ESCLUSIVA

Proteggere dati e IP con le security feature delle memorie flash

Bill Stafford
Marketing director
Embedded Flash-memory Segment
Numonyx

I componenti flash offrono diversi meccanismi per proteggere i dati, ognuno con specifici vantaggi per la protezione contro la lettura, la cancellazione o la scrittura

Si provi a immaginare che il sistema progettato venga modificato a sproposito, magari inavvertitamente. Può capitare che un fornitore di servizi, installando il proprio software, alteri il programma originale. Senza volerlo, certo. Il problema però esiste. Oppure, può capitare che gli hacker o i ladri di Proprietà Intellettuale (IP) si diano da fare per cancellare, copiare o clonare i dati memorizzati nel proprio sistema. Dopotutto, i ladri di IP hanno centinaia di milioni di dollari di incentivo per impadronirsi dei propri progetti (da una ricerca del Congresso USA, presentata nel documento "Bill S.522" del 7 febbraio 2007).
Non deve quindi sorprendere che i progettisti siano alla ricerca di un modo per proteggere l'integrità del sistema. La sorpresa, invece, è che una memoria flash può contenere all'interno dei suoi bit e dei suoi blocchi la chiave per la protezione del firmware, o addirittura del progetto hardware.
I componenti flash offrono diversi meccanismi per proteggere i dati: ognuno con specifici vantaggi per la protezione contro la lettura, la cancellazione o la scrittura. Queste funzioni per la sicurezza sono una barriera in più per rallentare potenziali hacker o malintenzionati e per fornire maggiori garanzie contro eventuali modifiche non intenzionali. Alcune delle funzioni di sicurezza delle memorie flash non aumentano neppure il costo del progetto finale. Anche se le funzioni di sicurezza più sofisticate possono incrementare il costo della memoria rispetto a una flash standard, si tratta comunque di un risparmio notevole rispetto all'uso di algoritmi crittografici hardware non basati su flash, o di funzioni nascoste, di operazioni autenticate, di applicazioni software per la crittografia.
Non tutti i produttori offrono le stesse funzioni; a volte neppure tutti i dispositivi dello stesso produttore. Il progettista deve scegliere il componente flash giusto per la sua applicazione finale considerando vari fattori tra cui le funzioni per la sicurezza, le prestazioni, la densità, le dimensioni e il costo.

Alla ricerca della giusta soluzione

Per valutare le varie opzioni innanzitutto è necessario identificare il problema da risolvere. Alcune caratteristiche particolari rispondono a esigenze specifiche, oppure fanno aumentare il costo.
La prima cosa da fare è stabilire che cosa sia importante proteggere tra i propri bit, dati, o codici di programma. Il progettista, per esempio, può decidere di proteggere il serial number (numero seriale del sistema elettronico), le chiavi di sicurezza, il "boot code" (programma di inizializzazione) o le informazioni finanziarie utilizzate per accedere a servizi a pagamento come la pay TV.
Quando si è stabilito cosa proteggere, bisogna valutare se i bit, i dati o il codice di programma possono essere modificati tramite attacchi esterni di tipo fisico, o tramite attacchi software. Un attacco software, per esempio, può provenire da Internet o da un applicativo di sistema. Un attacco fisico può essere la rimozione della memoria flash dalla scheda a circuito stampato. Infine, bisogna stabilire se il pericolo può avere origine intenzionale o involontaria. Le modifiche involontarie, dovute per esempio a un software non ben collaudato, normalmente sono più facili da evitare perché la causa del problema è meno sfuggente. Se si vuole invece proteggersi dall'attacco di un hacker o di un ladro, si può provare a quantificare il livello massimo di sforzo che, secondo la propria valutazione, vorrà dedicare all'impresa. Quanto più l'hacker è disposto a spendere tempo e denaro, tanto più si dovrà prestare attenzione alla sicurezza del progetto. Partendo da questi elementi, è necessario valutare quali siano le funzioni di sicurezza delle memorie flash che offrono un livello di protezione adeguato rispetto all'attacco potenziale che è stato identificato. Se, per esempio, è necessario proteggere il progetto da una modifica dei dati tramite Internet, il meccanismo di "block locking" (congelamento del con-

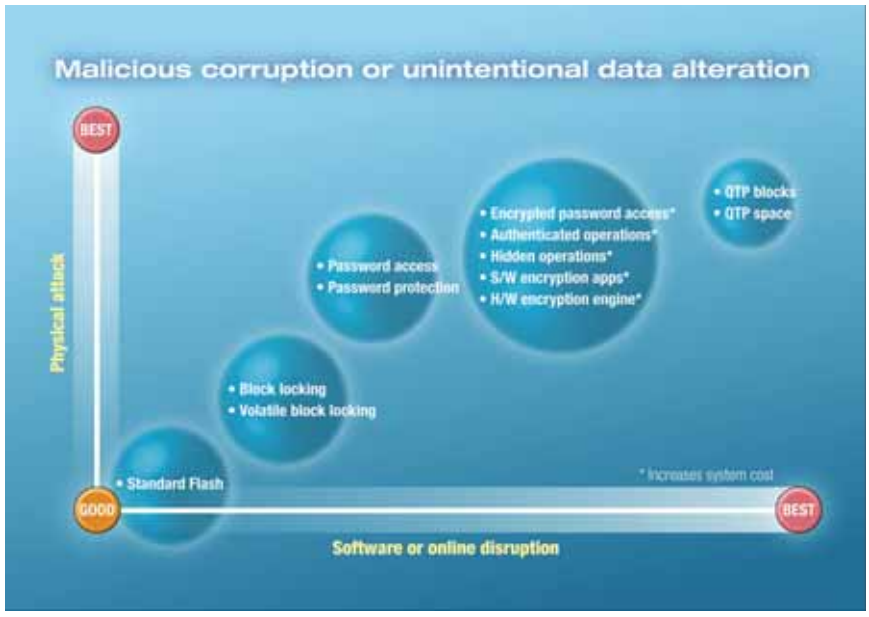

Fig. 1 - Diverse opzioni per la sicurezza offrono differenti livelli di protezione contro attacchi fisici o problemi software, azioni fraudolente o modifiche non intenzionali dei dati. È importante sottolineare che il costo del sistema aumenta se si aggiungono funzioni come il controllo di accesso con password crittografata, operazioni autenticate, operazioni nascoste o applicazioni di crittografia software e motori crittografici hardware

tenuto di un blocco di memoria) è già sufficientemente adeguato e una memoria OTP offre la migliore protezione possibile (Fig. 1). Se invece il sistema può essere attaccato da un ladro di Proprietà Intellettuale, disposto a rimuovere la flash per cercare di leggerne i dati con un programmatore di prom, allora si può ricorrere a una protezione un po' più costosa basata sulla codifica crittografica del contenuto della memoria (Fig. 2).

Analisi dettagliata delle varie funzionalità

Dal semplice "block locking" al più sofisticato controllo di accesso con password di decodifica, si deve valutare con attenzione quale sia la funzionalità più adatta ad affrontare il tipo e la provenienza dell'attacco fraudolento, con un costo accettabile per il proprio progetto.

Password di accesso

Alcuni componenti flash offrono una funzione di protezione tramite password che può complicare il lavoro dei malintenzionati e creare una barriera di protezione per rendere il sistema meno vulnerabile a essere copiato o clonato. I ladri di IP hanno bisogno di copiare i dati di sistema rapidamente e senza complicazioni. La protezione di accesso tramite password allunga i tempi, aumenta i costi e lo sforzo necessario per una semplice operazione di copiatura.

In base al tipo di flash, la password di accesso può essere utilizzata per proteggere tutta la memoria o solo alcuni blocchi selezionati evitandone la programmazione, la cancellazione o la lettura. È possibile impostare separatamente per ogni blocco il livello di protezione voluto. Prima che il sistema lasci la fabbrica per essere consegnato all'utente finale è necessario memorizzare una password a 64 bit nell'apposita area della flash. Una password corrispondente deve poi essere programmata nel microcontrollore di sistema.

Quando viene ricevuto un comando di lettura, modifica o cancellazione dei dati memorizzati nei blocchi protetti, il microcontrollore verifica la corrispondenza tra la password di sistema e quella memorizzata nel componente flash. Se l'esito è negativo, non è possibile leggere o modificare i dati. Se invece le due password corrispondono, si potranno leggere o modificare i singoli blocchi. In base al tipo di flash, i progettisti possono scegliere diverse modalità di protezione e inibire la lettura, la modifica o la sostituzione.

Protezione con password – un deterrente al furto di servizi

Utilizzare una password per la protezione contro letture non autorizzate è un meccanismo semplice ed economico per contrastare la distribuzione di chip flash pirata per accedere senza autorizzazione a servizi a pagamento. Usando chip flash duplicati, infatti, l'utente potrebbe accedere a servizi per i quali non ha sottoscritto l'abbonamento – una perdita secca di fatturato per il fornitore del servizio. Se invece il progettista ha utilizzato una password di protezione per la flash, il pirata si trova tra le mani componenti inutilizzabili.

Se un aspirante ladro di servizi cerca di leggere i dati nella flash, il dispositivo verifica la password a 64 bit. In caso di esito è negativo, viene generata in uscita solo una serie di "0". Il chip copiato non è utilizzabile.

Si supponga che il ladro riesca ad analizzare il traffico sul bus, a scoprire la password e copiare i dati dal chip. Quando inserirà la memoria piratata in un nuovo sistema, la password non corrisponderà a quella del microcontrollore e quindi, ancora una volta, il chip non sarà utilizzabile.

Protezione con password – un deterrente contro la copiatura e la clonatura di IP

Nel caso di clonatura, il ladro di IP deve copiare e produrre il progetto in tempi

Fig. 2 - Diverse funzioni di sicurezza offerte dalle memorie flash aiutano a proteggere dalla copiatura e dal furto della proprietà intellettuale. È importante sottolineare che l'aggiunta di queste funzioni può aumentare il costo del sistema

rapidi, prima che ne venga rilasciata una versione aggiornata che rende obsoleto il clone. La protezione della flash tramite password può essere sufficiente per creare un ritardo temporale tale da convincere il malintenzionato a cercare un obiettivo più facile – perché la flash protegge la firma hardware del sistema.
Un dispositivo flash con una password a 64 bit permetterà l'accesso solo a chi è effettivamente autorizzato.
Senza password, il "copiatore" che utilizza un programmatore di prom per leggere il contenuto del chip vedrà solo una sequenza di "0".
Se il copiatore decide di utilizzare delle tecniche di analisi del traffico sul bus per scoprire la password, ha bisogno di più tempo e denaro e l'operazione è più difficile. Questo ritardo dà al produttore un vantaggio temporale sul mercato rispetto alla possibile concorrenza proveniente dal prodotto clonato. Il produttore originale potrebbe addirittura riuscire a creare una versione aggiornata del progetto prima che i clonatori realizzino un prodotto realmente concorrente. Questa caratteristica di sicurezza, integrata nella flash, è un metodo economicamente molto conveniente per contrastare le perdite di fatturato conseguenti a un possibile furto di IP.

Password di accesso crittografata – maggiore sicurezza per i blocchi di IP

Una password a 64 bit complica già il lavoro di un clonatore o di un ladro di servizi. Ma una password crittografata offre un livello di protezione dei dati ancora maggiore. Un piccolo numero di dispositivi flash integra la possibilità di crittografare la password con un algoritmo implementato su silicio.
Entrambe le password della memoria flash e del microcontrollore sono crittografate. Il processore decodifica le password utilizzando un apposito algoritmo e ne conferma la validità. Chi analizza il traffico sul bus può leggere solo la password crittografata ma non è in grado di decodificarla. Quindi, senza la password decodificata il chip flash non è accessibile e l'IP è protetto.
I componenti flash con password crittografate di norma hanno un prezzo più elevato, perché l'algoritmo crittografico è implementato su silicio e fa aumentare il costo del componente. Tuttavia, il costo del chip flash può essere trascurabile rispetto alla potenziale perdita di fatturato. Se gli aggiornamenti successivi di un prodotto avvengono in tempi relativamente lunghi, l'utilizzo di una password crittografata può essere uno strumento fondamentale per impedire che il sistema clonato venga immesso sul mercato prima che il produttore originale abbia il tempo di commercializzarne una nuova versione.

Sezione OTP, programmabile solo una volta

Alcuni componenti flash comprendono una sezione programmabile una sola volta, OTP (One-Time Programming), un'area di sistema in cui i bit programmati vengono "congelati" in modo permanente. Una volta che ciò è avvenuto, i blocchi corrispondenti non possono essere più programmati o cancellati.
La sezione OTP è divisa in due segmenti. Uno viene programmato in fabbrica e contiene un numero univoco e non modificabile. Il secondo è lasciato a disposizione del progettista che può usarlo come desidera. Normalmente, i componenti flash con OTP mettono a disposizione fino a un massimo di 2112 bit per ogni segmento.

Blocchi OTP – inibire in modo permanente la possibilità di modifica

Molti componenti flash offrono un'ulteriore funzione OTP che permette di "congelare" in modo permanente il contenuto di alcuni blocchi della zona di memoria convenzionale. Questo tipo di implementazione è usato soprattutto per impedire eventuali modifiche che possono danneggiare l'integrità di sistema. Un fornitore di servizi, per esempio,

normalmente aggiunge il proprio software personalizzato al decoder TV del produttore. Il progettista non può sapere a priori quale sarà l'effetto sul sistema di questo software. Per proteggere il programma di inizializzazione (boot code) da eventuali modifiche o cancellazioni, può memorizzarlo in un blocco OTP che viene poi "congelato" in modo permanente. Il software del fornitore di servizi non potrà scrivere o cancellare questa parte di memoria "congelata", eliminando quindi possibili malfunzionamenti e le conseguenti richieste di assistenza tecnica.

Protezione hardware standard per le flash

La maggior parte delle flash prevede qualche forma di protezione hardware contro la scrittura, per prevenire la programmazione o la cancellazione di un blocco o dell'intero dispositivo. Per attivare la protezione hardware è necessario applicare a un determinato pin una tensione definita, tramite un collegamento sulla scheda o "settando" un bit su un piedino di I/O del processore. Prima di eseguire un comando di modifica, il chip flash verificherà il valore presente sul pin di protezione. Se il valore non è quello previsto per autorizzare la modifica, il chip non eseguirà il comando e non modificherà il programma o i dati.

Se è presente un valore di tensione valido sul piedino Program Supply Voltage (V_{pp}) o VPEN, sarà possibile modificare il contenuto dei blocchi della memoria principale del chip. Se invece V_{pp} o VPEN sono a massa, i blocchi non potranno essere cancellati o modificati. Quando V_{pp} o VPEN sono a massa, ogni tentativo di programmazione o cancellazione avrà esito negativo e verrà segnalato da un apposito bit nel registro di stato. Un altro tipo di meccanismo di protezione hardware contro la scrittura utilizza V_{pp}/WP (Write Protect) e permette di evitare la cancellazione o programmazione del contenuto del blocco inferiore o superiore della memoria. Se V_{pp}/WP=V_{IL} il blocco inferiore o superiore è protetto, in condizione di "Lock-Down" e non può essere modificato. Quando invece V_{pp}/WP=V_{IH} il "Lock-Down" viene rimosso e il blocco può essere protetto o sprotetto.

Protezione hardware – Una barriera difensiva contro gli attacchi Internet

Questo approccio hardware è una barriera difensiva poco costosa contro alcuni pericolosi programmi che possono infiltrarsi tramite Internet. Questi ultimi non sono in grado di modificare o cancellare i dati immagazzinati in una flash il cui contenuto è "congelato" utilizzando il meccanismo hardware descritto, a meno che non riescano prima a modificare il valore di tensione presente sul pin di protezione. Se, per esempio, un hacker cerca di entrare in un router, il suo programmino pirata cercherà di accedere alla memoria flash che, però, a sua volta verificherà il valore della tensione sul piedino di protezione del boot code. Se la verifica è negativa, il chip non verrà influenzato dal programma pirata e il router continuerà a funzionare come sempre.

Protezione software di blocchi di memoria

Alcune funzioni per la protezione dei blocchi di memoria possono essere di tipo "volatile" o "non volatile" e utilizzano comandi software per impedire la modifica accidentale dei dati.

Nel caso della protezione di blocchi di memoria utilizzando uno schema "volatile", ai bit di una matrice di memoria volatile vengono fatti corrispondere diversi blocchi della memoria principale del sistema. Ognuno di questi VPB (Volatile Protection Bit, bit volatili di protezione) può essere modificato separatamente, azzerato o settato quando è necessario. Tuttavia i bit VPB possono proteggere i blocchi solo se questi non sono già associati a bit NVPB (Non-Volatile Protection Bit, bit non volatili di protezione). Quando si spegne l'alimentazione di sistema o si esegue un reset hardware, i VPB tornano al valore originale e ripristinano lo stato originale di protezione dei rispettivi blocchi di memoria.

Invece, se si usa uno schema "non-volatile" lo stato di protezione dei blocchi di memoria rimane quello definito originariamente dal progettista anche dopo un reset o lo spegnimento dell'alimentazione. Ogni bit NVPB corrisponde a un singolo blocco, che può essere individualmente protetto (o non protetto). I bit NVPB possono essere azzerati con un commando di azzeramento o cancellazione.

Uno schema di protezione che utilizza NVPB è utile per garantire la protezione dei blocchi contro operazioni non intenzionali di scrittura, anche dopo un reset o uno spegnimento improvviso sistema.

La scelta del componente flash adeguato

Le funzioni di sicurezza di una memoria flash variano in base al produttore e al dispositivo. È importante tenerne conto assieme a densità, prestazioni, tecnologia, litografia, costo, dimensioni e package. Tutti questi fattori, insieme, contribuiscono al successo di un progetto e possono essere utilizzati per proteggerne le prestazioni e il posizionamento nel mercato. Le funzioni di sicurezza integrate nelle memorie flash offrono un'alternativa sicura ed economica per proteggere i blocchi di proprietà intellettuale (IP), il contenuto, i dati e l'integrità del sistema.

Numonyx
readerservice.it n. 8