

Re: Still Looking for that One, BRAVE, NASA and/or NAA Employee Re: Apollo One

Source: <http://sci.tech-archive.net/Archive/sci.space.history/2004-12/2286.html>

From: Herb Schaltegger (herb.schaltegger_at_gmail.com.invalid)

Date: 12/23/04

Date: Wed, 22 Dec 2004 20:11:22 -0600

In article <41cf1bc2.1583628@supernews.seanet.com>, fairwater@gmail.com (Derek Lyons) wrote:

> *Herb Schaltegger* <herb.schaltegger@gmail.com.invalid> wrote:
>
> > *In article* <vYydnbMJH4r3AITcRVn-uw@comcast.com>,
> > *"Christopher M. Jones"* <christopher.m.jones@gmail.com> wrote:
> >
> > > *Also, secrets do not necessarily naturally expire over*
> > > *time. There are certain techniques of cryptanalysis*
> > > *developed during and before WWII that are still kept*
> > > *very secret, for example.*
> >
> > *Very well-informed mathematicians and cryptanalysts like Schneier*
> > *disagree with cryptological security by obscurity.*
>
> *The problem is they think (wrongly) that *encryption methods* should*
> *not be protected by obscurity.[1] Christopher is talking about*
> **analysis methods*, which quite profitably can be protected via*
> *obscurity.*

I disagree with the "(wrongly)" portion of this statement and with Christopher's apparent argument that analysis methods can be profitably protected via security. It's just applied mathematics, after all, and the NSA has found during the preceding 20 years (much to its chagrin) that it does not have a monopoly on highly educated, talented and skilled mathematicians, cryptologists, cryptographers and coders. Expecting analytical methods discovered by eggheads in the Puzzle Palace to remain secret is not a very good practice.

> *Apples and Oranges.*
>
> *[1] A more accurate statement is that they should not *require**
> *obscurity for safe and effective performance, but they equally should*
> *not *need* obscurity for safe and effective performance. Thus*
> *incorporating obscurity into an otherwise robust cryptosystem adds a*

> *layer of protection.*

Point taken. That is a good summary of principals I did not address well but which are very valid considerations.

> *>A properly designed cypher system shouldn't require secrecy to be effective – it should just require the proper application of mathematics.*
>
> *Just because it doesn't require secrecy does not mean that secrecy should not be part of the overall communications system plan.*
> *Schneier misses that because he is a mathematician, not a security expert.*

Umm, he's both. And contrariwise, he does agree that secrecy (or rather, real security, not what the current administration calls "security") has it's place, specifically with regard to things such as physical security of key storage, prevention of code tampering, etc. (Which, in fairness, you noted below). He argues (persuasively in my opinion as both a mathematically-educated engineer – 12 hours short of a minor in math – and as a student of political process and history) that keeping algorithms, methods and codes themselves secret does nothing to add to true security in any sense.

> *(Like others of his ilk he also misses the fact that cryptology is just one small part of the much larger field of communications security, but it's the sexiest part and garners disproportionate attention.)*

Again, um . . . no. You're obviously not very familiar with Schneier's work except for his most famous, "Applied Cryptography"

> *At a minimum, hiding the cryptosystem in use on a given link denies the black hats an easy handle into the system.*

Except that in a properly designed crypto system, knowing the algorithms (and even the hardware used) should not be necessary – absent advances unknown in quantum computing (which I am not *completely* discounting), no one in the world can expect to break a 1024 bit RSA public-key system within the lifespan of the universe, still, decades after Whitfield and Diffie(*) invented public-key crypto.

(* And yes, I know that it now appears that British crypto folks invented it quite some time earlier and its invention was suppressed – however, see my comment about the NSA's unfortunate realization that they don't have a monopoly on genius)

> *>Because if the cryptosystem requires security, all it takes is one breach to render it entirely untrustworthy.*
>
> *Incorrect. *All* cryptosystems require some form of security, on the*

sci.space.history: Re: Still Looking for that One, BRAVE, NASA and/or NAA Employee Re: Apollo One

> *keys if nothing else. This keeps valuable information out of the
> hands of the black hats.*

Again, however, if the keys themselves are encrypted with a high-order algorithm, even physical possession of the keys shouldn't result in penetration of the system. And even if the keys are lost, you simply generate new ones. The keys themselves are secured unless the passphrase used to hash THEM is also compromised.

Which brings us back to physical security – don't write down passphrases, change them often, and keep your computer physically protected against tampering – which can result in installation of keyloggers, tampered code, etc. Because let's face it – is most email and communications worth hours or days or months' worth of time on some hypothesize super-duper-code-breaking machine that the world's experts all agree probably doesn't exist anyway, when you can break into the place and install a keylogger and a hidden camera to read the messages off the screen?

> *And keeping even the smallest scrap of information out of the hands of
> the black hats is the very cornerstone of communications security.*

Out of habit from more primitive days, not out of mathematical necessity.

> *D.*

--

Herb Schaltegger, B.S., J.D.

"Wow! This is like saying when engineers get involved, harmonic oscillations tear apart bridges."

~Hop David

<<http://www.angryherb.net>>