



The VAULT



APPLICATIONS

Digital Identity Solution
Mobile Connect | Mobile ID:
Mobilized and ready

INTERNATIONAL

Africa – Identity in Diversity

TECHNOLOGY

Internet of Things: What about
security? | Secure ID:
Why best in class
is worth it

MOBILE IDENTITIES

on the rise



“IoT challenges?
Security. *Security.*
SECURITY!”

An interview with Oliver Winzenried, CEO and Co-Founder at Wibu-Systems

The VAULT Magazine spoke to Oliver Winzenried, CEO and Co-Founder of Wibu-Systems about the future challenges for the Internet of Things sector. With billions of connected devices and ever increasing interest in Industry 4.0 solutions, smaller, medium-sized and even large companies have to get their strategy right. In this interview, we get an insight into the challenges, risks and common mistakes when it comes to implementing security solutions in Industry 4.0 processes.

□ *With an estimated 40.9 billion networked devices, from a security perspective, where do you see challenges for the Internet of Things?*

Three words: security, security, and security! For one, security has to be there if we want to use Internet of Things (IoT) devices the way they are meant to be used. Second, security is required to update and upgrade the functionality and features of IoT devices, so that we know they have not been tampered with or hacked in some manner during that process. Finally, security is required to monetize features in IoT devices and implement new business models that benefit not only the device's manufacturer, but its users as well.

Would you say that the industry as a whole has the same focus on security, or is it something that needs to be pushed more?

We definitely need to push this issue much more! We are only experiencing the IoT in its infancy right now. More and more things are becoming connected, and it is normal that when new technologies are being deployed and work as expected, the new features and new convenience will make everyone happy. People only get concerned about security when incidents happen, approximately six to 24 months after the introduction of the new technology. It is only then that people stop just talking about security and actually start implementing it. We should be implementing it in a way that we get security by design or by default. Security by design means that the devices are equipped with configuration options that enable security, while security by default means that the user gets the device configured in a way that ensures a certain level of security, regardless of the user's set-up or preferences. If you think about the original Wi-Fi access and routers for home use, they were initially complicated to configure (including the security protections that you needed); when you received them, you needed to configure the whole set-up yourself before you got Wi-Fi access. These days, you can get a Wi-Fi router that is much easier to configure, but there is a certain level of security already programmed and installed

within the set-up itself. This is what I mean when I talk about 'security by design' and 'security by default'.

So you would say that the next 24 months are critical for IoT security development?

I believe so. I really do.

Looking towards Industrie 4.0, what are the obstacles to successful implementation?

First of all, I believe that companies operating manufacturing facilities need to understand the value of flexible production. The next obstacle is that machines and production processes are normally used for extremely long time periods. You might have a machine or production process in place that is ten years old, but that is still a long way from being obsolete. These machines may have lifespans of twenty years or more. Still, machines and manufacturing processes need to be able to implement flexible production processes, according to the new Industrie 4.0 concepts – both in the plant itself and out in the field.

So it's a cost issue?

That, and technical feasibility. The machines may be so old that there is no feasible way to get Industrie 4.0 into existing production processes. But some machines and processes that are in their midlife cycle may be able to accommodate Industrie 4.0 principles.

There may also be obstacles due to companies' IP and the need for companies to safeguard their tools and know-how. Add to that a general lack of trust in cloud-based security systems and issues about missing standards. Finally, the biggest obstacle is a lack of education about this particular subject and the need to enable the workforce to understand it better and help them implement Industrie 4.0. The qualifications required to implement all of this correctly will be higher than those needed for normal production processes in a manufacturing plant. And we are talking about ongoing, life-long learning.

“ *Smaller, medium-sized, even large companies need to have a degree of interoperability, so standards are important to ensure flawless and secure communication when machines are brought together in large conglomerates.* ”

How would you advise companies that are about to invest in Industrie 4.0? In your experience, what are the most common mistakes that are made?

Most manufacturing requires a reasonable return on investment after a period of time, so the first thing that these companies need to do is think about the benefits of this process for their customers as their #1 priority. This could take the form of improving either the product or the production process itself. Companies should look to discover what could be improved in terms of non recurring costs, lead times, or product costs themselves. Perhaps, they might even think about where in the manufacturing process it might make sense to team up with others.

It is also important to consider how important it is for the company to remain in direct contact with their customers. Internet now offers a variety of ways and means for the customer to gain first-hand knowledge and even materials without going through the manufacturer. This in turn means that manufacturers also need to be aware of these alternative sources, and it might drive them to engage in more co-operations with Internet-based companies in order to maintain their business.

It's when we are looking at our own companies or our manufacturing process as a whole that we need to understand and agree on where Industrie 4.0 should be injected into the process. That is why it is important to have a flexible production system. By choosing the right point to insert Industrie 4.0, the production process can be improved in the sense of bringing down costs, streamlining order processing, speeding up re-tooling, increasing energy efficiency, and creating less waste.

There is a lot happening out there in these fields, so companies do well to follow what is happening around them and learn from the best practices available. There is no one guideline for everything; it will depend upon which activities a company is undertaking.

For instance, there is one company we worked with that offers superior clamping and gripping units for use in robotic applications. They have implemented Industrie 4.0 in their products and processes very well. Consider their gripper units: In the past they used mechatronic grippers. Then they added sensors into the gripping unit to create intelligent mechatronic grippers. Next, they added communication to create a cyber physical system. And finally, they added a web interface using IP communication to create a truly smart gripper, with secure OPC UA communication. Inter-

estingly, some of these grippers sometimes have to get customized "fingers" to handle specific customer products. Using a cloud-based system, the gripper fingers can be designed to fit the customer's parts and specific requirements and then manufactured using 3D printing, at low costs and with little wait. That's much more effective and cost-efficient compared to the time and resource-intensive process that would have been needed in the past.

We have also worked with a company that produces embroidery machines, and they have implemented a system to protect the customer-specific production data in their machines. The new system also allows them to control production output in remote locations (India etc.). The companies making their product on their machines can do so in the safe knowledge that the design in the data is secure and no product or similar product design will find its way onto the grey market.

These are just two examples of companies using Industrie 4.0 that are already active in the market today.

What I don't understand is why so many companies, especially small to medium-sized ones, are doing nothing in this area. They might be listening to some extent to what we are saying, but they continue to wait until others have implemented it first. This approach could easily backfire, as they are going to need a considerable amount of time to implement changes, while those that have already implemented the changes are more successful and have a real head-start over their competitors. I think all manufacturing companies would do well to actively implement these changes sooner rather than later.

“ *By choosing the right point to insert Industrie 4.0, the production process can be improved in the sense of bringing down costs, streamlining order processing, speeding up re-tooling, increasing energy efficiency, and creating less waste.* ”

Where do you see the role of national governments? Can the public sector support the private sector?

I believe they can, and they are already doing so in all of the world's most relevant economic powers. Look at China. They have an initiative called 'Made in China 2025' that is getting strong political and financial backing from the Chinese Government. It's a ten-year plan dedicated to comprehensively upgrading China's industry. They are not content with simply staying the factory of the world. Rather, they want to create new innovations, new products, and new brands themselves.

It's a similar story in Japan and South Korea, again with strong support from their governments. I think it's also the same in the US, but I don't have any specific details about public funding.

There are lots of programs coming from the military side, such as DARPA, with almost unlimited funds. The technology developed there is used in non-military applications as well. The European Commission is also doing good work with their ‘Horizon 2020’. Looking specifically at Germany, the situation is not bad. In fact, we are involved in several projects – so we can’t complain! However, speaking generally in terms of public funding compared to the scale of the economy as a whole, we are still lagging far behind, say, South Korea.

What governments can do is support research and development projects in cooperation with various research institutes and large enterprises. They must also create the legal framework that is necessary to get Industrie 4.0 mechanisms working. And they should support standardization to propel international cooperation and free trade. But then again, these are general tasks for governments everywhere. And let’s not forget helping local industry, so that they can retain their competitive advantages against others in the global market.

Could you please expand a little on the IUNO and DnSPro projects in Germany that you are part of? What are the benefits of these kind of collaborations, and what goals are you hoping to achieve?

Both of these projects see the involvement of Infineon. IUNO is a large project with a budget of 33 million EURO, partly funded by the BMBF, the Federal Ministry for Education and Research, with the mission to become the ‘National Reference Project for IT Security in Industrie 4.0’. It brings together a consortium of 14 companies and 7 research institutes. In Europe, the custom is for many projects to have a public tendering process, announced on the web, with a list of criteria for tenders from the private sector. IUNO was not announced in this way. Instead, several large enterprises (Bosch, VW etc) were approached directly. From my understanding, the reasoning behind this was to ensure that what would be developed in this project would later indeed be used in the production facilities of these large enterprises. That is an advantage for everyone.

We are participating in all use cases, and our goal is to adopt and improve our security solutions to fit these enterprises’ requirements that are revealed in the project. However, our main use case will be the creation of a digital marketplace for technology data used in production processes. Such a marketplace for production process and production data is ideal for Industrie 4.0, as companies using these marketplaces will be looking for flexible production processes and fast re-tooling or ways to speed up their production flows.

The knowledge from many of these manufacturing companies can be pooled in such a way that any one company can place its data in the marketplace. It knows that it actually benefits from sharing the information, while maintaining control over their IP at the same time. So, the DRM for the protection of the IP is very important. And, honestly, also very challenging.

These projects do not just come with many technical issues that need to be addressed; there are also legal considerations to enable us to use these systems on a larger scale. For instance, it could be rolled out to a small group of companies in Germany, or perhaps even internationally. There is still so much that needs to be done; we are only just at the start of the process. IUNO only started July 2015 and will continue for another two and a half years.

The other project – DnSPro – is a German anagram for ‘Dezentral kooperierende Sensor basierende Subsysteme für Industrie 4.0 Produktionsanlagen’ which can be translated as

‘Decentralized cooperating sensor-based subsystems for Industry 4.0 production facilities’. It’s basically about smart processing subsystems. The company that introduced us into this project is KHS, one of the world’s leaders in filling and packaging machines for drinks – either in PET or glass bottles – such as soft drinks, water, fruit juices, beer, and so on.

By using intelligent sensors and cyber physical systems, this company wants to improve its processes by reducing the time

it takes to change the filling system for different liquids, due to different pressures, flows, system settings, cleaning, and so on. This process can be monitored and improved with intelligent sensors.

Beyond the specific scope of this project, our goal is to reach an inside understanding of the industry’s requirements to be able to replicate the results obtained from this project in other manufacturing plants. This is only achievable if all the different stakeholders are willing to combine their competencies – plant operators on the one side and technology groups on the other. In the end, we should discover new solutions much faster. Standardization may also be a next step. The ultimate goal for Wibu-Systems is a wider adoption of our solutions over time and in many different use cases.

The results should also be available later to companies outside of the consortium, so that we can extend our customer target group for our solutions and slowly build up our business and competitive advantage.

There seems to be a lot of competing companies in these projects – how does that work? Is everyone pulling together at the moment?

“ *Security is required to monetize features in IoT devices and implement new business models that benefit not only the device’s manufacturer, but its users as well.* ”

*Oliver Winzenried*

I think that, when you are working on standards, it is necessary to work with all the global titans, including your competitors. Smaller, medium-sized, even large companies need to have a degree of interoperability, so standards are important to ensure flawless and secure communication when machines are brought together in large conglomerates. Standardization practically guarantees that different vendors can work together. It just makes sense to do the basic standardizing work together – even if you are competitors. When it eventually comes to the implementation and the details, every company needs to work with their strengths and unique advantages to ensure they are used in their specific implementations. This is the point where competition is at its strongest.

Why does Wibu-Systems take part in these industry initiatives?

We are part of many industry initiatives, but we only focus on our specific topic: protection, licensing, and security. We are working in markets as diverse as industrial automation and medical equipment, and the requirements are not always the same. The needs of customers in these different target groups are very different.

The only way for us to understand these industry requirements and adapt our solutions accordingly is to actively take part in these industry initiatives. ☒