Cybersecurity and standards

A safe connected world

DEKRA

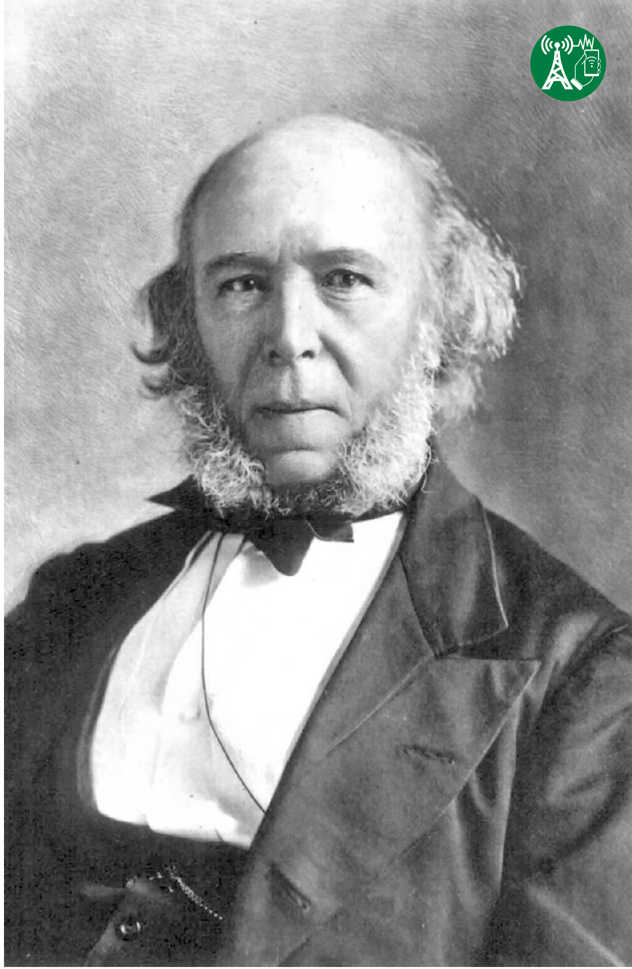
Summary:

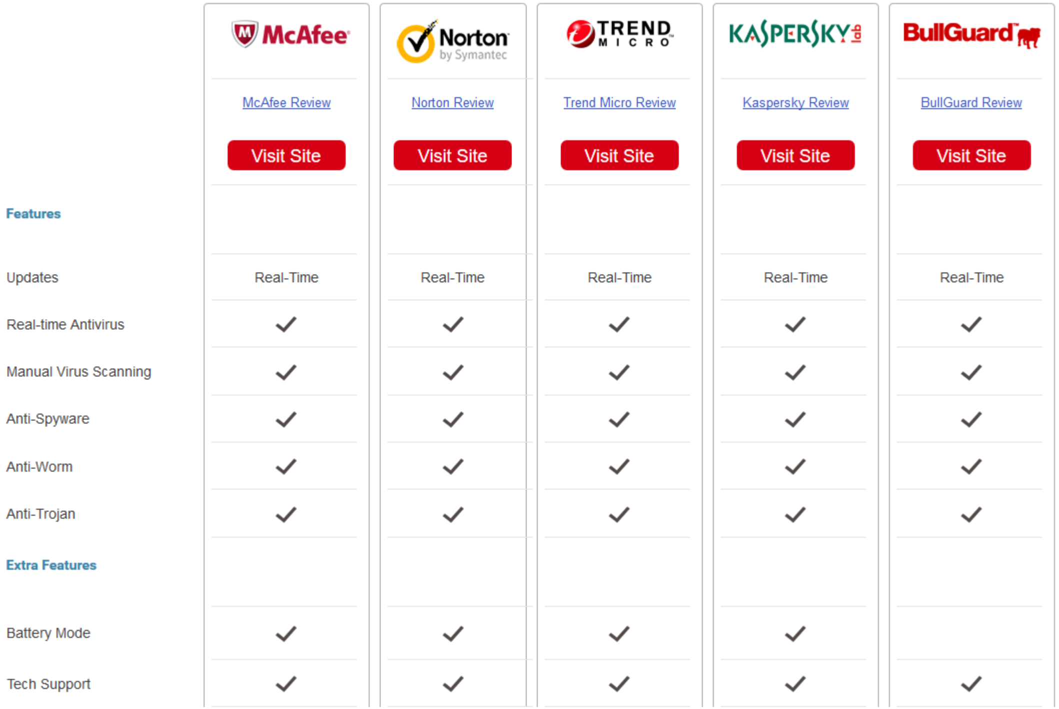
This talk will elaborate on the ever increasing need to show transparency and trustworthy from product vendors and service providers, showing how standards and third party certification play a critical role in the provision of this trust.

DEKRA

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.

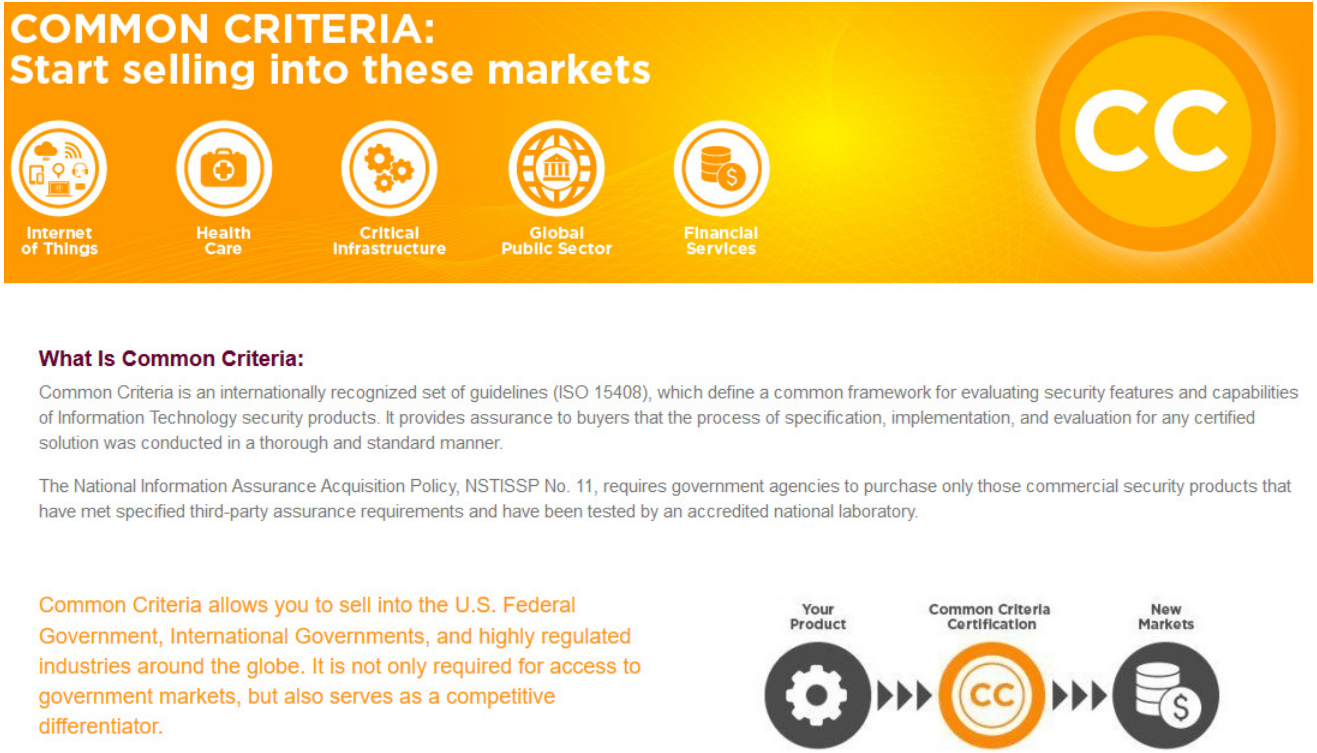
Herbert Spencer, 1864





	McAfee	Norton by Symantec	TREND MICRO	KASPERSKY lab	BullGuard
	McAfee Review	Norton Review	Trend Micro Review	Kaspersky Review	BullGuard Review
	Visit Site	Visit Site	Visit Site	Visit Site	Visit Site
Features					
Updates	Real-Time	Real-Time	Real-Time	Real-Time	Real-Time
Real-time Antivirus	✓	✓	✓	✓	✓
Manual Virus Scanning	✓	✓	✓	✓	✓
Anti-Spyware	✓	✓	✓	✓	✓
Anti-Worm	✓	✓	✓	✓	✓
Anti-Trojan	✓	✓	✓	✓	✓
Extra Features					
Battery Mode	✓	✓	✓	✓	
Tech Support	✓	✓	✓	✓	✓

Source: https://www.top10antivirussoftware.com/software-comparison



COMMON CRITERIA:
Start selling into these markets

What Is Common Criteria:

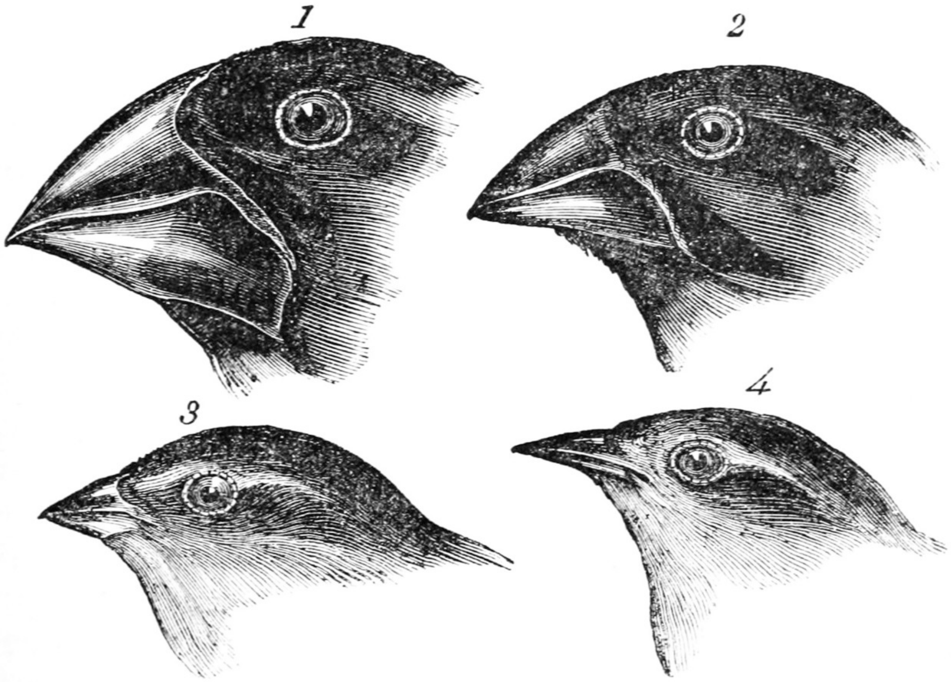
Common Criteria is an internationally recognized set of guidelines (ISO 15408), which define a common framework for evaluating security features and capabilities of Information Technology security products. It provides assurance to buyers that the process of specification, implementation, and evaluation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

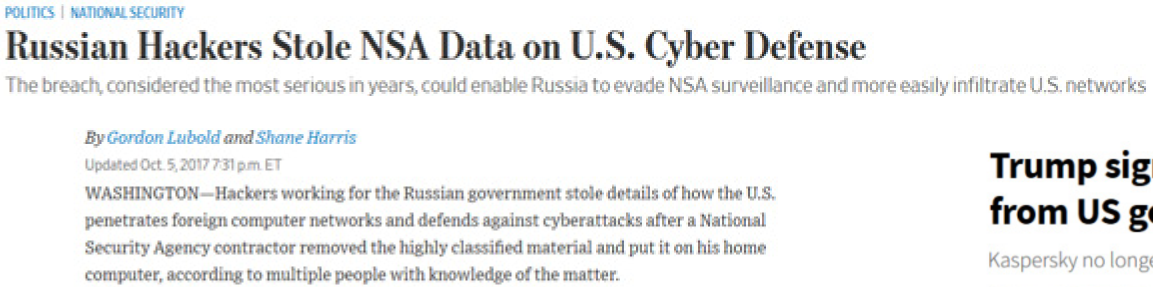


1. Geospiza magnirostris.
3. Geospiza parvula.

2. Geospiza fortis.
4. Certhidea olivasea.

Source: https://en.wikipedia.org/wiki/Darwin%27s_finches

In the wrong place at the wrong time



POLITICS | NATIONAL SECURITY

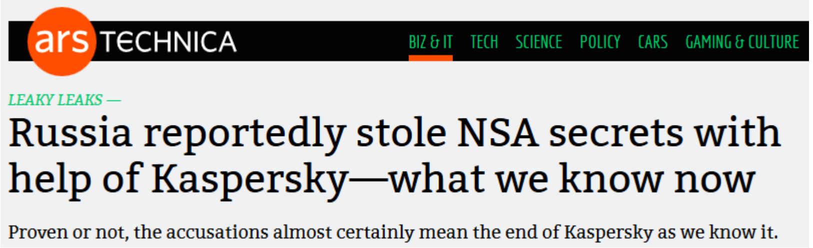
Russian Hackers Stole NSA Data on U.S. Cyber Defense

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

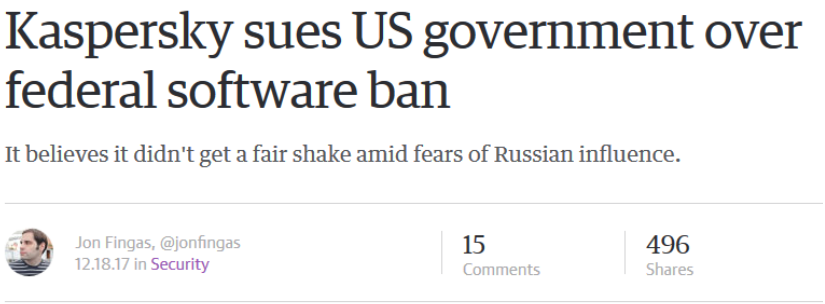
WASHINGTON—Hackers working for the Russian government stole details of how the U.S. penetrates foreign computer networks and defends against cyberattacks after a National Security Agency contractor removed the highly classified material and put it on his home computer, according to multiple people with knowledge of the matter.



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.



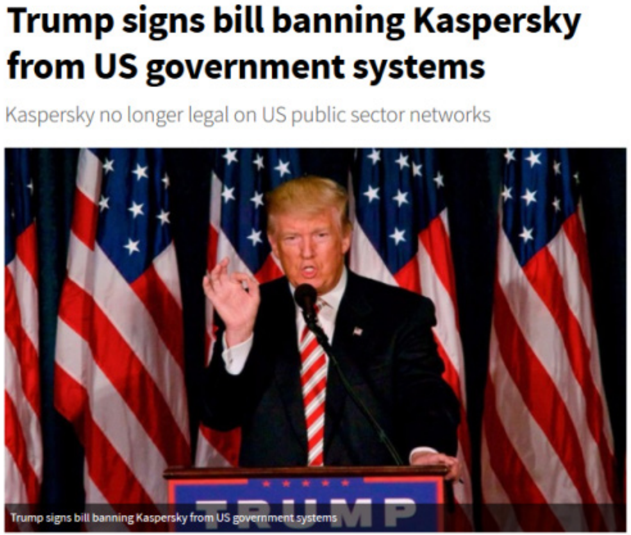
Kaspersky sues US government over federal software ban

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

Jon Fingas, @jonfingas
12.18.17 in Security

15 Comments

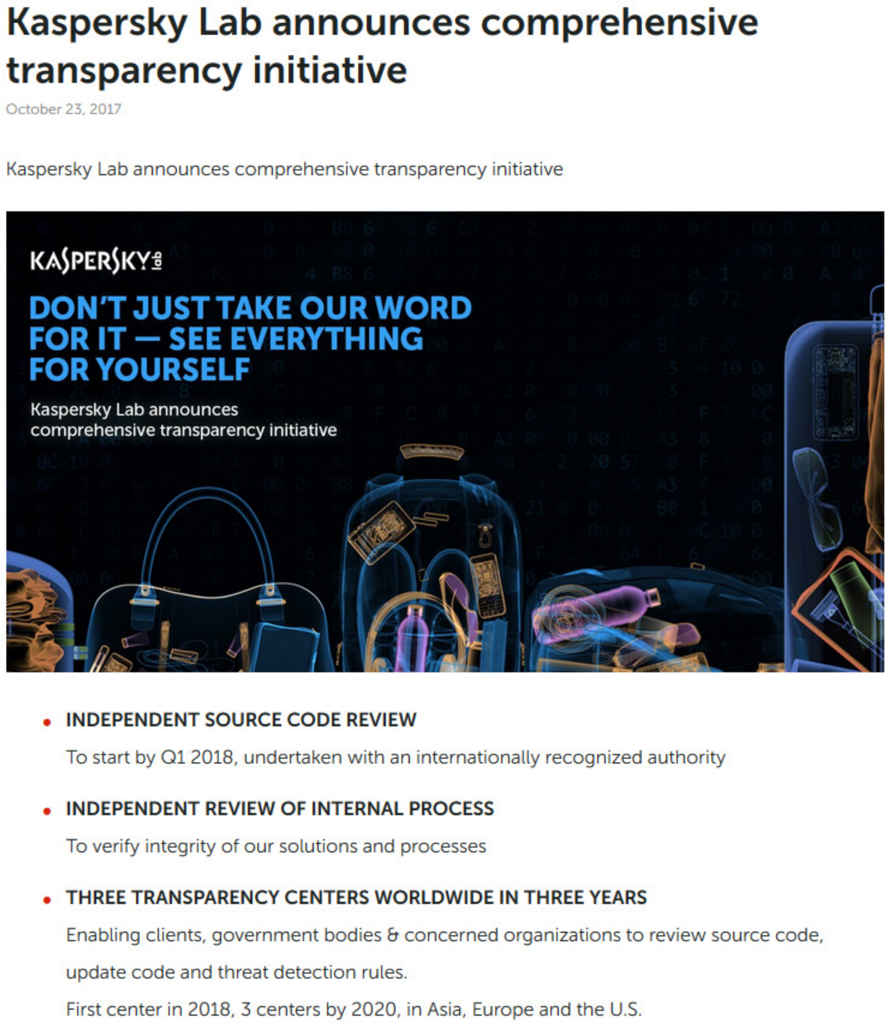
496 Shares



Trump signs bill banning Kaspersky from US government systems

Kaspersky no longer legal on US public sector networks

Trump signs bill banning Kaspersky from US government systems



Kaspersky Lab announces comprehensive transparency initiative

October 23, 2017

Kaspersky Lab announces comprehensive transparency initiative

KASPERSKY lab
DON'T JUST TAKE OUR WORD FOR IT — SEE EVERYTHING FOR YOURSELF
Kaspersky Lab announces comprehensive transparency initiative

- **INDEPENDENT SOURCE CODE REVIEW**

  To start by Q1 2018, undertaken with an internationally recognized authority

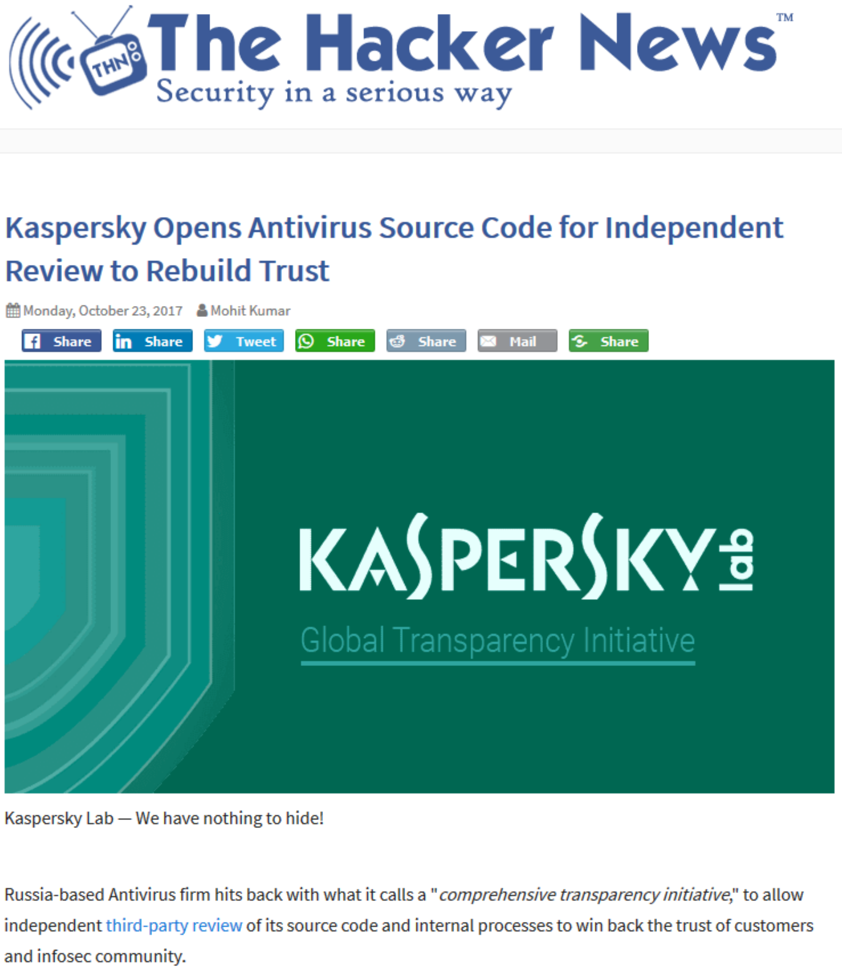
- **INDEPENDENT REVIEW OF INTERNAL PROCESS**

  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.



The Hacker News™

Security in a serious way

Kaspersky Opens Antivirus Source Code for Independent Review to Rebuild Trust

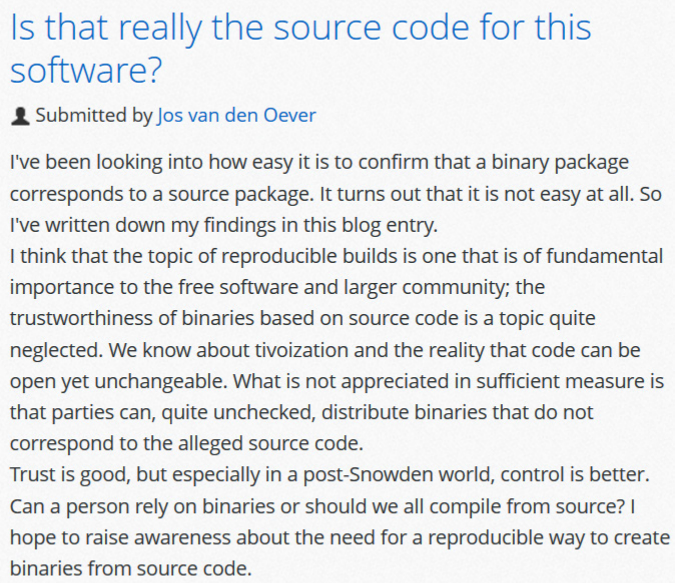
Monday, October 23, 2017 Mohit Kumar

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?

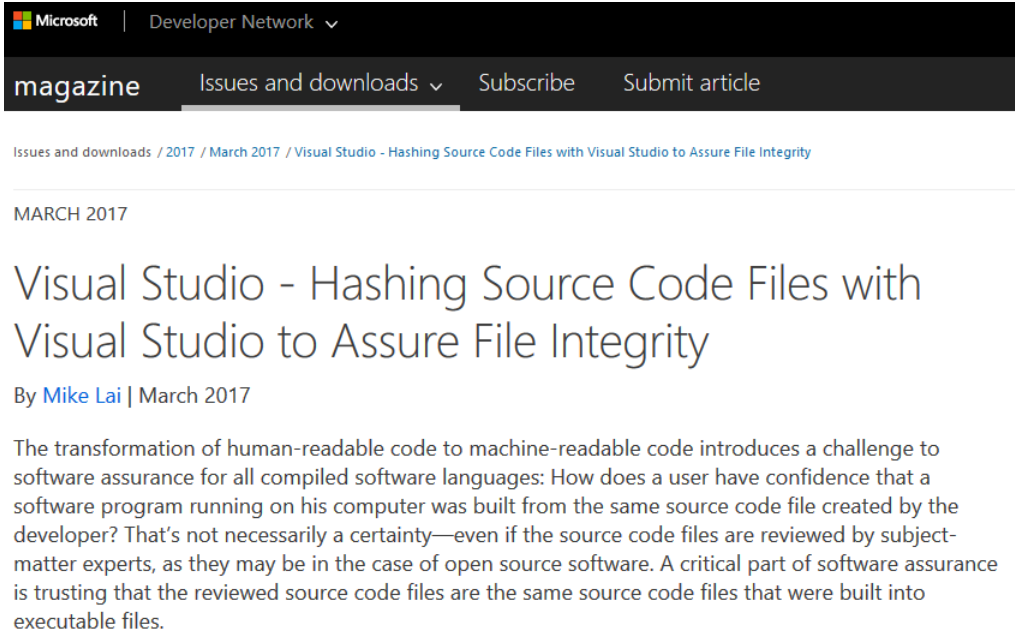
https://msdn.microsoft.com/en-us/magazine/mt795185
https://blogs.microsoft.com/microsoftsecure/2017/03/22/a-new-best-practice-to-protect-technology-supply-chain-integrity/ .
https://blogs.kde.org/2013/06/19/really-source-code-software
https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compromise
https://wiki.debian.org/ReproducibleBuilds



Is that really the source code for this software?

Submitted by Jos van den Oever

I've been looking into how easy it is to confirm that a binary package corresponds to a source package. It turns out that it is not easy at all. So I've written down my findings in this blog entry.
I think that the topic of reproducible builds is one that is of fundamental importance to the free software and larger community; the trustworthiness of binaries based on source code is a topic quite neglected. We know about tivoization and the reality that code can be open yet unchangeable. What is not appreciated in sufficient measure is that parties can, quite unchecked, distribute binaries that do not correspond to the alleged source code.
Trust is good, but especially in a post-Snowden world, control is better. Can a person rely on binaries or should we all compile from source? I hope to raise awareness about the need for a reproducible way to create binaries from source code.

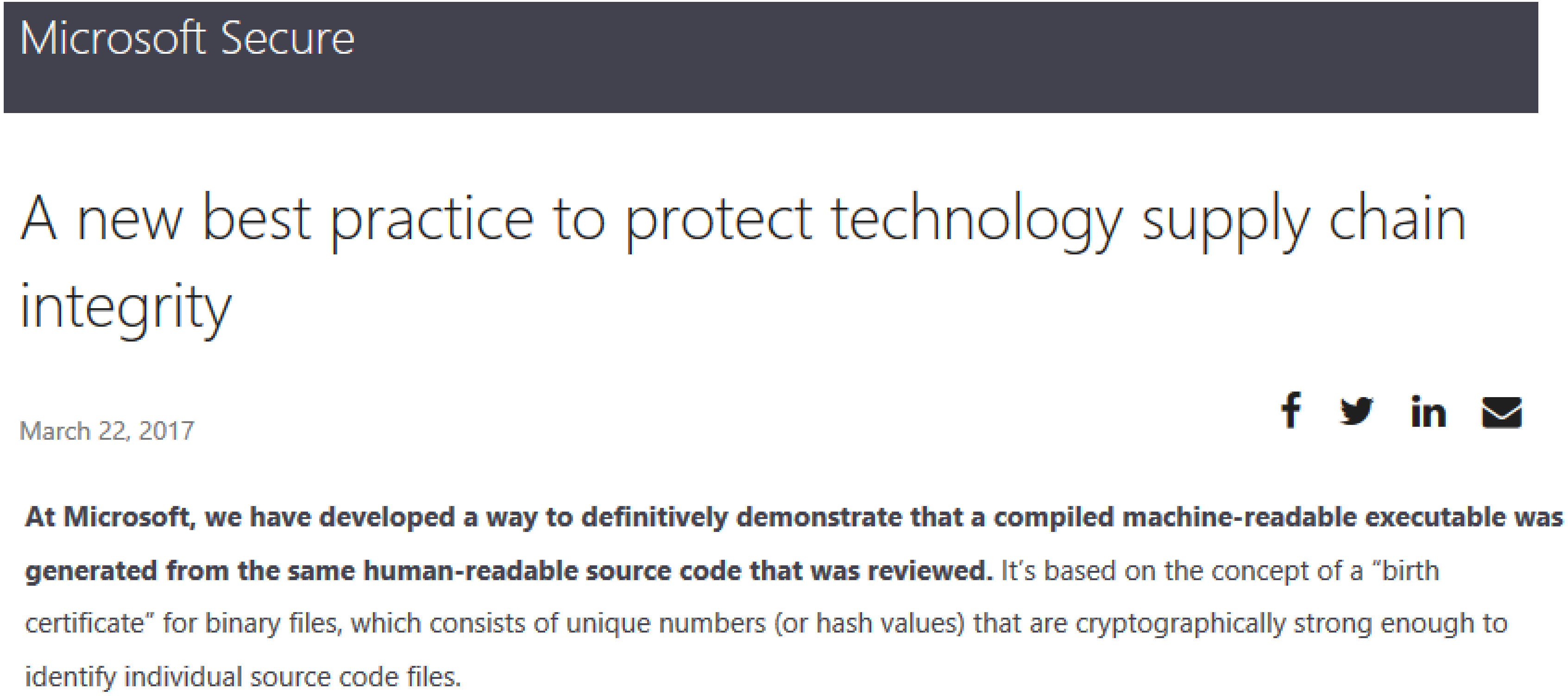

Microsoft
Developer Network
magazine
Issues and downloads
Subscribe
Submit article
Issues and downloads / 2017 / March 2017 / Visual Studio - Hashing Source Code Files with Visual Studio to Assure File Integrity

MARCH 2017

Visual Studio - Hashing Source Code Files with Visual Studio to Assure File Integrity

By Mike Lai | March 2017

The transformation of human-readable code to machine-readable code introduces a challenge to software assurance for all compiled software languages: How does a user have confidence that a software program running on his computer was built from the same source code file created by the developer? That's not necessarily a certainty—even if the source code files are reviewed by subject-matter experts, as they may be in the case of open source software. A critical part of software assurance is trusting that the reviewed source code files are the same source code files that were built into executable files.



Microsoft Secure

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

Mark Zuckerberg, the Facebook founder and CEO CREDIT: REUTERS/ROBERT GALBRAIT

Technology

Facebook scandal 'hit 87 million users'

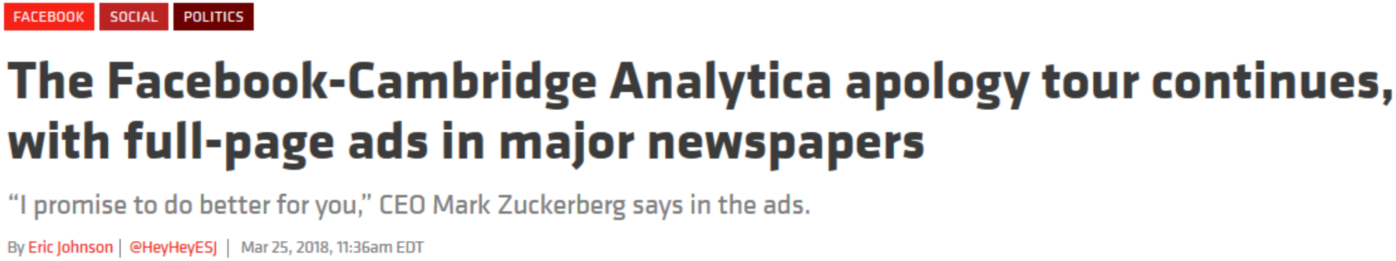
4 April 2018

BUSINESS NEWS MARCH 25, 2018 / 10:55 AM / 10 DAYS AGO

Americans less likely to trust Facebook than rivals on personal data

Reuters Staff

4 MIN READ

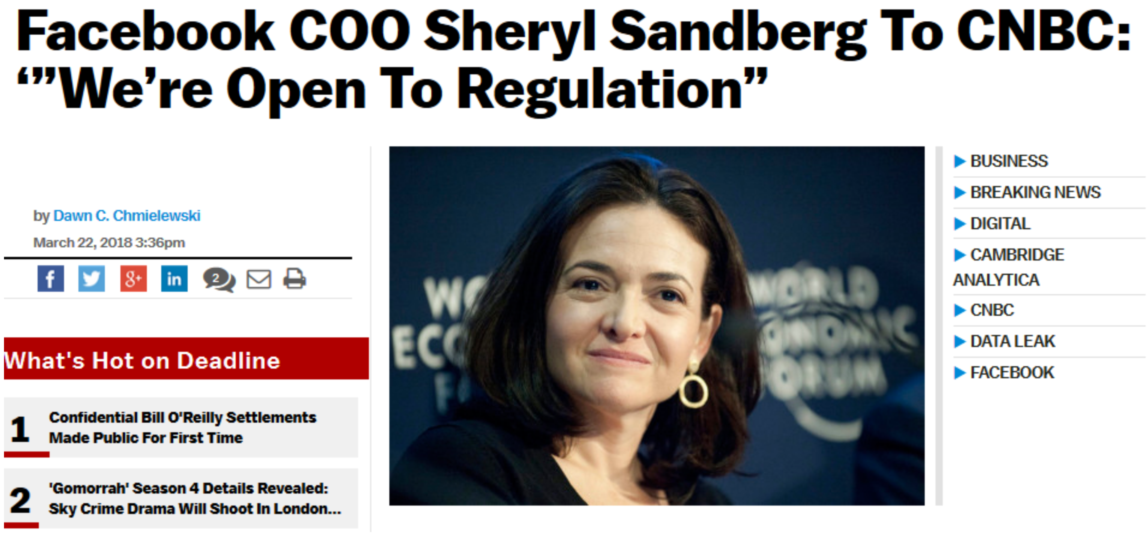


FACEBOOK SOCIAL POLITICS

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.

By Eric Johnson | @HeyHeyESJ | Mar 25, 2018, 11:36am EDT



Facebook COO Sheryl Sandberg To CNBC: "'We're Open To Regulation"

by Dawn C. Chmielewski

March 22, 2018 3:36pm

What's Hot on Deadline

1 Confidential Bill O'Reilly Settlements Made Public For First Time

2 'Gomorrah' Season 4 Details Revealed: Sky Crime Drama Will Shoot In London...

- ▶ BUSINESS
- ▶ BREAKING NEWS
- ▶ DIGITAL
- ▶ CAMBRIDGE ANALYTICA
- ▶ CNBC
- ▶ DATA LEAK
- ▶ FACEBOOK

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

DEKRA

Third party certification comes into play

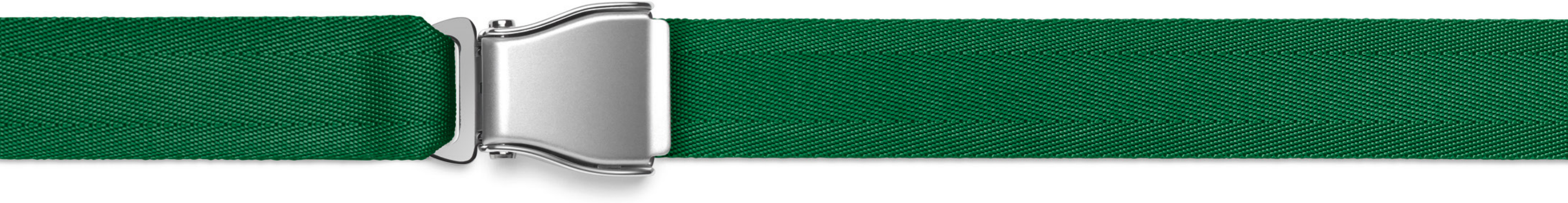
The cost of low trust is going to put companies out of business.

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