Na elektroniku všade okolo nás sme si už zvykli tak, že si jej prítomnosť ani nevšímame a je súčasťou nášho každodenného života. Niektoré elektronické zariadenia, resp. údaje v nich uchovávané a spracovávané, však predstavujú vážny prvok bezpečnosti majetku a súkromia, a tak je potrebné ich konštruovať s dôkladným zvážením všetkých možností ich zneužitia. Typicky sa jedná o údaje finančného charakteru a o prenos citlivých informácií, aj keď sú aj iné oblasti s podobným charakterom.

Obvykle sa tento problém zužuje na použitie bezpečného modulu, t.j. akejsi "šifrovacej skrinky", ktorá zabezpečuje zašifrovanie alebo bezpečné podpísanie (hash) údajov pred prenosom či uchovaním na menej zabezpečenom médiu, a na druhej strane aj samozrejme opačný proces - odšifrovanie, overenie podpisu. Bezpečnostný modul obsahuje teda hradware potrebné na šifrovanie (mikrokontrolér, FPGA, ASIC), a pamäť uchovávajúcu šifrovacie kľúče. A práve tieto kľúče sú predmetom najvyššieho stupňa ochrany pred odcudzením.

Paranoia (stihomam) je vážna psychiatrická diagnóza, avšak stav mysle návrhára bezpečného modulu je nie nepodobný tomuto stavu. Musí hrať akúsi virtuálnu hru na mačku a myš, odhadnúť možné spôsoby odcudzenia kľúčov, a proti nim postaviť niekoľko úrovní zábran a pascí. Bezpečnostný modul preto okrem spomínaných "funkčných" súčastí musí obsahovať aj sústavu snímačov, ktoré detekujú pokus o "vlámanie", a samozrejme aj mechanické zábrany - elektronika je zaliata vo vhodnej hmote a uzavretá v zavarenej oceľovej skrinke.

Zdalo by sa, že v prípade odpojenia skrinky od napájania budú kľúče v RAM jednoducho "zabudnuté". Nie je tomu tak - polovodičové pamäte uchovávajú svoj stav prekvapujúco dlho aj po odpojení napájania, čomu môže útočník ešte napomôsť prudkým schladením pamätí. Čo je ešte horšie - bežné pamäte si pri dlhodobom uchovávaní nejakého údaju vytvoria akýsi "odtlačok", nesymetriu vo vlastnostiach, ktorá umožní získať pôvodný stav pamäte aj po krátkodobom prepísaní. Pritom útočníkovi môže stačiť aj poškodený kľúč - zo znalosti metódy šifrovania (ktorá je obvykle štandardizovaná z množstva dôvodov zasluhujúcich si ďalší článoček) a časti zašifrovanej komunikácie sa môže dať poškodená časť kľúča zrekonštruovať.

Takže bezpečný modul musí obsahovať naviac aj zálohovaciu batériu (samozrejme s monitoringom jej stavu), aby bolo možné kľúče aktívne prepísať pri detekcii pokusu o narušenie (alebo trebárs nečakané ochladenie). Obsah pamäte musí byť tiež neustále prepisovaný, aby sa predišlo "odtlačeniu", zároveň však musí byť zachovaná integrita uchovávaných kľúčov.

A keďže je týchto "maličkostí" už pomerne dosť, úlohu vývojárovi takéhoto bezpečného modulu uľahčuje "dvojfirmie" Dallas-Maxim svojimi zvláštnymi bezpečnými dohliadacími obvodmi radu DS36xx. Nie je to náhoda - tieto obvody dopĺňajú ich portfólio bezpečných procesorov.

Vlastnosti

Základnou vlastnosťou všetkých obvodov radu DS36xx je sledovanie vstupov indikujúcich narušenie - monitor napájacieho napätia a zálohovacieho napätia, ďalej rôzny počet sledovaných analógových a digitálnych vstupov, záchytný register s výstupom indikujúcim narušenie a obvod hodín (RTC). Komunikácia s nadradeným procesorom je prostredníctvom sériovej zbernice typu I2C alebo SPI.

K tomuto je v jednotlivých obvodoch pridaný mix doplňujúcich vlastností:

- interná pamäť pre kľúč - jedná sa o pomerne malú RAM (64B-4kB) pre "master" kľúče, avšak ide o špeciálnu pamäť v ktorej sa nevytvára "odtlačok", a je automaticky a rýchlo vymazaná v prípade detekcie narušenia

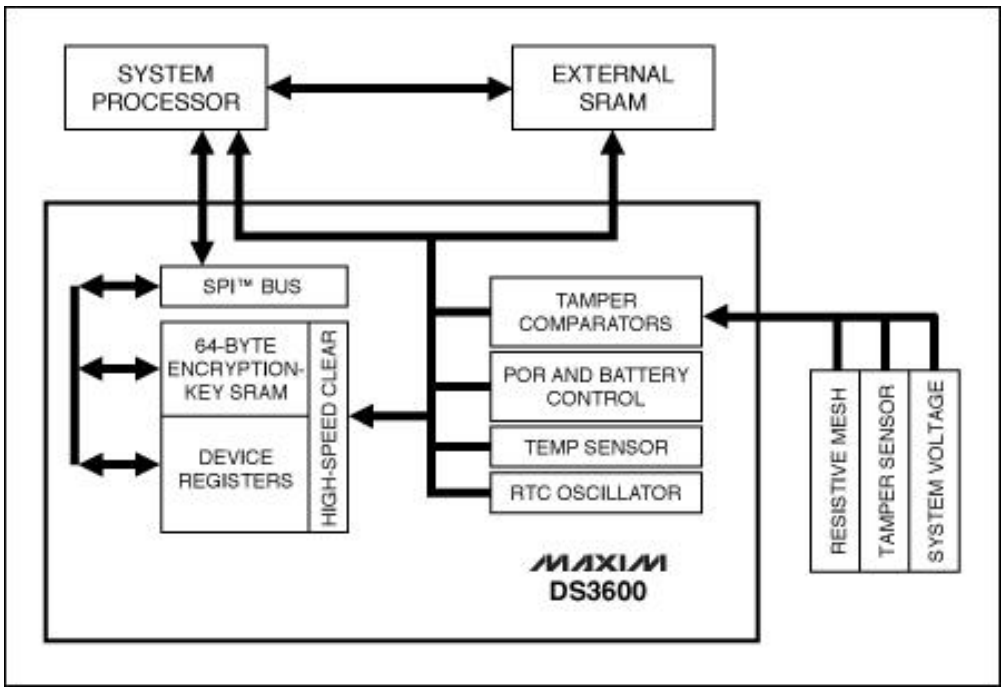
- podpora pre externú SRAM

- podpora pre zálohované externé obvody - jedná sa o obvyklé automatické prepnutie na zálohovacie napätie v prípade výpadku napájania

- generátor náhodného čísla

- monitor teploty - pre zabránenie útoku prudkým ochladením či prehriatím

Blokové zapojenie



Cena

Keďže sa jedná o citlivé záležitosti, dá sa očakávať, že tieto súčiastky nebudú vo voľnom predaji. Dokonca k nim nie je voľne stiahnuteľný ani datasheet - výrobca vyžaduje vyplnenie formulára, v ktorom žiadateľ odôvodňuje záujem o tieto obvody.

Odkazy

Prehľad konkrétnych produktov

Distribúcia

viď. Adresár