ProTego project summary

The ProTego project has been completed in December 2021. In the last three years, a European consortium consisting of 9 partners has performed research and innovation activities with the aim to provide tools for risk identification and assessment and data protection to reduce cybersecurity risks in hospitals and care centers.

The objectives for ProTego are the following:

1. Holistic approach to protect data from Electronic Health Records (EHR) against cyber risks generated by remote devices access, agnostic to health care IT infrastructure.
2. Improve situational awareness during an attack.
3. Protect sensitive data inside the hospital infrastructure and at the boundary between hospitals and Bring Your Own Device (BYOD) and Internet of Things (IoT) domains.
4. Cybersecurity solutions for Electronic Protected Health Information (ePHI) protection released as integrated toolkit.
5. Provision of an Educational framework: Methodologies and protocols for the correct usage of cyber-security tools, for attacks prevention and reaction to be used by health sector staff (IT and physicians) and patients.
6. Validate in scenarios involving emerging technologies in health care informatics: IoT and BYOD.

To draw conclusions about the results of the project and assess impact a questionnaire was designed to gather the opinion of the IT staff in the hospitals that participated in all the testing performed. The responses to the questionnaire show the anticipated real perception of adoption by those that would be responsible of the resulting product of the project in the hospitals. This is the questionnaire and the answers received from the hospitals in a unified way:

ID	Question
	Answer
#1	Does the scope covered by ProTego match areas in which there is a lack of cybersecurity controls within your organization? Explain which ones.
	Yes, ProTego covers cybersecurity aspects that we do not have covered. Some of them were on our roadmap, such as the incorporation of a SIEM tool. But there are others that provide very new possibilities that were not even contemplated: • the possibility of evaluating the system at design time System Security Modeller (SSM) • updating this evaluation in real time by integrating SSM and SIEM • the encryption of data at rest (Data Gateway) and the granularity in the definition of access rights, at the platform level (Access Control) • the protection of user devices preventing impersonation risks in the access to the health data (Continuous Authentication)

<table>
<tr><td>#2</td><td colspan="4">Do you think ProTego would help to reduce cyber-risks in your organization? Explain why.</td></tr>
<tr><td></td><td colspan="4">We believe that ProTego can effectively help reduce cyber-risks. By covering the previously described areas that are not currently being treated in our organizations, attack vectors can be managed in currently unprotected areas.
In addition, the educational material addressed to health staff can reduce the risks derived from incorrect human behaviour related to cyber security.</td></tr>
<tr><td>#3</td><td colspan="4">Do you think ProTego would increase situational awareness under an attack and improve the response time?</td></tr>
<tr><td></td><td colspan="4">Yes, mainly through the real-time information offered by the SIEM, we believe that the response to an eventual attack would be drastically reduced, which would undoubtedly help to reduce the impact.</td></tr>
<tr><td>#4</td><td colspan="4">Can you identify features offered by ProTego that apply to each item on the following table? Short description.</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><td colspan="2" rowspan="2">ProTego Toolkit</td><td colspan="3">Data stages</td></tr>
<tr><td>Data at rest</td><td>Data in transit</td><td>Data in use</td></tr>
<tr><td rowspan="3">Cyber-Security Dimensions</td><td>Confidentiality</td><td>Fine-grained definition of access grants to the data. Parquet encrypted files prevent data at rest to be read.</td><td>Isolation provided by Network slicing ensures confidentiality of data in transit.</td><td>Hardware Secure enclaves</td></tr>
<tr><td>Integrity</td><td>Parquet encrypted files prevent that data at rest to be modified.</td><td>Isolation provided by Network slicing ensures integrity of data in transit.</td><td>Hardware Secure enclaves</td></tr>
<tr><td>Availability</td><td>The integration technology applied (k8s, DevOps) allows the use of persistence layers that ensures availability, like NFS or EFS for cloud infrastructure.</td><td>Network slicing ensures the network resources needed to each service.</td><td>Hardware Secure enclaves</td></tr>
</table></td></tr>
<tr><td>#5</td><td colspan="4">Can you identify any feature offered by ProTego that is not covered by applications already in the market, as far as you know? List them.</td></tr>
<tr><td></td><td colspan="4">Mainly the features offered by the SSM, as it allows to assess the risk level of a system in design time, and also to assess the impact of future changes to the infrastructure.
Also, the real time integration of the SIEM and the SSM, which allows the SIEM to notify not only risks regarding events that have already occurred (by analysing vulnerabilities in infrastructures and applications) but notifying prospective situations if some change introduced in the design of the system that introduce new risks.
Finally, the Continuous Authentication provides the means to identify impersonation risks in the final user devices. There are some tools that allow managing the corporate devices, performs health assessments (assess the installed apps, patching level...) but as far as we know there is not any tool that assess the trustworthiness of the user that is using the device.</td></tr>
<tr><td>#6</td><td colspan="4">Do you think the ProTego toolkit would be suitable to be adopted in your organization? Explain why.</td></tr>
<tr><td></td><td colspan="4">In the previous answers it has been explained what features offered by ProTego are of interest, some of them are even novel and not offered by other tools already in the market. But assessing adoption is a vital point as a healthcare organization is an ecosystem from the IT perspective and new applications should integrate with the pre-existing ones. In that regard we can see interesting features in the ProTego toolkit:
• The integration framework is based on Kubernetes for deployment and orchestration of services. It allows almost any type of underlying infrastructure. It also allows easy scaling-up based on actual use.</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">The ProTego toolkit can be deployed in both cloud and or hospital premises, as it has been demonstrated in the pilots respectively
It bases the authentication in the JWT standard, and delegates authentication services in external IAMs, what allows to integrate the ACL (user management) with the corporate pre-existing one, something mandatory for the majority of organizations.
It uses FHIR as standard for health data format. It allows easy integration with external applications as the format of the data is well-known. It has allowed to integrate the toolkit with the hospital EMR, what is also mandatory, because it minimizes the isolated data silos and enriched the patient's data record, improving the business intelligence performed on that centralized repository. To be more precise, the toolkit has been integrated with Cerner Millennium, one of the top commercial EMRs.
The ProTego toolkit allows the adoption as a modular system, in a way that the organization can decide which components of the toolkit it decides to adopt at each point in time, allowing to delay those that are not of interest or need a deeper assessment or provide certain requirements before its adoption.
All in all, we think that the ProTego toolkit has addressed the adoption requirements in a successful way.</td></tr>
<tr><td>#7</td><td colspan="2">Which disadvantage can you see in the ProTego toolkit? Explain.</td></tr>
<tr><td></td><td colspan="2">They are not disadvantages per se, but we can foresee some aspects that may make it difficult for some organizations to adopt a toolkit like ProTego. They are mainly related with the fact that the toolkit is based on some of the newest standards, and most healthcare organizations are not still ready to use them. To be more precise:
the FHIR standard for data exchange is not yet widely adopted. Nowadays HL7 v2 and v3 are the most used and the majority of tools in the market are compatible with these versions. It's not a blocking problem, since custom developments can be easily developed to translate FHIR format from/to other data formats.
most healthcare organizations are not using DevOps technology, so the use of Kubernetes, Istio, etc. may not be affordable for them right now, not because of the cost of the technology in itself, since it is Open-Source, but for the cost in time, effort and other needed resources to tackle the projects involved. Nevertheless, it is undoubtedly the direction the industry is moving towards, and in a few years any organization would be required to use this kind of technology to use updated applications.
Along the same line, the use of JWT for authentication may not be yet implemented in many healthcare organizations.
In summary, the aspects that may prevent healthcare organizations to adopt the ProTego toolkit are related to the fact that it is based in forthcoming standards, and healthcare organizations need to improve their underlying technology and technical skills to face that challenge successfully. The features offered by these novel technologies could be a good incentive to move forward and accept the challenge.</td></tr>
<tr><td>#8</td><td colspan="2">Please summarize the opinion about the ProTego toolkit from the scope of each of the following roles you are in charge of:</td></tr>
<tr><td></td><td>Network operator</td><td>Network operators manage the network capabilities of the hospital. They need to guarantee that the network meets the necessary quality of service attributes</td></tr>
<tr><td></td><td></td><td>Through the Network Slicing tool, the ProTego toolkit provides the means for creating secured slices ensuring the confidentiality of the transmitted data. But it also allows a useful capability: assign the desired resources (bandwidth, especially over wireless networks) to each slice, which in turn increases availability. It has some direct applications for hospitals, for example a slice could be created to transmit DICOM data from medical devices to the unified repository, since this is a heavyweight data format</td></tr>
</table>

		and with this feature we could dedicate a portion of the resources, not affecting other services working under the same physical network.
	Data operator	Data operators are in charge of data flows and how they are stored within the hospital infrastructure. Data operators must guarantee that sensitive data is stored with an appropriate level of protection.
		The underlying technology in ProTego increases the security of data at rest providing an additional encryption feature, that is independent of what is provided by the underlying platform.
	Security operator	Security operators take care of the security concerns of the hospital infrastructure. These include controlling access to the hospital services, assessing the risk associated with the infrastructure, and monitoring the data exchange for possible attacks and foreseeable risks.
		The main features provided by the ProTego toolkit from a holistic perspective, that is, how the toolkit could be integrated with pre-existing IT systems, are: • it integrates with the organization's IAM, thus using a unique user database. This minimizes administration tasks avoiding duplicated information in different user repositories, and the risk of having them out of sync. • it offers integration with external applications, including medical devices, which is aligned with the strategy of reducing isolated data silos that are a main handicap of present medical device systems. • it introduces features to reduce risks of impersonation on the end user device. • it allows performing prospective assessments of the system in design time, allowing to assess the impact a potential change could have. • real-time integration of the SIEM with the SSM, which is a novel and powerful tool to minimize risks. • it is aligned with the NIST CSF, a worldwide recognized standard for cybersecurity assessment.
	System operator	System operators are responsible for installing, configuring and managing computer systems in the hospital infrastructure.
		The fact that the ProTego integration toolkit is based on Kubernetes allows for deployment on different platforms, including cloud premises. This versatility makes it easy to adopt from a system operator perspective, as it makes the management of the platform easier and allows scaling the platform requirements accordingly based on the use and demand.
	Administrator	Special role capable of making unrestricted, system-wide changes (e.g., registering accounts for other IT operators).
		The fact that the toolkit delegates the access permissions to the corporate IAM makes it easier to control the access to the data, as previously mentioned. Regarding administrator access to the platform, it is controlled by the base platform in use. For example, in the case of cloud infrastructures, the user definition and permissions defined in the corporate cloud account make it easier to manage the fine-grained access to the components offered by the cloud, allowing to define specific grants for specific maintenance and management actions.

To summarize the main aspects, the responders could identify features that are understood as useful to prevent or mitigate cyber risks in areas that have not been already covered in their hospitals, and even some of them are not provided by other products already in the market.

From a technical perspective, the versatility of the ProTego toolkit has been highlighted as a key factor to facilitate adoption, allowing to deploy it over different base infrastructures.

And from an organizational perspective, the modularity has been identified as useful, since the toolkit allows partial or progressive adoption, allowing each organization to find the right moment to introduce each component, as the organizational or corporate requirements could be met.

The positive results obtained in the final testing phase and the responses received from hospitals staff, demonstrate that the project has been a complete success.