Prof. Mirosław Kutyłowski

NASK – Państwowy Instytut Badawczy

Wrocław, 11.9.2024

Recenzja rozprawy doktorskiej

Provable countermeasures against Hardware Trojans

przedstawionej przez Małgorzatę Gałązkę

na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego

Rozprawa doktorska została przedstawiona jako samodzielny utwór oparty na trzech publikacjach, w których Pani Małgorzata Gałązka jest współautorem. Rozprawa ta spełnia w jednoznaczny sposób wymagania z art. 187:

1. świadczy o głębokiej znajomości tematyki ochrony sprzętu kryptograficznego przed atakami adwersarza określanymi jako „hardware Trojan". Co więcej, rozprawa świadczy o tym, że jej autorka należy do wąskiego grona osób które wniosły bardzo istotny wkład w rozwój tej dziedziny,
2. rozprawa pani Gałązki zawiera istotne, nowatorskie rozwiązania problemu możliwości ochrony przed „hardware Trojans". Przeważająca część wyników to konkretne, nietrywialne konstrukcje zabezpieczające przed atakiem.

Rozprawa zawiera bardzo szczegółowe deklaracje co do indywidualnego wkładu kandydatki w wyniki zawarte w pracach będących podstawą rozprawy. Wkład ten jest kluczowy w sensie pokonywania głównych wyzwań merytorycznych.

Przedmiot rozprawy

Rozprawa podejmuje niezwykle istotny temat w kontekście zaufania do komponentów kryptograficznych – podatności na modyfikacje sprzętu (np. dokonane przez producenta). Praca podejmuje temat ochrony na poziomie warstwy algorytmicznej: możliwości testowania sprzętu za pomocą dodatkowych funkcjonalności wbudowanych przez tzw. kompilator.

Pierwsza część rozprawy dotyczy sytuacji, gdy adwersarz może wpływać w konkretny sposób na wartości na określonych połączeniach i bramkach. Odpowiada to sytuacji znanej z ataków polegających na wprowadzaniu modyfikacji w zawartości domieszek w tranzystorach, i niewidocznych podczas skanowania optycznego. Model stosowany przez autorkę bardzo dobrze opisuje rzeczywisty problem. Zabezpieczenia zaproponowane w rozprawie (i pracach będących jej podstawą) mają postać dosyć elementarnych (i eleganckich z inżynierskiego punktu widzenia) dodatkowych komponentów i procedur. Ze względu na charakter modyfikacji i model adwersarza, standardowe metody testowania chipów nie były tu skuteczne. Zasadniczym wyzwaniem i pokonaną

trudnością było zagwarantowanie kompresji informacji dostarczanej na zewnątrz układu. Cel ten został osiągnięty za pomocą komponentów zwanych w rozprawie gadgetami. Sama konstrukcja oparta na elementarnych środkach jest zręczna i może mieć pewne zastosowanie w praktyce. Oczywiście, droga do konkretnych zastosowań w przemyśle wymagałaby oceny i optymalizacji na przykład pod kątem narzutu na powierzchnię układu. Niemniej jednak autorka wykazała, że cel może zostać osiągnięty przynajmniej w teorii. Tym samym, prace prowadzone przez Kandydatkę mogą i powinny być kontynuowane.

Druga część rozprawy dotyczy testowania sprzętu składającego się z niezaufanych komponentów obliczających (rzekomo) pewną funkcję F, oraz zaufanego menadżera mogącego używać kilku komponentów a ponadto testować je w początkowej fazie cyklu życia urządzenia.

W moim odczuciu druga część rozprawy jest nieco kontrowersyjna. Opis znaczenia wyników (także w oryginalnych pracach) jest nieco przerysowany. W istocie, badania mają zastosowanie dla funkcji F mającej charakter *random oracle*. Zaproponowany kompilator dotyczy w istocie prostego scenariusz i odpowiedzi na pytanie na ile komponenty obliczające F mogą oszukiwać, o ile nie ma wymiany informacji pomiędzy nimi odnoszącej się do interakcji z menadżerem. Już w sytuacji gdy mamy do czynienia z dwoma niezależnymi komponentami obliczającymi F, menadżer może wykorzystać swą przewagę polegającą na braku dostępu do informacji, ile i jakie zapytania kierowano do drugiego komponentu obliczającego F.

Mimo intuicyjnej jasności, że menadżer może zaszachować niezaufane komponenty uniemożliwiając im uniknięcie wykrycia oszustwa, przedstawienie ścisłego dowodu dla konkretnej strategii menadżera jest ciekawym pytaniem badawczym. Cytowana praca Kandydatki a także rozdział 4 rozprawy mają taki dowód przedstawić. Niestety moim zdaniem jest to wciąż „extended abstract" mający postać bardzo interesującego szkic; niemniej jednak jest to tylko szkic dowodu. Wielu szczegółów nie byłem w stanie odtworzyć i w sytuacji gdyby miał to być artykuł do czasopisma wnosiłbym o wniesienie znaczących uzupełnień.

Z drugiej stron, warto zaznaczyć, że rezultaty z rozdziału 4 nie odnoszą się wyłącznie do problematyki Trojanów hardware'owych – w istocie chodzi o zarządzanie ryzykiem w sytuacji wyników dostarczanych przez komponenty typu czarnej skrzynki. Jest to jeden z podstawowych problemów do rozwiązania na przykład w inżynierii programowania i metod testowania poprawności.

Jakość edycyjna

W przeważającej części rozprawa jest napisana w jasny i precyzyjny sposób, autorka umiejętnie eliminuje nieistotne szczegóły i unika zbędnej formalizacji, która w innych pracach częstokroć ukrywa brak istotnych treści.

Pozytywna ocena pod tym względem dotyczy głównie rozdziałów 1-3. Rozdział 4 pod tym względem odbiega od całości rozprawy i w przypadku recenzowania dla czasopism tą część skierowałbym do „major revision". Najlepszym fragmentem w rozdziale 4 jest opis konstrukcji dla komponentów F świadomych historii (ta część, według deklaracji jest głównym wkładem Kandydatki) i, pozostała część zawiera nawet pewną ilość oczywistych pomyłek edycyjnych, niezdefiniowanych oznaczeń i niezrozumiałych zdań.

Jakość rozprawy pod względem językowym jest bez zarzutu.

Konkluzja

Bez wątpienia rozprawa jest dowodem na dużą sprawność techniczną i dojrzałość Kandydatki pod względem umiejętności rozwiązywania istotnych problemów naukowych. Wyniki są istotne i stanowią ważny wkład w rozwój tej stosunkowo nowej dziedziny informatyki. Wyniki są dobrze osadzone w realiach i konieczności odpowiadania na istotne wyzwania praktyczne.

Jak wspomniałem powyżej, pewne zastrzeżenia wniosłem do rozdziału 4. Jednak gdyby z rozprawy usunąć cały rozdział 4, rozprawa nadal dawałaby mocne podstawy do nadania stopnia doktora. Tym samym niedociągnięcia edycyjne tej części, być może wnikające ze zmęczenia czy konieczności dochowania terminu, nie zmieniają całościowej jednoznacznej

pozytywnej

rekomendacji do nadania stopnia doktora na podstawie przedstawionej rozprawy.

Mirosław Kutyłowski