innovations
for high
performance
microelectronics

Energy efficient middleware design in support of user privacy

Peter Langendoerfer

IHP
Im Technologiepark 25
15236 Frankfurt (Oder)
Germany

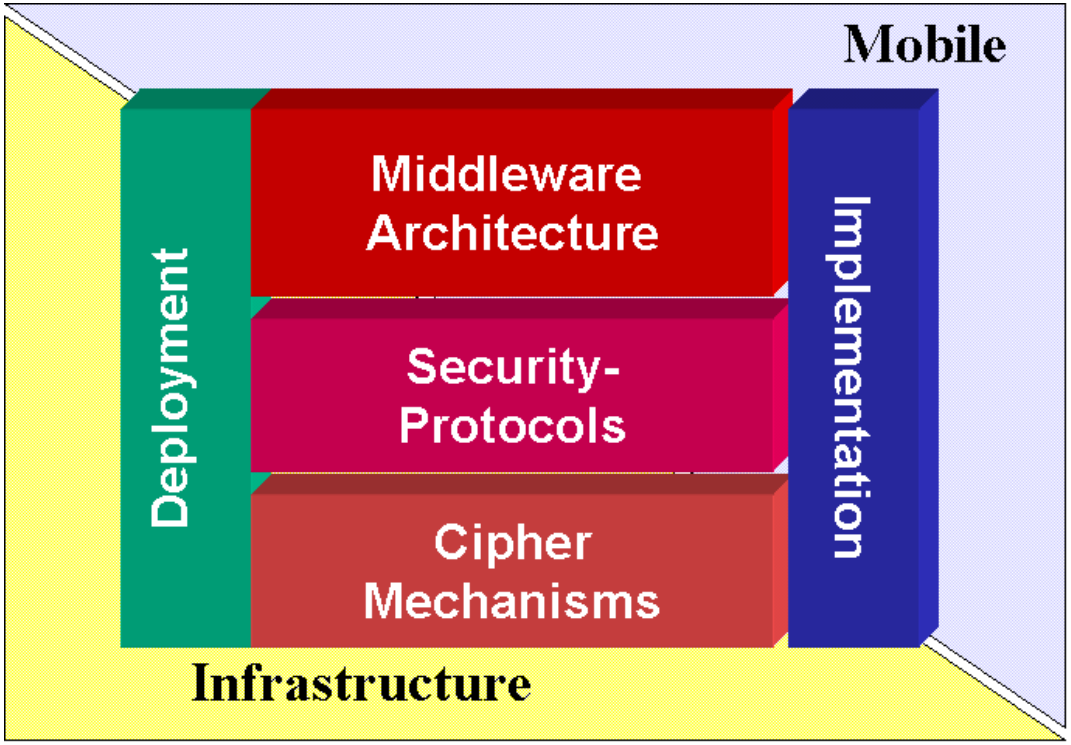
Outline

- **Motivation**
- **Case Study: PLASMA's vertical cross-layer approach**
- **Analysis of the state of the art**
- **Discussion of open issues**
- **References**

Why a vertical cross-layer Approach?

- **Consider only the platform?**
  - Lot of opportunities to improve the system are excluded
- **Consider only hardware accelerators?**
  - Limited flexibility
  - Only some specially equipped devices will benefit
- **Solution: Inter-domain Approach**
  - Take into account all aspects of the whole system
  - Adaptation to the different/changing situations

PLASMA‘ s vertical cross-layer Approach



Potential savings for combined RSA/ECC approach

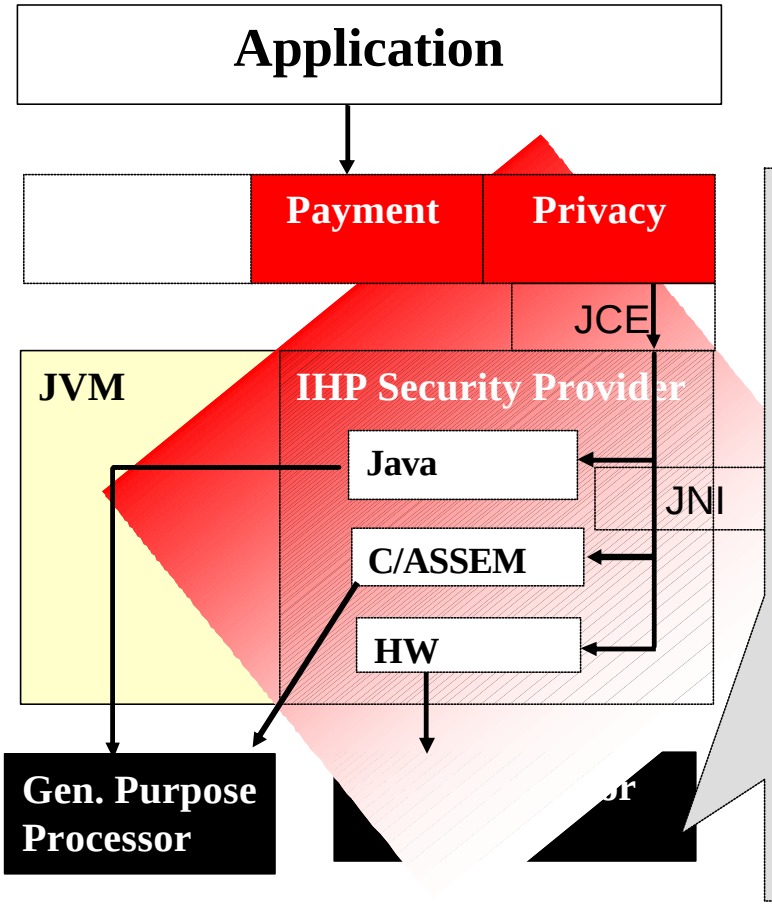
Computational load: signature generation/ verification 23/24;

Approach / Measured results	Combination	pure RSA: exp=3		pure ECC: B-163	
Speed up factor	K-163, RSA exp=3	47.0	14.4	1.6	2
Saved computing time [s]		458.9	859.1	5.6	64.63

Measurements done on HP Journada using the Miracle lib.

Values from literature measured on a Palm (J. Lopez et.)

HW/SW Architecture of the Mobile Device



Accelerator for ECC

- Complexity: ~40 000 gates
- Clock cycles per encryption of 233 bytes: 90 404
- Energy needed per encryption: 0.8mWs

Accelerator for AES

- Complexity: ~36 000 gates
- Clock cycles per encryption of 100 Mbit: 10 937 500
- Energy needed per encryption: 66 mWs

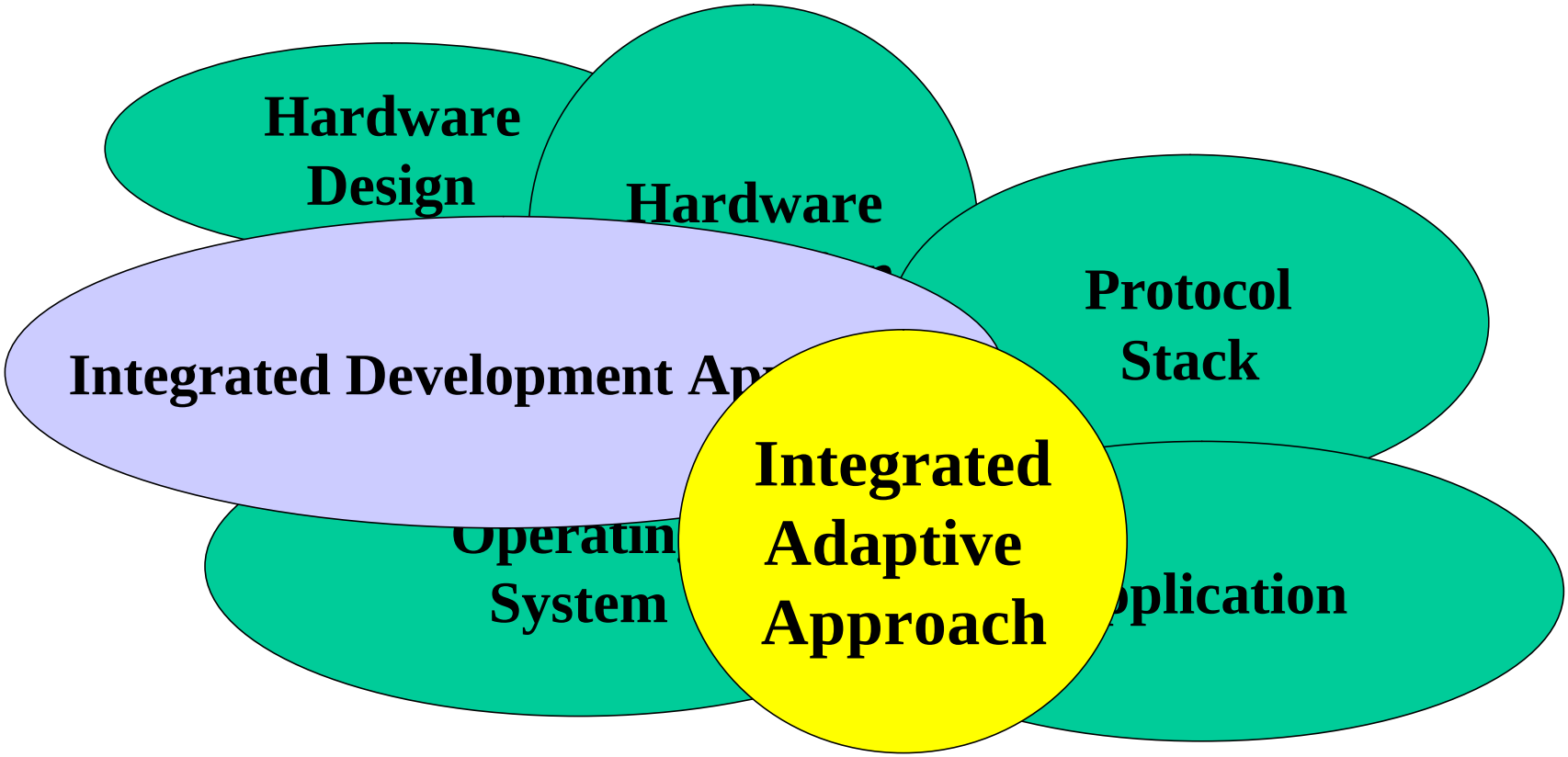
Performance compared to software solutions

- Two orders of magnitude less in energy consumption
- Two orders of magnitude less in time consumption

Analysis: State of the Art

- **Hardware Optimization Opportunities**
  - Specialized hardware e.g. ASICs [12],
  - Tuned HW components e.g. multiplier operand size [7]
  - Clock frequency/ Dynamic Voltage Scaling [7]
- **Protocol Stack Optimization**
  - Integrated Layer Processing [14, 15]
  - Protocol Layer Interaction [4, 8, 9]
- **Middleware Optimization (Adaptive/ a priori)**
  - Load shifting [5, 3]
  - Application specific optimizations [1, 6, 12]
  - Adaptive concepts [2]

What is missing/ What is needed



Open Research Topics

Further progress needs

- **Integrated Development (IDA)**
- **Integrated Adaptive Approach (IAA)**

Such as

- **Methodologies to develop IAA supporting systems**
- **Methodologies to exploit IAA for a certain application/environment**
- **Semantic description of optimization knobs**
- **IAA Management Plane**

PLUS your suggestions . . . . .

Thank you for your attention

Questions, Comments?

References

1. Radu Cornea, Shivajit Mohapatra, Nikil Dutt, Alex Nicolau, Nalini Venkatasubramanian, "*Interactive Managing Cross-Layer Constraints for Mobile Multimedia*", IEEE Workshop on Constraint-Aware Embedded Software(RTSS-2003) — Cancun, Mexico, December, 2003.

2. Shivajit Mohapatra, Nalini Venkatasubramanian. "*PARM: Power Aware Reconfigurable Middleware*", IEEE International Conference on Distributed Computer Systems (ICDCS-23), Rhode and Test in Europe (Date), 2004

3. Travis Newhouse, Joseph Pasquale *Resource-controlled Remote Execution to Enhance Wireless Network Applications*, Proceeding of ASWN'04, 2004

4. Gustavo Carneiro et al.: *Cross layer design in 4G Wireless terminals*, IEEE Wireless Communications, Vol 11, No 2, 2004 Island, May 2003.

5. Rajesh Krishna Balan *Powerful Change Part 2: Reducing the Power Demands of Mobile Devices*, Pervasive Computing Vol. 03, No. 2, 2004

References

6. Hans Van Antwerpen, et al.: *Energy-Aware System Design for Wireless Multimedia*, Panel on Platforms and Tools for Energy-Efficient Design of Multimedia Systems, Design Automization

7. Rex Min et al. *Energy Centric Enabling Technologies for Wireless Sensor Networks*, IEEE Wireless Communications, Vol 9, No 4, 2002

8. M. Methfessel, et. al: *Vertical Optimization of Data Transmission for Mobile Wireless Terminals*. IEEE Wireless Communications, 2002.

9. P. Langendörfer, et al.: *Shielding TCP from Wireless Link Errors: Retransmission Effort and Fragmentation.* The Journal of Supercomputing, Vol. 23, (3), 245-260, 2002.

References

10. P. Langendoerfer, et al.: *A vertical approach towards energy efficient application of cipher mechanisms in hot spots running location aware services*, International Conference on Advances in the Internet, Processing, Systems, and Interdisciplinary Research, 2003

11. P. Langendörfer , Z. Dyka, O. Maye, R. Kraemer: *A Low Power Security Architecture for Mobile Commerce.* Proceedings of 5th IEEE CAS Workshop on Wireless Communications and Networking, IEEE Society Press 2002.

12. W. Yuan, K. Nahrstedt, S. Adve, D. Jones, and R. Kravets, *Design and Evaluation of A Cross-Layer Adaptation Framework for Mobile Multimedia Systems*, in Proc. of SPIE/ACM Multimedia Computing and Networking Conference (MMCN'03), Santa Clara, CA, January, 2003.

13. Wanghong Yuan and Klara Nahrstedt, *A Middleware Framework Coordinating Processor/Power Resource Management for Multimedia Applications*, in Proc. of IEEE Globecom 2001, San Antonio, Texas, November, 2001.

References

14. M. Abbot, L. Peterson: *Increasing Network throughput by Integrating Protocol Layers*, IEEE/ACM Transaction on Networking, 1993

15. P. Langendörfer, H. König, R. Kraemer: *Evaluation of well-known Implementation Techniques for Application in Wireless Networks*. The Journal of Supercomputing (Kluwer), 20, 161-170, 2001.

