

Re: [Full-disclosure] comparing information security to other industries

## Re: [Full-disclosure] comparing information security to other industries

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-12/msg00364.html>

---

- *From:* coderman <coderman@xxxxxxxx>
  - *Date:* Tue, 19 Dec 2006 14:10:24 -0800
- 

On 12/19/06, Valdis.Kletnieks@xxxxxx <Valdis.Kletnieks@xxxxxx> wrote:

On Tue, 19 Dec 2006 12:16:29 PST, KT said:

So we have been dealing with information security from last 20 years

i'd argue this is closer to 40 years than 20. [0]

20 years after the first automobile, we'd gotten as far as a Model A or T or so.

1885 [1] to 1965 [2] for decent auto security. 80 years? add 10 years if you consider air bags the requisite threshold.

(Incidentally, the fact that we still have a lot of security issues isn't actually a software problem, so much as an innate lack of tools to help humans understand *\*any\** complex system, be it software, or the economy, or global climate, or....)

i argue that the vast majority of insecure computing problems are indeed software problems, in the sense that proper software design and development would fix them. consider the automobile theme, where a wheel, some pedals, and a few signalling levers allow you to operate a vehicle with more computers and technology than space faring vehicles from a mere 30 years past. these machines are usable and secure, despite their mind boggling technological complexity brought about over a hundred years of evolutionary and radical improvement.

let's side step the economics and inertia of existing software / IT practice and look at a future utopia for sake of argument:

Re: [Full-disclosure] comparing information security to other industries

Re: [Full-disclosure] comparing information security to other industries

A: usability is requirement #1 for security [3]. is configuring that IPsec IKE/ISAKMP key distribution and re-key policy iPod (tm) simple? how about generating PKI infrastructure for those OpenVPN connections? "security" products are so ridiculously complicated it's a wonder anyone is able to use them. for a good laugh, write down the steps required to configure full disk encryption and a strong VPN from your laptop to a server. LOL, ROFFLE, etc.

B: capability based computing is the norm, as identity based access control is fundamentally flawed [4]. if you've only heard of capability based security in passing, consider this an underscore of the systemic and pervasive nature of our willful ignorance of good practice.

C: consumers can recognize and compare the merits of security built into systems they use, with producers willing and able to emphasize security considerations during design, implementation, testing, and support/integration phases of production and life cycle [5].

99.5% of existing problems disappear in such a world, leaving mostly insider fraud to be addressed via process and policy. we can get there, but it ain't gonna happen soon...

0. "Capability-Based Computer Systems – Chap. 3 Early Capability Architectures"  
<http://www.cs.washington.edu/homes/levy/capabook/>  
[ref: Dennis and Van Horn @ MIT using Capabilities to describe secure composition in 1966]

1. "History of the Automobile"  
[http://en.wikipedia.org/wiki/History\\_of\\_the\\_automobile](http://en.wikipedia.org/wiki/History_of_the_automobile)

2. "Unsafe at Any Speed"  
[http://en.wikipedia.org/wiki/Unsafe\\_at\\_Any\\_Speed](http://en.wikipedia.org/wiki/Unsafe_at_Any_Speed)

3. "Secure Interaction Design"  
<http://www.ischool.berkeley.edu/~ping/sid/>

4. "Capability Security Model"  
<http://c2.com/cgi/wiki?CapabilitySecurityModel>

5. "Build Security In"  
<https://buildsecurityin.us-cert.gov/>

---

Full-Disclosure – We believe in it.

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

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