Θέματα Διπλωματικών Εργασιών

Εργαστήριο Ενσωματωμένων Υπολογιστικών Συστημάτων (ESLab)

1 – Υλοποίηση εργαλείων ηλεκτρονικού αυτοματισμού (Electronic Design Automation) για εφαρμογές ασφάλειας υλοποιημένες σε FPGA

Περιγραφή

Η πλειοψηφία των σύγχρονων ψηφιακών εφαρμογών (IoT, τραπεζικές εφαρμογές κλπ.) βασίζονται σε κρυπτογραφικές υλοποιήσεις για την παροχή ικανοποιητικών επιπέδων ασφάλειας. Η ύπαρξη επιθέσεων υλικού όπως για παράδειγμα οι επιθέσεις πλευρικού καναλιού (Side Channel Analysis attacks) και οι επιθέσεις εισαγωγής σφαλμάτων (Fault Injection attacks) είναι δυνατόν να υποβαθμίσουν σημαντικά και έως να εξαλείψουν το επιθυμητό επίπεδο ασφάλειας [1, 2].

Στην παρούσα πτυχιακή εργασία θα γίνει χρήση υπαρχόντων βιβλιοθηκών (πχ SpyDrNet, Repidwright) για την υλοποίηση εργαλείων ηλεκτρονικού αυτοματισμού με στόχο την αύξηση της απόδοσης και τη μελέτη ιδιοτήτων ασφάλειας, FPGA υλοποιήσεων (πχ κρυπτογραφικών).

Θα αποκτηθεί εμπειρία στο το σύνολο των εργαλείων σύνθεσης για Xilinx FPGAs, σε επιθέσεις υλικού και στη σχεδίαση εργαλείων ηλεκτρονικού αυτοματισμού για εφαρμογές ασφάλειας σε αρχιτεκτονικές FPGA.

Παραδοτέα

- Ο κώδικας των EDA αλγορίθμων με χρήση των βιβλιοθηκών που θα επιλεγούν
- Οι αναλύσεις των επιπέδων ασφάλειας μέσω των υλοποιημένων EDA αλγορίθμων και η σύγκρισή τους με τα αποτελέσματα πειραματικών επιθέσεων υλικού
- Αναφορά διπλωματικής εργασίας
- Οδηγός χρήσης του εργαλείου
- Video με τις δυνατότητες των εργαλείων και τα βασικά αποτελέσματα

Ενδεικτική βιβλιογραφία και αναφορές

[1] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

[2] Barenghi, Alessandro, Luca Breveglieri, Israel Koren, and David Naccache. "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures." Proceedings of the IEEE 100, no. 11 (2012): 3056-3076.

Επιβλέποντες

Θάνος Παπαδημητρίου – thanospap@unipi.gr, a.papadimitriou@go.uop.gr

2 – Υλοποίηση επιθέσεων υλικού μέσω ανάλυσης σφαλμάτων

Περιγραφή

Η πλειοψηφία των σύγχρονων ψηφιακών εφαρμογών (IoT, τραπεζικές εφαρμογές κλπ.) βασίζονται σε κρυπτογραφικές υλοποιήσεις για την παροχή ικανοποιητικών επιπέδων ασφάλειας. Η ύπαρξη επιθέσεων υλικού όπως για παράδειγμα οι επιθέσεις εισαγωγής σφαλμάτων (Fault Injection attacks) είναι δυνατόν να υποβαθμίσουν σημαντικά και έως να εξαλείψουν το επιθυμητό επίπεδο ασφάλειας [1, 2].

Στην παρούσα πτυχιακή εργασία θα σχεδιαστεί μια βιβλιοθήκη επιθέσεων εισαγωγής σφαλμάτων. Αρχικά θα μελετηθεί η σχετική βιβλιογραφία και έπειτα θα υλοποιηθούν επιθέσεις υλικού μέσω εισαγωγής σφαλμάτων καθώς και μια πλατφόρμα εισαγωγής σφαλμάτων με χρήση clock glitch ή/και voltage glitch με το οποίο θα εισαχθούν σφάλματα σε κρυπτογραφικούς αλγορίθμους (AES).

Παραδοτέα

- Επιθέσεις εισαγωγής σφαλμάτων
- Πλατφόρμα εισαγωγής σφαλματων
- Οι αναλύσεις των επιπέδων ασφάλειας κρυπτογραφικών υλοποιήσεων
- Αναφορά διπλωματικής εργασίας
- Οδηγός χρήσης επιθέσεων και πλατφόρμας
- Video με τις δυνατότητες των εργαλείων και τα βασικά αποτελέσματα

Ενδεικτική βιβλιογραφία και αναφορές

[1] Kazemi, Zahra, Athanasios Papadimitriou, Ioanna Souvatzoglou, Ehsan Aerabi, Mosabbah Mushir Ahmed, David Hely, and Vincent Beroulle. "On a low cost fault injection framework for security assessment of cyber-physical systems: Clock glitch attacks." In 2019 IEEE 4th International Verification and Security Workshop (IVSW), pp. 7-12. IEEE, 2019.

[2] Barenghi, Alessandro, Luca Breveglieri, Israel Koren, and David Naccache. "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures." Proceedings of the IEEE 100, no. 11 (2012): 3056-3076.

[3] Zussa, Loic, Jean-Max Dutertre, Jessy Clediere, and Assia Tria. "Power supply glitch induced faults on FPGA: An in-depth analysis of the injection mechanism." In 2013 IEEE 19th International On-Line Testing Symposium (IOLTS), pp. 110-115. IEEE, 2013.

Επιβλέποντες

Θάνος Παπαδημητρίου – thanospap@unipi.gr, a.papadimitriou@go.uop.gr

3 – Επιθέσεις Πλευρικού Καναλιού σε Νευρωνικά Δίκτυα

Περιγραφή

Η πλειοψηφία των σύγχρονων ψηφιακών εφαρμογών (IoT, τραπεζικές εφαρμογές κλπ.) βασίζονται σε κρυπτογραφικές υλοποιήσεις για την παροχή ικανοποιητικών επιπέδων ασφάλειας. Η ύπαρξη επιθέσεων υλικού όπως για παράδειγμα οι επιθέσεις πλευρικού καναλιού (Side Channel Analysis attacks) και οι επιθέσεις εισαγωγής σφαλμάτων (Fault Injection attacks) είναι δυνατόν να υποβαθμίσουν σημαντικά και έως να εξαλείψουν το επιθυμητό επίπεδο ασφάλειας [1, 2].

Στην παρούσα πτυχιακή εργασία θα γίνει χρήση υπαρχόντων επιθέσεων υλικού σε νευρωνικά δίκτυα. Αρχικά θα μελετηθεί η σχετική βιβλιογραφία και θα επιλεγεί μια υλοποίηση νευρωνικού δικτύου με χρήση High Level Synthesis. Έπειτα θα υλοποιηθούν επιθέσεις υλικού με στόχο το reverse engineering του νευρωνικού δικτύου [3].

Παραδοτέα

- Νευρωνικά δίκτυα
- Εργαλείο επιθέσεων πλευρικού καναλιού
- Οι αναλύσεις των επιπέδων ασφάλειας των δικτύων
- Αναφορά διπλωματικής εργασίας
- Οδηγός χρήσης του εργαλείου
- Video με τις δυνατότητες των εργαλείων και τα βασικά αποτελέσματα

Ενδεικτική βιβλιογραφία και αναφορές

[1] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

[2] Barenghi, Alessandro, Luca Breveglieri, Israel Koren, and David Naccache. "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures." Proceedings of the IEEE 100, no. 11 (2012): 3056-3076.

[3] Batina, Lejla, Shivam Bhasin, Dirmanto Jap, and Stjepan Picek. "{CSI}{NN}: Reverse engineering of neural network architectures through electromagnetic side channel." In 28th USENIX Security Symposium (USENIX Security 19), pp. 515-532. 2019.

Επιβλέποντες

Θάνος Παπαδημητρίου – thanospap@unipi.gr, a.papadimitriou@go.uop.gr