Towards Auditing of Control-Flow Integrity

Luke Atherton - Supervised by: Konstantinos Markantonakis

Information Security Group, Smart Card and IoT Security Center

Royal Holloway, University of London

The Smart Card and Internet of Things Security Centre

Objectives

- Investigate existing method providing control-flow integrity;
- Propose a solution for enabling the audit of control-flow integrity.

Introduction

- With the expected proliferation of drone-based services in smart cities comes the need for further regulation and security;
- Secure channel protocols tend to assume a prior relationship between communicating entities. A multi-stakeholder environment, such as a smart city, offers the potential for a multiplicity of drone-based applications, requiring many organizations to interact with each other;
- In this paper, we propose a group-based Certificateless Authenticated Key Agreement (CL-AKA) protocol, which enables trusted communication between untrusting parties, i.e. entities that belong to different organizations.

Protocol Initialization

The initialization phase is performed offline and prepares entities for the online key agreement procedure. It is split into six algorithms: setup, set-ephemeral-key, partial-private-key-extract, set-secret-value, set-private-key, and set-public-key. The initialization phase aims to provide each user u_i with a private/public key pair, respectively $\langle D_i, x_i \rangle$ and $\langle q_i, P_i \rangle$.

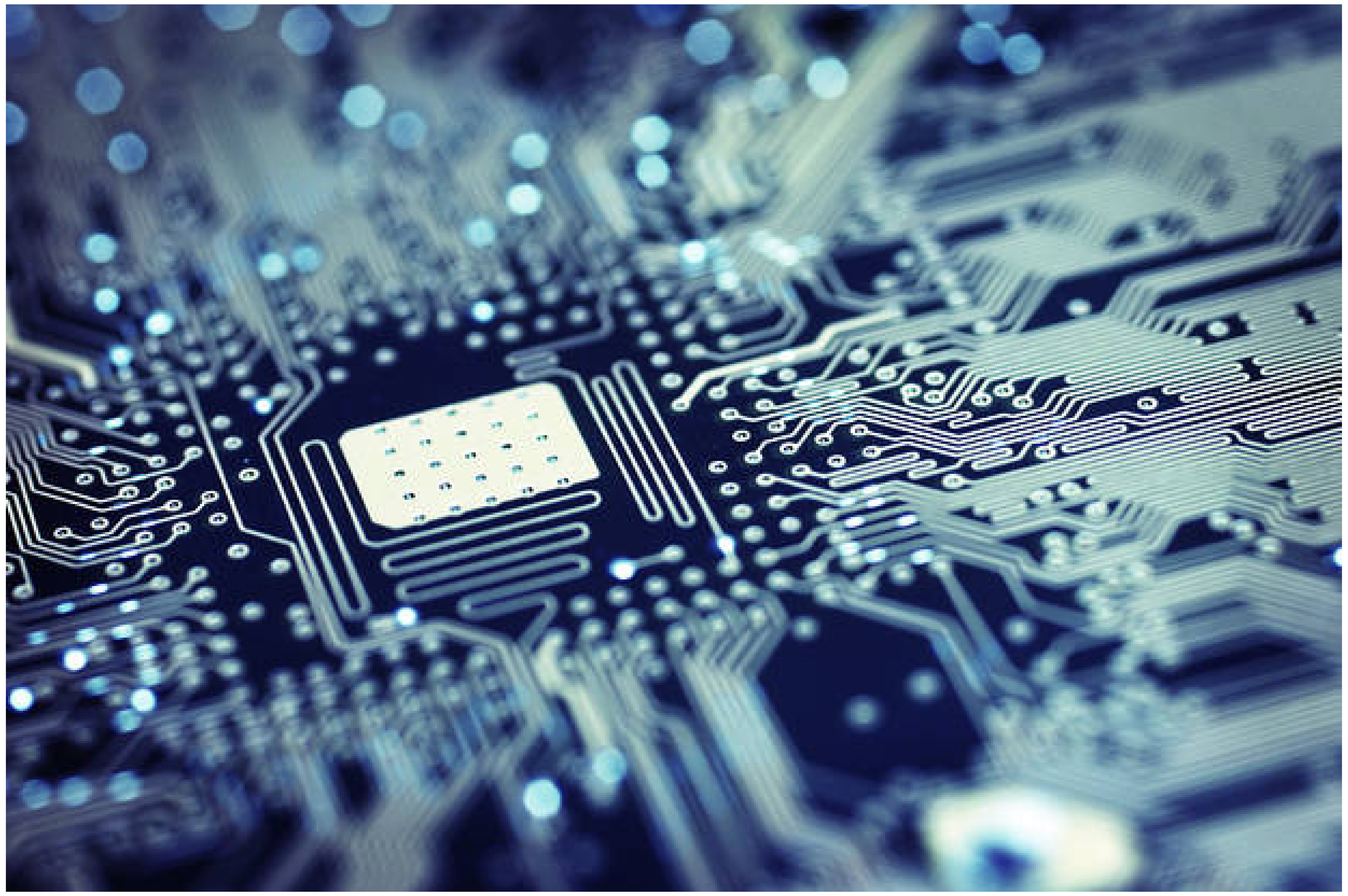

Figure 1:UAV swarm in smart city

Key Agreement

Setup Each user u_i sends a key establishment request, containing its temporary identity TID_i, partial public key q_i, and expiration date/time t_i of its partial public key.

Round 1 Each user u_i verifies that t_j is not out-of-date. Upon successful verification, u_i chooses a random $r_i \in \mathbb{Z}_q^*$, $k_i \in \{0,1\}^k$, and generates a set of ephemeral keys $P_{i,j} = r_i(q_j P + P_0) = r_i(q_j + s)P$ for $1 \leq j \leq n$ and $j \neq i$. Each user u_i then broadcasts the set of $P_{i,j}$ along with $H_3(k_i)$.

Round 2 Upon reception of $H_3(k_j)$ and $P_{j,i}$, each user u_i computes $sid_i^w = H_3(k_1)||...||H3(k_n)$. Each user u_i then generates the set of $t_{j,i} = e(P_{j,i}, D_i)^{x_i} P_j^{r_i} = g^{r_j x_i + r_i x_j}$, $V_{j,i} = H_2(t_{j,i}||sid_i^w)$, and $K_{j,i} = V_{j,i} \oplus k_i$. The set of $K_{j,i}$ is broadcast.

Key generation Upon reception of $K_{i,j}$, u_i computes $\tilde{k}_j = V_{j,i} \oplus K_{i,j}$ and checks whether $H_3(\tilde{k}_j) = H_3(k_j)$ is valid. Upon successful verification, each

Evaluation

- The *Syther* tool will be used to formally analyze the protocol;
- The experimental setup will consist of a set of Raspberry Pi 2 Model B+ System-on-Chip, communicating via wireless LAN interface.
- The number of users n taking part in the key agreement is a critical parameter to the computational cost and its effects will be analyzed. We expect the bilinear pairings to be the most expensive operations.

Criteria	Protocol
Number of rounds	2
Number of modular exponentiations	$n-1$
Number of bilinear pairings	$n-1$
Number of elliptic curve scalar point multiplication	$3n-2$

Benefits

The proposed protocol enables confidentiality, message integrity, and authenticity in subsequent communication. Provisioning untrusted UAV networks with trusted communication provides ground for further research and applications:

- Collaborative cybersecurity deterrence mechanism;
- Network extension using trusted relay nodes;
- Collaborative mission exercise, e.g. time-critical operations;
- Anonymous communication for user privacy.

Conclusion

The proposed protocol enables a fleet of UAVs to derive a unique symmetric key. It captures the following security properties: mutual authentication, mutual key agreement, joint key control, key freshness, entity revocation, non-repudiation, forward secrecy, known-key security, and conditional privacy. Since the protocol is certificateless-based, the necessity for a public key infrastructure is eliminated, as well as the key escrow problem. This research paper will be submitted to the *DASC 2018* conference.

References

Contact Information

- Web: https://scc.rhul.ac.uk/
- Email: benjamin.semal.2018@live.rhul.ac.uk