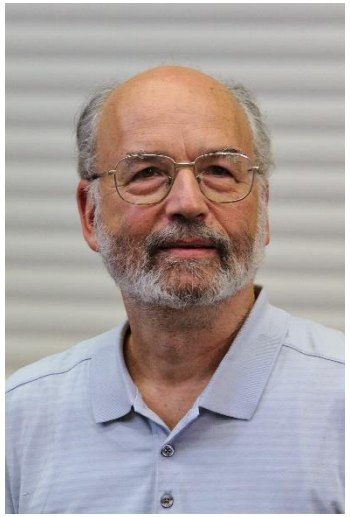
The Unfalsifiability of Security Claims:
and what we can do about it

Cormac Herley

Microsoft Research

“Non-crypto security will remain a mess.”

A. Shamir, Ten year predictions, 2002.



Some things claimed to be necessary are impossible

Portfolio of passwords:

A1: Passwords should be random and strong

A2: Passwords should not be re-used across accounts

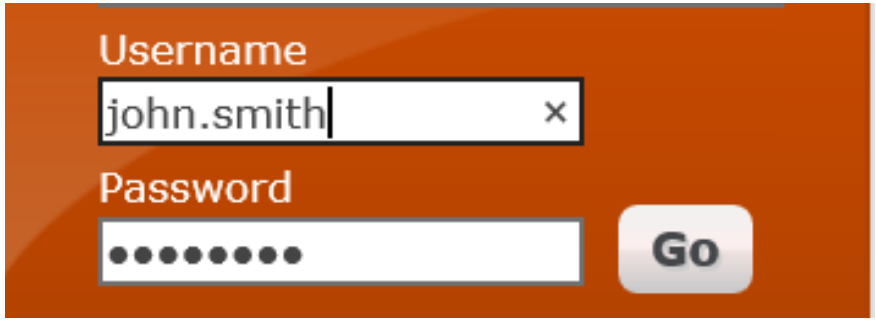
Suppose N=100 accts @ lg(S)=40 bits/password:

$$\text{Effort}(N) = N \cdot \lg(S) + \lg(N!)$$

$$= 4000 + 524 = 4524 \textit{ random bits}$$

Equiv. to memorizing: 1361 places of pi, order of 17 packs of cards ……

Password Masking



Stop Password Masking

by **JAKOB NIELSEN** on June 23, 2009

Topics: Technology User Behavior

Summary: Usability suffers when users type in passwords and the only feedback they get is a row of bullets. Typically, masking passwords doesn't even increase security, but it does cost you business due to login failures.

- Schneier (June 26, 2009): “I agree with this”
- Epic flamewar in blogosphere
- Schneier (July 3, 2009): “So was I wrong? Maybe. Okay, probably”

Why is such a simple question so hard?

Why?

How do we end up insisting on the necessity of things that are provably impossible (with 30s of arithmetic)

How do we end up not being able to decide whether a simple measure helps or not?

“A secure system must defend against all possible attacks, including those unknown to the defender.”

F. Schneider, Blueprint for a Science of Cyber-security

Q: Is this a definition or a claim?

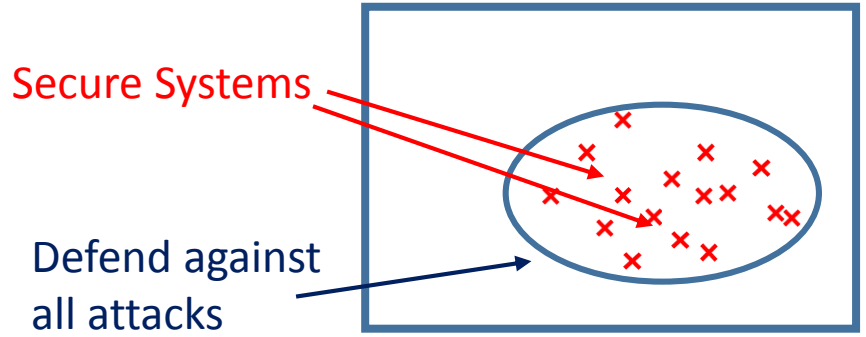
"A secure system must defend against all possible attacks, including those unknown to the defender."

Definition:

- Secure System ≜ Defends against all possible attacks

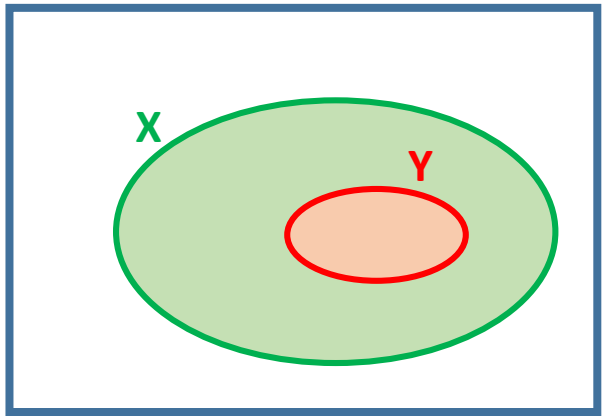
Claim:

- Systems ***found*** to be secure ***always*** defend against all attacks



Claims of necessary conditions for security are unfalsifiable

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



Want to avoid bad outcomes. Define $\mathbf{Y}$:

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

Claim: no observation falsifies $\mathbf{X} \supset \mathbf{Y}$.

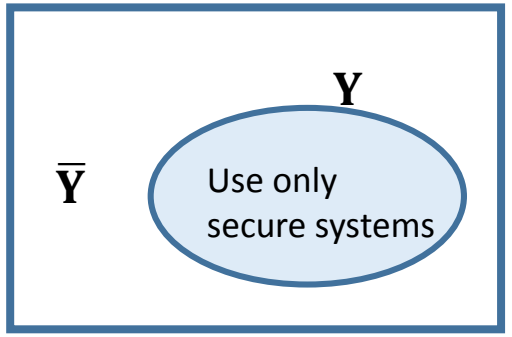
Proof: to falsify $\mathbf{X} \supset \mathbf{Y}$ must show $\overline{\mathbf{X}} \cap \mathbf{Y}$ is not empty.

But can't find $x \in \mathbf{Y}$. ■

In words: Falsifying claim that X is necessary for security requires finding something secure that doesn't do X.

Definitions don't describe the world

$\mathbf{Y}$ = {Secure Systems} ≜ Defends against all possible attacks



Divide population by use secure systems or not: $\mathbf{Y}$, $\overline{\mathbf{Y}}$

Strongest statement we can make about difference?

Outcome for $\mathbf{Y}$ vs. $\overline{\mathbf{Y}}$	
Average case better?	N
Representative case better?	N
At least one case better?	N
Rule out possibility of no difference?	N
Possible difference?	Y

If attain unattainable state we get impossibly narrow claim

Security by design goals?

"Secure" if design goals met: $\{X_0, X_1, X_2, \ldots, X_{N-1}\}$.

$$\mathbf{Y}_g \triangleq \bigcap_i \mathbf{X}_i$$

We ***can*** find members of $\mathbf{Y}_g$

Claim that:

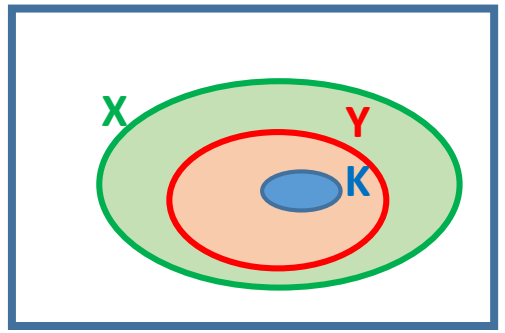
- $\mathbf{Y}_g$ sufficient (i.e.$\mathbf{Y}_g \subset \mathbf{Y}$) is falsifiable [find $x \in \mathbf{Y}_g \cap \overline{\mathbf{Y}}$]
- $\mathbf{Y}_g$ necessary (i.e. $\mathbf{Y}_g \supset \mathbf{Y}$) not falsifiable [find $x \in \overline{\mathbf{Y}_g} \cap \mathbf{Y}$]

- That goals are sufficient is falsifiable, but claim that necessary is not

Insecurity is the *possibility* of bad outcomes?

Define $\mathbf{K}$:

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



Clearly everything that will happen can happen: $\mathbf{K} \subset \mathbf{Y}$

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

So must claim $\mathbf{K} \approx \mathbf{Y}$

"Attackers can (and will) use any means they can." Pfleeger&Pfleeger

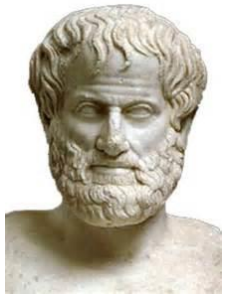
- Tautology + unfalsifiable claim

"Bad outcome possible
means
bad outcome will happen"

equiv. $\mathbf{K} \Rightarrow \mathbf{Y}$ means $\overline{\mathbf{K}} \Rightarrow \overline{\mathbf{Y}}$

Denying the Antecedent:

$X \Rightarrow Y$ does not mean $\overline{X} \Rightarrow \overline{Y}$



Defend against attack(X) => Safe from attack(X).

Do not defend against attack(X) ≠> Succumb to attack(X)

"Impossible to avoid weak passwords and re-use in 100-account portfolio. Florencio et al, Usenix Security 2014.

A	Is re-use a real threat vector?	Y
B	Do bad things happen because of re-use?	Y
C	Can we eliminate that risk by avoiding re-use?	Y
D	Does it follow that you should not re-use?	N

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”	Tautological for all X

Improvement rather than binary security?

How do we falsify

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

If (Outcome($\mathbf{X}$) ≈ Outcome($\overline{\mathbf{X}}$)) is claim refuted?

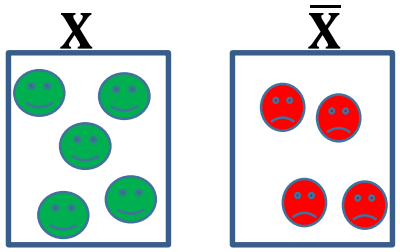
- Outcome with lifeboats ≈ Outcome w/o lifeboats
- Adaptive attacker
- Statistical significance

So what can we do?

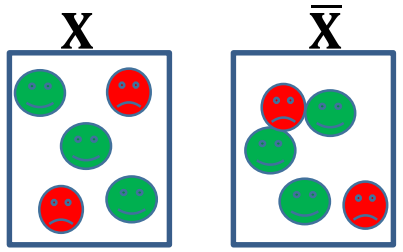
Falsifiable claim

$$\text{Outcome}(\mathbf{X}|\langle\text{cond}\rangle) > \text{Outcome}(\overline{\mathbf{X}}|\langle\text{cond}\rangle)$$

Specify conditions under which observable outcome expected.



Confirmed



Refuted

Failure to do this even in obvious cases:

- $\mathbf{X}$ = {Choose strong password}
- $\mathbf{X}$ = {Password masking}

So what? Consequences of unfalsifiability

- **Self-correction is one-sided**
- **Systems of constraints with no solution**
- **Subjective comparison of measures?**
  - Which hi-assurance measures can we neglect for low-assurance?
- **Compare based on assumptions only if you know what they are**
  - Costs=0, Prin. Easiest Access → License to be sloppy about assumptions
- **Evidence doesn't matter**
  - Pointless to even examine if nothing can alter the conclusion

One-sided Self-Correction: new attacks argue X_i in, nothing can argue X_i out

Collection of defensive measures $M = \{X_0, X_1, X_2, \ldots, X_{N-1}\}$

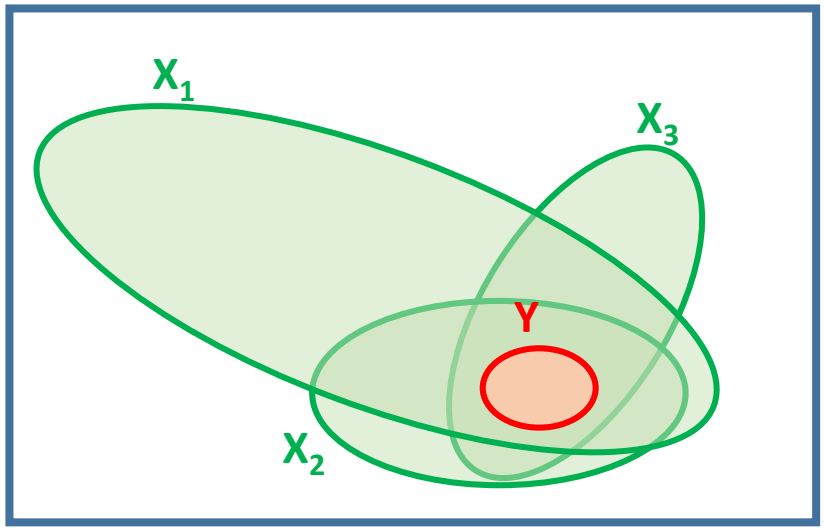
- M not sufficient demonstrated by new attack that "steps outside" model

- M not necessary is not falsified by any possible observation.
  - M could be over-complete (no solution)
  - M could be redundant (measures that do nothing)
  - There might be far simpler measure than X_j

Upgrading sufficient to necessary → Over-constrained problems

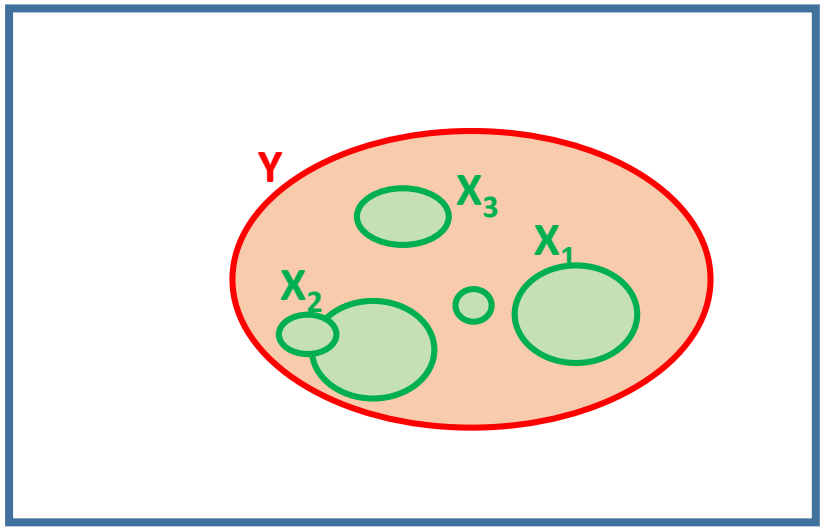
Simultaneous ***necessary*** conditions:

$$\bigcap_i \mathbf{X}_i \supset \mathbf{Y}$$



Simultaneous ***sufficient*** conditions:

$$\bigcap_i \mathbf{X}_i = \phi$$



Example over-constrained problems:

1. Avoiding pwd re-use is sufficient to counter some attacks; but impossible to achieve across N=100 portfolio
2. Intersection of conditions we think are necessary of a replacement for passwords = empty.

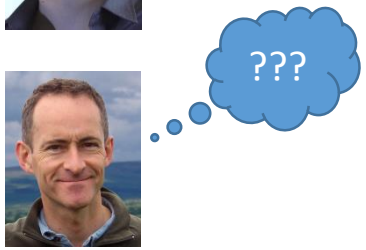
Which High-assurance measures should I use for low-assurance?

Set of measures ***Snowden*** needs to protect his stuff

$$M = \{X_0, X_1, X_2, \ldots, X_{N-1}\}$$

What measures does ***Cormac*** need to protect his stuff?

$$C \subset M$$



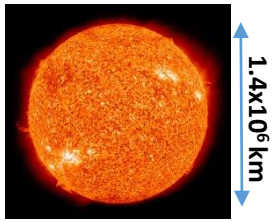
Compare measures X_a and X_b?

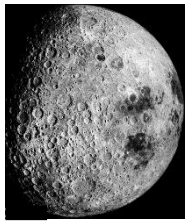
$$\text{Assumptions(a)} \overset{?}{\gtrless} \text{Assumptions(b)}$$

Acknowledging can't do everything empty w/o ability to compare

1. Realism of assumptions poor basis for comparison

- Newtonian Mechanics: point masses, vacuum, elastic collisions.





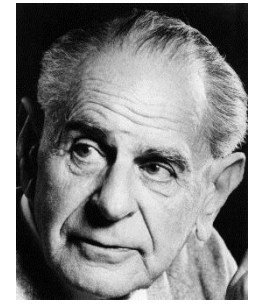
- Accuracy of predictions not realism of assumptions.

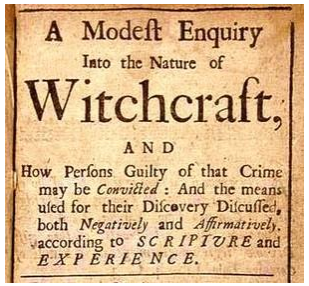
2. Can't compare assumptions if we don't know what they are

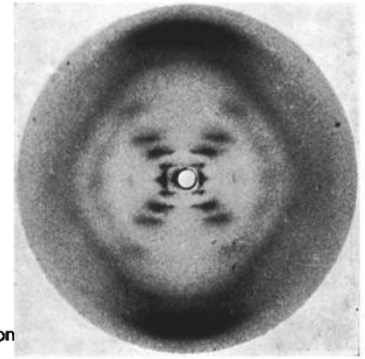
Why do we do password aging?

- "As best as I can find, some DoD contractors did some back-of-the-envelope calculation about how long it would take to run through all the possible passwords using their mainframe, and the result was several months." Spafford.
- "Tradition!!" P. Gutman

Is Computer Security a Pseudo-Science?

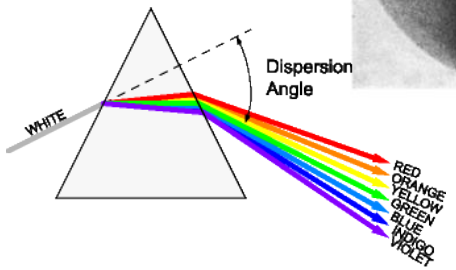


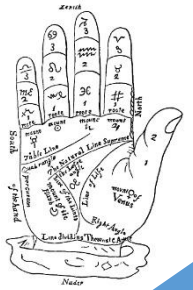


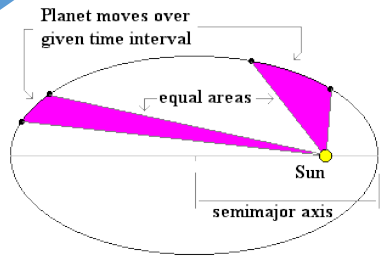


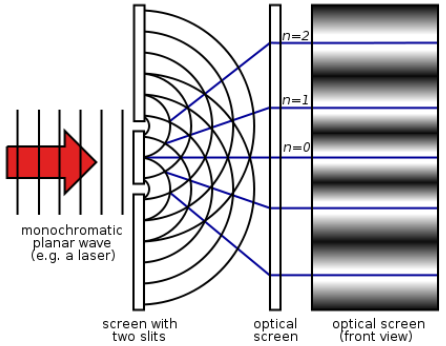
Your password must meet the following guidelines:

- 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: ! @ # $ % ^ & * ( ) + ?









WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages

Pseudoscience

From Wikipedia, the free encyclopedia

For a broader coverage related to this topic, see Pseudo-scholarship.
See also: List of topics characterized as pseudoscience

Pseudoscience is a claim, belief or practice which is incorrectly presented as scientific, but does not adhere to a valid scientific method, cannot be reliably tested, or otherwise lacks scientific status.[1] Pseudoscience is often characterized by the use of vague, contradictory, exaggerated or unprovable claims, an over-reliance on confirmation rather than rigorous attempts at refutation, a lack of openness to evaluation by other experts, and a general absence of systematic processes to rationally develop theories.

A field, practice, or body of knowledge can reasonably be called pseudoscientific when it is presented as consistent with the norms of scientific research, but it demonstrably fails to meet these norms.[2] Science is also distinguishable from revelation, theology, or spirituality in that it offers insight into the physical world obtained by empirical research and testing.[3] Commonly held beliefs in popular science may not meet the criteria of science.[4] "Pop science" may blur the divide between science and pseudoscience among the general public, and may also involve science fiction.[4]

Part of a series on
Science

Formal	[show]
Physical	[show]
Life	[show]
Social	[show]
Applied	[show]
Interdisciplinary	[show]
Philosophy · History	[hide]

Basic research · Citizen science · Fringe science · Protoscience ·

To be secure your password must:

- be at least 8 characters long
- contain one number from [0-9]
- contain one lowercase letter [a-z]
- contain one uppercase letter [A-Z]
- contain one special character: !@#$%&()+?

Pseudoscience?

- Something beyond the unfalsifiable claim is meant by this
  - But what?

Why are *our* unfalsifiable claims to be accepted but others be rejected?

"Crypto backdoors are a vital tool in fighting crime" FBI Director Comey

"Consensus of senior defense and intelligence officials in the U.S. government is that NSA surveillance may well be the only thing that can stop the next terrorist from blowing apart innocent Americans." M. Hirsh

£2.50 | ONLY £2.00 TO PRINT MEMBERS

Y TIMES

British spies betrayed to Russians and Chinese

Tom Harper, Richard Kerbaj and Tim Shipman

RUSSIA and China have cracked the top-secret cache of files stolen by the fugitive US whistleblower Edward Snowden, forcing MI6 to pull agents out of live operations in hostile countries, according to senior officials in Downing Street, the Home Office and the security services.

Western intelligence agencies say they have been forced into the rescue operations after Moscow gained access to more than 1m classified files held by the former American security contractor, who fled to seek protection from Vladimir Putin, the Russian president, after mounting one of the largest leaks in US history.

Senior government sources confirmed that China had also cracked the encrypted documents, which contain details of secret intelligence techniques and information that could allow British and American spies to be identified.

One senior Home Office official accused Snowden of having "blood on his hands", although Downing Street said there was "no evidence of anyone being harmed".

Sir David Omand, the former director of GCHQ, said the news that Russia and China had access to Snowden's material was a "huge strategic setback" that was "harming" to Britain, America and their Nato allies.

Snowden, a former contractor at the CIA and National Security Agency (NSA), downloaded 1.7m secret documents from western intelligence agencies in 2013 and released details of sensitive surveillance programmes to the media.

In an interview filmed in Hong Kong in which he unmasked himself as the source, Snowden said he acted out of a desire to protect "privacy and basic liberties" and claimed the NSA and GCHQ were operating mass surveillance programmes that targeted hundreds of millions of innocent people.

Last week a report by David Anderson QC, announced after Snowden's disclosures, concluded the intelligence agencies should retain their powers for the "bulk collection" of communications data, but that the power to issue warrants for intrusive surveillance should be stripped from ministers and handed to judges.

Two weeks after his initial leak in June 2013, Snowden fled Hong Kong for Moscow where he claimed political asylum. He has remained under the protection of Putin's regime since.

In an email to a sympathetic US senator in July 2013 Snowden claimed that "no intelligence service" could "compromise the secrets I continue to protect", saying he was trained in techniques that would "keep such information from being compromised even in the highest threat counter-intelligence environments (ie. China)".

However, since he exposed western intelligence-gathering methods, the security services have reported increasing difficulty in the monitoring of terrorists and other dangerous criminals via digital communications including email, phone contact, chat rooms and social media.

And last night David Cameron's aides confirmed the

Continued on page 2 ▶▶

Conclusions

- **“Think like an attacker” emphasizes measures may be insufficient**
  - Don’t even have a culture of checking necessity
  - Extending the list for Snowden rather than reducing for rest of us
- **Stop treating slogans like Newton’s Laws**
  - “There is a tradeoff between usability and security”
  - “No security through obscurity”
- **Stop invoking security exceptionalism**
  - We make mistakes the way others do:
    - Sloppy thinking, confirmation bias, vague claims, jumping to conclusions
- **“Security” is just a term that facilitates muddle**