Security Task Group

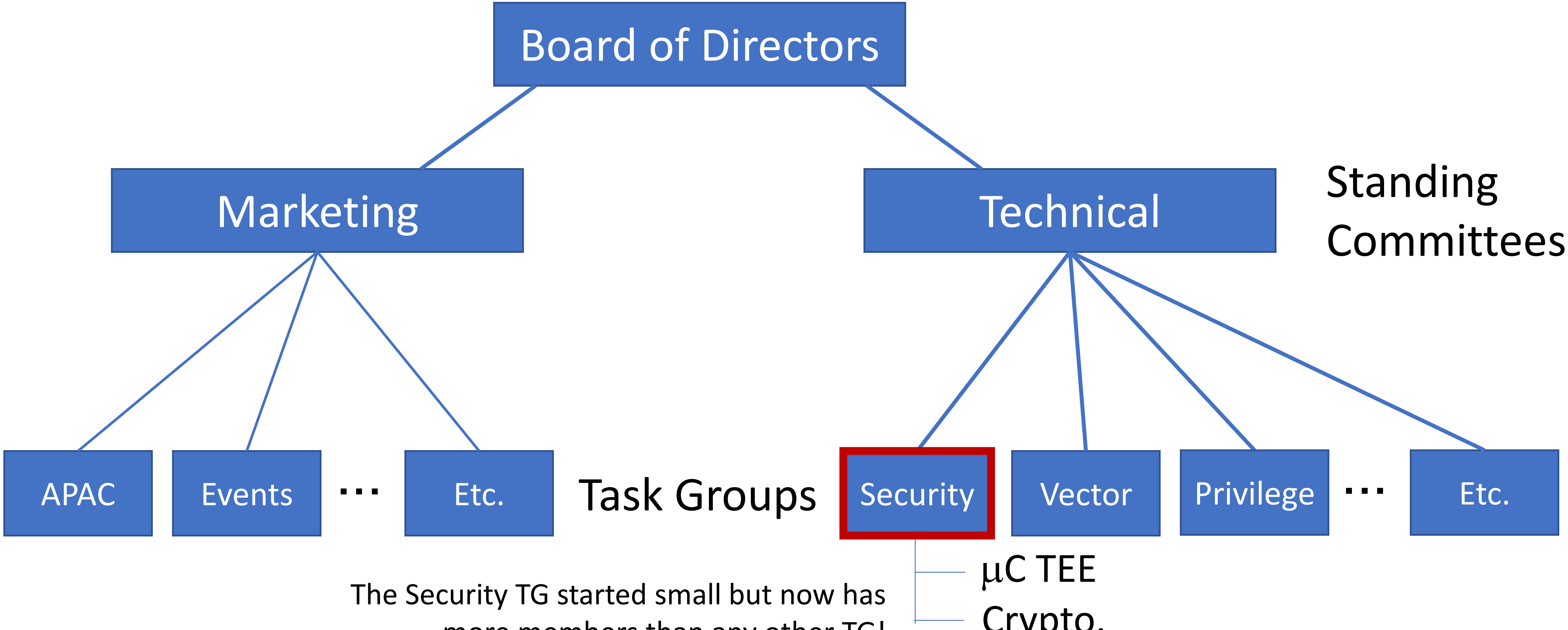
Presented by Richard Newell

Vice-Chair

May 9, 2018

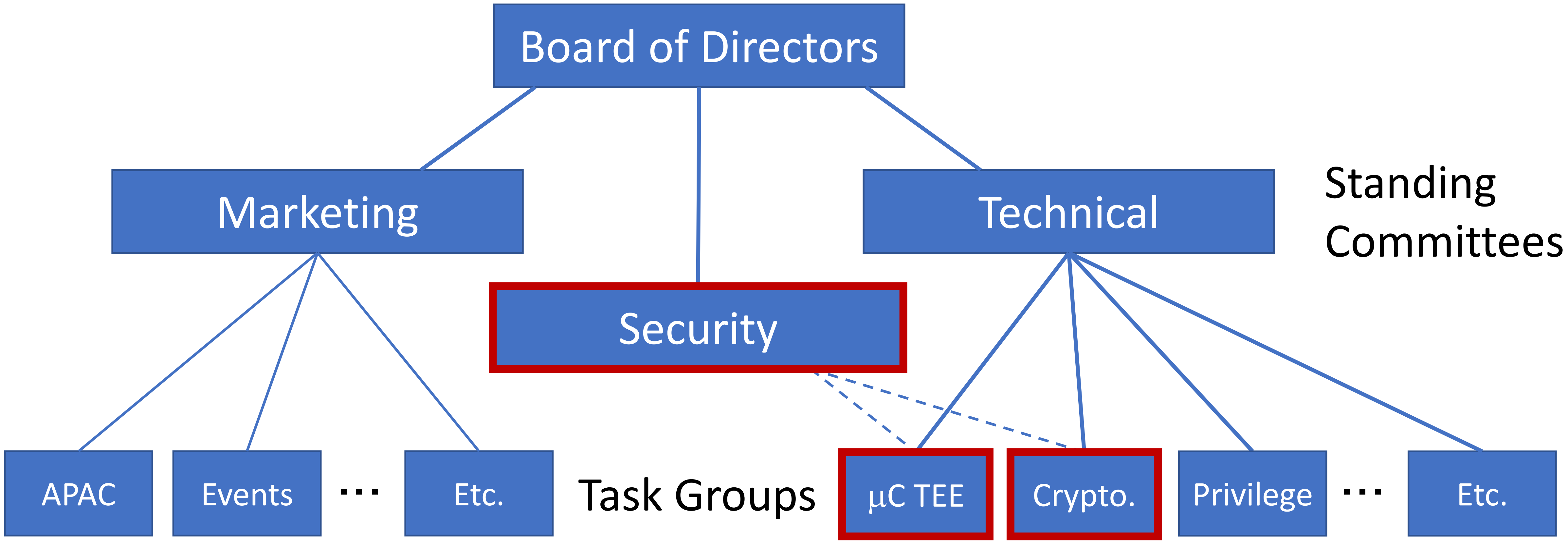
8th RISC-V Workshop, Barcelona

Security Group Organization – Before last week



The Security TG started small but now has more members than any other TG!

Security Group Organization – After last week



(First two task groups planned)

Security Standing Committee Charter (approved)

Security Steering Committee Main Goals:

- Promote RISC-V as an ideal vehicle for the security community
- Liaise with other internal RISC V committees and with external security committees
- Create an information repository on new attack trends, threats and countermeasures
- Identify top 10 open challenges in security for the RISC-V community to address
- Propose security committees (Marketing or Technical) to tackle specific security topics
- Recruit security talent to the RISC-V ecosystem (e.g., into committees)
- Develop consensus around best security practices for IoT devices and embedded systems

Charter (continued)

- General Activities to support Security Steering Committee Goals:
- Develop a repository with information about new processor centric threats, security trends, attacks and countermeasures
- Wiki page or equivalent with links to external publications
- Develop a taxonomy of security domains such as
    - Attacks and countermeasures,
    - Secure execution environments,
    - Cryptography
    - Secure memory management
    - Parallel and concurrent execution in secure environments
    - Virtualization
- Assess the state-of-the-art in those domains
    - Already solved, known solutions but not implemented, …
- Invite internal/external expert speakers to present on new attacks and countermeasures, security solutions in other domains, …
- Interpret attacks and assess threats in the RISC V context
- Discuss security best practices to address new threats in those domains
- Develop and publish security guidelines, do's and don'ts
- Choose which domains are candidates for action by the Foundation.
- Propose setup of New Technical Committees to address actionable domains
    - Cryptography Extensions
    - Trusted Execution Environment
    - …
- Review and liaise with other RISC V committees that are about to finalize specifications to identify any additions that could be made today to take security into consideration;
    - Privilege spec
    - Hypervisor spec
    - Virtualization
    - Debug
    - Formal analysis
    - Compliance
- External facing activities
    - Develop and publish position papers, security whitepapers
    - Publish expert opinions and statements on new threats and trends
- Liaison activities
    - Liaise with other relevant industry or standards security groups such as TCG, GP, PCI, NIST, DARPA, Linux Foundation

Charter (continued)

Timeline for first deliverables:

Now:
- Setup a weekly/biweekly conference call for committee meetings
- Propose Setup of New Technical Committees on Crypto Extensions and Trusted Execution Environment
- Develop information repository

Every other week or once a month, on a regular basis,
- Invite expert speakers from security industry or standards groups, etc.
- Monitor ongoing new security trends and discuss how to best address (position paper, expert opinion, security whitepaper, propose to create a new Tech Committee – more rarely)
- Define new tasks and assign owners to tasks; present and review results

First identified tasks until next workshop (December):
- Develop taxonomy on security domains
- Identify top 10 security challenges to be worked on
- Review specs and engage with other RISC V committees for security feedback and input into specs
- Select and engage with a first security industry group outside of RISC V

Longer term objectives:
- Develop and publish security best practices and security guidelines
- Engage with more external industry security groups

Appointed Chair – Dr. Helena Handschuh (Rambus)

HELENA HANDSCHUH is Rambus Fellow and Vice President of Security Architecture at Rambus, Inc. Her research and responsibilities include: managing the foundational security technologies team of 20 technology experts; research in crypto and post-quantum crypto; research in power analysis and side-channel attacks and countermeasures; building prototypes and showcasing technology to customers, partners, and events; security architecture for new products and services; prototyping of new products and security standardization. She was formerly a Technical Director of Cryptography Research, Inc., and Chief Technology Officer at Intrinsic-ID. She was also the manager of the Applied Cryptography and Security Group and manager of the Card Application Security team at Gemplus (now Gemalto). She is a volunteer Research Fellow at the KU.Leuven, Belgium. She authored more than 50 peer-reviewed papers and holds 18 patents in the areas of security and cryptography.

Dr. Handschuh earned an M.S. in networks and communication engineering from the Ecole Nationale Superieure de Techniques Avancees (ENSTA, Paris), an M.S. in algorithms and cryptography from the Ecole Polytechnique, and a Ph.D. in cryptography from the Ecole Nationale Superieure des Telecommunications (ENST, Paris).

Appointed Vice-Chair – Dr. Joseph Kiniry (Galois)

Dr. Joseph Kiniry is a Principal Scientist at Galois. Previously, he was a Full Professor at the Technical University of Denmark where he was the Head of the Software Engineering section. Since the early 2000s he has held permanent positions at four universities in Denmark, Ireland, and The Netherlands. Dr. Kiniry has extensive experience in formal methods, high-assurance software and hardware engineering, foundations of computer science and mathematics, and information security. Specific areas that he has worked in include software and hardware verification foundations and tools, digital election systems and democracies, smart-cards, smart-phones, critical systems for nation states, and CAD systems for asynchronous hardware.

Task Group & Charter (proposed): Trusted Execution Environment for Microcontroller-Class Processors

- The goal of this working group is to develop a specification that serves as extension of privilege spec, to support trust execution environment on embedded RISCV processors. Specifically, RISCV core with M/U mode and physical memory protection but without S/H mode and virtual addressing mechanism. The working group is also aiming to develop all necessary components including compiler, simulation model, hardware and software APIs to support the specification.

Chair μC-TEE task group (proposed) – Joe Xie (nVidia)

Joe Xie is a senior hardware manager in nVidia’s multimedia hardware department. He manages a hardware and architecture team. The team is responsible for building embedded security processor subsystem, the processor is been used in over 20 hardware engines in GPU and Tegra™ SOCs. The team is also responsible for building a high performance crypto accelerator engine for Tegra SOCs and GPUs.

Task Group & Charter (proposed): Cryptography Extensions

- The cryptographic extensions technical committee will propose ISA extensions to the vector extensions for the standardized and secure execution of popular cryptography algorithms. To ensure that processor implementers are able to support a wide range of performance and security levels the committee will create a base and an extended specification. The base will be comprised of low-cost instructions that are useful for the acceleration of common algorithms. The extended specification will include greater functionality, reserve encodings for more algorithms, and will facilitate improved security of execution and higher performance. The scope will include symmetric and asymmetric cryptographic algorithms and related primitives such as message digests. The committee will also make ISA proposals regarding the use of random bits and secure key management.

Chair Crypto task group (proposed): Rich Newell (Microsemi)

Richard Newell serves as senior principal product architect at Microsemi and plays a key role in architecting the security features for the current and future generations of flash-based FPGAs and SoC FPGAs. Richard has an electrical engineering background with experience in hardware security and cryptography, analog and digital signal processing, control systems, inertial sensors and systems, and FPGAs. He is an alumnus of the University of Iowa. Richard is the recipient of sixteen U.S. patents, and is a member of the Tau Beta Pi and Eta Kappa Nu honorary engineering societies.

Thanks!