SPYRUS®

Ten security questions to consider...

...before deploying your IoT hardware

Q1: Has the vendor of the IoT device you are considering using made any representations as to the device's embedded security?

- Does the vendor provide guidance on risk management of an IoT deployment that maps the purchaser's target level of residual risk to a required assurance level? For example, IoT systems for financial services, telemedicine or advanced driver assistance systems (ADAS) may have a high potential risk profile and require the highest assurance of privacy and anti-tamper. Conversely, a smart IoT backyard sprinkler system would likely require a much lower assurance level.
- Does the vendor provide guidance on balancing the assurance level across the IoT devices in a common network? If high and low assurance components are mixed, is there an indicator of what residual system risk may result?
- How does the purchaser know these representations to be true?
- IoT product representations about security that have not been verified by a third party validation such as a FIPS 140-2 or similar certification should be substantiated by reliable sources. This should include verification by the original security component manufacturer.
- Guidance should encourage the buyer to reassess the risk of any deployed IoT system on a regular basis and continuously evaluate maintenance and upgrade decisions as new threats emerge.

Q2: Does the IoT device include hardware that is certified for security? If so what certification and to what level?

- For medium risk deployments and above, the IoT device should include FIPS 140-2 Level 3 certified hardware such as the SPYRUS Rosetta enabled products.
- For deployments at highly risk-adverse sites, both FIPS 140-2 and Common Criteria certification to a specified protection profile would be recommended. For higher risk scenarios, including sensitive information for law enforcement and/or homeland security additional dual layer cryptographic protection solutions may be required.
- Buyers should be aware of emerging standards in the NIST SP 800 series that may currently, or in the future, apply to IoT risk scenarios. A recent highly relevant publication is SP800-160 that deals with "Engineering of Trustworthy Secure Systems". Products certified against these standards will provide a higher mitigation factor than uncertified devices.

Q3: What testing has the security hardware used by the IoT device undergone from a security perspective?

- All Rosetta microSDHC and SPYCOS 3.0 component have been FIPS 140-2 Level 3 certified.
- The SPYRUS USB-3 products, such as the P-3X and secure Windows-To-Go products, have also been FIPS 140-2 Level 3 certified and also include a PKI HSM certified to FIPS 140-2 Level 3 and EAL5+ Common Criteria.
- The SPYRUS TrustedFlash™ (full disk encrypted Rosetta microSDHC) is currently in the validation process for a FIPS 140-2 Level 3 certification.

Q4: How is the firmware for the IoT device upgraded?

- The upgrade mechanism should include an authentication mechanism, which provides assurance that the source is genuine. This should be done over a secure communication channel, which also authenticates the upgrade portal to the IoT device being upgraded.
- The use of strong cryptographic assurance through digitally signed upgrade content is essential at every risk level.

Q5: What authentication mechanism does the vendor use to upgrade the IoT device Firmware?

- How secure is the mechanism being employed? It should provide countermeasures to protect against the expected threats in the environment in which it will operate. FIPS 140-2 Level 3 authentication over a secure channel that satisfies SP 800-56A or equivalent key establishment is essential, as well as suitable symmetric key sizes for the session key for moderate to high risk scenarios.
- SPYRUS Rosetta products can be integrated to provide a hardware-based, high assurance authentication mechanism.
- IoT firmware updates should also be verified against malware infusion or corruption through the use of digital signature methods. SPYRUS Rosetta products contain the capability for verification of both RSA and ECDSA methods to only allow unaltered updates from an authenticated source to be accepted.

Q6: Is the IoT device insulated against malware such as zombie malware that may instigate a DDOS attack; and if so, how?

- In recent times the hijacking of IoT connected devices to create "bot swarms" which support Distributed Denial of Service (DDOS) attacks has become a significant concern. State of the art DDOS incident response countermeasures and procedures are essential. These will evolve with current safeguard network technology and ISP response posture.
- IT security staff must have or prepare a comprehensive incident response plan. This should describe roles and responsibilities, procedures and communications. Without the assurance of a tested plan, an information security breach may become repeatedly worse and more costly to the organization and individuals dependent on IoT functionality, data availability and integrity.
- SPYRUS devices contain the Rosetta Micro as a "hardware root of trust", providing an EAL5+ tamper resistant, FIPS 140-2 Level 3 "trust anchor" that sharply mitigates hijacking and spurious command interference.

Q7: Is the IoT device intended to be deployed in a safety critical or financial critical environment?

- This requires extra assurance that the security of the IoT device cannot be compromised, as security representations made by the vendor become significant, and require more thorough investigation.
- SPYRUS offers, in addition to the Rosetta hardware security module and its other security products, licenses to patented technology, which act upon the content or payload information to ensure that the application is cryptographically authenticated to work with the particular IoT device, and capable of setting privileges and limitations under which the application can operate. This mitigates masquerading attacks by unauthorized software developers or injection attacks by hackers. The points raised in Question 1 are also highly relevant to this issue.

Q8: What is the impact of any representations made by Vendor concerning security?

- In order to sell their IoT products, vendors will make representations concerning the functionality of their products so that they stand out in an increasingly crowded market. The real issues that arise concern the warranties the IoT device provider is offering and any limitation of liability that follows. Security of IoT devices must not be limited to internal security but should extend to external security. That is, not only should the IoT device be protected against malware that can interrupt the operations of the IoT Device but it should also be protected against malware that could use the IoT device as a vehicle for further attacks against third party environments. A current example is the Mirai Botnet, which attacks IoT endpoints directly and circumvents firewall and network protection. One solution to request of the vendor in order to mitigate such malware threats would be for the vendor to verify that only applications that are digitally verified by cryptographic signature from trusted sources have the permission to execute on the device. Legal ramifications can arise and as such careful consideration needs to be taken in dealing with IoT contracts.

Q9: Does the IoT device (s) need to be integrated into other systems and where does the risk sit for this?

- The deployment of IoT devices is unlikely to be isolated from other systems. This is a connected world and as such the benefit of IoT is the interconnection of such devices. Hence, IoT device integration will most likely impact legacy system environments which can have a flow down affect to various pre-existing contractual arrangements. Care needs to be undertaken especially with limitation of liability clauses as they may suddenly apply. A contractual audit is suggested so that the risks involved are better understood and consequential liabilities are bounded. In particular, the system integrator for the IoT device must take a responsibility to verify safe secure operation in the delivered system under a scenario of various attacks and, in order to minimize operational and legal risks, the IoT vendor selection should be made on the basis of the device security provisions to mitigate and defend against such attacks.

SPYRUS®

Q10: Does the IoT device collect any data (including meta-data) that would fall within any privacy/security regime?

Privacy and security is becoming an important issue from a legal perspective. All IoT devices collect data and if that environment includes human interaction then an added complexity is involved. Some typical concerns are:

- What private information is being collected?
- How does a user "opt out" of collection of private data?
- Where that data is stored from both a jurisdictional perspective and a security position?
- Who has access to that data
- Is the IoT vendor precluded from accessing the data once the device ownership is transferred?
- How is the collected going to be used?
- Will data analytics or machine learning be involved as a backend process?

The technology for IoT is evolving at a rapid pace and security is an essential element that must not be overlooked. Most IoT devices do not have appropriate security embedded and as such additional technology should be deployed such as HSM (Hardware Security modules) which can greatly assist in reducing risk. Further, the law is ever changing and class actions are becoming more prevalent in this area so it is prudent to obtain legal advice in all of these areas so that you better understand the risks involved and how to treat those risks to manageable level and if an incident does arise how to mitigate the impact upon your business. Finally, regulators are now taking a keen interest in the deployment of IoT devices as evidenced by an increasing number of actions against networking and other providers.

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

SUITE B ON BOARD

Western Region/Asia/Pacific Region
Tom Dickens
(408) 392-4324 phone
tdickens@SPYRUS.com

Central Region
Steve Tonkovich
(630) 215-9393 phone
stonkovich@spyrus.com

Eastern Region / EMEA
Rich Skibo
(732) 329-6006
rskibo@spyrus.com