TRUSTED® COMPUTING GROUP

TCG Update
JRF Workshop

Thorsten Stremlau
TCG Marketing Workgroup Chair

TRUSTED COMPUTING GROUP

TCG UPDATES

- TCG in 2020:
- 7 press releases written and distributed, 1 in progress, 10 in the pipeline
- 25 features written and published, 8 awaiting coverage (5 currently being drafted)
- 10 blogs written and published, 2 being drafted (3 in the pipeline)
- 3 newsletters written and distributed, 1 in progress
- 11 event media partnerships secured
- 10 events with speaker opportunities secured
- 9 Awards submitted
- 7 podcasts recorded,
- 1 TCG webinar completed and 1 in the pipeline
- 1 website audit completed
- 2 videos completed, 1 video in process

TRUSTED® COMPUTING GROUP

2020 results so far

Press release, feature articles and industry mentions

- **658** pieces of media coverage so far
- **725 million** viewers

TRUSTED COMPUTING GROUP

Recent Event Participation

Presenting TCG on the virtual stage

FIERCE Technology

MedTech Innovation Week
'How Technology is Tackling the Pandemic' - *Scott Piper, Lenovo*

IIoT World

Social Media Interview
Steve Hanna, Infineon

electronica

Embedded Tutorial Webcast
'Solving Common IoT Security Problems with TPM' - *Nicholas Lau, Infineon*

IoT Security Summit

Virtual Event
Panel Moderator - *Steve Hanna, Infineon*

iot device security conference

Virtual Event
Session 2 IEC 62443: How to Achieve the Highest Levels of Industrial Security - *Steve Hanna, Infineon*

CyberRisk Alliance
Business Intelligence Resources

Endpoint Security e-Summit
'Use the Security You Already Bought' - *Steve Hanna, Infineon*

TRUSTED COMPUTING GROUP

Recent Event Participation

Presenting TCG on the virtual stage

MedTech Innovation Week
'How Technology is Tackling the Pandemic' - *Scott Piper, Lenovo*

Social Media Interview
Steve Hanna, Infineon

Embedded Tutorial Webcast
'Solving Common IoT Security Problems with TPM' - *Nicholas Lau, Infineon*

Virtual Event
Panel Moderator - *Steve Hanna, Infineon*

Virtual Event
Session 2 IEC 62443: How to Achieve the Highest Levels of Industrial Security - *Steve Hanna, Infineon*

Endpoint Security e-Summit
'Use the Security You Already Bought' - *Steve Hanna, Infineon*

Coming in 2021: TCG Hackathon best TCG contributions published and prizes.

TRUSTED® COMPUTING GROUP

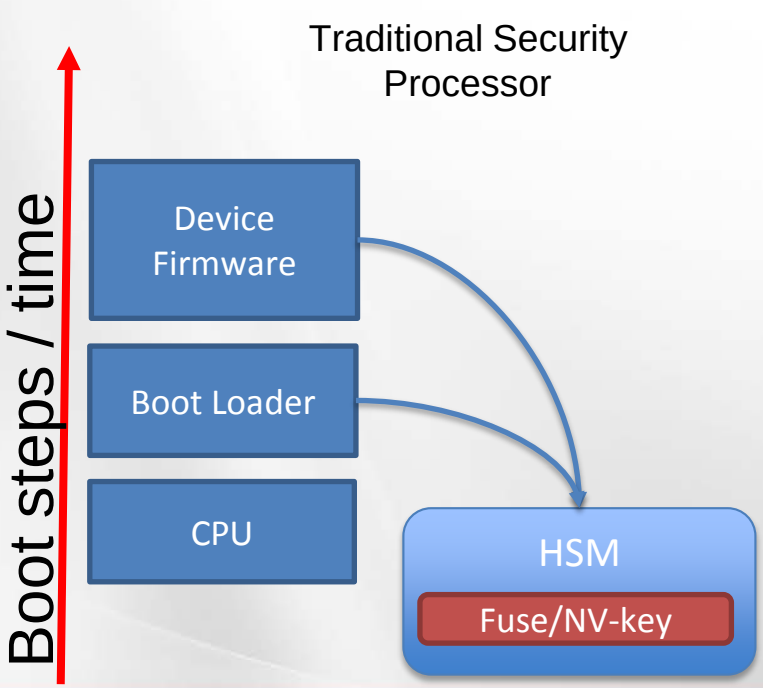
DICE / CYRES / FIM / RIM

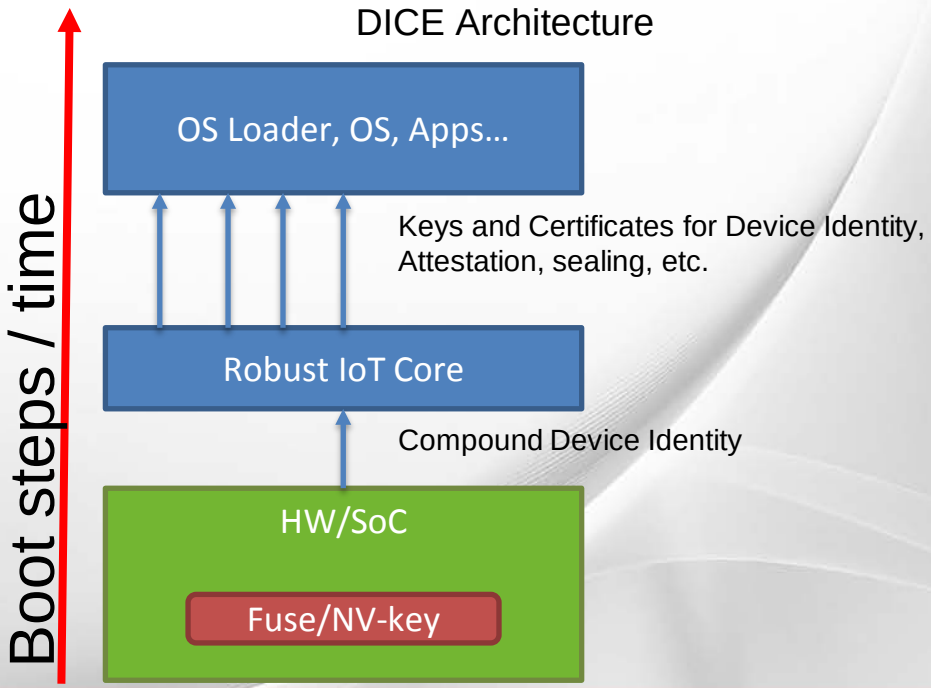
TRUSTED® COMPUTING GROUP

DICE

- Device Identifier Composition Engine (DICE, TCG)
- A specification from the Root of Trust for Measurement subgroup in the Trusted Computing Group (TCG)
- Foundational security for HW at near zero cost
- Simple hardware requirements mean DICE is adaptable to most any system or component
- Provides HW-based identity and attestation, and a foundation for sealing, data integrity, device recovery and update

THE DICE MODEL

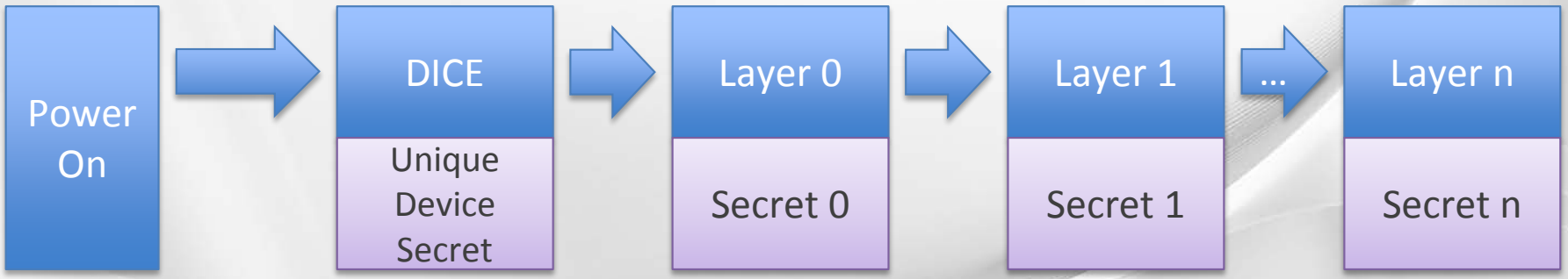




TRUSTED COMPUTING GROUP

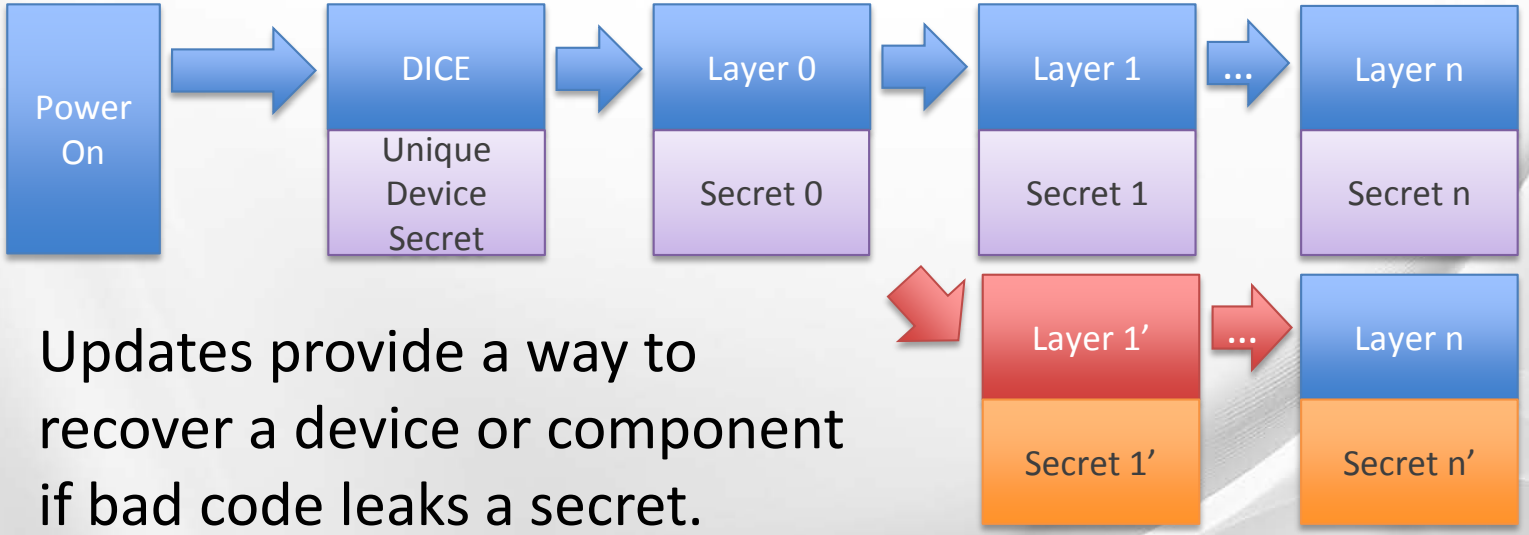
THE DICE MODEL

- Power-on (reset) unconditionally starts the DICE
- DICE has exclusive access to the Unique Device Secret
- Each layer computes the secret for next layer (via One Way Function)
- In this derivation chain, each layer must protect the secret it receives



WHEN SOMETHING CHANGES

- The branch illustrates the result of a code/config change

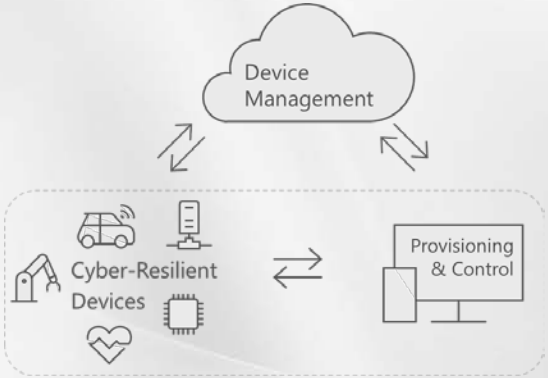


- Updates provide a way to recover a device or component if bad code leaks a secret.

CyRes Workgroup (NISTSP800-193)

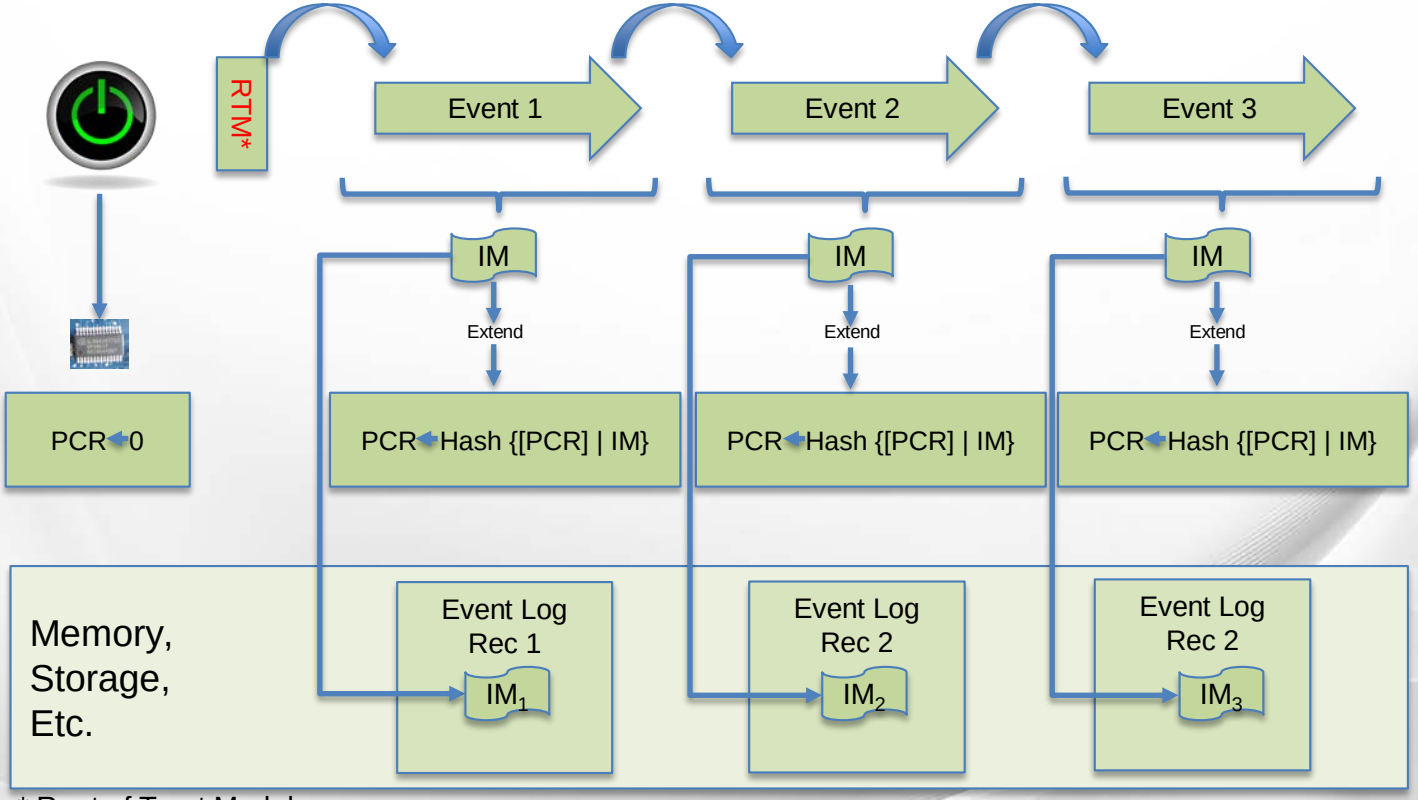
Cyber Resilient Devices using TPM 2.0 Rev 1.59 ACT

All Internet-connected devices should be designed to protect themselves against network-based attacks. As such, Device Vendors must employ a wide range of hardware and software-based protection technologies to keep systems secure. Unfortunately, bugs and misconfigurations still lead to damaging exploits. Recovering a badly compromised computing device today usually involves manual intervention.



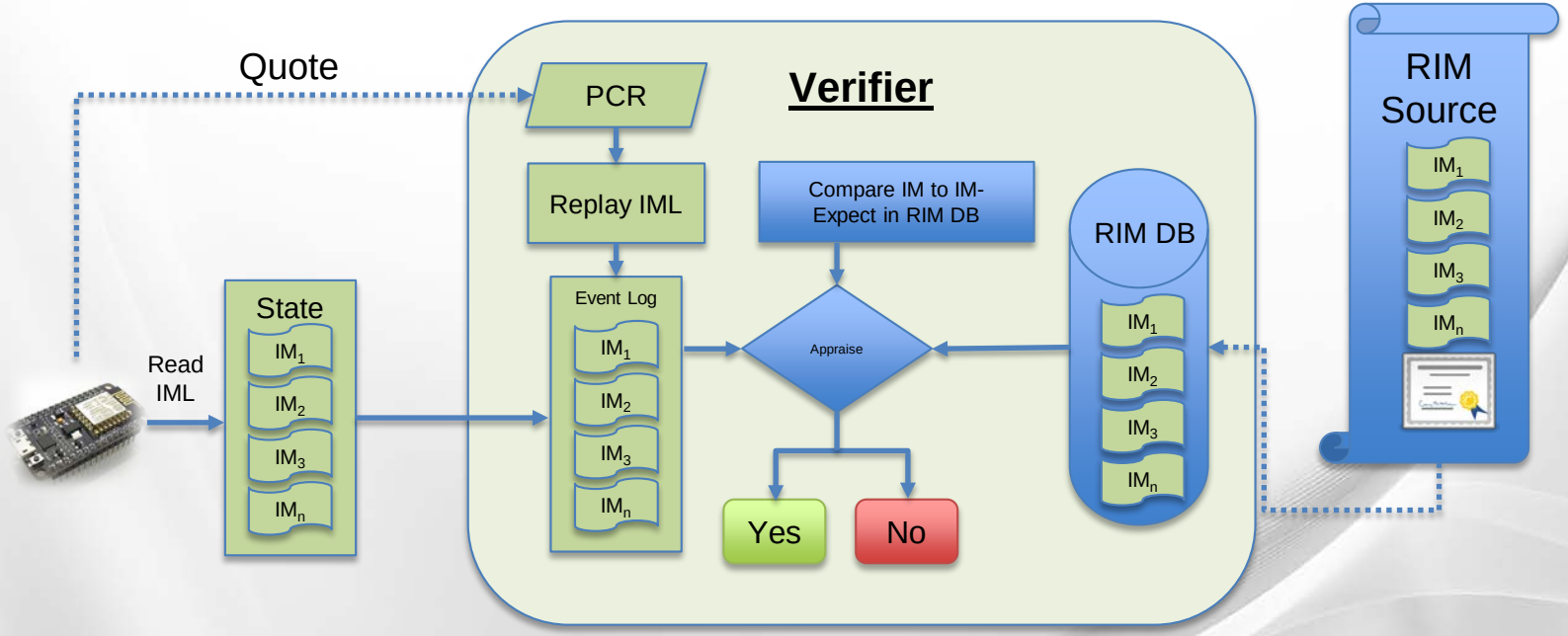
The solution uses the new Authenticated Countdown Timer (ACT) feature in TPM 2.0 Rev 1.59 as an “active” component to help recover devices to a healthy state. Remote update and recovery, enforcement of device policy, and remote management of this Cyber-Resilient device is demonstrated

Firmware Integrity Measurement



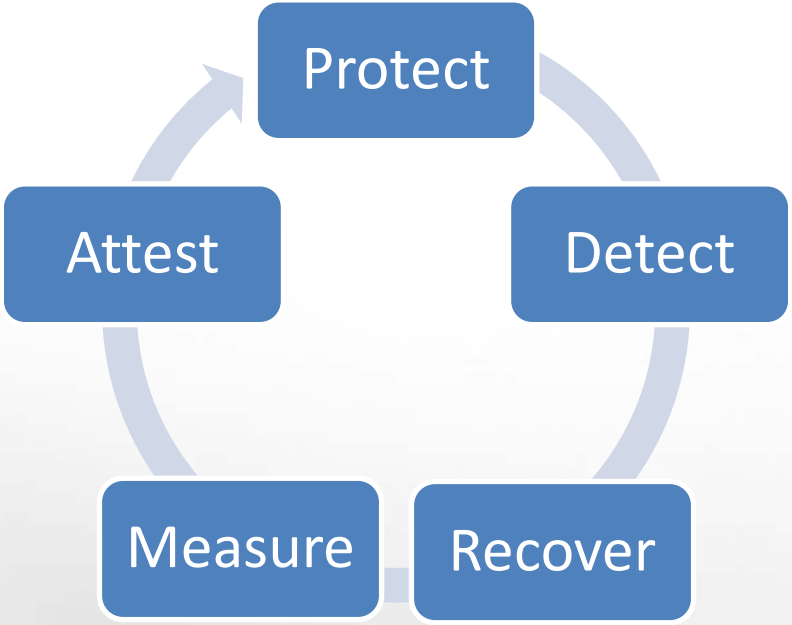
* Root of Trust Module

Reference Integrity Manifest



TRUSTED COMPUTING GROUP

TPM - CYRES – DICE – FIM and RIM working together to get customers over the finish line faster



https://trustedcomputinggroup.org/membership/

TRUSTED COMPUTING GROUP

TCG Update
まとめ

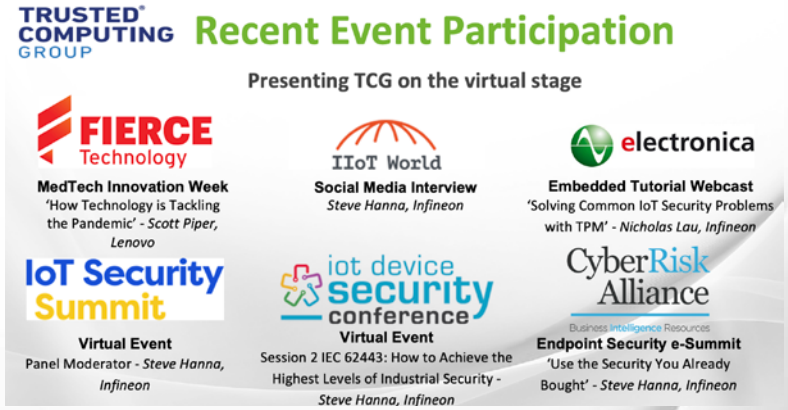
JRFワークショップ　12月17日

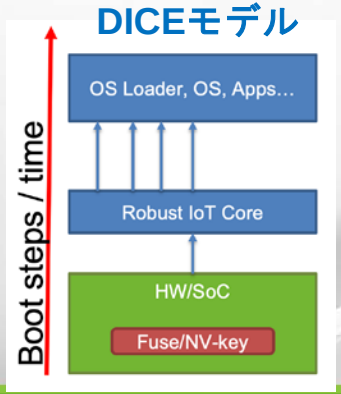
TCG 副理事
Lenovo Research
河 野　誠 一

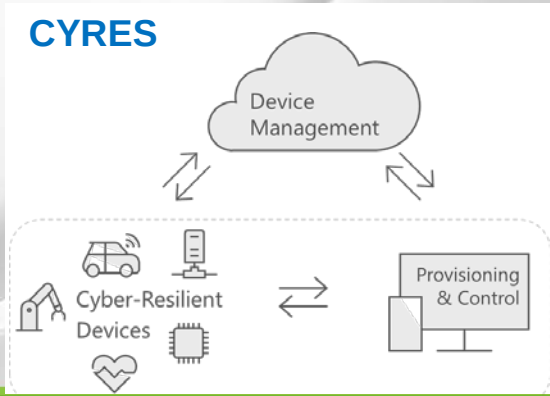
WG活動紹介

- TCG技術の
  プロモーション

- 注目されている技術
  DICE / CYRES / FIM / RIM







TRUSTED COMPUTING GROUP

TPM - CYRES – DICE – FIM - RIM

活発な標準化仕様の議論がされてます!

TPM, CYRES, DICE, FIM, RIM, IoT, Automotive

詳細技術情報　- TCGメンバーのみです
議論内容・参加　- TCGメンバーのみです
公開情報　- 誰でも可です・・・が・・・

TCGメンバーへ：技術部会への積極的な参加を
まだメンバーでない方へ：是非TCGへの加入を

https://trustedcomputinggroup.org/membership/

TRUSTED® COMPUTING GROUP

ありがとうございました