Crypto-Chain: A Relay Resilience Framework for Smart Vehicles

Abubakar Sadiq Sani, Dong Yuan, Elisa Bertino, Zhao Yang Dong

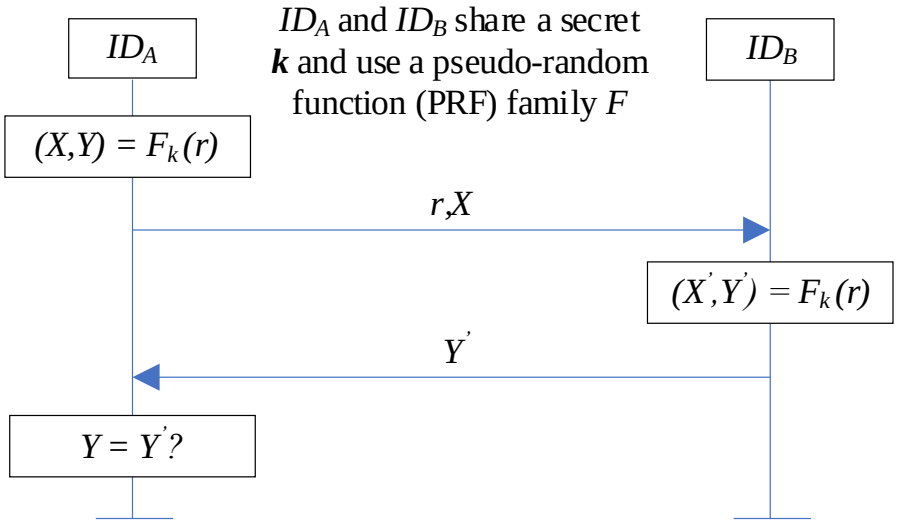
University of Greenwich
London, United Kingdom

Contents

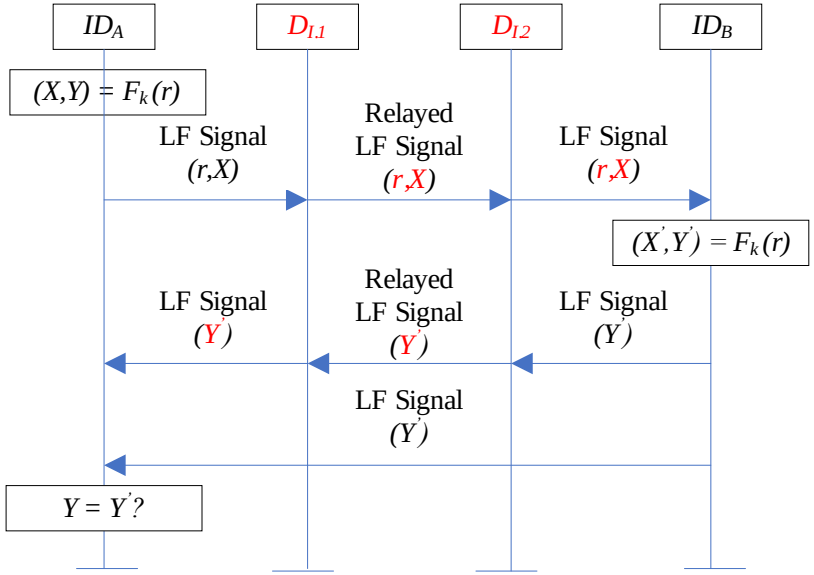
- The present state of Smart Vehicles
- Application of Universal Composability for relay resilience
- Today's relay security affairs in Smart Vehicles
- A bit of existing relay resilience solutions for Smart Vehicles
- Our key contributions
- Notion of Relay Resilience
- Crypto-Chain in a nutshell
- Relay resilience with Crypto-Chain
- Security and Performance Analyses of Crypto-Chain
- Implementation of Crypto-Chain
- Case Study on Megamos Crypto and Hitag-AES/Pro
- Conclusion and Future Work

Smart Vehicles as we know it

- Smart vehicles are susceptible to relay attacks by which an active adversary initiates a communication between two devices or users to bypass security defences or recover secret cryptographic keys.
- Cryptographic protocols such as Megamos crypto used in smart vehicles are vulnerable to relay attacks



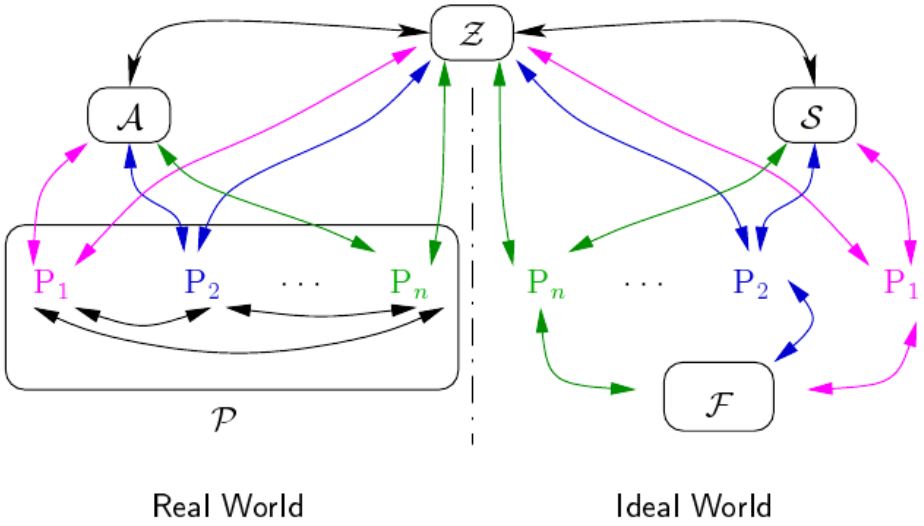
Megamos Crypto authentication protocol



Relay attacks on Megamos Crypto authentication protocol

Application of Universal Composability for Relay Resilience

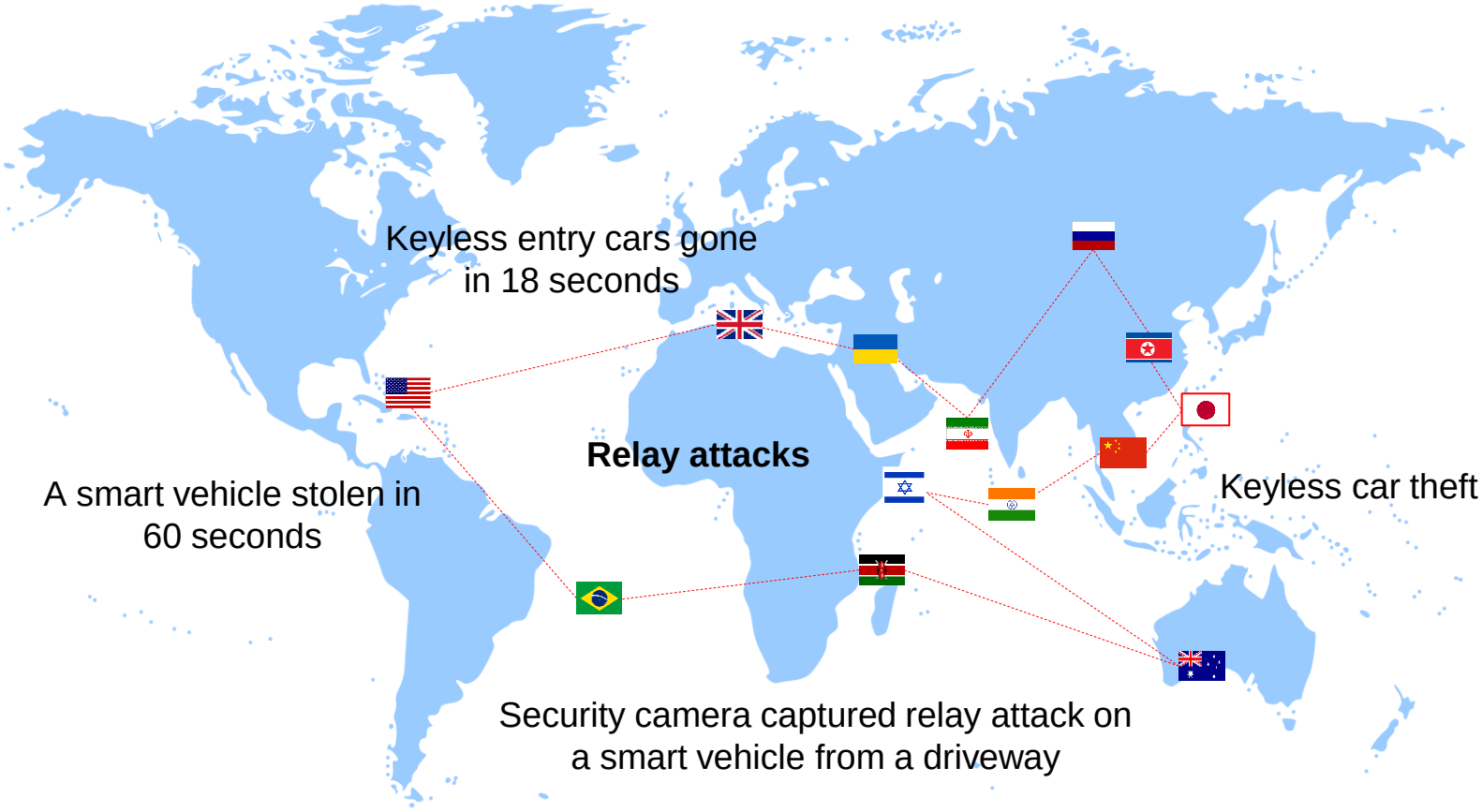
- In general, universal composability allows modular design and analysis of cryptographic protocols for relay resilience.
- In universal composability, we have real and ideal protocols/functionalities. An ideal protocol represents the desired behaviour and intended security of a protocol. The ideal protocol represents the protocol to design and analyze and should be at least as secure as the real protocol.



General Notion of Universal Composability

- *Z*: environment
- *F*: Ideal protocol
- *P*: Real protocol
- *A*: Adversary in real world
- *S*: Simulator/Adversary in ideal world

Today's Relay Security Affairs in Smart Vehicles



A basic taxonomy of relay attacks on smart vehicles around the world

A bit of Existing Relay Resilience Solutions for Smart Vehicles

- Verdult et al. [1] proposed some measures to mitigate relay attacks. These measures include randomly generating secret keys, redesigning weak ciphers, and using immobilizers that implement AES 128-bit encryption algorithm.
- Wan et al. [2] proposed to use key derivation schemes for car appliances to provide relay resilience and prevent the use of vehicles without permission.
- Francillon et al. [3] proposed mitigation measures to prevent relay attacks on passive keyless entry and start (PKES) systems in smart cars.
- Li et al. [4] proposed a smartphone-enabled user context detection system for relay attack mitigation.

[1] Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer.

[2] A security module for car appliances.

[3] Relay attacks on passive keyless entry and start systems in modern cars.

[4] User Context Detection for Relay Attack Resistance in Passive Keyless Entry and Start System.

Our Key Contributions

- In universal composability, we extend Kusters's theorem that handles concurrent composition of a fixed number of protocol systems to handle chainings of cryptographic operations.
- An ideal crypto-chain functionality F_{CC} that uses our new theorem and supports several cryptographic primitives, such as dynamic multi-factor authentication (DMA) and knowledge-based key exchange (KKE).
- An ideal functionality for mutual authentication and key derivation F_{MKD}.
- Crypto-Chain, a novel relay resilience framework for smart vehicles. It consists of F_{CC} and F_{MKD}.
- Using Crypto-Chain to construct the first mutual authentication and key derivation protocol (MKD) based on DMA and KKE for relay resilience in smart vehicles.
- MKD analysis and implementation.
- Mitigating relay vulnerabilities in Megamos Crypto and Hitag-AES/Pro.

Extended Composition Theorem

- **Extended notions of simulation-based security:** We extend the definition of strong simulatability. To do this, we equip the real and ideal protocols/functionalities with a sequence of cryptographic operations such that an operation always depends on the preceding one, i.e., the operation relies on the preceding operation, to prevent bypass of cryptographic operations and support relay resilience.
- Handles the concurrent composition of a fixed number of protocol systems with a sequence of cryptographic operations that rely on one another.
- **Theorem:** Let P_1, P_2, F_1, F_2 be protocol systems with a sequence c of cryptographic operations c_1, c_2, and c_3 such that P_1 and P_2 as well as F_1 and F_2 only connect with each other via their I/O interfaces and for every k, $P_k[c] \leq_R F_k[c]$, iff $P_k[c_i(c_{i-1})] \leq_R F_k[c_i(c_{i-1})]$, where $i \in \{1,2,3\}$. Then, $P_1[c_3(c_2(c_1))] || P_2[c_3(c_2(c_1))] \leq_R F_1[c_3(c_2(c_1))] || F_2[c_3(c_2(c_1))]$, for $k \in \{1,2\}$.
- …
- …

Notion of Relay Resilience

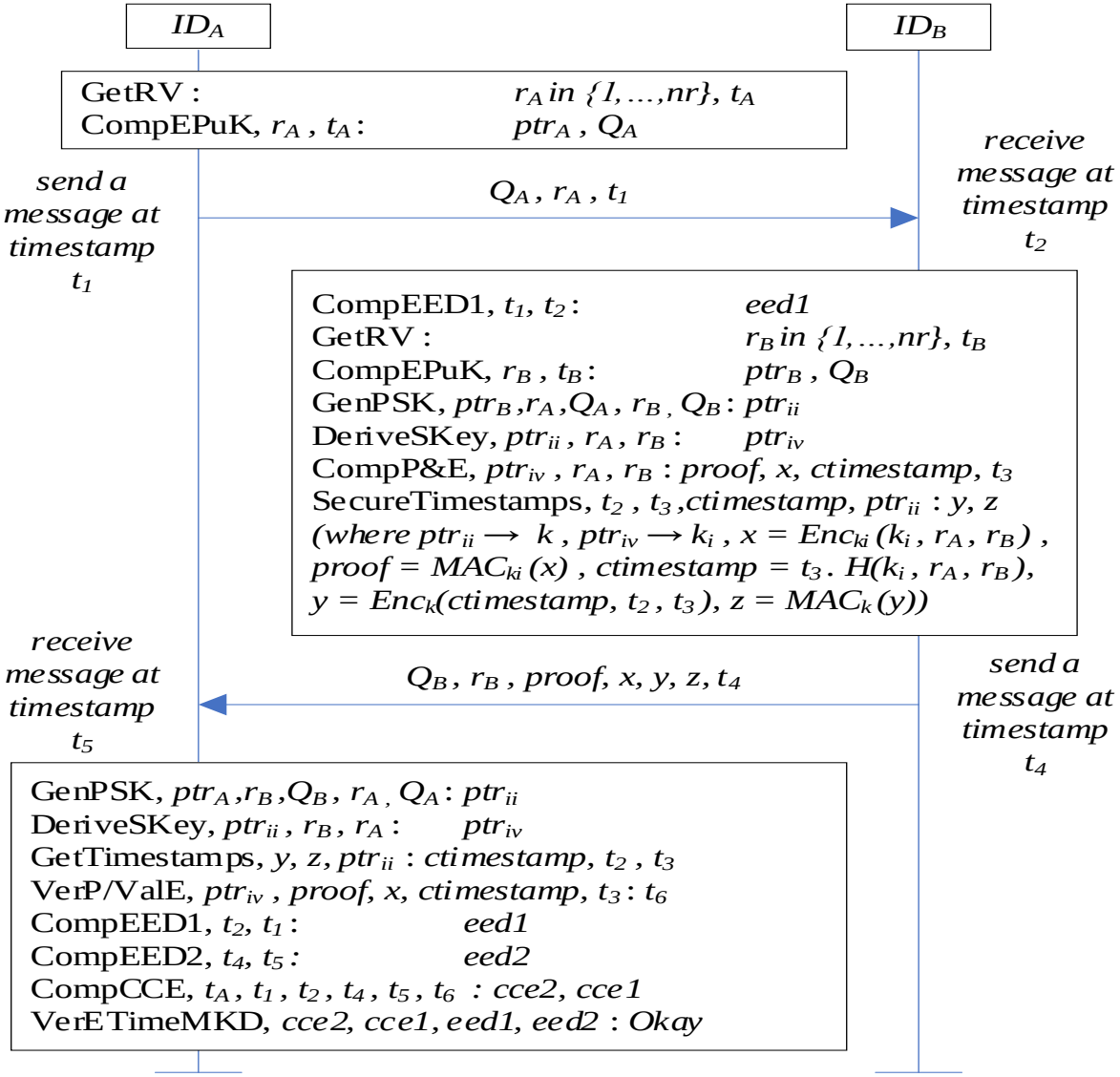
- **Definition:** Let s be a session between users ID_A and ID_B with a set of attributes att_A and att_B, respectively. Let c be a sequence of cryptographic operations in s using att_A and att_B to establish a cryptographic timestamp $ctimestamp$. Then, s is relay resilient iff $s(ctimestamp)$ is valid for $a(att_A.att_B.c)$.
- A relay attack means that a session is weaker than the prescribed one.
- Agreement on the users' attributes and knowledge of the cryptographic operations and cryptographic timestamps is essential for relay protection.
- The users' attributes for relay protection play a role similar to mutual authentication, while the knowledge of the computation time of cryptographic operations and cryptographic timestamps play a key derivation role.
- Relay protection should depend on inputs to the negotiation and the negotiation itself.

Crypto-Chain in a nutshell

Cryptographic commands of F_{CC} and P_{CC}	Operations of F_{MKD}
Generate a fresh ephemeral random value (GetRV)	Start and finalise a mutual authentication and key derivation
Generate a fresh ephemeral private key and compute its corresponding ephemeral public key (CompEPuK)	Computer End-to-End Delay (EED) of a data packet (CompEED1/CompEED2)
Generate a fresh preshared key (GenPSK)	Get secured timestamps (GetTimestamps)
Shared secret key derivation (DeriveSKey)	Access commands of F_{CC}
Compute a cryptographic proof and a cryptographic timestamp (CompP&E)	Verify computation time of cryptographic operations (CompCCE)
Verify a cryptographic proof and validate a cryptographic timestamp (VerP/ValT)	Verify the expected time of completing a mutual authentication and key derivation (VerETimeMKD)

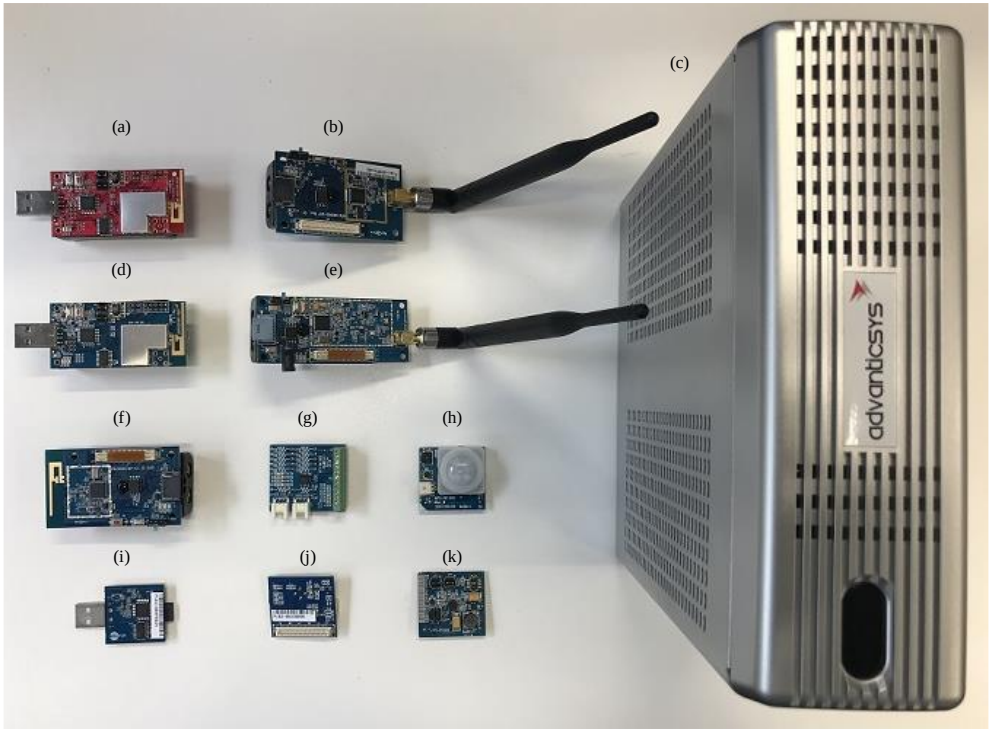
Note: (I) The combination of authentication mechanisms in GetRV, CompEPuK, GenPSK, DeriveSKey, CompP&E, and VerP/ValT commands represent the DMA/ (II) The combination of authentication and key exchange mechanisms in CompEPuK and GenPSK commands represent the KKE.

Mutual Authentication and Key Derivation Protocol (MKD)



Implementation and Analyses of MKD

Implementation of MKD using IEEE 802.15.4 modules to meet our maximum 10 msec latency target of smart vehicles. The modules are widely used in smart vehicles.



Photograph of IoT security and privacy testbed in our laboratory. Notations: (a) XM1000 mote module, (b) CM3000 sensor node, (c) network infrastructure, (d) CM5000 sensor node, (e) CM3300 sensor node, (f) CM4000 sensor node, (g) EX1000 – sensor board, (h) SE1000 sensor board, (i) USB1000 interface module, (j) DS1000 sensor board.

Implementation and Analyses of MKD (2)

- The maximum computational cost required for MKD execution between two users (i.e., initiator and responder) are as follows: (I) The responder requires ≈1.1255 s; and (II) The initiator requires ≈1.1256 s.
- We simulate MKD using the Network Simulator 3 (NS-3) to measure its EED and further validate its relay resilience. The maximum size of message to be transmitted by the key derivation initiator and responder is ≈384 bits and ≈1,760 bits, respectively.
- The EED of MKD is ≈8.2573 ms, which is less than our maximum 10 ms latency target of smart vehicles applications systems such as cooperative driving and automated overtaking. This result further validates the efficiency of Crypto-Chain (based on the transmitted messages).
- Each of the initiator and responder should have a maximum EED (supported by the size of the message) to verify the EED of the message received and the responder should verify the computation time of cryptographic operations to prevent an attacker from tampering or shortening the distance of communication.

Implementation and Analyses of MKD (3)

- To show relay resilience using MKD, we use one our sensors as an attacker to relay data packets between the two users in our simulation. The EED1 with route of the initiator to attacker to responder is 8.0086 ms and the EED2 with route of the responder to attacker to initiator is 8.1293 ms. This shows that EED1 is not directly proportional to EED2.
- Our simulation further validates the relay resilience capabilities of Crypto-Chain based on the transmitted messages and EED values.
- Note that: (I) Our implementation and analyses focus on demonstrating the efficiency of our framework via satisfying our 10 ms latency target and illustrating its relay resilience capability.

Case Study – Megamos Crypto

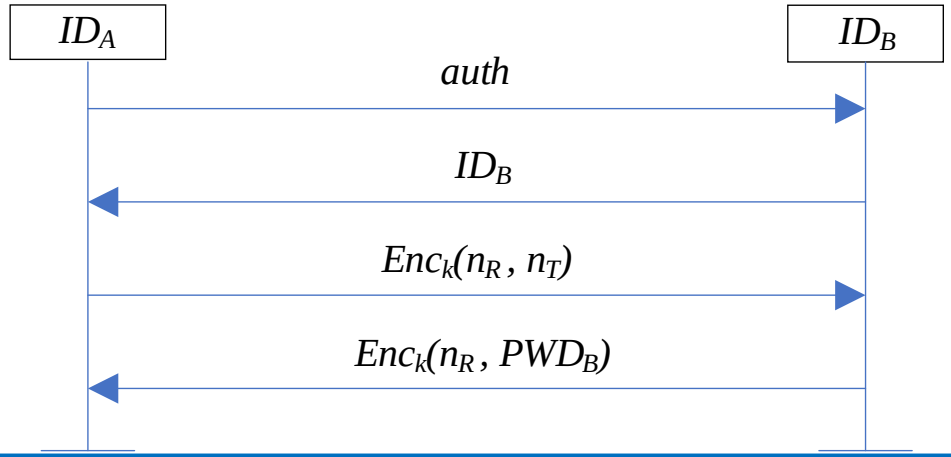
- The Megamos Crypto is a symmetric cryptosystem. This system is designed to act as a vehicle anti-theft solution between a vehicle and a car key. These devices have a microprocessor chip that incorporates the Megamos Crypto. We extracted and described the authentication protocol in the Megamos Crypto. It is based on a pre-established shared secret key and PRF.
- The Megamos Crypto does not mitigate relay attacks and thus cannot realize F_{MKD}. To see this, we consider the following setting: an honest initiator authenticates an honest responder that provided a random value r_B. The responder instance might have received a genuine public key and a random value, say (Q_A, r_A) in the first message of the protocol. The Megamos Crypto does not guarantee that (i) the initiator and responder sent (Q_A, r_A) and r_B, respectively, and that (ii) an attacker did not relay (Q_A, r_A) and r_B . The attacker can relay r_B and (Q_A, r_A) as a relay attack does not manipulate the messages transmitted between the initiator and responder.

Case Study – Megamos Crypto (2)

- We have no security guarantee for the transmitted messages and the attacker can easily let the initiator and responder accept r_B and (Q_A, r_A), respectively. While this is not a direct attack on the protocol, it shows that the security of the Megamos Crypto is not sufficient to mitigate relay attacks.
- The fixes for this problem in our setting are given as follows:
  - Enhance the first message of the protocol with a timestamp and equip the protocol with CompEED1 operation of F_{MKD} to compute EED, and
  - Equip the protocol with all the commands of F_{CC} and VerETimeMKD operation of F_{MKD} to avoid the reliance on pre-established shared secret key for authentication in the Megamos Crypto and provide mutual authentication and key derivation security guarantees. Thus, using F_{MKD} provides an Enhanced Megamos Crypto as described in the above fixes.

Case Study – Hitag-AES/Pro

- The Hitag-AES/Pro is a smart vehicle immobilizer transponder based on AES 128-bit encryption algorithm. We extract the authentication protocol in Hitag-AES/Pro as depicted in the figure below. Implementing AES 128-bit algorithm does not guarantee relay resilience as a relay attack can still be performed irrespective of the cryptographic algorithms deployed.
- A fix for this problem in our setting is to have a cryptographic proof during encryption and verify the proof during decryption using CompP&E and VerP/ValT commands of F_{CC}, respectively, and then use VerETimeMKD operation of F_{MKD} to validate the expected time of completing the protocol execution.



Conclusion and Future Work

- Extended Kusters's universal composition theorem on a fixed number of protocol systems.
- Introduced cryptographic primitives such DMA and KKE
- Proposed Crypto-Chain, which provides essential cryptographic commands (via F_{CC}) and operations (via F_{MKD}) for relay resilience
- Implemented and analysed MKD with the support of Tmote Sky sensors and NS3 simulation tool
- Analysed relay capabilities of Crypto-Chain via MKD; Mitigated relay attacks in smart vehicles
- Meeting latency target of smart vehicle applications
- Demonstrated usefulness of Crypto-Chain by enhancing Megamos Crypto and Hitag-AES/Pro
- Future work: (I) Apply Crypto-Chain to other real-world protocols. (II) Extend Crypto-Chain further mitigate ransomware attacks in smart vehicles.

Thank you

s.sani@greenwich.ac.uk