APRIL 2017

WHAT EMBEDDED AND IOT DEVELOPERS THINK ABOUT IOT SECURITY

A LOOK AT SURVEY DATA IN 2017

Trusted Computing Group
3855 SW 153rd Drive
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Security is one of the frequently cited major concerns with increasing internet connectivity. Working with Embedded Computing Design (ECD), the Trusted Computing Group (TCG) conducted an Internet of Things (IoT) Security Survey January to February 2017 to find if and how designers were addressing these concerns.

With broad interest in IoT security and more specifically in embedded product/systems security, the IoT survey targeted those currently involved in specifying, creating or otherwise in developing, testing and marketing embedded and/or IoT devices. This report analyzes the answers from 252 respondents, 231 of which provided complete responses.

WHO RESPONDED?

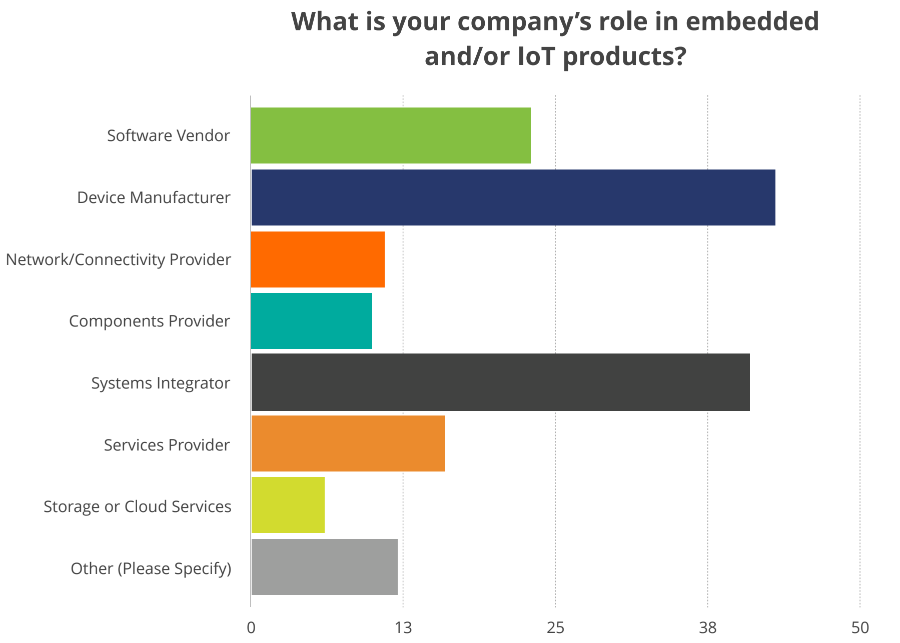


Figure 1 Respondents had eight categories to specify their company's role in embedded/IoT products.

The first question asked, "What is your company's role in embedded and/or IoT products?" The vast majority (over 80%) work for either a device manufacturer or system integrator ***(Figure 1)***.

The second question dealt with the person responding to the survey and asked, "What is your role in embedded and/ or IoT products?" In this case, the vast majority (again, over 80%) are either a hardware or software developer/ engineer ***(Figure 2)***.

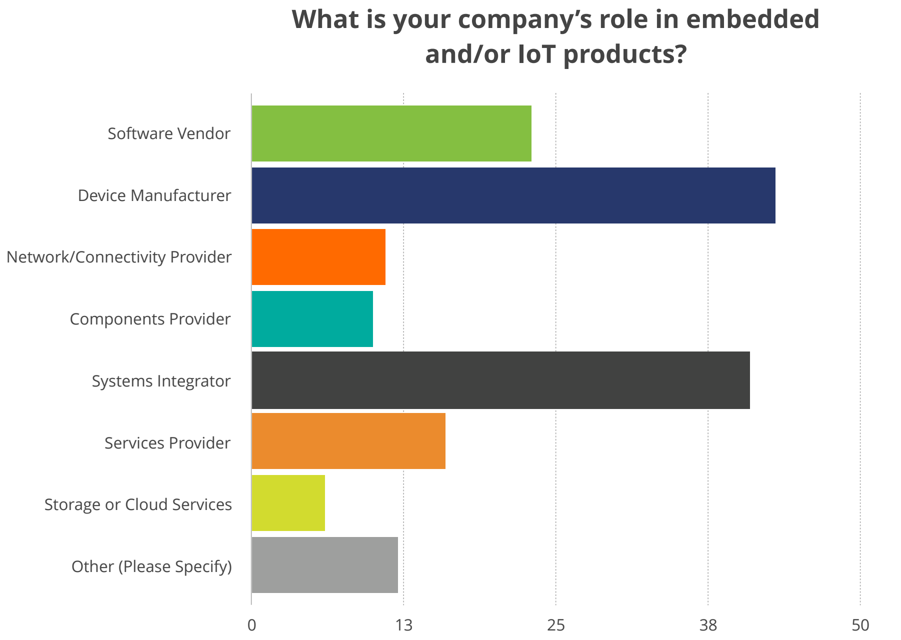
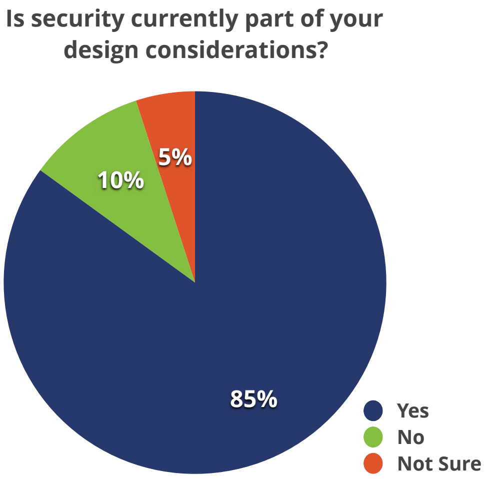


Figure 2 Respondents had 10 categories to identify the role they fulfilled in their company.

SURVEY RESULTS

In the survey, security was a part of the design considerations for 85% of the respondents and slightly less than 10% indicated that it was not. Of those who said security was not a part of current design criteria, the reasons range from not necessary, not a customer requirement, too much trouble and too expensive being almost equally weighted at slightly over 10% each ***(Figure 3)***. The predominant reason with over 50% justifying lack of attention to security in their design approach was that it was handled in another part of the system.



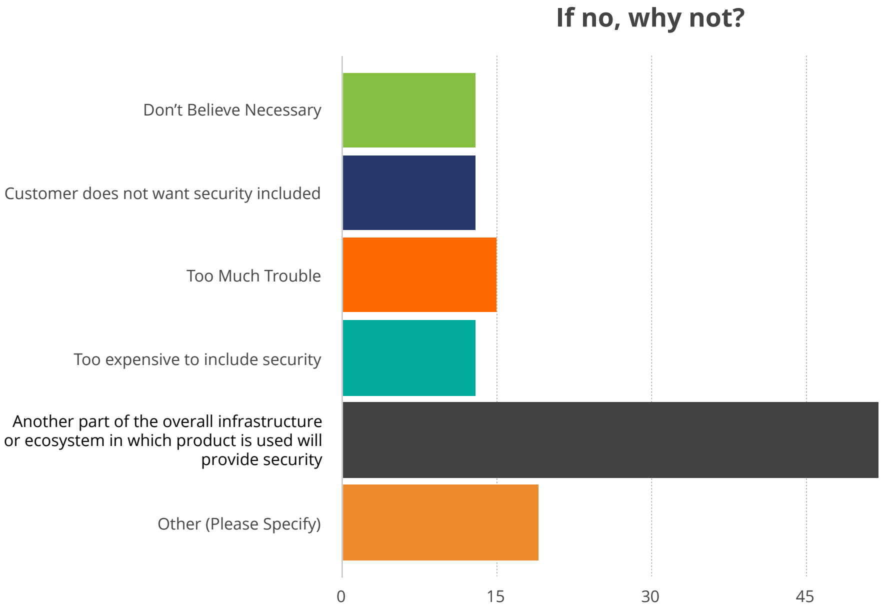


Figure 3 Reasons to not consider security in current designs.

THE ROLE OF TRUST IN EMBEDDED AND IOT PLATFORMS

In general, establishing trust in things is somewhat similar to establishing trust in people or brands. There has to be a basis for and ability to confirm trust. For objects, a Root of Trust (RoT) provides the starting point. A standards-based RoT establishes the foundation for building trust and a hardware root of trust (HRoT) is widely accepted as more secure than software that can be more easily breached by attackers.

TCG's Trusted Platform Module open standard defines a HRoT and its associated security aspects. The TPM specification has been adopted as an international standard ISO/IEC 11889:2015. Through NIST SP 800-164 and National Security Agency (NSA) HAP, or High Assurance Program and other programs, the TPM is being implemented in numerous U.S government security efforts.

TCG's Trusted Platform Module standard addresses secure device identity, user authentication, secure boot, secure software updates, secure communications (especially when used in conjunction with TCG's Trusted Network Communications (TNC) specification, secure storage (especially when used with TCG's self-encrypting drives (SEDs) specification) and privacy protection.

The recently announced TPM 2.0 implements a "library" approach that allows users to choose applicable aspects of TPM functionality for different implementation levels and levels of security and extends the computing/server capability to a variety of embedded devices.

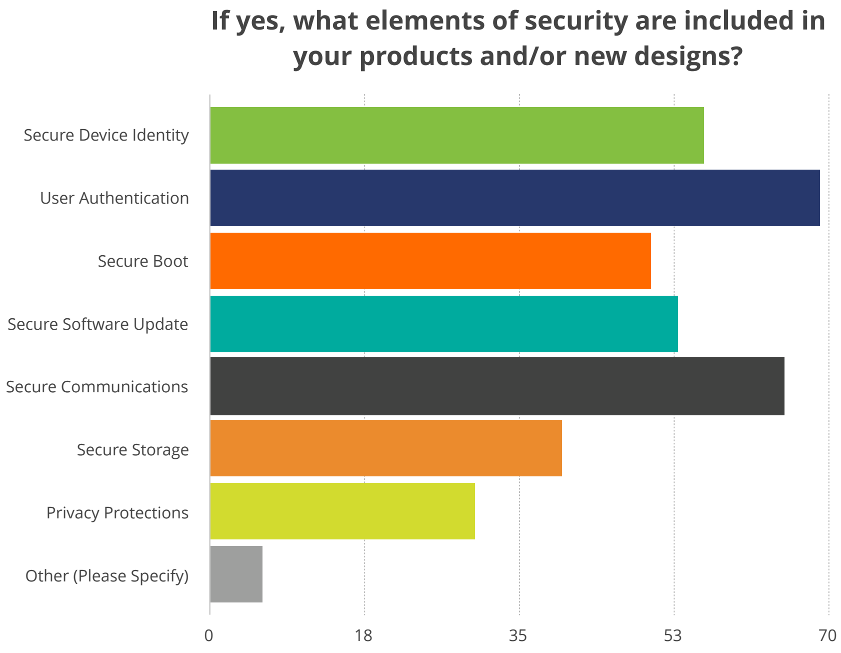


Figure 4 Security aspects included in respondents' products and/or new designs.

For those who indicated that security was an integral part of their designs, the security elements included in products and/or new designs fall into several categories ***(Figure 4)***. Ranging from slightly less than 30% privacy protection to almost 70% for user authentication, seven distinct areas were identified as important design considerations.

By addressing security, the respondents and their companies' goals ranged from improving reliability, increasing safety, reducing fraud, avoiding recalls, addressing potential liabilities and protecting user privacy with different levels of importance ***(Figure 5)***. Increased safety and protecting confidential data were the two leading goals with over 65% for each one. The lowest identified goal was to avoid recalls with slightly less than 20% addressing this goal.

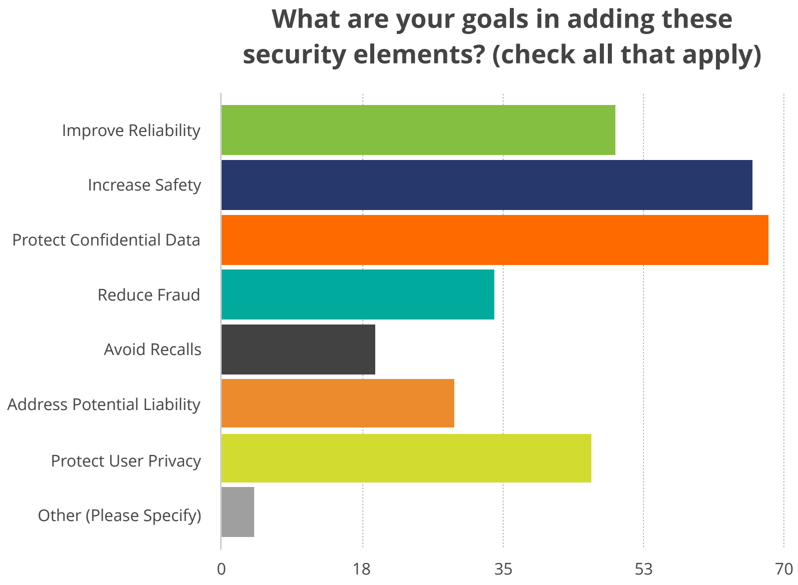
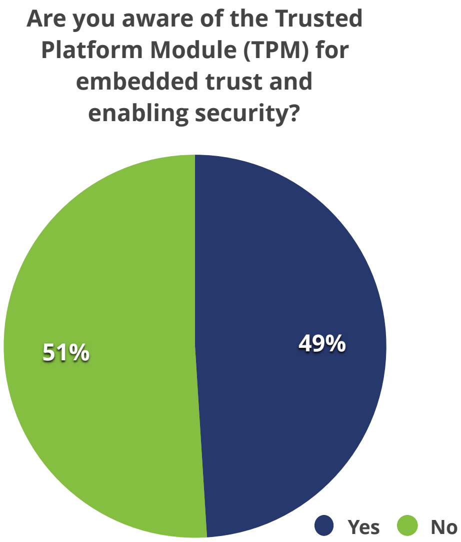


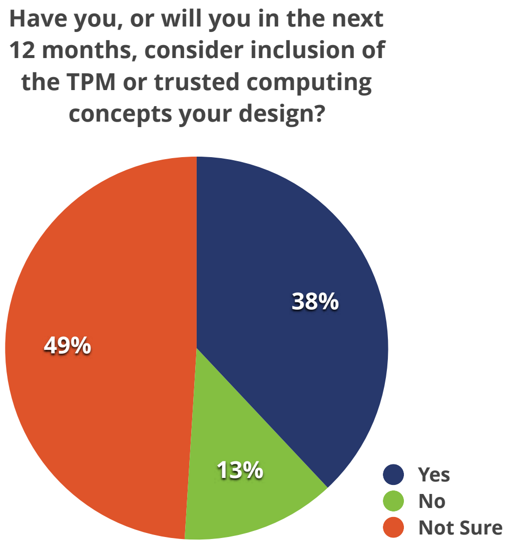
Figure 5 Identified security design goals with their associated significance to respondents.

With experts from industry leading hardware and software suppliers, TCG has been addressing security by developing open specifications to improve the trust and security of computers, servers, networks and more for well over 10 years. When asked if they were aware of the Trusted Platform Module for embedded trust and enabling security, respondents were essentially equally split between yes and no.

Within the next 12 months, 38% of the 251 respondents will consider inclusion of the TPM or trusted computing concepts developed by TCG in their design, with 13% not including them and 49% not sure. Of those who answered no or are unsure, 142 identified four specific alternatives being considered as well as divine intervention to prevent security problems ***(Figure 6)***.

With the time invested considered quite valuable, over 80%+ of the respondents were interested in obtaining the results of the survey.





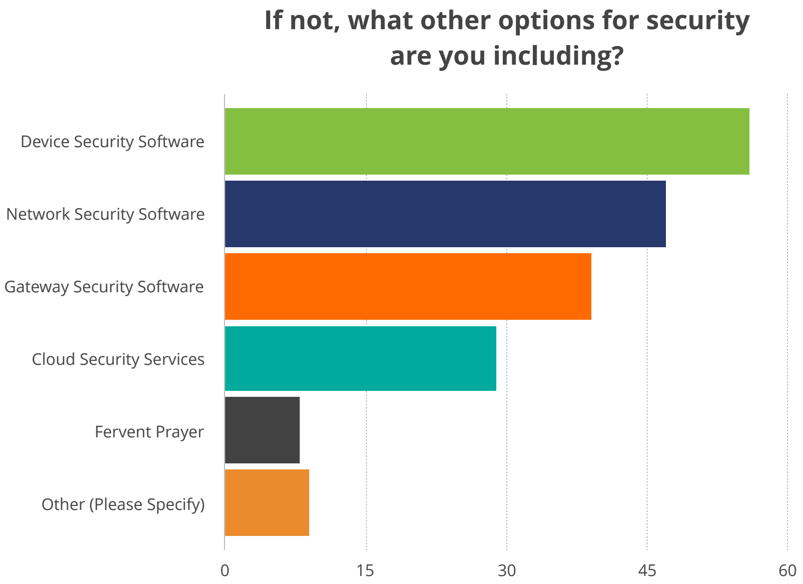


Figure 6 Other options to avoid the risks of an insecure product/system.

CONCLUSIONS

The goal of this survey was to determine and quantify the extent that embedded systems experts took into account the need for trust and security in their product activities. With security as a part of the design considerations for 85% of the respondents and the elements of security that are included in products and/or new designs and identified security design goals quantified, embedded systems experts, for the most part, have prioritized the roll that security currently plays in their designs.

The high level of respondents who are interested in receiving the results of the survey indicates that competitive and peer pressure could play a significant role in increasing security and trust in future designs.

The number of respondents who were unaware of TCG's TPM indicates that there is a continuing need for increased awareness among embedded engineers. Even those who were aware of the TPM may not be fully up to speed with the latest version, TPM 2.0, targeted specifically for embedded applications.

RECOMMENDATIONS

Despite the reasonably high level of awareness shown by respondents, ongoing awareness efforts of the Trusted Computing Group should increase the ease of implementing security and desired level of trust in current and future designs.

The recently release TPM 2.0 specification extends the benefits of hardware-based trust to embedded applications. Specific market segments that have indicated a need for improved trust in embedded products include smart vehicles, smart factories, smart buildings, smart homes and even smart cities – essentially any market where increased connectivity could attract hackers. In addition to unauthorized product/system access, the hackers could obtain confidential data, proprietary information including financial transaction details and in general wreak havoc on unprotected or poorly protected systems through access allowed by unprotected or poorly protected embedded and connected devices.

To avoid application security issues, embedded designers need to determine the implications that connecting their product to the internet could have to the end system design and take appropriate actions to mitigate the problems. The Trusted Computing Group and its member companies provide a variety of resources in these efforts. TCG's ***"Guidance for Securing IoT Using TCG Technology"*** is a specific starting point for the next step and includes several references for further information. *(See Below)*

RESOURCES TO HELP DESIGNERS AND DEVELOPERS OF EMBEDDED SYSTEMS

SUGGESTED READING FOR IMPROVED SECURITY/TRUST UNDERSTANDING

1. "Trusted Platform Module 2.0: A Brief Introduction," Trusted Computing Group

2. "Trusted Network Communications," Trusted Computing Group

3. "Guidance for Securing IoT Using TCG Technology Version 1.0, Revision 21," Trusted Computing Group

4. "Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age," SANS Institute InfoSec Reading Room

5. "Why TPM 2.0?"

6. "Establishing Network Equipment Security," Trusted Computing Group

7. An "open access" book intended to get one started with TPMs:
A Practical Guide to TPM 2.0 - Using the Trusted Platform Module in the New Age of Security, Arthur, Challener, 2015

8. A reference book intended to help explain TPMs: Trusted Computing Platforms - TPM2.0 in Context, Proudler, Chen, Dalton; Springer, 2014

USER GUIDES/PUBLICATIONS

1. "Intel® Trusted Platform Module User Guide," Intel

2. "ST33TPMF2ESPI, Trusted Platform Module 1.2 & 2.0 with TCG SPI interface," STMicroelectronics

3. "OPTIGA™ TPM, Protecting integrity and authenticity of embedded devices and systems," Infineon Technologies

DEVELOPMENT KITS

1. "Get Started - Trusted Platform Module," Microchip Technology