

Re: What does Security include?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5495.html>

From: Simon Johnson (ckwop_at_hotmail.com)

Date: 05/31/04

Date: Mon, 31 May 2004 12:00:19 +0000 (UTC)

"flip" <flip_alpha@safebunch.com> wrote in message
news:1085974143.420338@news-1.nethere.net...

> *Hi All,*

>

> *I was wondering what the breadth of security is typically defined to
> entail?*

> *For example, we always hear of security and it can include such things as
> physical security, intrusion detection, firewalls, protocols,
> cryptography,*

> *cryptology, cryptanalysis, disaster recovery schemas, passwords,*

> *communications security, compusec, trashsec, privacy, network security,
> et.*

> *al.*

>

> *Do people use a different word when referring to security in the context
> of*

> *crypto?*

>

> *What do people mean here when they say security?*

The meaning of security depends on the context. That much is obvious. In general you can define what we mean by security in terms of a protocol and the ability to pervert that protocol.

A cryptosystem is secure if the effort required to derail the objectives of that system is feasible to even the most equipped adversary.

Often a weaker definition is deployed in terms of cost. For example, a safe is secure if the value of the things you're protecting is less than the cost required to break the safe. The problem with this is defining cost. For example, what is the cost of someone reading my diary? Or perhaps more reasonable for business what is the cost of a 133t|st breaking into the FTP account for my web space and putting a giant penis on the main page? This cost to the business is *something* but what that something is requires some black magic to establish. What if someone worked out an ingenious combination of attacks who's costs by themselves are far greater than the

sci.crypt: Re: What does Security include?

cost of the thing your protecting but together their cost is much lower? How can we anticipate these costs?

In almost all of classical cryptography we can adopt the former definition. For example, if someone found a break on AES that could recover the key with 2^{64} known plain-texts and around 2^{80} work we'd all consider it broken simply because it was designed to require 2^{128} work to break. However, the situation is different in the real world in that we have to adopt the latter definition to get any work done. Given truly huge resources, stealing money from a bank is child's play. The point is that few have the resources to do the job trivially and it's this realisation that changes the game. Now we want to make the problem as hard as we can for the most number of people and in doing so (hope to) reduce the risk of a break.

Someone once said: "In theory, theory and practice are the same. In practice, they are not"

The different definitions come from this difference.

Simon.