

RE: Biometrics

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-07/0243.html>

From: Vinsik, Steven C (*Steven.Vinsik_at_unisys.com*)

Date: 07/18/05

Date: Mon, 18 Jul 2005 14:56:48 -0400

To: "Ansgar -59cobalt- Wiechers" <bugtraq@planetcobalt.net>, <security-basics@securityfocus.com>

-----Original Message-----

From: Ansgar -59cobalt- Wiechers [mailto:bugtraq@planetcobalt.net]

Sent: Wednesday, July 13, 2005 10:44 AM

To: security-basics@securityfocus.com

Subject: Re: Biometrics

On 2005-07-12 Vinsik, Steven C wrote:

- > *Good point in bringing up potential security issues with biometrics.*
- > *Biometrics are certainly not a cure all for security, but should be*
- > *considered as another layer in a layered security approach. I also*
- > *agree that a compromised biometric presents a serious problem, but if*
- > *multi-factor authentication is employed, then a single point of*
- > *compromised authentication does not allow access.*

I brought this up mainly because the OP was talking about password elimination.

- > *The only time I would recommend using a biometric as the sole*
- > *authentication mechanism would be in a low security/ low risk*
- > *situation where a compromise would have a minimal impact.*

Even then I would rule out fingerprint systems. Fingerprints are great for police work (because people tend to leave them around), but they are not very good for authentication purposes (for the very same reason).

Forensic fingerprint analysis and fingerprint authentication are two completely different applications. As an example of a low security fingerprint authentication, I would look at admission to Disney World. They have used a finger geometry biometric system for season pass holders for years. It is a low security and low risk implementation of utilizing biometric technology.

- > *While it is true that fingerprints can be acquired and possibly*
- > *copied, I would consider it far more difficult for an outsider to*
- > *acquire a persons' fingerprint and successfully recreate it to log*
- > *into a system remotely. An insider may have an easier time of*

SecurityFocus BASICS: RE: Biometrics

- > *acquiring the latent fingerprint from a co-worker, but the task of*
- > *re-creating this image into a workable fake finger is difficult.*

No. In fact it's relatively easy. Please read the article about forging fingerprints I mentioned in my previous mail. It describes *one* way of doing that (there are several others).

[...]

- > *Many of the fingerprint readers of today, which are of any quality,*
- > *have built in mechanisms to detect when a fake finger is placed on the*
- > *fingerprint reader platen. While this is certainly not foolproof and*
- > *there are always exceptions to the rule, I would submit that a*
- > *fingerprint is in general going to be more secure than a password.*

Most definitely not. There are *far* too many ways to trick fingerprint readers into accepting a forged fingerprint. Not to mention FAR and FRR.

There are ways to trick a fingerprint reader, but they can enhance an existing security infrastructure.

The bottom line of the point I was trying to make is that biometrics can provide increased security in a layered security approach. It is much better to use: Something you have (a card), something you know (a PIN), and something you are (a biometric) then it is to only use one or two of these options by itself.

Regards
Ansgar Wiechers

--

"All vulnerabilities deserve a public fear period prior to patches becoming available."

--Jason Coombs on Bugtraq