.365.868.340.000		1.162.523.670.191.530.000.000.000
11		3.670.344.486.987.780		52.036.560.683.837.100.000		296.443.535.898.841.000.000.000.000
12		95.428.956.661.682.200		1.276.768.762.387.900.000.000		75.593.101.654.204.400.000.000.000.000
13		2.481.152.873.203.740.000		200.028.539.268.670.000.000.000		19.276.240.921.822.100.000.000.000.000.000
14		64.509.974.703.297.200.000		12.401.769.434.657.500.000.000.000		4.915.441.435.064.640.000.000.000.000.000
15		1.617.298.342.205.730.000.000		768.909.704.948.767.000.000.000.000		1.253.437.565.941.480.000.000.000.000.000.000
16		43.608.742.899.428.900.000.000		47.672.401.706.823.500.000.000.000.000		319.626.579.315.078.000.000.000.000.000.000.000
17		1.133.827.315.385.150.000.000.000		2.955.688.905.823.060.000.000.000.000.000		81.504.777.725.345.000.000.000.000.000.000.000.000
18		29.479.510.200.013.900.000.000.000		183.252.712.161.030.000.000.000.000.000.000		20.783.718.319.963.000.000.000.000.000.000.000.000.000
19		766.467.265.200.362.000.000.000.000		11.361.668.153.963.000.000.000.000.000.000.000		5.299.848.171.590.560.000.000.000.000.000.000.000.000.000
20		19.528.146.895.209.406.000.000.000.000		704.423.425.546.998.000.000.000.000.000.000.000		1.351.461.283.755.590.000.000.000.000.000.000.000.000.000.000
10		ditwaslaai	8	31Bavo50	6	c92dr5
15		ditwaslaai	12	31Bavo50Woef	9	c92dr5%k
20		ooitwaslaai	16	31Bavo50WoefSliim	12	c92dr5(%k936



Possibilities

40

CRANIUM: applied privacy and beyond...

- 95/46: art 17, in Belgian Privacy Law: art 16 "§ 2. The controller or his representative in Belgium, if any, must (...) 2° ensure that the number of individuals acting under his authority, as well as access to the data and the possible operations carried out on it, are limited to what is necessary for these individuals to fulfil their obligations or to whatever is necessary for the requirements of the service;"

http://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf

- GDPR: draft art 30 Security of processing 2. The measures referred to in paragraph 1 shall at least: (a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

• Risk:

- Only something you know is one factor authentication: can be guessed or intercepted for a replay attack
- Keystroke logger: software, hardware, malware

41

CRANIUM: applied privacy and beyond...

KeyGrabber Wi-Fi Premium

The world's first hardware keylogger with built-in Wireless LAN support! This keylogger connects to the Internet through an Access Point, and sends captured keybc E-mails. With this **Wi-Fi hardware keylogge** silently monitor a computer from anywhere just by checking your mailbox! Ultra stealth for software. [\[more...\]](#)

KeyGrabber

ver. USB 4 GB - \$ | €
ver. PS/2 4 GB - \$ | €



• Solutions:

- Two/three factor auth: e.g. Google authenticator, integrates with...
 - biometrics
- eID reader: X509v3 legal signature
- <https://fidoalliance.org/about/overview/>

42

CRANIUM: applied privacy and beyond...

copyrighted material!!

PASSWORDLESS EXPERIENCE (UAF standards)

SECOND FACTOR EXPERIENCE (U2F standards)

CRANIUM
APPLIED PRIVACY

CRANIUM: applied privacy and beyond...

Passwordless UX (Universal Authentication Framework protocol)
User carries client device with UAF stack installed
User presents a local biometric or PIN
Website can choose whether to retain password

Second Factor UX (Universal 2nd Factor protocol)
User carries U2F device with built-in support in web browsers
User presents U2F device
Website can simplify password (e.g. – 4 digit pin)

43

copyrighted material!!

NSA headquarters Fort Meade

CRANIUM
APPLIED PRIVACY

7. The unencrypted cloud 44

CRANIUM: applied privacy and beyond...

95/46 art 17 (...)

- 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
- 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
 - - the processor shall act only on instructions from the controller,
 - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
- GDPR: draft: more limitations for the data processor

• Risk:

- Leakage
- Data no longer under our sole control
- NSA / FISA / other governments

45

CRANIUM: applied privacy and beyond...

From Snowden docs: Microsoft's Skydrive (now Onedrive) interception through PRISM

(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection
 By NAME REDACTED on 2013-03-08 1500

(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)

• Solution:

- Boxcryptor or others
- Wuala, Teamdrive, Spideroak

- More: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

46

CRANIUM: applied privacy and beyond...



copyrighted material!

- thank
- you



CRANIUM
APPLIED PRIVACY

47

CRANIUM: applied privacy and beyond...