Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Πατρών

Οκτώβριος 2025

Cryptographic Acceleration with GPUs (N E O)

- Υλοποίηση AES, RSA και κρυπτογραφίας Ελλειπτικών Καμπυλών (ECC) σε CUDA.
- Σύγκριση ρυθμοαπόδοσης (throughput) με υλοποιήσεις σε CPU (OpenSSL).
- Συνεισφορά: Πρόταση για GPU-offloading σε VPNs ή συστήματα ασφαλών μηνυμάτων.
- **Εργαλεία/Τεχνολογίες:** CUDA/OpenCL, OpenSSL (για benchmarks), WolfSSL (lightweight crypto library), Python (PyCUDA), Nsight Compute (GPU performance analysis).

Attribute-Based Encryption for Secure Data Sharing in Cloud Environments (N E O)

- Μελέτη και υλοποίηση Attribute-Based Encryption (ABE) για ασφαλή διαμοίραση δεδομένων στο cloud.
- Ανάπτυξη proof-of-concept εφαρμογής όπου οι χρήστες αποκτούν πρόσβαση σε κρυπτογραφημένα δεδομένα με βάση χαρακτηριστικά (attributes) και πολιτικές πρόσβασης (access policies).
- Σύγκριση Key-Policy ABE (KP-ABE) και Ciphertext-Policy ABE (CP-ABE) ως προς ασφάλεια και απόδοση.
- Εφαρμογή μηχανισμών ανάκλησης δικαιωμάτων (revocation) και ελέγχου ταυτότητας χρηστών.
- **Συνεισφορά:** Ανάπτυξη πρωτοτύπου για ασφαλή διαχείριση κλειδιών και πολιτικών πρόσβασης σε cloud ή IoT περιβάλλοντα.
- **Εργαλεία / Τεχνολογίες:** Python ή C++ με βιβλιοθήκες ABE (π.χ. Charm-Crypto, libbswabe, CP-ABE toolkit), OpenSSL, Flask ή Django για web interface, MongoDB ή PostgreSQL για αποθήκευση metadata, Docker για ανάπτυξη στο cloud (AWS/Azure/Local).

~~**Design and Evaluation of a Software Defined Perimeter (SDP)**~~

- ~~Ανάπτυξη πρωτοτύπου πρόσβασης δικτύου με αρχή “zero-trust” χρησιμοποιώντας VyOS ή OpenVPN + έλεγχο ταυτότητας βασισμένο σε ταυτότητα.~~
- ~~Σύγκριση με παραδοσιακές λύσεις VPN ως προς καθυστέρηση (latency), ασφάλεια και επεκτασιμότητα.~~
- ~~Ανάδειξη του πώς το SDP αποτρέπει την πλευρική κίνηση (lateral movement) σε παραβιασμένα δίκτυα.~~
- ~~**Εργαλεία/Τεχνολογίες:** VyOS, OpenVPN, WireGuard, strongSwan, Docker, Kubernetes, Wireshark, iperf3, Prometheus + Grafana (για monitoring).~~

~~**Machine Learning for Intrusion Detection Systems (IDS)**~~

- ~~Συλλογή δεδομένων δικτυακής κίνησης (dataset CIC-IDS 2017 ή πραγματικά δεδομένα εργαστηρίου).~~
- ~~Εκπαίδευση μοντέλων ML/DL για ταξινόμηση κακόβουλης έναντι κανονικής κίνησης.~~
- ~~Αξιολόγηση της απόδοσης και της ανθεκτικότητας των μοντέλων απέναντι σε επιθέσεις αντιπαλότητας (adversarial evasion).~~

Για περισσότερες πληροφορίες επικοινωνήστε: Κυριάκος Βλάχος kvlachos@ceid.upatras.gr

Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Πατρών

- **Εργαλεία/Τεχνολογίες:** Python (scikit-learn, TensorFlow, PyTorch), CIC-IDS-2017 / UNSW-NB15 datasets, Wireshark, Zeek (Bro IDS), Jupyter Notebook, CUDA-enabled GPUs.

Ransomware Detection and Mitigation at the Network Layer

- Προσομοίωση συμπεριφοράς ransomware σε ελεγχόμενο εργαστηριακό περιβάλλον.
- Παρακολούθηση ανωμαλιών στην κίνηση SMB/HTTP/DNS.
- Πρόταση συστήματος ανίχνευσης βασισμένου σε χαρακτηριστικά ροής (flow-based features).
- **Εργαλεία/Τεχνολογίες:** Controlled VM lab (VirtualBox/VMware), Wireshark, Suricata, Zeek IDS, Python (Scapy για packet analysis), ELK stack (Elasticsearch + Logstash + Kibana) για ανάλυση logs.

Post-Quantum Cryptography for Secure Communications

- Υλοποίηση σχημάτων κρυπτογράφησης βασισμένων σε πλέγματα (lattice-based) ή συναρτήσεις κατακερματισμού (hash-based).
- Σύγκριση απόδοσης με RSA/ECC σε περιβάλλοντα TLS ή VPN.
- Δοκιμή σε περιορισμένα περιβάλλοντα (ενσωματωμένα συστήματα ή IoT).
- **Εργαλεία/Τεχνολογίες:** Open Quantum Safe (liboqs), OpenSSL (με PQC υποστήριξη), TLS testbed (nginx + Apache), Python (cryptography library), Raspberry Pi ή ESP32 για IoT tests.

Full Disk Encryption and Secure Boot Implementation in Linux Systems (N E O)

- Υλοποίηση πλήρους κρυπτογράφησης δίσκου (Full Disk Encryption – FDE) σε Linux με χρήση LUKS2.
- Διαχωρισμός κρυπτογραφημένων partitions (/, /home, /swap) και μη κρυπτογραφημένων περιοχών (π.χ. /boot ή /boot/efi).
- Ενεργοποίηση και ρύθμιση Secure Boot (με δικά σου κλειδιά) για προστασία από μη εξουσιοδοτημένη εκκίνηση.
- Ανάλυση της διαδικασίας εκκίνησης (boot chain) και αξιολόγηση της ασφάλειας σε περιπτώσεις φυσικής πρόσβασης (π.χ. κλοπή συσκευής).
- Υλοποίησε σε νέο ή se εν λειτουργία VM σε περιβάλλον Azure
- **Συνεισφορά:** Ανάπτυξη ασφαλούς οδηγού εγκατάστασης και αξιολόγηση της επίδρασης της πλήρους κρυπτογράφησης στην απόδοση και στην εμπειρία χρήστη.
- **Εργαλεία / Τεχνολογίες:**
  LUKS2, dm-crypt, GRUB2, Secure Boot (UEFI), systemd-boot, TPM 2.0 (Trusted Platform Module), cryptsetup, GnuPG, `fio` / `hdparm` για μετρήσεις απόδοσης, Ubuntu / Debian / Arch Linux για δοκιμές.

Για περισσότερες πληροφορίες επικοινωνήστε: Κυριάκος Βλάχος kvlachos@ceid.upatras.gr