

[Full-disclosure] comparing information security to other industries –

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-12/msg00369.html>

- *From:* Albert <caruabertu@xxxxxxxx>
 - *Date:* Wed, 20 Dec 2006 10:41:38 +0100
-

my mileage differs.

Far east competition using quality engineering and giving >2 years guarantees around the 1980s made the crucial difference, not the intervening >120 years since the invention of the modern car engines OTTO DIESEL and WANKEL.

cf.: http://en.wikipedia.org/wiki/Timeline_of_motor_and_engine_technology

In 1973 most cars sold were as buggy as software is today. New models suffered from design faults, poor choice of materials and mass recalls were the order of the day.

20 years is thus more like the time needed for the complex machinery to be made reliable, given the right legal penalties and consumer pressures.

p.s. Nowadays, cars have not one but several processors and computers inside these days – and are still reliable and resilient, easy to use etc...

regards
Albert

|-----Original Message-----

|From: coderman [<mailto:coderman@xxxxxxxx>]

|Sent: 19 December 2006 23:10

|To: Valdis.Kletnieks@xxxxxx

|Cc: KT; full-disclosure@xxxxxxxxxxxxxxxxxxxx; websecurity@xxxxxxxxxxxxxxxx

|Subject: [WEB SECURITY] comparing information security to other industries –

|
|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:

|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

[Full-disclosure] comparing information security to other industries –

| 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

| 2. "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/>

The Web Security Mailing List:

| <http://www.webappsec.org/lists/websecurity/>

| The Web Security Mailing List Archives:

| <http://www.webappsec.org/lists/websecurity/archive/>

| <http://www.webappsec.org/rss/websecurity.rss> [RSS Feed]

Full-Disclosure – We believe in it.

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

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