

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/2004-12/2274.html>

From: Derek Lyons (fairwater_at_gmail.com)

Date: 12/23/04

Date: Thu, 23 Dec 2004 01:25:33 GMT

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.

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.

>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. (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.)

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

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

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

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

D.

--

Touch-twice life. Eat. Drink. Laugh.

-Resolved: To be more temperate in my postings.

Oct 5th, 2004 JDL