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:
\[
\text{Effort}(N) = N \cdot \lg(S) + \lg(N!)
\]
\[
= 4000 + 524 = 4524 \text{ random bits}
\]

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 $\triangleq$ Defends against all possible attacks

Claim:
• Systems *found* to be secure *always* defend against all attacks
Claims of necessary conditions for security are unfalsifiable

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

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

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

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

But can’t find $x \in \mathcal{Y}$.

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

\[ Y = \{\text{Secure Systems}\} \triangleq \text{Defends against all possible attacks} \]

Divide population by use secure systems or not: \( Y, \; \bar{Y} \)
Strongest statement we can make about difference?

<table>
<thead>
<tr>
<th>Outcome for ( Y ) vs. ( \bar{Y} )</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Average case better?</td>
<td>N</td>
</tr>
<tr>
<td>Representative case better?</td>
<td>N</td>
</tr>
<tr>
<td>At least one case better?</td>
<td>N</td>
</tr>
<tr>
<td>Rule out possibility of no difference?</td>
<td>N</td>
</tr>
<tr>
<td>Possible difference?</td>
<td>Y</td>
</tr>
</tbody>
</table>

If attain unattainable state we get impossibly narrow claim
Security by design goals?

“Secure” if design goals met: \(\{X_0, X_1, X_2, \ldots, X_{N-1}\}\).

\[
Y_g \triangleq \bigcap_i X_i
\]

We can find members of \(Y_g\)

Claim that:

- \(Y_g\) sufficient (i.e. \(Y_g \subseteq Y\)) is falsifiable [find \(x \in Y_g \cap \overline{Y}\)]
- \(Y_g\) necessary (i.e. \(Y_g \supseteq Y\)) not falsifiable [find \(x \in \overline{Y_g} \cap Y\)]

- That goals are sufficient is falsifiable, but claim that necessary is not
Insecurity is the *possibility* of bad outcomes?

Define $K$:

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

Clearly everything that will happen can happen: $K \subseteq Y$

A subset of $Y$ is no help in finding a superset of $Y$

So must claim $K \approx Y$

*“Attackers can (and will) use any means they can.”* Pfleeger & Pfleeger

* Tautology + unfalsifiable claim

“Bad outcome possible means bad outcome will happen”

equiv. $K \Rightarrow Y$ means $\overline{K} \Rightarrow \overline{Y}$
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) \(\neq\) Succumb to attack(X)

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

<table>
<thead>
<tr>
<th></th>
<th>Is re-use a real threat vector?</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Do bad things happen because of re-use?</td>
<td>Y</td>
</tr>
<tr>
<td>C</td>
<td>Can we eliminate that risk by avoiding re-use?</td>
<td>Y</td>
</tr>
<tr>
<td>D</td>
<td>Does it follow that you should not re-use?</td>
<td>N</td>
</tr>
</tbody>
</table>
if (you don’t do X) then <claim>

<table>
<thead>
<tr>
<th>&lt;claim&gt;</th>
<th>Unfalsifiable or tautological for all X</th>
<th>Unfalsifiable for all X</th>
<th>Tautological for all X</th>
</tr>
</thead>
<tbody>
<tr>
<td>“you are not secure”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“a bad outcome will occur”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“a bad outcome can occur”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Improvement rather than binary security?

How do we falsify

\[ \text{Security}(X) > \text{Security}(\overline{X}) \]

If \((\text{Outcome}(X) \approx \text{Outcome}(\overline{X}))\) is claim refuted?

- Outcome with lifeboats \(\approx\) Outcome w/o lifeboats
- Adaptive attacker
- Statistical significance
So what can we do?

Falsifiable claim

\[ \text{Outcome}(X | \text{<cond>}) > \text{Outcome}(\bar{X} | \text{<cond>}) \]

Specify conditions under which observable outcome expected.

Failure to do this even in obvious cases:

- \( X = \{\text{Choose strong password}\} \)
- \( X = \{\text{Password masking}\} \)
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:
\[ \cap_i X_i \supset Y \]

Simultaneous **sufficient** conditions:
\[ \cap_i X_i = \emptyset \]

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

\[ M = \{X_0, X_1, X_2, ..., X_{N-1}\} \]

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

\[ C \subset M \]

Compare measures \( X_a \) and \( X_b \)?

\[ \text{Assumptions}(a) \preceq \text{Assumptions}(b) \]

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: ! @ # $ % ^ & * ( ) + ?
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. 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. Science is also distinguishable from revelation, theology, or spirituality in that it offers insight into the physical world obtained by empirical research and testing. Commonly held beliefs in popular science may not meet the criteria of science. "Pop science" may blur the divide between science and pseudoscience among the general public, and may also involve science fiction.
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

...
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