

# RE: [Full-disclosure] RE: [ISN] How To Save The Internet

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-03/0790.html>

---

*Glenn\_Everhart\_at\_bankone.com*

*Date:* 03/23/05

Date: Wed, 23 Mar 2005 15:41:01 -0500

To: <Arndt.WA@forces.gc.ca>, <jasonc@science.org>, <gillett david@fhda.edu>, <jericho@attrition.on

The point might be better made here that we have many security models that assume that whatever runs on a box is run at the behest of the person using the box. In reality lots of what runs (particularly mobile code but there exist many examples) is not running as the agent of the box owner nor of the person using the box (who may be the same, maybe not). They are in effect independent agents, but not humans.

Logically they should be controllable and should have access controls a box owner may assign so that their access permissions are granted as one might grant a guest, hostile alien, mad dog, best friend, employee, or whatnot. I see VERY few cases where anyone in the industry (security or computer) has taken this seriously.

That a consumer might prefer to buy only a system where he can make all these decisions is a related issue. (Ditto for corporations.) Also whether the current legal morass over intellectual property is of social value is another issue.

That the need to recognize the existence of multiple subjects of very different trust levels in a computer system exists, is clear. The number of systems that do so is not so large as is needed.

A heritage of systems designed as multi-user from the get-go should help support such distinctions (as a single-user design heritage may not) because more subsystems will be designed expecting to be able to run in isolated and non-God-privileged accounts. Still, over-reliance on accounts running as "local system" or "root" or the like undermines such separation, and while there have been a number of attempts at identifying autonomous code (including some of my own), there's certainly not much of that kind of control in popular OS releases.

Nor is there much up-front discussion for consumers of what they can control, what someone wants to control in spite of them, and what choices they need to exert.

Full-Disclosure: RE: [Full-disclosure] RE: [ISN] How To Save The Internet

One last bit: I have seen numerous cases, where companies were providing supposedly secure and needed subsystems whose control they did not want their users touching, where such systems caused chaos or totally undermined system security. This was not only on PCs; various model mainframes, including IBM, were involved in some of the horror stories. As a result I feel very uncomfortable about a notion that someone wants control over my computer, which can function despite all I may do, to run his private code. Once bitten, twice shy. Or should I say: "fool me once, shame on you. Fool me twice, shame on me." ?

Glenn Everhart

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

From: full-disclosure-bounces@lists.grok.org.uk  
[mailto:full-disclosure-bounces@lists.grok.org.uk] On Behalf Of  
Arndt.WA@forces.gc.ca  
Sent: Wednesday, March 23, 2005 11:24 AM  
To: jasonc@science.org; gillett david@fhda.edu; jericho@attrition.org  
Cc: sberinato@cio.com; full-disclosure@lists.grok.org.uk; isn@c4i.org;  
bugtraq@securityfocus.com  
Subject: [Full-disclosure] RE: [ISN] How To Save The Internet

Jason Coombs wrote:

- >
- > *David Gillett wrote:*
- > > *are the various rights of the owner*
- > > *of the CPU, the \*operator\* of the*
- > > *CPU, and the owner of the \*data\*,*
- > > *each of whom may have a more or*
- > > *less legitimate say in what code*
- > > *actually gets executed.*
- >
- > *Nonsense. Absurd, ridiculous nonsense.*
- >
- > *There is only one party who has any say over what code gets*
- > *executed by a CPU: the owner of that physical property.*
- >
- > *Everyone else can go fly a kite.*

Hold on. If you're dealing with a large company or government department, who "physically owns" the computer in question, you can't tell me that they're going to micromanage exactly what goes on with that system. They'll delegate the authority off to someone who'll actually run the equipment. That sounds like an "\*operator\* of the CPU" to me...

- >
- > *Take your intellectual property fantasies and your heady*
- > *legal concerns to law school, they have no place in security*
- > *technology.*

I don't read "intellectual property" anywhere in David's position at all. He quite rightly separates the three obvious stakeholders in any computer system, be it a desktop or a huge data storage facility.

When you're dealing with a system that's primary function is serving up reams of data (say a database), the access to that data will involve someone running "code" (read: an application). This access cannot be controlled solely by the maintainer of the computer(s) and other equipment that make up the DB. Similarly, isn't going to be the DBA, who's role is to maintain the data contained in the DB, either. In this example, a user running queries against that DB is exercising control and most certainly has a "say in what code actually gets executed" as a result. I don't think I need to point out that this user could even be someone external to your organisation, but I will anyway...

>  
<Snip out Intellectual Property driven rant>

I'm not trying to flame or troll here. I just think that in the world we live in now, where computers (and the CPUs they contain) are "operated" by various stakeholders, it is a hard sell to say that only one entity controls the resources in question. As the "owner" of the CPU, you might be able to say when it will be available (NO, I don't like you. Power off), but this won't help the bottom line. Same thing with an the folks assigned the role of "operator" – they're there to enable the business, not impede it. Users, be they your own or the customers your system is designed to serve, will always get a say. The issue here, as I see it, is to properly govern how the rights assigned.

Like it or not, we're all here to ultimately make the end users happy. Besides, isn't security supposed to support and improved your operations? Your approach would, IMHO, do the opposite...

Alex Arndt  
CISSP, GCIA

---

Full-Disclosure – We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia – <http://secunia.com/>

\*\*\*\*\*  
This transmission may contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. If you received this transmission in error, please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. Thank you  
\*\*\*\*\*

Full-Disclosure: RE: [Full-disclosure] RE: [ISN] How To Save The Internet

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>