SIEMENS
Ingenuity for life

Siemens Digital Industries Software

Ensuring the security of engineering software – A large air-frame manufacturer case study

Executive summary

Corporations around the world are suffering from the relentless rise of cyber-crime, cyber-espionage and cyber-terrorism. In addition to severely harming a company's reputation, breaches into their secure systems threaten customers' privacy, safety, and wellbeing. Reported cases make up only a fraction of the attacks that occur daily. In 2016 alone, the Online Trust Alliance tallied 82,000 cyber "incidents" (Online Trust Alliance, 2017). However, they estimate the actual number of incidents to be over 250,000 due to the frequency with which cyber-attacks go unreported (Online Trust Alliance, 2017). Year over year, the occurrence of cyber-crime is rising, and the extent and damage of the attacks is increasing.

Artem Kornilov
Technical Director

Cyber-crime: Targets and impact

Figure 1: Information about the F-35 Fighter was stolen in a notable cyber-security breach.

Commercial organizations, especially those with government contracts, and government agencies are the most common targets of cyber-attacks due to the valuable information they possess. In one dramatic example, information related to the F-35 Joint Strike Fighter, P-8 Poseidon patrol plane, C-130 Hercules cargo plane, Joint Direct Attack Munition (JDAM) bomb, and future Australian Navy ships was exfiltrated from an Australian defense firm in November of 2016 (figure 1; Ars Technica, 2017).

There are a variety of motivations that cyber-criminals have when attacking companies. Sometimes it is to access sensitive information, likely with the intent to steal intellectual property. Other times they will aim to disrupt or delay the design process of a new product or project. The attack could also be focused on compromising the product functionality itself by tampering with critical areas of the design. For example, by changing the insulating material around certain wires during design, a third-party could more easily monitor the activity of the final product via electromagnetic radiation. Design data may also be completely destroyed, sabotaging months or years of design work.

The increased frequency and severe consequences of cyber-security breaches have alarmed large corporations around the world. As a result, companies are taking greater measures to secure their information throughout their supply chains. This paper will examine how vendors like Siemens Digital Industries Software are rising to meet new rigorous security demands.

Securing enterprise software solutions

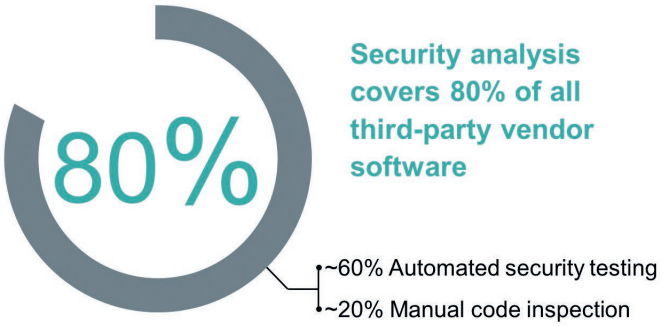

Figure 2: Companies are seeking to establish a uniform procedure for securing their vendors' software.

Preventing cyber-security breaches is crucial to a company's reputation and to the successful operation and growth of its business. The cost of inaction is too high as a breach in security could cause massive financial loss for the company, or the leaking of sensitive information. As a result, manufacturers around the world have conceived and implemented multi-faceted secure software development programs, strengthening cyber-security for all the software they use.

These programs place an intense focus on reducing the risk and cost posed by security vulnerabilities in third-party software through testing and secure development practices. Teams of security experts frequently work directly with software suppliers to help them realize the benefits of integrating software security into their development process. Working with vendors in this manner is a fundamental component of hardening manufacturer systems.

Most security initiatives begin with internal software solutions and networks. However, security teams have observed an evolution in hacking techniques in step with the security improvements being implemented. As companies reinforced their own networks and software, hackers began targeting their supply chains. Supply chains tend to provide much larger attack surfaces for hackers because large companies use a lot of third party software. Each software vendor widely varies in their development process and security investment for their software products, giving hackers more opportunities to gain access to a company's data. As one security expert recently stated, "We are only as secure as our supplier's secrets."

In response, companies are expanding their security programs to collaborate specifically with software vendors on establishing uniform procedures for software security (figure 2). A common first step is to incorporate a security assessment of the vendor's products into the procurement process. The results of this assessment can be compiled and supplied to a company's management to inform their decisions during the procurement process.

Software assessments may also include an independent third-party scan of the vendor's software for security vulnerabilities. A complete, detailed report of the findings of the security scan is provided to the vendor, while the prospective customer receives only a high-level summary. This approach enables the vendor to protect their intellectual property while providing necessary visibility to companies interested in their solutions. Vendors can choose their own operating procedures while giving manufacturers a uniform security assessment comparable across vendors.

After establishing a record of clean security reports, vendors and their customers will collaboratively evaluate the vendor's secure software development lifecycle (S-SDLC) process as a whole. In some cases, vendors may demonstrate processes that are robust enough to routinely deliver products that meet security requirements. Customers will consider this vendor a trusted provider that employs robust S-SDLC without need for ongoing supervision or constant assessment.

The vendor perspective

Advanced security capabilities are a necessary feature for cutting-edge engineering software in today's market. More and more companies are asking their software vendors to perform systematic verification of the security of their software. Yet, there are important factors for vendors to consider when investing in improved product security.

Security is traditionally a concern of IT or a dedicated security department, not each of the software development teams. Security is also a personnel problem, meaning that HR will be involved to create and host trainings on how to handle data properly. Overall, the push for more secure software will require teams to collaborate that have not done so previously, creating a need for new processes.

Furthermore, enhancing the security of sophisticated software requires a holistic approach. The vendor must add security features, like data encryption or an audit trail, and harden their software by identifying weaknesses in the code and resolving them. Third-party content present in the vendor's software must also be secured to produce a truly secure software solution. These enhancements serve as a differentiation in the marketplace, both in terms of increased security and the quality improvements in the software that will come as a result of the critical and detailed analysis of its code.

In sum, a vendor's decision about investing in product security should be based on the impact that it may have on the sustainable growth of their business. So, it is crucial for their customers to clearly and compellingly convey how increased product security would affect their procurement preferences, buying decisions, publicity and more. Establishing industry security standards for vendors to meet would greatly simplify this decision by turning it into a question of how much security above the minimum to achieve. Once a vendor decides to invest in securing their products, it is crucial that they seek to achieve this in the most effective and efficient manner to maximize positive impact on their business.

Securing the capital portfolio

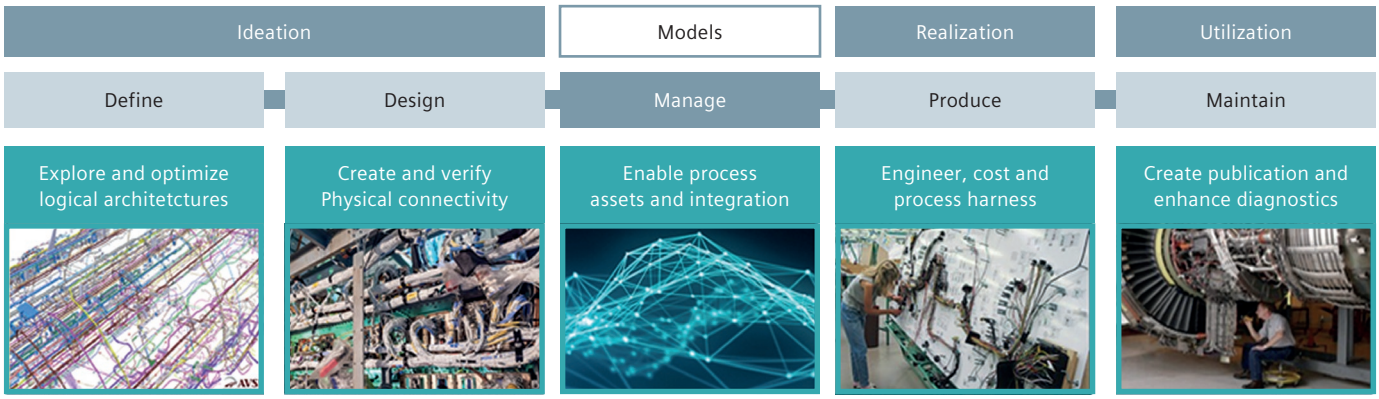

Figure 3: Siemens Capital software suite supports the full lifecycle of electrical systems and wire harnesses.

Siemens has been engaging with its customers on the subject of security since 2011. Siemens Digital Industries Software security enhancements hinged on the efforts of its IT department. Siemens IT heads overall engagement with companies on security, drove vendor selection and budgeted money for the security training and security scanning tools, and coordinated security engagement across Siemens divisions. As part of this engagement, Siemens has selected the Capital electrical system design and integration software suite to participate in the advanced security program.

Siemens Capital software suite supports the full lifecycle of electrical systems and wire harnesses from early electrical and electronic architectural exploration through production design to manufacturing preparation and maintenance in the field (figure 3). The Capital solution, that can be deployed on premises or in the cloud, is multi-tiered and data-centric, with thick and web-based clients. The Capital suite serves as an appropriate example of the approach required to secure a software solution because it covers a wide breadth of commonly used software technologies and design approaches.

To begin their security enhancements, the Capital team clearly identified goals for the desired process and then secured executive management sponsorship within Siemens. The impact of securing the Capital electrical system design and integration suite reaches beyond any single division. Therefore, a collaboration with IT and sales was undertaken to present the case to Siemens' executive management. Once they received approval, the Capital software development division organized a security project team to achieve three goals to secure the Capital suite:

1. Address existing security weaknesses
2. Prevent introduction of new security weaknesses
3. Establish culture of security via training and sharing of best practices.

To address existing security weaknesses the Capital software team used a cloud-based solution to perform static application security testing (SAST). SAST techniques were chosen because they provide greater code coverage to supplement the dynamic application security testing (DAST) the Capital software team already used as part of its S-SDLC. The cloud-based SAST solution scanned the Capital suite's code and produced a list

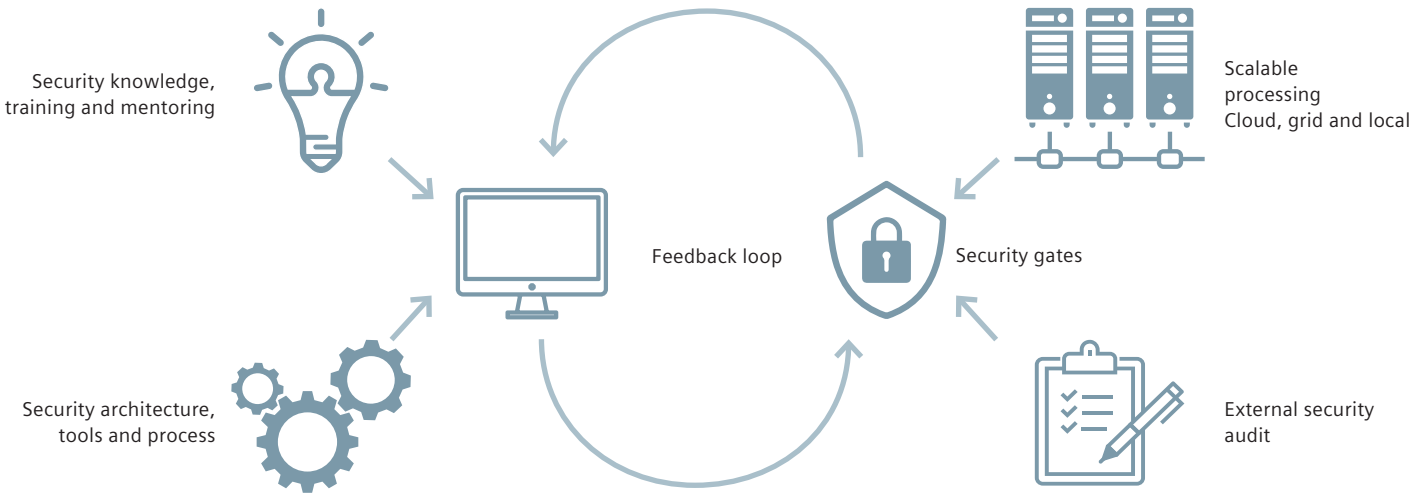

Figure 4: Short feedback loops enabled more agile identification and remediation of flaws.

of existing security weaknesses. This list was used to estimate the effort needed to resolve each of the flaws. Then, the weaknesses were grouped and prioritized for efficient remediation. The weaknesses with the greatest potential for impact were addressed first, and related weaknesses were addressed together. This process lead to the remediation of all weaknesses in the millions of lines of code that comprise the Capital suite.

Next, the team identified common patterns and formulated best practices tailored to the Capital suite's code base, tools and processes. One of the key takeaways is that SAST assessments report significant numbers of false positives, identifying security weaknesses where there are none. Cloud-based solutions eliminate many of these false positives, but a significant number remains that must be addressed by Siemens Digital Industries Software engineers. So, a set of practices was created for identifying false positives and justifying their suppression, including a review and approval process to determine the authenticity of the false positives identified. These best practices were first published on a divisional engineering blog, and then discussed in periodic engineering community meetings.

Cloud-based solutions were additionally helpful due to regular updates that enabled the tools to identify new types of security weaknesses. As a result, the Capital team was able to re-scan code that had previously been determined clean to find and resolve new security weaknesses. Fully realizing the benefits of these recurrent updates, however, required a robust scanning process and an ongoing investment in finding and addressing security weaknesses, even in code already scanned.

The remediation of weaknesses was tracked by continuously delivering code changes and rerunning SAST scans. The Capital software team developed automated scripts to perform tasks including packaging of code for SAST scans and loading scan results into its unified code metrics platform. As part of a larger Siemens security initiative, Siemens Digital Industries Software is focusing on making it easier to develop secure software by evolving the architecture and design of the code. This is being accomplished by routinely minimizing and securing the application's attack surface, and by proactively managing security risks.

The complexity of SAST techniques and the size of the Capital solution's code base meant that the time required for each scan was substantial, resulting in a relatively long feedback loop for the software engineers. To mitigate this, the Capital software team adopted a complementary set of tools that provided shorter feedback loops at the expense of the coverage of the SAST scans (figure 4). The shortest feedback loop was provided by security focused static code analysis continuously running in the background of the integrated development environment used by software engineers. For this, the Capital team chose the JetBrains™ IntelliJ code inspection static code analysis

Figure 5: Computer-based trainings were used to improve security knowledge.

engine paired with the open-source Find Security Bugs SAST solution.

In addition to providing faster feedback loops, these tools integrated security into automatic quality gates that govern code and test deliveries by checking for unit test completion, unit test coverage, and code duplication. Code delivery is gated between the engineer and the team, and the team and release. This ingrained security into the process of developing software and increased protections with no additional effort for individual software engineers, addressing the second of the security goals.

For the third goal, establishing a culture of security, the Capital team worked with IT and HR to procure and administer computer-based security training for software and quality assurance engineers. Security Innovations™ was chosen as the training provider. The curriculum was tailored to best match the Capital solution technology stack and specific needs of various teams. Timely participation in the training was driven by a divisional initiative, tracked by training completion metrics against a deadline. The security training was also integrated into the onboarding process for new employees.

The Capital team adopted three primary approaches to security training. First were instructor lead quality assurance trainings for security testing. These sessions focused on reinforcing and refining techniques that the Capital development team has applied since it began its engagement with security conscious customers in 2011. For example, Siemens Digital Industries Software has used DAST which assesses applications by attacking it as a hacker would and observing the results. Second, the Capital team adopted computer-based trainings on secure software development through a third party provider, Security Innovations. Three course bundles were created, one each for developers, web engineers, and security engineers. Each course bundle concentrated on security concerns specific to each job (figure 5). For example, the developer bundle included topics like “creating secure Java code foundations”, “creating secure Java code”, and “the Open Web Application Security Project top 10 threats and mitigations”. Finally, a security project team was tasked with developing a list of best practices to be shared throughout Siemens Software. This list was shared through Siemens Digital Industries Software central IT organization.

Addressing open source security

Another major concern for design tool vendors is the use of open-source software (OSS) from third party developers. OSS comprises a sizable portion of many powerful software solutions, including the Capital suite. Indeed, OSS is a valuable tool for businesses, saving months or days of development time. However, OSS has the potential to introduce flaws into an otherwise secure software solution. It falls on the vendor to ensure that OSS is secure when considering its use in a software solution.

Open-source software must be analyzed with SAST scans individually, and in the context of the code it is to be used in, before shipping it in the vendor's product. If issues are found it is important to resolve them, or to lobby the OSS developers to fix the issues themselves. Publicly available security vulnerability databases are also important resources in this process. These databases track known vulnerabilities in software and publish them in a searchable format. The National Vulnerability Database (NVD) is a notable example (National Institute of Standards and Technology, 2018).

Simply paying greater attention to the security of OSS, however, is not enough. Serious consideration must be paid to the reduction or mitigation of its use. Each development team should review their usage of OSS to determine if it is possible to upgrade, remove, or replace its function. Mitigation of security weaknesses in OSS may be accomplished with workarounds in the vendor's code to replace or wrap the function performed by the OSS, lobbying the OSS developer to resolve detected issues, or switching to another solution with greater security. A list of security best practices for the use of OSS should also be developed and shared to help spread solutions. Finally approval of OSS use must include review of its impact on security.

Key lessons and achievements

By systematically training, developing, and sharing security best practices Siemens Digital Industries Software was able to institutionalize the process of creating secure software products. This process has become ingrained into the development life cycle to ensure that secure practices continue.

As a result, Siemens, has achieved excellent security standards through its long-running engagement with security-conscious customers. These customers; commitment to S-SDLC development clearly demonstrated to Siemens the value of investing in greater security. By hardening its security practices, Siemens Digital Industries Software achieved a number of additional benefits. Siemens improved its product development infrastructure with best practices learned during security activities, leading to increased productivity. Siemens also created more robust code in terms of both security and quality for the Capital electrical system design and integration solution, improving its competitiveness.

Finally, the security trainings improved employee satisfaction by providing dedicated time for the employees to learn important and marketable skills.

This accomplishment was enabled by several key steps on the journey to secure software development processes. First, Siemens Digital Industries Software systematically employed security scans and training to identify and remediate weaknesses in the Capital electrical system design and integration solution, leading to consistently clean summary reports up to the Open Web Application Security Project (OWASP) and other standards (OWASP, 2018). The short feedback loop achieved by using several different security scanning products in turn enabled weaknesses to be identified and resolved quickly. This was key to establishing Siemens' S-SDLC. Next, Siemens established a precedent of sharing lessons, knowledge and skills about increasing security throughout its enterprise.

Securing the enterprise's future

Today, companies are investing in the development of robust, comprehensive, and powerful safeguards against the numerous cybersecurity threats of the modern world. This is the culmination of the critical observation that cyber-criminals began targeting not just major corporations, but their supply chains as well. Companies have identified two important features their secure software development programs should possess. First, it is important to establish organization across the company. A uniform process for ensuring software security across all departments is crucial to the security of the enterprise as a whole. Second, it is critical that security programs establish consistent engagement between vendors and company management. This ensures that each vendor is meeting equal standards and receiving equal treatment.

On their journey to enhanced software security, Siemens' Capital team set benchmarks for responsiveness and the delivery of secure products and processes up to modern standards. In doing this, the Capital team also demonstrated that even large and powerful software solutions like Capital could conform to rigorous security requirements, despite their complexity.

Software vendors, however, are not solely responsible for the creation of secure products. Customers exert significant influence over the development of secure products through their buying decisions and the content included in their RFI and RFP. Customers should seek vendors with robust S-SDLC processes and established cultures of secure development. RFI and RFP should also emphasize that vendors take responsibility for the security of third party content present in their products, perform DAST and SAST security testing, and regularly produce clean security reports. By placing greater priority on software security, customers and vendors can ensure their products and processes will more effectively protect them.

References

1. Gallagher, S. (2017, October 13). Australian defense firm was hacked and F-35 data stolen, DOD confirms. Ars Technica. Retrieved from https://arstechnica.com/information-technology/2017/10/australian-defense-firm-was-hacked-and-f-35-data-stolen-dod-confirms/
2. National Institute of Standards and Technology (2018). National vulnerabilities database. Retrieved from https://nvd.nist.gov/ .
3. Online Trust Alliance (2017, January 25). Consumer data breaches level off while other incidents skyrocket. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/consumer-data-breaches-level-while-other-incidents-skyrocket .
4. Open Web Application Security Project (2018). Welcome to OWASP. The Open Web Application Security Project. Retrieved from https://www.owasp.org/index.php/Main_Page.

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software, a business unit of Siemens Digital Industries, is a leading global provider of software solutions to drive the digital transformation of industry, creating new opportunities for manufacturers to realize innovation. With headquarters in Plano, Texas, and over 140,000 customers worldwide, we work with companies of all sizes to transform the way ideas come to life, the way products are realized, and the way products and assets in operation are used and understood. For more information on our products and services, visit siemens.com/plm.

siemens.com/plm

© 2019 Siemens Product Lifecycle Management Software Inc. Siemens, the Siemens logo and SIMATIC IT are registered trademarks of Siemens AG. Camstar, D-Cubed, Femap, Fibersim, Geolus, GO PLM, I-deas, JT, NX, Parasolid, Polarion, Simcenter, Solid Edge, Syncrofit, Teamcenter and Tecnomatix are trademarks or registered trademarks of Siemens Product Lifecycle Management Software Inc. or its subsidiaries or affiliates in the United States and in other countries. All other trademarks, registered trademarks or service marks belong to their respective holders.
77783-C4 5/19 C