Justifying Security Measures

Cormac Herley
Microsoft Research

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 ridicules public guidelines for internet passwords as impossible even for spies to follow

Every British citizen is effectively a suspect, Martin warns

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 numeric keypad rules to protect their accounts by inventing awkward new passwords for every site was in the Air Force by that time, but the Air Force didn’t use it. The Air Force was using 128-bit encryption and the password rules were just a way to help the Rest of Us remember our 128-bit encryption.
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:

\[ x \in \begin{cases} Y & \text{bad outcomes will be avoided} \\ \overline{Y} & \text{otherwise} \end{cases} \]

Claim: no observation falsifies \( X \supset Y \).

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

But can’t find \( x \in Y \). ■

X is necessary for Y
equiv. \( X \supset Y \)
equiv. \( \overline{X} \Rightarrow \overline{Y} \)
Denial.
Anger.
Bargaining.
Depression.
Acceptance.
1. Security by threat model?

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

\[ Y_g \triangleq \bigcap_i X_i \]

We can find members of \(Y_g\)

Claim that:

• \(Y_g\) sufficient (i.e. \(Y_g \subset Y\)) is falsifiable [find \(x \in Y_g \cap \overline{Y}\)]

• \(Y_g\) necessary (i.e. \(Y_g \supset Y\)) not falsifiable [find \(x \in \overline{Y_g} \cap Y\)]

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

Define $K$:

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

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

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

“Bad outcome possible means bad outcome will happen”

equiv. $K \Rightarrow Y$ means $\overline{K} \Rightarrow \overline{Y}$
3. Proving necessary conditions

Statement contradicted by no observation
⇒ consistent with every observation
⇒ makes no promise about anything observable

Proved necessary conditions ≡ Tautological restatement of unfalsifiable assumption
4. Security isn’t binary?

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
if (you don’t do X) then <claim>

<table>
<thead>
<tr>
<th>&lt;claim&gt;</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>“you are not secure”</td>
<td>Unfalsifiable or tautological for all X</td>
</tr>
<tr>
<td>“a bad outcome will occur”</td>
<td>Unfalsifiable for all X</td>
</tr>
<tr>
<td>“a bad outcome can occur”</td>
<td>Unfalsifiable or tautological for all X</td>
</tr>
</tbody>
</table>
“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?
Pseudo-Science?

Something (falsifiable) is meant behind the unfalsifiable claim
5. Acceptance: OK, we didn’t mean this *literally*

When we say:

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

We actually mean, e.g.

\[ \text{Outcome}(X|ABCD) > \text{Outcome}(\overline{X}|ABCD) \]

For assumptions A, B, C, D ......
Security($X$) > Security($\overline{X}$)

versus

Outcome($X | ABCD$) > Outcome($\overline{X} | ABCD$)

1. Expanded scope
2. Forgotten/implicit and vague assumptions
3. Justification for $X$ rests on plausibility/scope of $ABCD$
Forgotten/Implicit assumptions: $P_1 = f%dQjkiyeP\,\,\,P_2 = snoopy237$

Security($P_1$) > Security($P_2$)

Outcome($P_1$) > Outcome($P_2$)
Forgotten/Implicit assumptions: $P_1 = f%dQjkiyp\text{ef}$
$P_2 = \text{snoopy237}$

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

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

A. Password file leaks
Forgotten/Implicit assumptions: \( P_1 = f\%dQjkiypef \)
\( P_2 = \text{snoopy237} \)

\[
\text{Security}(P_1) > \text{Security}(P_2)
\]

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

A. Password file leaks
B. Password file not stored plaintext
Forgotten/Implicit assumptions: $P_1 = \text{f%dQjkiyptef}$
\[ P_2 = \text{snoopy237} \]

Security($P_1$) > Security($P_2$)

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

A. Password file leaks
B. Password file not stored plaintext
C. Or reversibly encrypted
Forgotten/Implicit assumptions: $P_1 = f%dQjkiyqef$
$P_2 = snoopy237$

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

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

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

Security(\(X\)) > Security(\(\overline{X}\))

versus

Outcome(\(X|ABCD\)) > Outcome(\(\overline{X}|ABCD\))
How to falsify:

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

Falsifying $\equiv$ What would convince $X$ doesn’t improve outcomes

$\equiv$ Listing \textit{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

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

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

\[ \text{Outcome}(X|ABCD) > \text{Outcome}(\overline{X}|ABCD) \]

- 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?

Justifying Security Measures, Esorics 2017