Cybersecurity and standards

A safe connected world
Summary:

This talk will elaborate on the ever increasing need to show transparency and trustworthy from product vendors and service providers, showing how standards and third party certification play a critical role in the provision of this trust.
This survival of the fittest, which I have here sought to express in mechanical terms, is that which Mr. Darwin has called 'natural selection', or the preservation of favoured races in the struggle for life.

Herbert Spencer, 1864
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-Time</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Real-Time AntiVirus</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual Virus Scanning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Anti-Spyware</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Anti-Worm</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Anti-Trojan</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Extra Features</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery Mode</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Tech Support</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Source: https://www.top10antivirussoftware.com/software-comparison
COMMON CRITERIA: Start selling into these markets

What Is Common Criteria:

Common Criteria is an internationally recognized set of guidelines (ISO 15408), which define a common framework for evaluating security features and capabilities of Information Technology security products. It provides assurance to buyers that the process of specification, implementation, and evaluation for any certified solution was conducted in a thorough and standard manner.

The National Information Assurance Acquisition Policy, NSTISSP No. 11, requires government agencies to purchase only those commercial security products that have met specified third-party assurance requirements and have been tested by an accredited national laboratory.

Common Criteria allows you to sell into the U.S. Federal Government, International Governments, and highly regulated industries around the globe. It is not only required for access to government markets, but also serves as a competitive differentiator.

Source: www.corsec.com
Three cases

Source: https://en.wikipedia.org/wiki/Darwin%27s_finches
In the wrong place at the wrong time

Russian Hackers Stole NSA Data on U.S. Cyber Defense

The breach, considered the most serious in years, could enable Russia to evade NSA surveillance and more easily infiltrate U.S. networks

By Gordon Lubold and Shane Harris
Updated Oct. 5, 2017 7:31 p.m. ET
WASHINGTON—Hackers working for the Russian government stole details of how the U.S. penetrates foreign computer networks and defends against cyberattacks after a National Security Agency contractor removed the highly classified material and put it on his home computer, according to multiple people with knowledge of the matter.

ars TECHNICA

LEAKY LEAKS —
Russia reportedly stole NSA secrets with help of Kaspersky—what we know now

Proven or not, the accusations almost certainly mean the end of Kaspersky as we know it.

Kaspersky sues US government over federal software ban

It believes it didn't get a fair shake amid fears of Russian influence.

Trump signs bill banning Kaspersky from US government systems

Kaspersky no longer legal on US public sector networks
Kaspersky Lab announces comprehensive transparency initiative

- **INDEPENDENT SOURCE CODE REVIEW**
  To start by Q1 2018, undertaken with an internationally recognized authority

- **INDEPENDENT REVIEW OF INTERNAL PROCESS**
  To verify integrity of our solutions and processes

- **THREE TRANSPARENCY CENTERS WORLDWIDE IN THREE YEARS**
  Enabling clients, government bodies & concerned organizations to review source code, update code and threat detection rules.
  First center in 2018, 3 centers by 2020, in Asia, Europe and the U.S.

Kaspersky Lab — We have nothing to hide!

Russia-based Antivirus firm hits back with what it calls a "comprehensive transparency initiative" to allow independent third-party review of its source code and internal processes to win back the trust of customers and InfoSec community.
Enough is enough?

https://msdn.microsoft.com/en-us/magazine/mt795185
https://blogs.kde.org/2013/06/19/really-source-code-software
https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise
https://wiki.debian.org/ReproducibleBuilds
A new best practice to protect technology supply chain integrity

March 22, 2017

At Microsoft, we have developed a way to definitively demonstrate that a compiled machine-readable executable was generated from the same human-readable source code that was reviewed. It’s based on the concept of a “birth certificate” for binary files, which consists of unique numbers (or hash values) that are cryptographically strong enough to identify individual source code files.
Enough is enough!

New poll reveals Facebook's standing with Americans has slumped after Cambridge Analytica scandal

Technology

Facebook scandal 'hit 87 million users'

4 April 2018

Mark Zuckerberg, the Facebook founder and CEO. Credit: Reuters/Robert Galbraith

Americans less likely to trust Facebook than rivals on personal data

Reuters Staff
The Facebook-Cambridge Analytica apology tour continues, with full-page ads in major newspapers

“I promise to do better for you,” CEO Mark Zuckerberg says in the ads.

Facebook COO Sheryl Sandberg To CNBC: “We’re Open To Regulation”
Thesis:

The survival is for the trustworthiest.

Assertion:

Third party scrutiny and evaluation is the best path to trustworthiness.
You like potato and I like potahto.
Standards come into play

Standards are documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.

Regulators and governments count on ISO standards to help develop better regulation, knowing they have a sound basis thanks to the involvement of globally-established experts.

The approach and need for standards may be different, but we have a common need for them.

Source: ISO
Third party certification comes into play

The cost of low trust is going to put companies out of business.

Self declaration of trustworthiness seems not to be sufficient nowadays. Each daily summary of product vulnerabilities and company pitfalls is a sound proof.

The front-end integrators, product vendors and service providers need to start mitigating their supply chain risks if they want to survive.

Third party participation is required in all aspects of trust building: standards development, verification, validation and certification of technology, processes and services.
Thank you

Miguel Bañón
Global Technology Leader for Cybersecurity

mbp@epoche.es