erties of the tomography problem into the domain of algebraic methods, replacing the generic matrix representation with convolution-based filter operators. The idea is to compute one or more filters h for the FBP algorithm in such a way that the resulting FBP reconstruction resembles the image computed by a more expensive iterative method. Surprisingly, it is possible to obtain image quality almost identical to that of iterative methods with the computational performance of FBP, making the approach suitable for industrial use in high-throughput, limited-data scenarios.

In May 2017, CWI started the FleX-ray lab, where a highly flexible X-ray CT system is combined with high-performance computing capabilities, making it possible to rapidly prototype novel computational methods for 3D X-ray imaging, and experiment with various geometrical scanning configurations. Due to their combination of computational efficiency and accuracy in limited data scenarios, algebraic filter methods can potentially enable the effective use of 3D imaging for quality control in a broad range of food products, which we are currently exploring further in ongoing research projects with high-tech partners from the food industry.

3D reconstruction of a pomegranate from high-resolution X-ray CT data, clearly showing the complex internal morphology and textures. This dataset is publicly available [3].

References:
[1] D.M. Pelt and K.J. Batenburg: "Improving Filtered Backprojection Reconstruction by Data-Dependent Filtering", IEEE Transactions on Image Processing, 23(11), 4750-4762, 2014
[2] L. Plantagie and K.J. Batenburg: "Algebraic filter approach for fast approximation of nonlinear tomographic reconstruction methods", J. Digital Imaging, 24(1), 013026, 2015
[3] DOI: 10.5281/zenodo.1144086

Please contact:
Joost Batenburg, Robert van Liere
CWI, The Netherlands
joost.batenburg@cwi.nl,
robert.van.liere@cwi.nl

Security Threats and Risk Analysis of an IoT Web Service for a Smart Vineyard

by Massimo Borrelli, Vanes Coric, Clemens Gnauer, Jennifer Wolfgeher and Markus Tauber (FH Burgenland)

The grape-growing industry is changing as growers increasingly combine technology with traditional growing methods in smart vineyards. If wine makers want to maximise the potential of their plants, it is no longer enough to rely on gut-feeling, but rather on locally gathered environmental data. These data help to accurately plan individual tasks, such as fertilisation, plant protection, and harvesting. This is where automated and IT-supported farming, or smart farming, comes into play.

While smart farming is a significant trend with substantial literature in the areas of IoT and the Cloud, very little attention has been paid to security in this area. Carrara et al. [1] have established an IoT based management program collecting data on temperature and relative humidity. Zachariadis and Kaskalis [2] measured critical environmental measurements with the data being sent via SMS, and Patil and Thorat [3] monitored water, climate, pests and diseases of the grape and provided this information via a Webinterface. But none of these studies have addressed related security concerns.

To this end, we have developed a representative service oriented architecture (SOA) based application and conducted a structure security analysis to identify typical security issues in smart farming applications – in our use case, a smart vineyard. For such a use case it is important to get accurate and actual climate data from the vineyard. To achieve this, a device was established over a period of three months that collects local data in the vineyard. Information like temperature, wind strength, direction and soil humidity is then stored in a database and transmitted via a web service so that it can be accessed easily through a web interface. For this a prototype has been built with a Raspberry Pi v3 and a DHT22 temperature sensor and a humidity sensor. The Raspberry Pi uses the operating system Raspbian without GUI. An Apache2 web server is installed for the delivery of the weather information on a web interface. The database server that we use is MySQL where the data from the sensors is stored, as is the hardcoded data for wind speed and wind direction. A python script is used to collect the data from the sensor and to store this data into the database. PHP7 is also installed in the device which is used for the programming of the web service. Figure 1 shows a representation of the prototype, its assets and data flows.

The development of this prototype has helped us acquire an understanding of the impact of threats to the system components. The assets that have been considered for the security threats and risk analysis include: the Raspberry Pi, the database and the web service. Out of the CIA triangle (availability, integrity and confidentiality), availability is the most important asset, while confidentiality and integrity apply only to the data included in the database.

To critically assess the prototype, the OWASP Top Ten [L1] and OWASP IoT Top Ten [L2] catalogues have been consolidated to identify the threats that would affect such a solution. These catalogues have been chosen because of the IoT nature of our service, as well as being relevant to rate the web application security.

Each of the three assets have been assessed against all attack vectors included in these catalogues, to deter-

mine the major threats and the assets most likely affected, as showed in the following charts. The number of points given to each vector is based on the DREAD methodology for risk assessment. Ranging from 0 to 15, the figures 2 and 3 show the threats with the greatest impact on our assets (where not applicable a value of 0 was used).

The results of the security threats revealed that the following risks might impact the identified assets:

- Data loss and corruption is the main consequence of the various attack vectors affecting the database, undermining the integrity of the data
- A denial of service attack would bring the service down and thus poses a significant issue to the service availability
- The Raspberry Pi, being the device where the software is running and the sensors are connected to, needs to be protected against physical attacks that might remove storage media or access the software via USB ports. This would also affect the service availability and compromise its functionality.

Deploying a smart farming web service and relying on IoT technology is a fundamental step ahead to improve productivity within the vineyard industry, but the security aspects of the web service need to be considered as well. The topic of security needs to be further discussed by assessing different and much broader IoT setups. Understanding threats and the risks arising from the service infrastructure and IoT is the most relevant starting point to design safe solutions that reduce risks or alternatively help to minimise the impact of security breaches.

Links:

[L1] https://kwz.me/hbz

[L2] https://kwz.me/hbA

References:

[1] M. Carrara, et al.: "An innovative system for vineyard management in Sicily", Journal of Agricultural Engineering, 41(1), pp. 13-18, 2010.

[2] S. Zachariadis, T. H. Kaskalis: "An Embedded System for Smart Vineyard Agriculture", 2nd Pan-Hellenic Conference on Electronics and Telecommunications - PACET´12, Thessaloniki, Greece, 16-18 March 2012.

[3] S.S. Patil, S.A. Thorat: "Vinayard monitoring and recommendations using wireless sensor network: a study", International conference on computing, communication and energy systems (ICCCES-16), January 2016.

Figure 1: Prototype, assets and data flows.

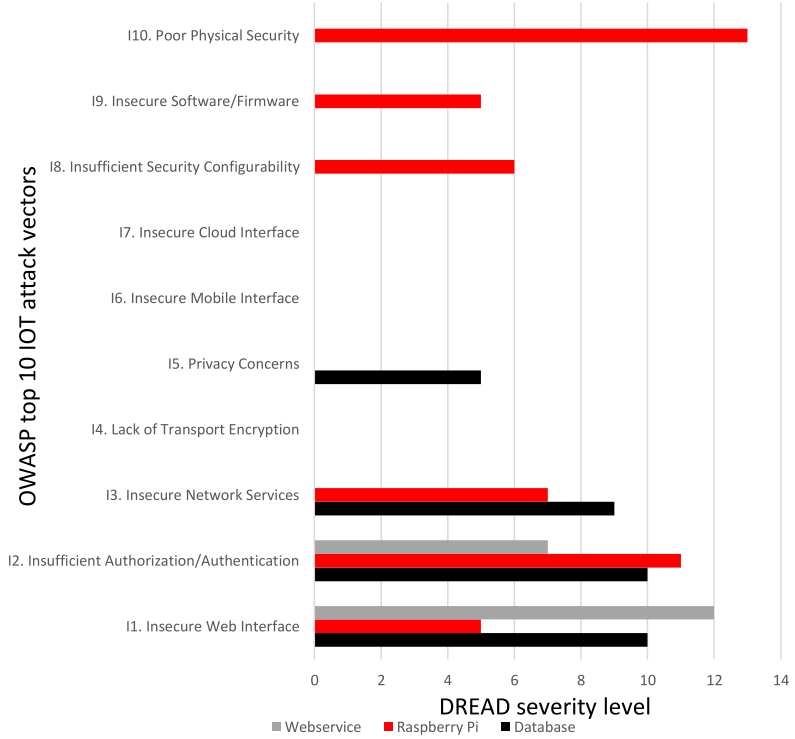

Figure 2: Weighted impact of OWASP top 10 IOT attack vectors on prototype assets.

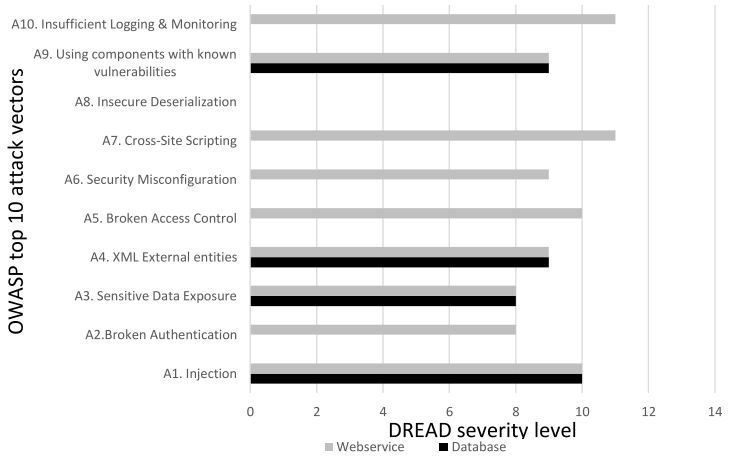

Figure 3: Weighted impact of OWASP top 10 attack vectors on prototype assets.

Please contact:

Massimo Borrelli
FH Burgenland, Austria
+43 664 3823105
1710781023@fh-burgenland.at

Markus Tauber
FH Burgenland, Austria
+43 5 7705 4321
markus.tauber@fh-burgenland.at