The Unfalsifiability of Security Claims

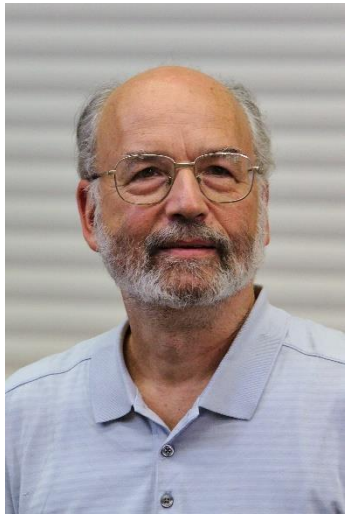
Cormac Herley

Microsoft Research

Based on: Unfalsifiability of security claims, Proc. Nat. Acad. Sciences, 2016

“Non-crypto security will remain a mess.”

A. Shamir, Ten year predictions, 2002.



Some things claimed to be necessary are impossible

Portfolio of passwords:

1: Passwords should be random and strong

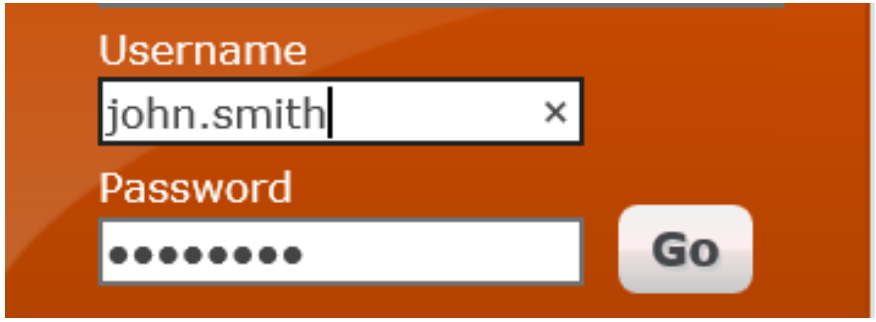
2: Passwords should not be re-used across accounts

Suppose N=100 accts @ 40 bits/password:

$N \cdot \lg(S) + \lg(N!) = 4000 + 524 = 4{,}524$ *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 how to answer a simple question?

“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?

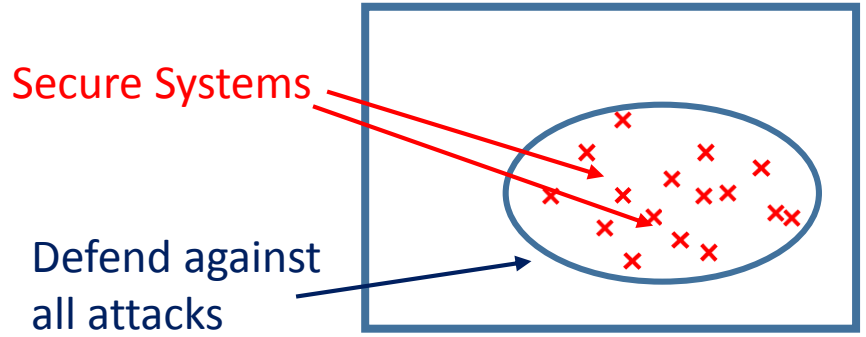
"A secure system must defend against all possible attacks, including those unknown to the defender."

Definition:

- Secure System ≜ Defends against all possible attacks

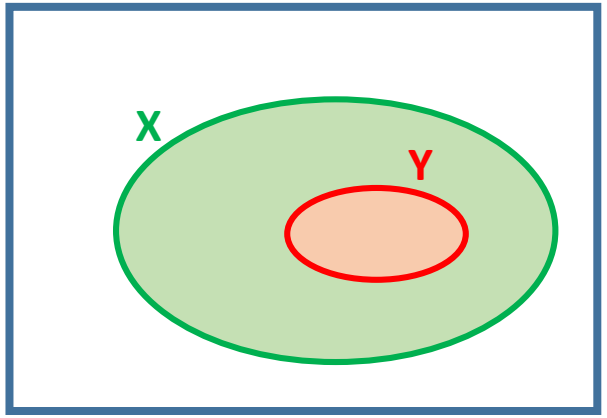
Claim:

- 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 $\mathbf{X} \supset \mathbf{Y}$.

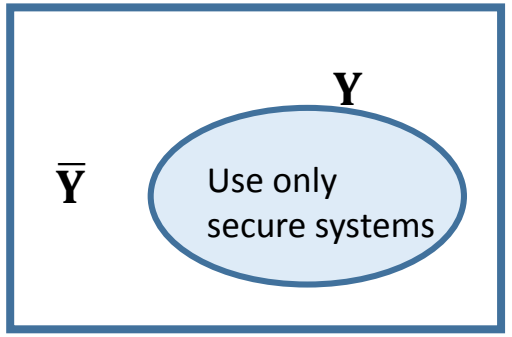
Proof: to falsify $\mathbf{X} \supset \mathbf{Y}$ must show $\overline{\mathbf{X}} \cap \mathbf{Y}$ is not empty.

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



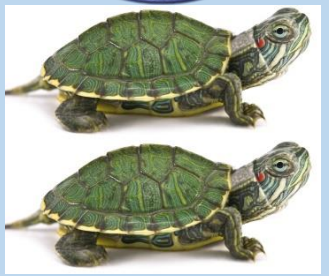
Divide population by use secure systems or not: $\mathbf{Y}$, $\overline{\mathbf{Y}}$

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

Alternatives: Denial. Anger. Bargaining. Depression. Acceptance.

1. Security by design goals
2. Insecurity = possibility of bad outcomes
3. Security is proved not observed
4. Security isn’t binary



1. Security by design goals?

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

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

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

Claim that:

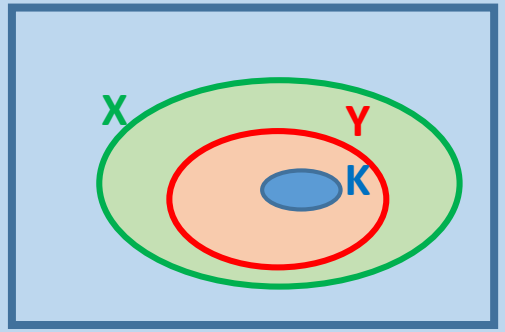
- $\mathbf{Y}_g$ sufficient (i.e.$\mathbf{Y}_g \subset \mathbf{Y}$) is falsifiable [find $x \in \mathbf{Y}_g \cap \overline{\mathbf{Y}}$]
- $\mathbf{Y}_g$ necessary (i.e. $\mathbf{Y}_g \supset \mathbf{Y}$) not falsifiable [find $x \in \overline{\mathbf{Y}_g} \cap \mathbf{Y}$]

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

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

Define $\mathbf{K}$:

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



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

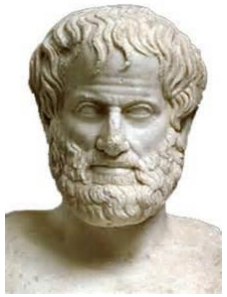
- Tautology + unfalsifiable claim

"Bad outcome possible
means
bad outcome will happen"

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

Confusing sufficient for necessary:

$X \Rightarrow Y$ 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

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

	Verifiable	Falsifiable
A bad guy can	Y	N
A bad guy cannot	N	Y

4. Security isn't binary?

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

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

What the world looks like if claim is……

True

False

Your reward will not be (observable) in this world.

So what? Consequences of unfalsifiability

- **Self-correction is one-sided**
  - Waste: when we go wrong we stay wrong
- **Over constrained problems**
- **How select between unfalsifiable claims?**
  - Which hi-assurance measures can we neglect for low-assurance?

Self-Correction becomes one-sided :

new attacks argue counter-measures in, nothing can argue one out

Assume attacker capabilities →C = $\{c_0, c_1, c_2, \ldots, c_{N-1}\}$

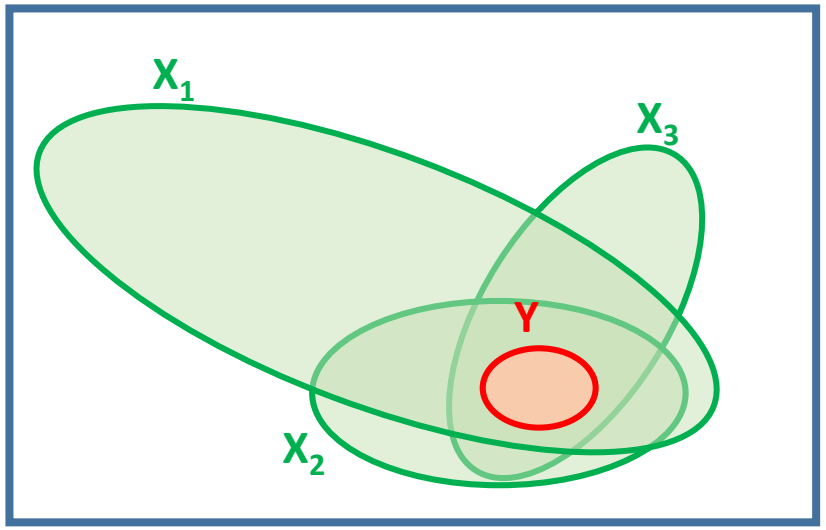
Collection of defensive measures M = $\{X_0, X_1, X_2, \ldots, X_{N-1}\}$

- **M not *sufficient* clear when new attack "steps outside" model**
- **M not *necessary* is not falsified by any possible observation.**

Confusing sufficient for necessary:
→ Over-constrained problems

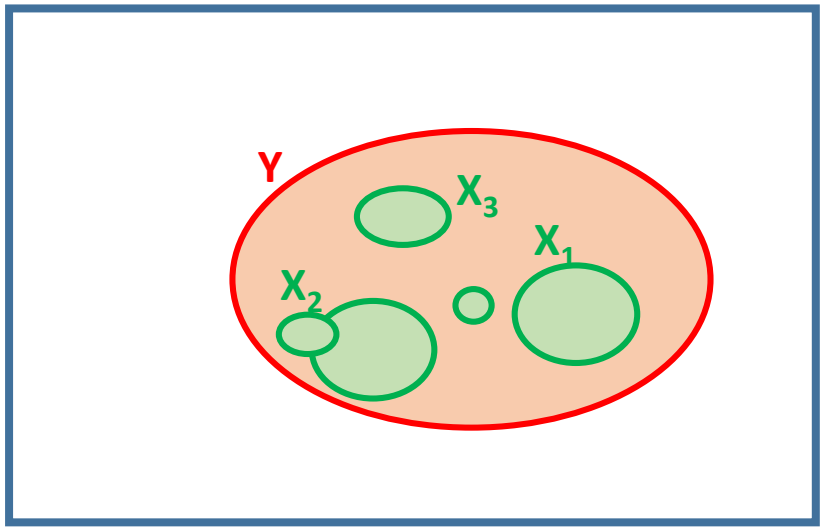
Simultaneous ***necessary*** conditions:

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



Simultaneous ***sufficient*** conditions:

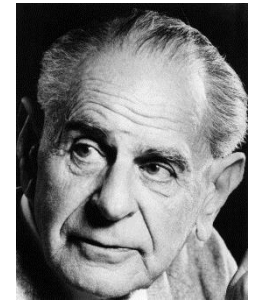
$$\bigcap_i \mathbf{X}_i = \phi$$

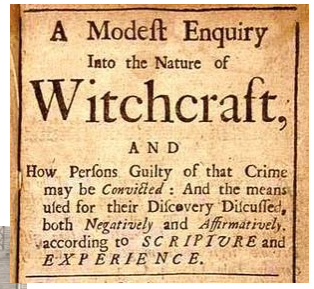


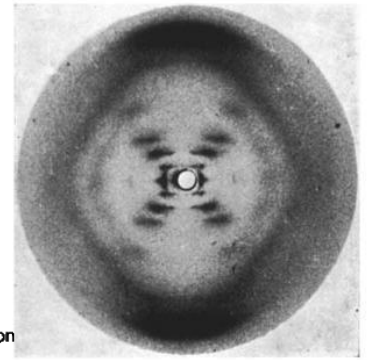
Example over-constrained problem:

- Avoiding pwd re-use is sufficient to counter some attacks; but impossible to achieve across N=100 portfolio

Is Computer Security a Pseudo-Science?

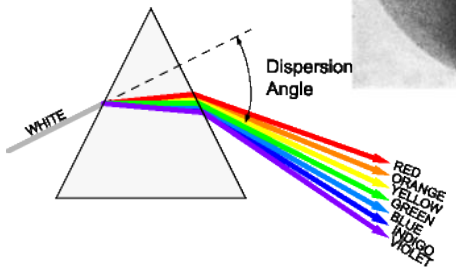


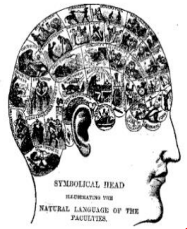


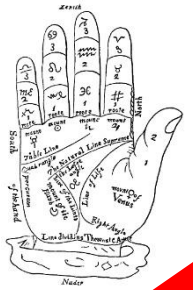


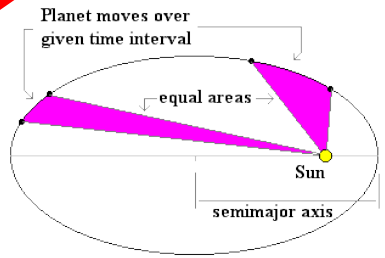
Your password must meet the following guidelines:

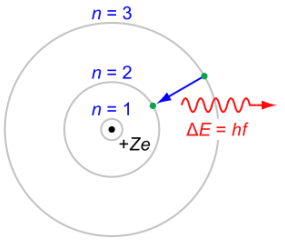
- be at least 8 characters and no more than 20
- contain one number from [0 - 9]
- contain one lowercase letter [a - z]
- contain one uppercase letter [A - Z]
- contain one of these special symbols: ! @ # $ % ^ & * ( ) + ?

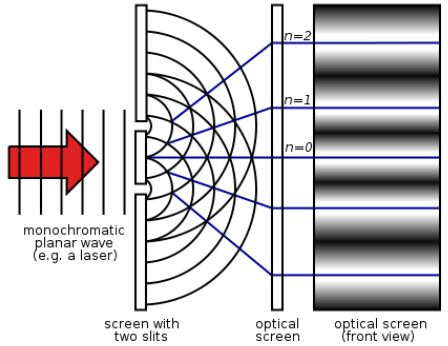












Your password must meet the following guidelines:

- 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:

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

We actually mean, e.g.

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

For assumptions A, B, C, D …….

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

versus

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

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

The narrower the set that falsifies justification the narrower the promise

Forgotten/Implicit assumptions: P_1 = f%dQjkiypef
P_2 = 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

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

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

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

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

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

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

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

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

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

$$Outcome(P_1 | ABCD) > Outcome(P_2 | ABCD)$$

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

What would it take to show that I'm wrong?

Falsifying ≡ Explicitly stating what X rules out

The smaller the set that falsifies justification the smaller the promise

"Nothing falsifies! I have a proof!"

Justification promises nothing.

"Don't know what falsifies"

Don't know what X promises.

Nothing falsifies => X Promises nothing

A: “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 not made impossible by X}

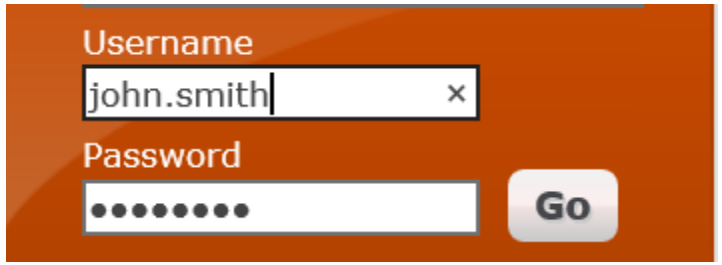
B: “if you don’t use a Faraday cage then a bad guy who gets close can steal your keys over EM”

Can't be immune to contradiction and make useful claims about experience

Don’t know what falsifies
=> Don’t know what X promises

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



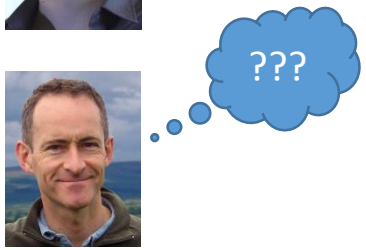
Which High-assurance measures should I use for low-assurance?

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

Unfalsifiable claims are good fun

- **“The only secure system is unplugged, encased in concrete and buried underground.”**
- **“What percent of the Fortune 100 have been hacked? 100%”**
- **“There are two kinds of people: those who've been hacked and those who just don't know it yet.”**

Why are *our* unfalsifiable claims OK 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

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."

£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

- **Problem in the way we reason about problems**
  - **Unfalsifiable, vague, implicit claims**
- **Muddled justification statements**
  - Overstating strength of evidence
- **Worry about over-estimating attackers as well as under**
  - Abundance of caution does not lead to abundantly cautious soln
- **What would it take to convince me that I'm wrong?**