Abstract:

Side-channel attacks represent a serious threat to the security of encrypted firmware updates: if the secret key is leaked, then the firmware is exposed and can be replaced by malicious code or be stolen. In this work, we show how simple anomaly detection measures can effectively increase the security of encrypted firmware updates at minimum cost. Our method is based on the simple observation that firmware payloads have a specific structure (machine code), which can be easily verified at runtime in order to react to side-channel attacks. This enables performing proactive measures to limit the number of measurements that can be taken when a side-channel attack is detected. We tested the viability of our approach through simulations and verified its effectiveness in practice on a TI MSP430 microcontroller using a software implementation of AES. Our approach represents a step forward towards increasing the security of firmware updates against side-channel attacks: it effectively increases the security of firmware updates, has only
negligible overhead in terms of code size and runtime, requires no modification to the underlying
 cryptographic implementations, and can be used in conjunction with countermeasures such as
 masking and re-keying to further enhance the side-channel resistance of a device.

Stichworte: Side-Channel Analysis, Anomaly Detection, Embedded Devices, Secure Firmware Updates, Decryption

Dewey Dezimalklassifikation (Liste): 620 Ingenieurwissenschaften

Kongress- / Buchtitel: 9th International Symposium on Foundations & Practice of Security (FPS)

Kongress / Zusatzinformationen: Quebec, Canada

Datum der Konferenz: 10/2016

Jahr: 2016

Quartal: 4. Quartal

Jahr / Monat: 2016-10

Monat: Oct

Revied: ja

Sprache: en

WWW: https://www.fps2016.fsg.ulaval.ca/no_cache/home/

Occurences:
- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

entries: