EXECUTIVE UPDATE
Data Analytics & Digital Technologies, Vol. 21, No. 13

CUTTER CONSORTIUM
Access to the Experts

Fiducia ex Machina

by Jon Geater

There is huge potential for transformation and innovation in businesses all across the value chain if they can automate operations with artificial intelligence (AI) and intelligent processes. But something is holding this back, and often the reasons cited are security risks and trust issues. Many think that the more power that we vest in machines, the more harm they will do. But, as we explore in this *Executive Update*, what if we could reverse that? What if we could harness AI and other digital technology to achieve *fiducia ex machina:* "trust from the machines"?

You are likely familiar with the phrase *deus ex machina*: "god out of the machine." Great thinkers from as far back as Aristotle been using it as a plot device in their stories to describe a surprising, almost miraculous event that solves seemingly impossible problems. Just when all seems lost, the world is saved.

What if we could harness AI and other digital technology to achieve fiducia ex machina: "trust from the machines"?

More recently, Alex Garland's 2014 film *Ex Machina* brings a much more literal interpretation to the words to chronicle the god-like rise in power of AI machines, although with a much less positive outlook than the original Aristotelian ideal.

All too often, it's the latter interpretation that prevails: the more power that we vest in machines, the more harm they will do. But what if we could reverse that? What if we could harness AI and other digital technology to achieve *fiducia ex machina*: "trust from the machines"? Major governments around the world are starting to believe we can.

Understanding Digital Transformation

Talk of digital transformation, Industry 4.0, and data-driven business models abound, but it seems much less is truly happening. Digital transformation is much more than just taking an existing business model and putting it on the Internet: to get the benefits, it's essential to change the business to be oriented around system-wide data exchange, automating operations with AI and intelligent processes.

As such, there is huge potential for efficiency and innovation in businesses all across the value chain — from raw materials through

The *Executive Update* is a publication of Cutter Consortium's *Data Analytics & Digital Technologies* practice. ISSN: 2381-8816.

manufacturing and service delivery — if they can connect and share operating information, demand/supply signals, service-quality information, and the like. But something is holding this back, and often the reason quoted is security risk. Technology is ahead of industry's appetite to use it.

To overcome this, there is a need to transform not just the business processes but also the IT technology that supports them. Typically, when security concerns arise the first reaction is to close things down, lock data away, reach for another firewall. But that maintains a perimeter silo mentality that prevents data from flowing while providing very incomplete protection for today's threat landscape.

Data-driven business models require the flow of data between partners, and so it follows that we need to switch the security focus from confidentiality — keeping data secret — to integrity and authenticity.

Data-driven business models require the flow of data between partners, and so it follows that we need to switch the security focus from confidentiality — keeping data secret — to integrity and authenticity: letting data flow, but always ensuring you know exactly where it came from and that the data you receive is truly the data that was sent. In other words: if data is the fuel of your AI machine, then make sure you are running on clean fuel from verified sources.

In my opinion, we are a very long way from truly intelligent machines — true AI — but what we do have in spades is a wasted potential for industrial automation and connectivity.

The 2021 US Executive Order on Improving the Nation's Cybersecurity

All this is slowly being understood by those in power.

Back in 2018, reflecting on the 2017 WannaCry attack and 1,000 other such incidents, the UK Joint Committee on the National Security Strategy called for "*resilience, not security,*" noting that:

> *... [it is] impossible to predict [changes in threat, the identification of vulnerabilities, and new methods of attack] far enough in advance to institutionally prepare for them all.*

The executive order highlights some technical fundamentals that are required to address the modern-day threat.

In May 2021, the US government published its "Executive Order on Improving the Nation's Cybersecurity." The order clearly lays out how the US, too, is moving to a model of traceable and active trust, away from the secret, black-box silos of the past:

> *In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.*

In addition to improvements in standards and operations, the executive order highlights some technical fundamentals that are required to address the modern-day threat: removing barriers to sharing threat intelligence, zero trust, and taming the software supply chain.

Removing Barriers to Sharing Threat Intelligence

All too often, businesses feel inhibited in sharing what they learn about weaknesses and vulnerabilities. For vendors it means admitting to mistakes and for users it means facing reputational damage and fines. The natural inclination is to downplay problems, but in the long run this doesn't help anyone. We need an environment that encourages fast and open communication of problems and a culture that is understanding of (occasional, honest) mistakes in digital provision.

Beyond the nuances of making selective disclosures within carefully curated stakeholder communities, the executive order speaks directly of lifting regulatory and contractual prohibitions on sharing for the greater good, removing a key area of fear for large businesses with liability worries.

Modernizing Security Approaches with Zero-Trust Architecture

There is no perfect security. Attackers will find weak links. Changes in the environment will produce new threats or change the economic calculus of risk. Formerly secure software will degrade and be found insecure sooner or later.

> *The "zero" does not suggest that there's no trust at all, but rather that there is nothing in which you have* absolute *trust.*

A zero-trust approach accepts this and chooses to focus on building systems that are safe in spite of this reality. It takes the view that no single component should be able to dictate or override the security of the whole system. The "zero" does not suggest that there's no trust at all, but rather that there is nothing in which you have *absolute* trust. Always verify before trusting. Build systems and processes with natural cross-checks and validation in them.

When it comes to operational and compliance data, this means always verifying your sources. Just because you trusted someone yesterday doesn't mean they're trustworthy today. If you need to rely on data for a long time (e.g., compliance data and handling trails) make sure it is stored in a tamper-evident and immutable store separate from the place you originally received it.

Improving Security of the Software Supply Chain

The last but most immediate area of focus is the digital supply chain. Recent high-profile attacks such as those on Solar Winds and Kaseya have shown how important it is to understand what is in your infrastructure and what risk it poses to your business.

Building in the idea that you can't secure what you can't see, the order calls for transparency and traceability of all components of the digital supply chain from software bills of materials (SBOMs) immediately to configurations, AI models, and live data in the future.

The requirement to publish and securely distribute SBOMs is a great starting point. This move clearly recognizes that software is only secure until it's not, but rather than eschewing innovation and holding industry back, we can now embrace innovation and fast-moving software while retaining the power to understand and control risks.

A New Target: Dynamic Resilience

By adopting the techniques espoused by the executive order, supply chain partners can exchange critical information quickly, meaning that everyone has the fullest context possible for making the best possible decisions.

In short, what all of this means is that instead of trying to predict and avoid every possible threat before embracing connectivity, we must move to accept that risks are unpredictable and dynamic, and that the best defense is to be alert to changes in circumstances, adaptive to changes in risk, and resilient in the face of failure.

So how to operationalize this? If a context-aware, dynamic approach is needed, then how do we get the best context into our dynamic decision-making machinery? This is where *collaborative operations* come in. By adopting the techniques espoused by the executive order, supply chain partners can exchange critical information quickly, meaning that everyone has the fullest context possible for making the best possible decisions.

Traditional security approaches are still relevant, of course, but they need to be deployed in a way that supports connectivity for the long term. Once again, rather than locking data away or getting too deep into device-centric security, large gains can be made by investing in tools and techniques that enable data exchange and concentrate on assurance of that data in these three dimensions:

1. **Provenance.** Do you know where your data came from, how it was generated, and what quality guarantees it has?

2. **Governance.** Can you control the flow of data so that it gets to all the right places at the right time while remaining protected?

3. **Immutability.** Can you go back and demonstrate what data you had on hand and justify decisions strongly in the case of an audit or dispute?

Trustworthy & Explainable AI

This value chain–wide sharing of trustworthy information in near real time is what should unlock the confidence required not only to make fast data-driven decisions, but even to automate them:

- **Sharing threat intelligence** delivers control and defenses to the good guys as quickly as possible, making bad guys work harder and shrinking their window of opportunity.
- **Zero trust** means important tasks can be delegated to machines and AI systems, confident that glitches in one will be caught by others.
- **Adding transparency to the digital supply chain** enables software innovation and choice to flourish while providing every stakeholder in the value chain with the opportunity to make their own strongly informed business risk–based decisions.
- **With demonstrable continuous assurance of the data exchanged,** new ways of working can stand up to existing audits and regulatory checks.

With collaborative operations enabled by these simple yet powerful techniques, I believe we can indeed build trust out of the machines.

About the Author

Jon Geater is cofounder and CTO of Jitsuin, where he applies his expertise in cryptography, cybersecurity, and blockchain to the challenging issues of the Internet of Things and digital transformation. With 20+ years' experience in commercial crypto, hardware, and cybersecurity — leading technology and product teams at the cutting edge of technology and security innovation — he is dedicated to furthering the industry through open collaboration and has founded/edited successful industry standards in the areas of trusted execution, trusted computing, payments cryptography, and enterprise key management. Mr. Geater has also served multiple terms in official leadership and technical positions at Digital Twin Consortium, Hyperledger, PCI Council, OASIS, GlobalPlatform, and TCG. Prior to these roles, he held senior global technical positions at Thales e-Security, Trustonic, ARM, and nCipher, where he built chip-to-cloud solutions for payments, mobile, aerospace, automotive, and industrial security while leading large global teams of experts innovating the next big thing in security. Mr. Geater also has hands-on experience in designing and implementing security for large direct expansion systems, such as the UK smart energy grid and the cybersecurity framework for the UK's only fully autonomous on-road, self-driving car trials. He can be reached at jon.geater@jitsuin.com.

About Cutter Consortium

Cutter Consortium is a unique, global business technology advisory firm dedicated to helping organizations leverage emerging technologies and the latest business management thinking to achieve competitive advantage and mission success. Through its research, training, executive education, and consulting, Cutter Consortium enables digital transformation.

Cutter Consortium helps clients address the spectrum of challenges technology change brings — from disruption of business models and the sustainable innovation, change management, and leadership a new order demands, to the creation, implementation, and optimization of software and systems that power newly holistic enterprise and business unit strategies.

Cutter Consortium pushes the thinking in the field by fostering debate and collaboration among its global community of thought leaders. Coupled with its famously objective "no ties to vendors" policy, Cutter Consortium's Access to the Experts approach delivers cutting-edge, objective information and innovative solutions to its clients worldwide.

For more information, visit www.cutter.com or call us at +1 781 648 8700.