GRAMMATECH

THE ROLE OF STATIC ANALYSIS IN MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

INTRODUCTION

The FDA, recognizing the need for more robust security in medical devices, issued its guidance on managing cybersecurity in 2014. The growth of wireless, networked, and Internet-connected devices means that medical devices are more at risk than ever before. In addition, medical devices deal with patient safety and privacy unlike other classes of devices. Risk management (including security hardening and vulnerability management) is the cornerstone of medical device software development, and static analysis plays a key role in the process.

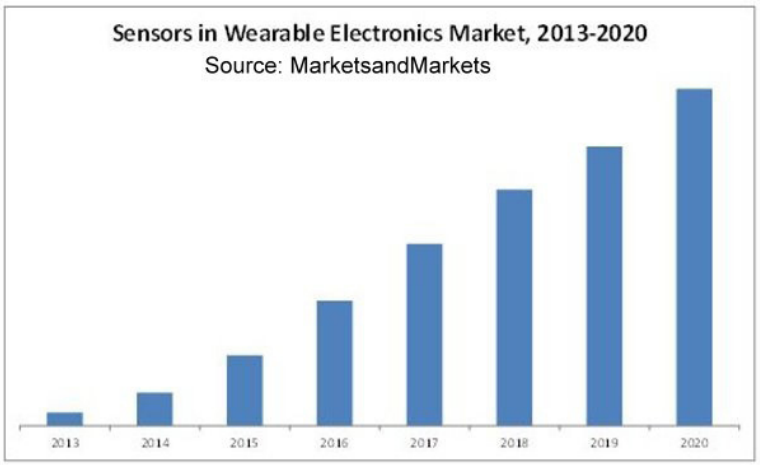

Figure 1: Wearables are primed for huge growth in the next few years. These are just one segment of medical devices concerned with security. *Source: Wearable Sensor Market Poised for Rapid Growth*

FDA GUIDANCE AND STATIC ANALYSIS

Home health care and medical "wearables" are increasing exponentially and are just one area of growth for medical devices. As with other medical and IoT opportunities, there are safety, security, and privacy concerns associated with this growth. Figure 1 to the left indicates the level of growth forecast.

The FDA-published guidance is quite broad, giving high-level direction for managing security. It includes a strong argument for automated tools, based on the following guidelines:

- **Manufacturers should address cybersecurity during the design and development of the medical device:** As something GrammaTech has been communicating for some time, building in security from the start (rather than adding it on later in development) is the key. More on this follows.
- **The design and development approach should appropriately address identification of assets, threats, and vulnerabilities:** Static analysis integrates seamlessly with good software development processes and specifically aids in detection and identification of security vulnerabilities in code and binaries.
- **Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients and the likelihood of a threat and of a vulnerability being exploited:** Using tainted data analysis, GrammaTech CodeSonar can trace the source of data throughout the software to indicate potential vulnerabilities from outside sources.
- **In the premarket submission, manufacturers should provide documentation related to the cybersecurity of their medical device:** Static analysis tools provide reporting tools to assist in process documentation, test completion, and software readiness.

SECURING MEDICAL DEVICES

Static analysis is an important part of a security-first design and development approach. GrammaTech recommends four steps to improve an existing development process, prioritizing security and making it a top-level requirement:

1. **Design with a "security-first" philosophy.**
   For highly-connected medical devices, security must be a prime consideration during all stages of development. The smart development team builds security requirements, development, and testing into the risk management plan, schedule, and budget. To address the potential unknowns and risks with device security, automated software tools are a significant boon to security assurance.

2. **A system-wide threat assessment and analysis.**
   Your medical device is part of a larger clinical environment – understanding the potential security issues at a system level is critical. Assessing the known and theoretical attack vectors to your device is essential in order to identify the security risks that feed into your risk management plan.

3. **Leverage automated tools as much as possible.**
   Security adds additional burdens to development teams and is often outside the realm of developers' expertise. Automated static analysis, for example, can find defects and security threats in code that traditional manual and automated techniques miss. Static analysis is now an essential component in the security assurance tool set.

4. **Use binary analysis to ensure the quality and security of third party code.**
   Reliance on third-party software and software of unknown quality and security is risky. Binary static analysis (and a combination of source and binary analysis) provides an automated technique for analyzing third-party software, ensuring it meets the whole system's quality and security standards.

THE RETURN ON INVESTMENT FOR STATIC ANALYSIS

Static analysis tools are highly recommended by software safety standards, and for good reason. The majority of software development costs come from fixing problems in code, so finding defects early in the development cycle can save costs dramatically. Static analysis helps reduce risk, cost, time, and money in the following ways:

- **Finds defects before unit testing:**
  Static analysis tools can be used right at the developer's desktop environment and can prevent defects before they enter the build system and the unit test phase of development.

- **Finds defects that testing misses:**
  Unit testing, even on projects demanding high code-coverage levels, can still miss important defects.

» **Prevents defects in the first place:**

Enforcing strict coding standards, such as MISRA C, can help prevent many classes of defects in code from the beginning. Enforcing good discipline in coding and creating a develop-analyze-test micro cycle for small code changes can prevent many defects from being created in the first place.

» **Analyzes SOUP:**

Use of third-party code such as commercial off-the-shelf software (COTS) and open-source software is common in medical device software development. Software of unknown pedigree (SOUP) needs to be managed carefully for safety and security before inclusion in a device. Static analysis tools can analyze third-party source and binaries to discover defects and security vulnerabilities in software that could be impossible to test otherwise.

» **Accelerates premarket submission:**

Static analysis (and many other testing and lifecycle management tools) provides automated documentation to support testing, coding standard, and quality/robustness evidence. Much of the manpower used in satisfying safety certifications is documentation and evidence production – automation (specifically static analysis) reduces this burden significantly.

CONCLUSION

Static analysis and application lifecycle management tools fit well with the FDA's published guidance on managing cybersecurity in medical devices. Following a "security-first" mindset and process, manufacturers can build-in security rather than make it an add-on. Static analysis tools provide tangible benefits within development to reduce risk, cost, and time.

REFERENCES:

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
A Four-Step Guide to Security Assurance for IoT Devices
Static analysis essential for affordable safety critical software

GrammaTech, Inc. is a leading developer of software-assurance tools and advanced cybersecurity solutions. GrammaTech helps organizations develop and release high quality software, free of harmful defects that cause system failures, enable data breaches, and increase corporate liabilities in today's connected world. GrammaTech's CodeSonar is used by embedded developers worldwide.