imec Editie | april 2017

Data science and data security

Chips met vingerafdruk maken de online wereld veiliger

Door kleine variaties tijdens de productie is elke chip anders en dat maakt het mogelijk om chips eenvoudiger te identificeren, zodat online applicaties veel veiliger worden.

Door kleine variaties tijdens de productie is elke chip anders dan alle andere. Voor chipontwerpers is dat een nachtmerrie: alle chips van een bepaald type moeten zich immers exact hetzelfde gedragen. Maar veiligheidsexperts zien een potentieel voordeel: de kleine variaties zijn precies als vingerafdrukken bij mensen, ze geven elke chip een uniek profiel. En dat maakt het mogelijk om chips eenvoudiger te identificeren, zodat online applicaties veel veiliger worden. Zowel het imec-team dat onderzoek doen naar variabiliteit in de chipproductie als het team dat werkt aan de beveiliging van hardware behoren tot de wereldtop. Samen beschikken ze over de expertise om chips met vingerafdrukken te ontwikkelen. Dit is dan ook een van de hoekstenen van het imec-onderzoek om de veiligheid en privacy van de miljarden toekomstige IoT-devices te verbeteren.

Geen enkele chip is identiek aan de andere

Als je zelfrijdende auto de opdracht krijgt om je aan de luchthaven te komen oppikken, hoe kan die auto dan weten of hij werd opgeroepen door die ene smartphone die daarvoor is gemachtigd? Misschien was het wel een kopie? Hierin schuilt dus een beveiligingsrisico: mensen zijn uniek en kunnen zo worden geïdentificeerd, elektronische toepassingen (nog) niet. Vingerafdrukken en andere biometrische kenmerken maken mensen uniek. Ze zijn gemakkelijk te meten en heel moeilijk na te maken. Maar dat geldt niet voor het groeiend aantal slimme toepassingen met een internetconnectie, zoals zelfrijdende auto's, drones, IoT-sensoren... In de elektronicawereld is het veel moeilijker om echt van namaak te onderscheiden.

Een voor de hand liggende, gemakkelijke en goedkope oplossing zou erin bestaan om elke chip bij de productie een unieke identificatiecode mee te geven. Als de chip dan door een applicatie wordt gecontacteerd -'challenged' noemen beveiligingsexperts dit - dan zendt ze een uniek signaal uit op basis van die identifier (of een cryptografische sleutel die van de identifier is afgeleid). De toepassing controleert dan of het signaal geldig is en de schip dus te vertrouwen is.

Maar echt veilig is dit niet, want een tweede, kwaadwillige chip zou dezelfde identifier kunnen gebruiken.

In plaats van zo'n willekeurige identificatiecode hebben we dus nood aan een code die fysisch bij een chip hoort, een code die geen enkele andere chip kan hebben. De oplossing is wat experts een 'physically unclonable function' of PUF heten, zeg maar een niet na te bootsen fysieke functie die de rol van een menselijke vingerafdruk vervult. Deze functie kan gemaakt worden op basis van de ontelbare willekeurige variaties tijdens de productie aan de chip. Die variaties maken elke chip uniek; op nanoschaal is het eenvoudigweg onmogelijk om twee identieke chips te fabriceren. Onderzoekers breken er al een tijdje hun hoofd over hoe ze dat unieke karakter van chips kunnen gebruiken om elke chip onweerlegbaar te identificeren. Dat leverde een hele reeks voorstellen voor PUF's op, telkens met sterke én zwakke punten.

"Naarmate de afmetingen van chips kleiner worden, stijgt het relatieve belang van variabiliteit voor de prestaties van de chips. En wereldwijd beschikken maar weinig onderzoekers over zoveel kennis over het beperken van variabiliteit als onze experts," zegt Thomas Kallstenius, Program Director Security and Distributed Trust bij imec. "Bovendien hebben wij door de recente uitbreiding van imec nu ook een R&D-groep in huis die inzake de beveiliging van hardware wereldwijd groot aanzien geniet. Samen bestrijken zij nu alle domeinen om chips met een unieke vingerafdruk af te leveren."

Hoe zou de ideale vingerafdruk eruit zien?

"Wat wij proberen te bereiken, is dat de chipidentiteit niet langer steunt op een programma dat in de circuits is geïnstalleerd, maar op de fysieke kenmerken van de chip zelf. Zo'n identiteit is uniek en niet te kopiëren, omdat ze niet langer is beschermd door (te kraken) wachtwoorden en cryptografie, maar steunt op willekeurige, oncontroleerbare fysieke kenmerken die onmogelijk te reproduceren zijn," zegt Ingrid Verbauwhede, die bij imec-COSIC-KU Leuven de groep embedded systems en hardware leidt.

Voorbeelden van PUF's die wetenschappers al getest hebben zijn zogeheten arbiter PUF's, ring oscillator PUF's of SRAM PUF's. Deze laatste soort bijvoorbeeld maakt gebruik van het feit dat een SRAM-cel bij het inschakelen de waarde 0 of 1 aanneemt op basis van haar kenmerken op nanoschaal. Het uitlezen van zo'n SRAM-bank van een chip na het inschakelen is dus een goed vertrekpunt voor een unieke vingerafdruk.

Ingrid Verbauwhede: “Alle voorgestelde PUF-types vertonen voor- én nadelen. Sommige kosten meer, bijvoorbeeld omdat je extra schakelingen moet toevoegen. Andere hebben een vingerafdruk die na een tijdje wijzigt, veroudert dus. En nog andere blijken bij nader onderzoek toch niet zo veilig te zijn omdat ze bv regelmatigheden vertonen. Daarom zijn wij nog altijd op zoek naar nieuwe methodes om PUF’s te maken, zonder een beroep te doen op schakelingen, dus op basis van de kenmerken van de transistoren zelf in de nieuwste technologie-nodes.”

De ideale vingerafdruk van een chip moet stabiel zijn en gemakkelijk af te lezen. Het gebruik van de vingerafdruk mag niet veel tijd en energie kosten en de vingerafdruk mag na verloop van tijd niet veranderen. Hij moet bovendien uniek zijn voor één bepaalde chip en vrijwel onmogelijk na te bootsen in een andere chip. De vingerafdruk mag evenmin af te leiden zijn uit alle informatie (of sleutels) die de chip verspreidt. Ten slotte moet hij inbraakvrij zijn: als iemand de chip fysiek probeert te ontcijferen, moet de vingerafdruk zichzelf vernietigen of veranderen.

Ingrid Verbauwhede: “Zo’n vingerafdruk kan je op twee manieren gebruiken. In de eerste plaats om de chip te authenticeren, zodat je de zekerheid hebt dat dit de correcte chip is. Je stuurt er een challenge naartoe en je krijgt op basis van de vingerafdruk een respons terug. Je vergelijkt die respons dan met je database van alle legitieme antwoorden. Deze database is op voorhand samengesteld en moet natuurlijk afgeschermd worden. En - dit is heel belangrijk - elke challenge mag maar één keer gebruikt worden, want anders kan een hacker de combinatie van challenge en respons onderscheppen en gebruiken om de chip te hacken.”

“De tweede toepassing van de vingerafdruk van chips is als basis om cryptografische sleutels aan te maken. Dit is wat complexer, omdat je extra algoritmes en hulpdata nodig hebt om de sleutels 100% veilig te maken. Maar het resultaat is dan wel een sleutel die is afgeleid van de willekeurige eigenschappen van chips en niet van een opgeslagen geheim of fysieke processen die kunnen worden onderschept.”

Een vingerafdruk op basis van “gebrandmerkte” transistoren

Dimitri Linten is R&D manager bij imec. Samen met zijn collega’s bestudeert hij de variaties bij de productie van de nieuwste generaties transistoren. En momenteel onderzoekt hij ook hoe deze variaties nuttig kunnen zijn om nieuwe PUF’s aan te maken. “De problemen met sommige andere PUF’s hebben ons geleerd dat wij vooral moeten uitkijken naar vingerafdrukken waarvoor geen extra circuits of processen nodig zijn en die hun hele levensduur stabiel blijven.”

De nieuwe methode die het team ontwikkelde steunt op de intrinsiek willekeurige posities waarin het gate oxide van transistoren een soft breakdown doormaakt. De oxidelaag aan de gate is uiterst dun gemaakt. Door herhaaldelijk spanning aan te leggen bouwen zich willekeurige defecten op in het gate oxide. Op een bepaald ogenblik ontstaat doorheen deze defecten een lekstroompad door de gate, als een soort "brandmerk". "Op dat moment maakt de transistor een soft breakdown door en kan hij zijn taak niet langer vervullen," zegt Dimitri Linten. "Wat ons daarin interesseert, is de willekeurige positie van de plaats van het lekstroompad tussen de source en de drain in het gate oxide. Die positie kan worden gemeten."

"Eigenlijk zijn de oxide breakdowns een verouderingseffect. Terwijl het toch onze bedoeling moet zijn om een chip zo lang mogelijk gezond te houden en veroudering zoveel mogelijk te beperken of te vertragen. Daarom zouden we een apart circuit kunnen reserveren waarop met we met opzet een hoge spanning zetten om de gates te verplichten soft breakdown-paden te vormen. Wij dwingen dat gedeelte van de chip dus om heel snel te verouderen en als neveneffect krijgen we een willekeurige vingerafdruk. In vergelijking met vingerafdrukken die op SRAM's steunen, biedt deze PUF ons een meer robuuste aflezing: er zijn minder foutencorrecties en naverwerking nodig."

De manier waarop deze vingerafdruk tot stand komt - door initialisatie na de productie - biedt een extra voordeel voor de beveiliging. De meeste PUF's komen bij de productie zelf tot stand en kunnen dus door de fabrikant worden uitgelezen. Dit houdt een veiligheidsrisico in, aangezien een derde partij kennis van de geheime identifier kan verwerven. Bij de door imec toegepaste oxide breakdown is het daarentegen de applicatiebouwer (een autoconstructeur, bijvoorbeeld) of zelfs de eindgebruiker die de PUF kan activeren. Geen enkele andere partij kent dan de echte identiteit van de chip.

Uitgebreide hardwarebeveiliging

Om deze PUF's toe te passen in commerciële chips is er nog veel onderzoek en werk nodig, maar de onderzoekers zien alvast veel toepassingsmogelijkheden. Zij denken onder andere aan chips voor de draadloze besturingsnetwerken in auto's, industriële machines of medische apparatuur. Thomas Kallstenius: "Dit zijn voorbeelden van bijzonder kwetsbare netwerken. Ze gebruiken veel kleine, geconnecteerde processoren die op elkaar vertrouwen om de juiste actie te ondernemen. Het is dus essentieel dat zij op een uiterst veilige manier in staat zijn om elkaar te authenticeren en te vertrouwen. Precies daarvoor zorgt hardwarebeveiliging."

De R&D naar PUF's bij imec past in onze ruimere inspanningen om efficiënte en energiezuinige beveiliging en privacy te ontwikkelen voor de miljarden sensoren, controleprocessoren en communicatie-nodes van het wereldwijde IoT. Onze onderzoekers buigen zich ook over hardware-based true random number generators, public-key cryptografie met zeer laag stroomverbruik, efficiënte symmetrische encryptie en proven correct code.

Meer weten?

Onderzoek naar oxide-breakdown PUF's wordt gedeeltelijk gefinancierd door de Europese Commissie in het kader van het Horizon 2020 onderzoeks- en innovatieprogramma, subsidieovereenkomst nr. 644052 HECTOR. Een eerste proof-of-concept van deze PUF's wordt gepresenteerd op het IEEE International Reliability Physics Symposium, dat dit jaar van 2 tot 6 april plaatsvindt in Monterey (VS).