NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

1999-2024 / 25 YEARS

The VAULT

25
secure
The VAULT
Security on the Move
ecitizen
transactions
next generation
Securing the world One application at a time
What's the next big choice for smart security?
Tailormade security: The right fit for government ID applications
SCORE!
THE SPECTRUM OF ID STANDARDS
APPLICATION TRICK OR TREAT?
Who will be first to mobilize your ID?

25 YEARS OF THE SILICON TRUST

1999
2024
The VAULT
Identity management goes global
MOBILE IDENTITIES
The BLOCKCHAIN Issue
BORDER CONTROL ALONG INTERNATIONAL STANDARDS
BRAVE NEW WORLD
THE BIOMETRICS ISSUE
A NEW DIGITAL FUTURE?
FIDO & AUTHENTICATION TECHNOLOGIES
NFT & NFC, ID & TOKENS
SECORA™ ID
REAL or FAKE
AUTHENTICATION & ACCESS CONTROL
POST-QUANTUM CRYPTOGRAPHY

GUEST OPINION

Preparing for THE FUTURE of *CYBERSECURITY:* *Navigating* NEW FRONTIERS and *protecting* what MATTERS

By Oliver Winzenried, CEO and Founder, WIBU-SYSTEMS AG

As technology evolves at an unprecedented rate, groundbreaking innovations such as quantum computing, synthetic biology, and brain-computer interfaces (BCIs) are set to reshape industries and redefine everyday life. However, each of these advancements brings new cybersecurity challenges that, if unaddressed, could have serious implications for individuals, businesses, and society.

In this article, we delve into six emerging technologies on the horizon, exploring the opportunities and cybersecurity risks they bring, and examining how Wibu-Systems can support and protect these developments with innovative solutions.

1. Quantum Computing

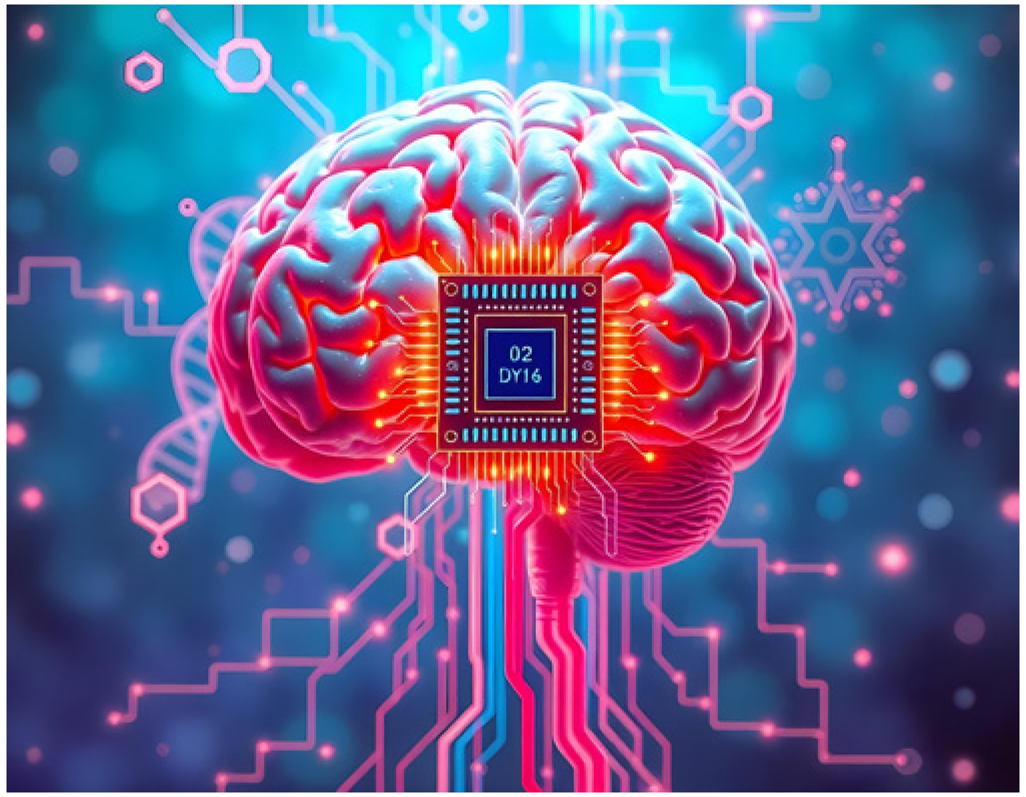
Quantum computing promises to be one of the most transformative advancements of our time, offering the potential to solve complex problems beyond the scope of traditional computers. Fields such as cryptography, climate modeling, and drug discovery could be revolutionized by its speed and processing power. However, quantum computing's power also presents risks: existing encryption standards, the backbone of modern cybersecurity, could become vulnerable.

The impact of quantum computing is twofold. In an ideal scenario, organizations proactively adopt quantum-resistant algorithms to keep data secure while benefiting from quantum's computational capabilities. However, if the development of quantum outpaces defense measures, it could lead to a cybersecurity crisis, potentially exposing sensitive information on a global scale. Wibu-Systems is actively preparing for this future by exploring quantum-resistant encryption for its solutions. By enhancing CodeMeter, its flagship technology, to counter quantum-based threats, Wibu-Systems is committed to ensuring data security for the post-quantum era.

2. Synthetic Biology and DNA Data Storage

Synthetic biology and DNA data storage represent a frontier in biotechnology, with potential applications in healthcare, environmental restoration, and data preservation. Through synthetic biology, scientists can design new organisms to address specific challenges, from waste consumption to resource production. DNA data storage, meanwhile, offers vast potential as an efficient, long-term medium with low energy needs.

However, synthetic biology raises concerns about intellectual property and biosecurity, as any vulnerability in the systems managing engineered organisms or storing DNA data could lead to unauthorized access or misuse. A future where synthetic biology is widely used could mean that sensitive bioinformatics and proprietary engineering techniques require protection from cyber threats. Wibu-Systems could secure synthetic biology applications and DNA storage solutions by managing access to software used in these fields, ensuring that only authorized users can interact with sensitive bioengineering processes or retrieve data from DNA storage.



3. Neuromorphic Computing

Neuromorphic computing, modeled after the human brain, enables highly efficient processing and self-learning capabilities. This technology has potential applications in autonomous vehicles, robotics, and real-time IoT, with the ability to process data quickly and with low energy demands. However, neuromorphic systems face unique cybersecurity challenges, as they require specialized security measures that go beyond traditional computing.

In the best scenario, neuromorphic computing enables smarter, faster systems across industries without compromising security. However, if neuromorphic devices lack adequate protections, they could be susceptible to unauthorized control or data manipulation, particularly in applications like autonomous vehicles or industrial machinery. Wibu-Systems can support the secure deployment of neuromorphic systems by managing licenses and access to applications running on neuromorphic hardware. CodeMeter can also facilitate secure updates, helping manufacturers and operators protect neuromorphic devices from cyber threats as they become more integral to daily operations.

4. Brain-Computer Interfaces (BCIs)

Brain-computer interfaces (BCIs) are emerging as a transformative technology that enables direct communication between the brain and digital devices. BCIs have potential applications in healthcare, gaming, and beyond, offering new ways to assist individuals with disabilities or enhance human cognition. However, BCIs also introduce a unique set of cybersecurity risks, as they involve sensitive neural data that could be manipulated or accessed by unauthorized parties.

With secure deployment, BCIs could improve accessibility and provide users with new capabilities. But in a worst-case scenario, cybercriminals could exploit vulnerabilities in BCI systems to manipulate or extract neural data. Wibu-Systems could play a vital role in securing BCI applications by using CodeMeter to manage licenses and protect access to software controlling BCIs. This ensures that only authenticated, authorized users can interact with these sensitive systems, protecting both the user's privacy and the integrity of neural data.

5. Tokenized Economies and Decentralized Autonomous Organizations (DAOs)

Tokenized economies and DAOs are redefining how communities and organizations govern and participate in economic activities. By using tokens and blockchain technology, DAOs enable decentralized decision-making and allow participants to hold a direct stake in the organizations they engage with. However, as DAOs and tokenized economies grow, they face new cybersecurity challenges around smart contract security, fraud prevention, and data integrity.

In a positive scenario, tokenized economies could offer new models for governance and economic participation, making communities more inclusive and resilient. However, without adequate security, DAOs could be vulnerable to hacks and fraud, potentially leading to financial loss for participants and instability within these digital communities. Wibu-Systems could support the secure operation of tokenized economies by providing solutions that protect smart contracts and manage licenses for DAO-related software. By ensuring that only verified participants can interact with these systems, CodeMeter can help preserve the integrity and security of tokenized ecosystems.

OLIVER WINZENRIED *began his entrepreneurial career immediately after completing his studies, and focused on electronic and ASIC design, hardware, microcontroller and embedded application development for consumer electronics, automotive and industrial engineering. With Marcellus Buchheit at his side, he founded Wibu-Systems in 1989, and remains the company's CEO to this day.*

6. Critical Infrastructure and Cyber Resilience

The increasing digitalization of critical infrastructure—such as power grids, water systems, and transportation networks—has improved efficiency and service reliability. However, it has also introduced new vulnerabilities, making these systems prime targets for cybercriminals and state-sponsored attacks. A breach in critical infrastructure can lead to widespread service disruptions, with severe consequences for public safety and economic stability.

In a secure future, critical infrastructure would be cyber-resilient, ensuring that essential services remain operational even under attack. But without sufficient defenses, these systems could become highly vulnerable, jeopardizing public safety and disrupting entire communities. Wibu-Systems is well-positioned to support critical infrastructure providers with CodeMeter's robust software protection and access control capabilities. By embedding security within software licenses and enforcing strict authentication, Wibu-Systems helps secure critical infrastructure and protect essential services from potential cyber threats.

Securing the future demands a foundation of trust, collaboration, and proactive security.

Trustworthy AI, reliable electronics, and human-centric security and cyber hygiene practices will empower individuals and reinforce confidence in technology. Meanwhile, securing the supply chain and implementing Zero Trust Architecture will prevent vulnerabilities across complex digital ecosystems. Digital sovereignty will allow organizations to maintain control over critical data and infrastructure, enhancing resilience. Achieving these goals requires sustained research and development by both private and public sectors, driving innovative cybersecurity solutions. Together, these efforts will shape a secure and trustworthy digital future. ☒

WIBU SYSTEMS

35 YEARS 1989-2024 Propelling Your Business To New Heights

CodeMeter – An Endless Virtuous Cycle for Your Business Growth

PROTECT YOUR SOFTWARE with cutting edge encryption and obfuscation technologies

MEET YOUR CUSTOMERS' demands with a versatile and scalable licensing system

REAP THE REWARDS from your work on a global scale, and repeat the entire process

Meet the EXPERTS!

+49 721 931720
sales@wibu.com
www.wibu.com

SECURITY
LICENSING
PERFECTION IN PROTECTION