

# ***Justifying Security Measures***

Cormac Herley

Microsoft Research

Based on: [Unfalsifiability of security claims](#), Proc. Nat. Acad. Sciences, 2016  
[Justifying Security Measures](#), Esorics 2017

# To be secure.....

You must do everything

but

You can't do everything

Choose a strong password.  
Choose upper and lower-case.  
Choose digits and special characters.  
Choose length.  
Choose a different password for every account.  
Choose to change them every 90 days.  
Choose two-factor authentication.  
Chose an anti-virus from a reputable vendor.



**Now why would I want to do any of that?**

(h/t @Thorsheim)

UK's cyber-security chief x

www.independent.co.uk/news/uk/politics/uk-cyber-security-chief-gchq-internet-passwords-guidelines-ciaran-martin-national-...

**INDEPENDENT** News InFact Politics Voices **Indy/Life**

News > UK > UK Politics

# UK's cyber-security chief ridicules public guidelines for internet passwords as impossible even for spies to follow

Every British citizen is effectively...  
Martin warns

Joe Watts Political Editor | @JoeWatts\_ | Tue

32 shares

https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

File Edit View Favorites Tools Help

DOW JONES, A NEWS CORP COMPANY

DJIA ▲ 21832.39 0.36% S&P 500 ▲ 2466.09 0.34% Nasdaq ▲ 6393.85 0.29% U.S. 10 Yr ▼ -11/32 Yield 2.099% Crude Oil ▲ 49.14 0.99% Euro ▲ 1.1923 0.07%

# THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate

Subscribe Now | Sign In  
**\$1 for 2 Months**

Search

A-HED

## The Man Who Wrote Those Password Rules Has a New Tip: N3v\$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By *Robert McMillan*  
Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of “NIST Special Publication 800-63, Appendix A.” The 8-page primer advised people to protect their accounts by inventing awkward new

**Why did it take us 40 years to figure out  
we were wrong?**

## Focus on reasoning not conclusion:

- *“Choose a strong password”*
- *“Choose an anti-virus”*
- *“Choose different passwords each account”*

What does a solid justification look like?

***“The only secure system is unplugged, encased in concrete and buried underground.”***

***=> Necessary conditions for security unfalsifiable***

# Claims of necessary conditions for security are unfalsifiable

Can't show that something is not necessary for security.

Why? Falsifying claim that  $X$  is necessary for security requires finding something secure that doesn't do  $X$ .

Want to avoid bad outcomes. Define  $Y$ :

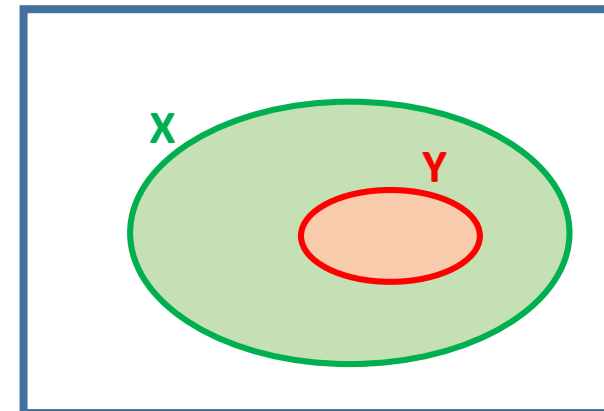
$$x \in \begin{cases} Y & \text{bad outcomes will be avoided} \\ \bar{Y} & \text{otherwise.} \end{cases}$$

**Claim:** no observation falsifies  $X \supset Y$ .

**Proof:** to falsify  $X \supset Y$  must show  $\bar{X} \cap Y$  is not empty.

But can't find  $x \in Y$ . ■

$X$  is necessary for  $Y$   
equiv.  $X \supset Y$   
equiv.  $\bar{X} \Rightarrow \bar{Y}$



**Denial.**

**Anger.**

**Bargaining.**

**Depression.**

**Acceptance.**

# 1. Security by threat model?

“Secure” if threat goals met:  $\{X_0, X_1, X_2, \dots, X_{N-1}\}$ .

$$Y_g \triangleq \bigcap_i X_i$$

We *can* find members of  $Y_g$

Claim that:

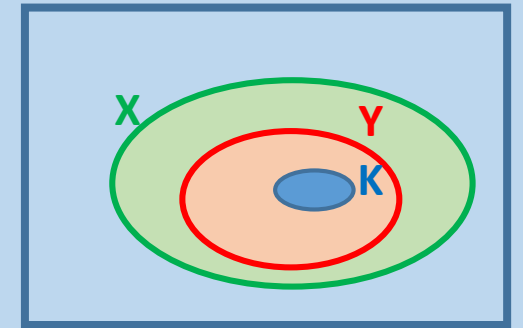
- $Y_g$  sufficient (i.e.  $Y_g \subset Y$ ) is falsifiable [find  $x \in Y_g \cap \bar{Y}$ ]
- $Y_g$  necessary (i.e.  $Y_g \supset Y$ ) not falsifiable [find  $x \in \bar{Y}_g \cap Y$ ]
- That goals are sufficient is falsifiable, but claim that necessary is not



## 2. Insecurity is the *possibility* of bad outcomes?

Define  $\mathbf{K}$ :

$$x \in \begin{cases} \mathbf{K} & \text{bad outcomes cannot happen} \\ \overline{\mathbf{K}} & \text{otherwise.} \end{cases}$$



Everything that cannot happen will not happen:  $\mathbf{K} \subset \mathbf{Y}$

A subset of  $\mathbf{Y}$  is no help in finding a superset of  $\mathbf{Y}$

“Bad outcome possible

means

bad outcome will happen”

equiv.

$$\mathbf{K} \Rightarrow \mathbf{Y} \text{ means } \overline{\mathbf{K}} \Rightarrow \overline{\mathbf{Y}}$$

# 3. Proving necessary conditions

Statement contradicted by no observation

⇒ consistent with every observation

⇒ makes no promise about anything observable

Proved necessary conditions  $\equiv$  Tautological restatement of unfalsifiable assumption



## 4. Security isn't binary?

How do we falsify:

$$\text{Security}(\mathbf{X}) > \text{Security}(\bar{\mathbf{X}})$$

If  $(\text{Outcome}(\mathbf{X}) \approx \text{Outcome}(\bar{\mathbf{X}}))$  is claim refuted?

- Outcome with lifeboats  $\approx$  Outcome w/o lifeboats
- Adaptive attacker
- Statistical significance

if (you don't do X) then <claim>

<claim>	
"you are not secure"	Unfalsifiable or tautological for all X
"a bad outcome will occur"	Unfalsifiable for all X
"a bad outcome can occur"	Unfalsifiable or tautological for all X

“if you don’t choose a strong password then  
your account will be hacked”

Observation: I’ve used 6-char lowercase pwd at Amazon for 17 years.

**Heads I’m right, Tails you’ve just been lucky so far.**

“If you don’t use a unique password per acct then a bad guy who gets one can get into your other accts”

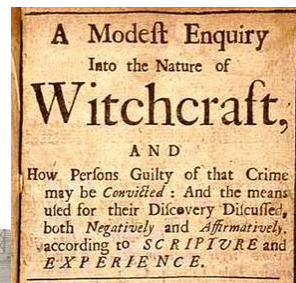
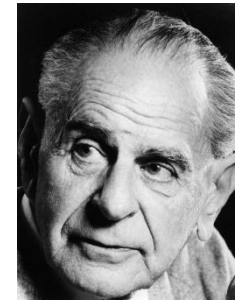


if (you don’t do X) then{  
    a bad guy can do something blocked by X}



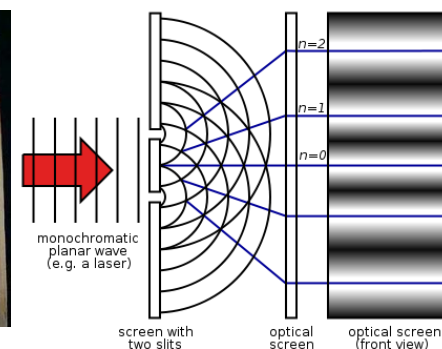
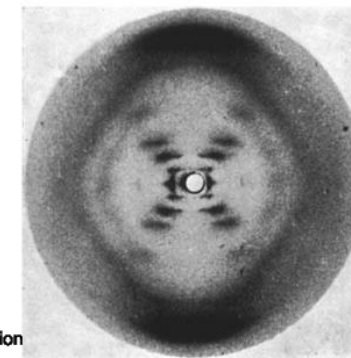
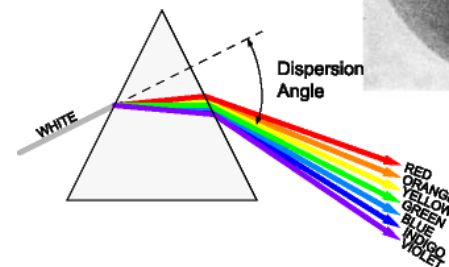
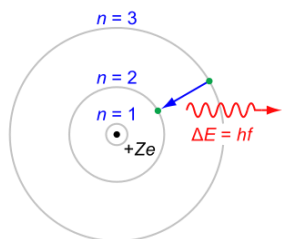
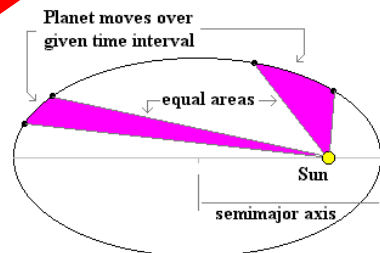
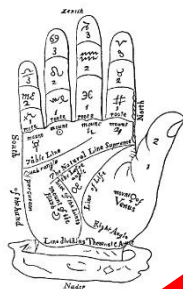
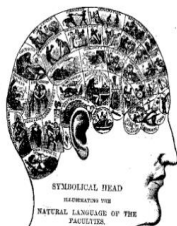
“If you don’t use a Faraday cage then a bad guy who gets close can steal your keys over EM”

# Is Computer Security a Pseudo-Science?



Your password must meet the following guidelines:

- be at least 8 characters and no more than 20
- contain one number from [0 - 9]
- contain one lowercase letter [a - z]
- contain one uppercase letter [A - Z]
- contain one of these special symbols: ! @ # \$ % ^ & \* ( ) + ?



Your password must meet the following guidelines:

- be at least 8 characters and no more than 20
- contain one number from [0 - 9]
- contain one lowercase letter [a - z]
- contain one uppercase letter [A - Z]
- contain one of these special symbols: ! @ # \$ % ^ & \* ( ) + ?

## Pseudo-Science?

Something (falsifiable) is meant behind the unfalsifiable claim

## 5. Acceptance: OK, we didn't mean this *literally*

When we say:

$$\text{Security}(\mathbf{X}) > \text{Security}(\bar{\mathbf{X}})$$

We actually mean, e.g.

$$\text{Outcome}(\mathbf{X} | ABCD) > \text{Outcome}(\bar{\mathbf{X}} | ABCD)$$

For assumptions A, B, C, D .....

Security(**X**) > Security( $\bar{\mathbf{X}}$ )

versus

Outcome(**X** | ABCD) > Outcome( $\bar{\mathbf{X}}$  | ABCD)

1. Expanded scope
2. Forgotten/implicit and vague assumptions
3. Justification for X rests on plausibility/scope of ABCD

Forgotten/Implicit assumptions:  $P_1 = \text{f\%dQjkiypef}$   
 $P_2 = \text{snoopy237}$

$\text{Security}(P_1) > \text{Security}(P_2)$

$\text{Outcome}(P_1) > \text{Outcome}(P_2)$

Forgotten/Implicit assumptions:  $P_1 = f\%dQjkiypef$   
 $P_2 = snoopy237$

$\text{Security}(P_1) > \text{Security}(P_2)$

$\text{Outcome}(P_1 | A) > \text{Outcome}(P_2 | A)$

A. Password file leaks

Forgotten/Implicit assumptions:  $P_1 = f\%dQjkiypef$   
 $P_2 = snoopy237$

$\text{Security}(P_1) > \text{Security}(P_2)$

$\text{Outcome}(P_1 | AB) > \text{Outcome}(P_2 | AB)$

- A. Password file leaks
- B. Password file not stored plaintext

Forgotten/Implicit assumptions:  $P_1 = f\%dQjkiypef$   
 $P_2 = snoopy237$

$\text{Security}(P_1) > \text{Security}(P_2)$

$\text{Outcome}(P_1 | ABC) > \text{Outcome}(P_2 | ABC)$

- A. Password file leaks
- B. Password file not stored plaintext
- C. Or reversibly encrypted

Forgotten/Implicit assumptions:  $P_1 = f\%dQjkiypef$   
 $P_2 = snoopy237$

$\text{Security}(P_1) > \text{Security}(P_2)$

$\text{Outcome}(P_1 | ABCD) > \text{Outcome}(P_2 | ABCD)$

- A. Password file leaks
- B. Password file not stored plaintext
- C. Or reversibly encrypted
- D. Password reset not forced

Security(**X**) > Security( $\bar{\mathbf{X}}$ )

versus

Outcome(**X** | ABCD) > Outcome( $\bar{\mathbf{X}}$  | ABCD)

1. The importance of being literal
  - Claims most useful when taken literally
2. Errors are directional
  - Always claim more, never less
3. Implicit/vague/forgotten assumptions
  - Inability to falsify => forgotten assumptions

How to falsify:

$$\text{Outcome}(\mathbf{X} | ABCD) > \text{Outcome}(\bar{\mathbf{X}} | ABCD)$$

Falsifying  $\equiv$  What would convince X doesn't improve outcomes  
 $\equiv$  Listing *all* of the assumptions

*Can't falsify  $\equiv$  Don't know all the assumptions*

*"You should change your password regularly"*

**Hard to argue we've been questioning assumptions if we can't list them**

# What falsifies any of these?

Choose a strong password.

Choose upper and lower-case.

Choose digits and special characters.

Choose length.

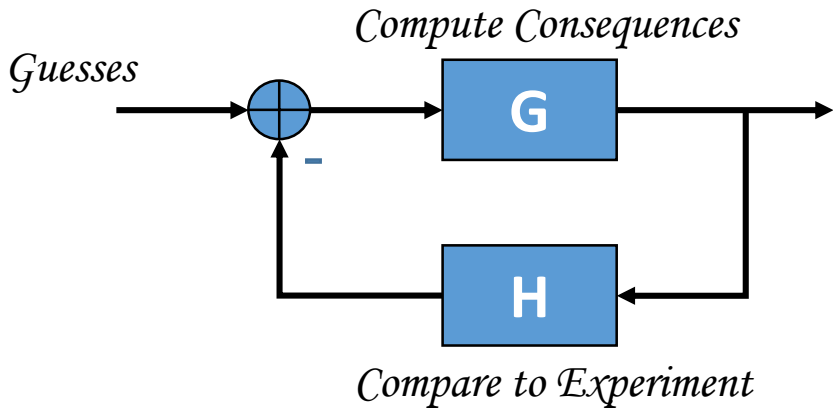
Choose a different password for every account.

Choose to change them every 90 days.

Choose two-factor authentication.

Chose an anti-virus from a reputable vendor.

# Falsifiable vs Unfalsifiable $\equiv$ Feedback vs No-feedback



Over time:

- Iterative improvement
- Errors get caught



Over time:

- No change
- Errors persist indefinitely



# Useful identities

$$\text{Security}(\mathbf{X}) > \text{Security}(\bar{\mathbf{X}})$$

- Claim is unfalsifiable  $\equiv$  Not amenable to feedback

$$\text{Outcome}(\mathbf{X} | ABCD) > \text{Outcome}(\bar{\mathbf{X}} | ABCD)$$

- Don't know what falsifies  $\equiv$  Don't know assumptions

# Conclusions

- **Problem in the way we reason about problems**
  - Heads I'm right, Tails you've just been lucky so far
  - If it doesn't work for all X don't use for any X
- **Feedback**
  - Can't falsify justification → Shut off from feedback
- **What would it take to convince me that I'm wrong?**

Based on: [Unfalsifiability of security claims](#), Proc. Nat. Acad. Sciences, 2016  
[Justifying Security Measures](#), Esorics 2017