GROUP A4: SQ1 – SQ5

LUCAS DAVI (UNIVERSITÄT DUISBURG-ESSEN, DE)
FATEMEH GANJI (UNIVERSITY OF FLORIDA – GAINESVILLE, US)
TIM ERHAN GÜNEYSU (RUHR-UNIVERSITÄT BOCHUM, DE)
FAREENA SAQIB (UNIVERSITY OF NORTH CAROLINA – CHARLOTTE, US)
AHMAD-REZA SADEGHI (TU DARMSTADT, DE)
SQ3: CAN YOU GIVE AN EXAMPLE OF A SECURITY FAILURE DUE TO INSECURE COMPOSITION

• At different levels of abstraction
• Supply chain threats, the assumption model of foundry is trusted.
• Design in-house, overbuilding and piracy.
• Microarchitecture level (Rowhammer bugs)
• DRAM failure, the assumption model is RAM is reliable and no bit flips will occur.
• Cryptographic algorithm: Software or implementation errors (Memory corruption).
• Automotive: Thread model versus assumption. No encryption or source information.
SQ4: WHAT IS THE FOUNDATION OF COMPOSITION

- Clear requirements, and assumptions that fit reality.
- Security metrics and confidence of metrics.
- Formal construction flow of integrating countermeasures.
- Side effects of the protection countermeasures need to be modeled (Side channel and fault injection).
- New opportunities for attack. (Self healing logic can be exploited)
- Formal methods to measure and verify the security assumptions.
- Stress Testing, to test all the corner cases (Worst case scenarios). Coverage and Assurance.
SQ2: WHAT DOES IT MEAN TO SECURELY COMPOSE TWO ELEMENTS

• Supply chain: Security features on chip and the player such design house and foundry.
• Assumptions need to formulated, with a unified attack model: Resources and capabilities of adversaries.
• Microarchitectural Level (Rowhammer Attack): DRAM and software running the memory. Access control and integrity checks on DRAM using software and new memory hardware design.
• Cryptographic designs: Algorithms vs implementation. Mathematically strong algorithms and secure interfaces and implementation.
• System level (CANBus): Abstract isolation, and standard security measures.
SQ1: HOW WOULD YOU HANDLE COMPOSABILITY

IDEAL WORLD

REAL WORLD
SQ5: HOW DO YOU VERIFY REMOTE IDENTITY OF A CONNECTED DEVICE?