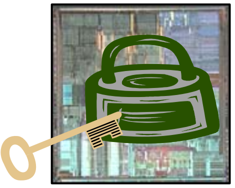
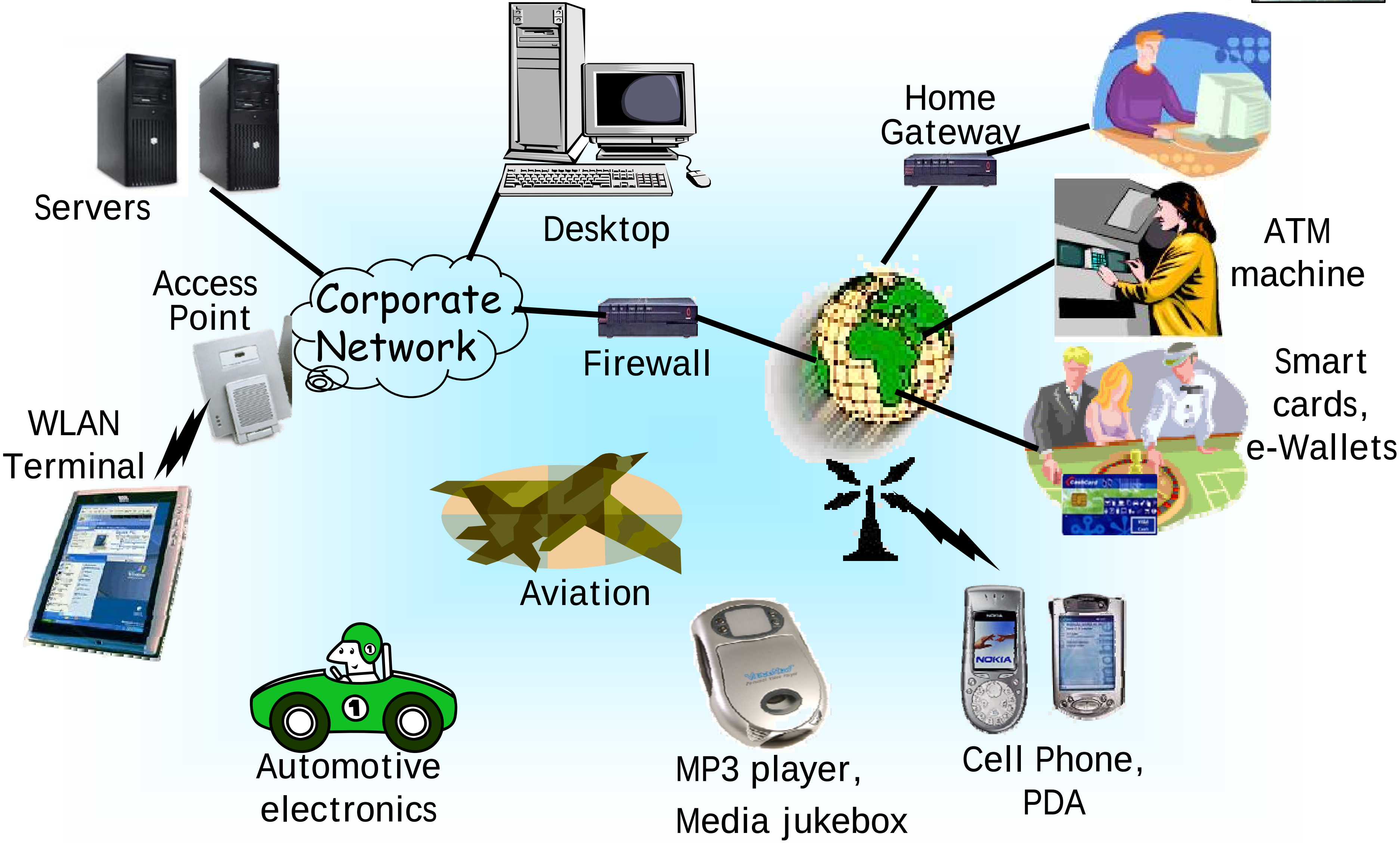
SoC: Security-on-chip !



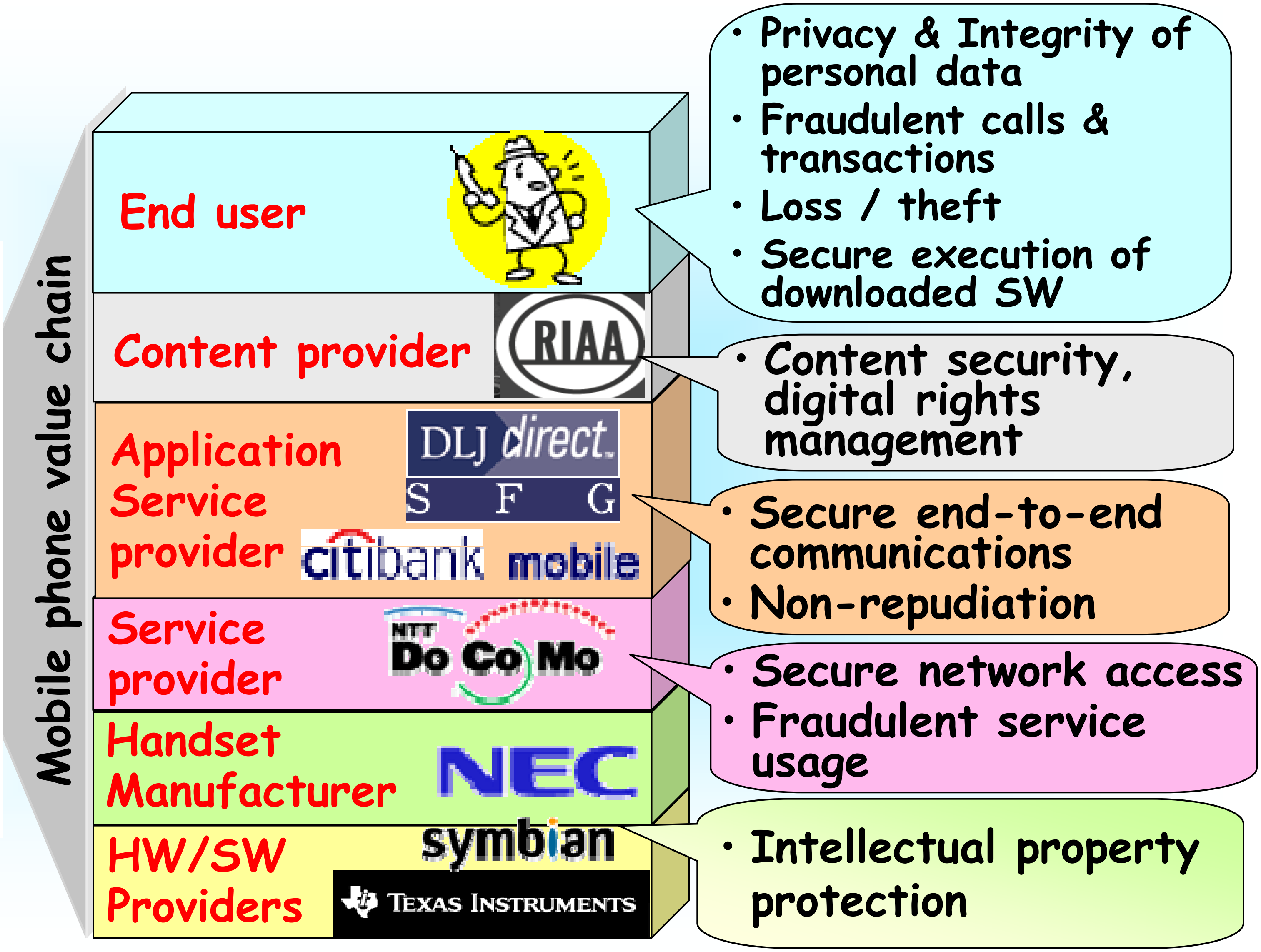
MPSoC (July 2005)

Srivaths Ravi
NEC Laboratories America
Princeton, NJ

Ubiquitous Security Concerns



Security Concerns for an Example Device (3G Cell Phone)



Mobile phone value chain

End user

Content provider

Application Service provider

Service provider

Handset Manufacturer

HW/SW Providers

- Privacy & Integrity of personal data
- Fraudulent calls & transactions
- Loss / theft
- Secure execution of downloaded SW

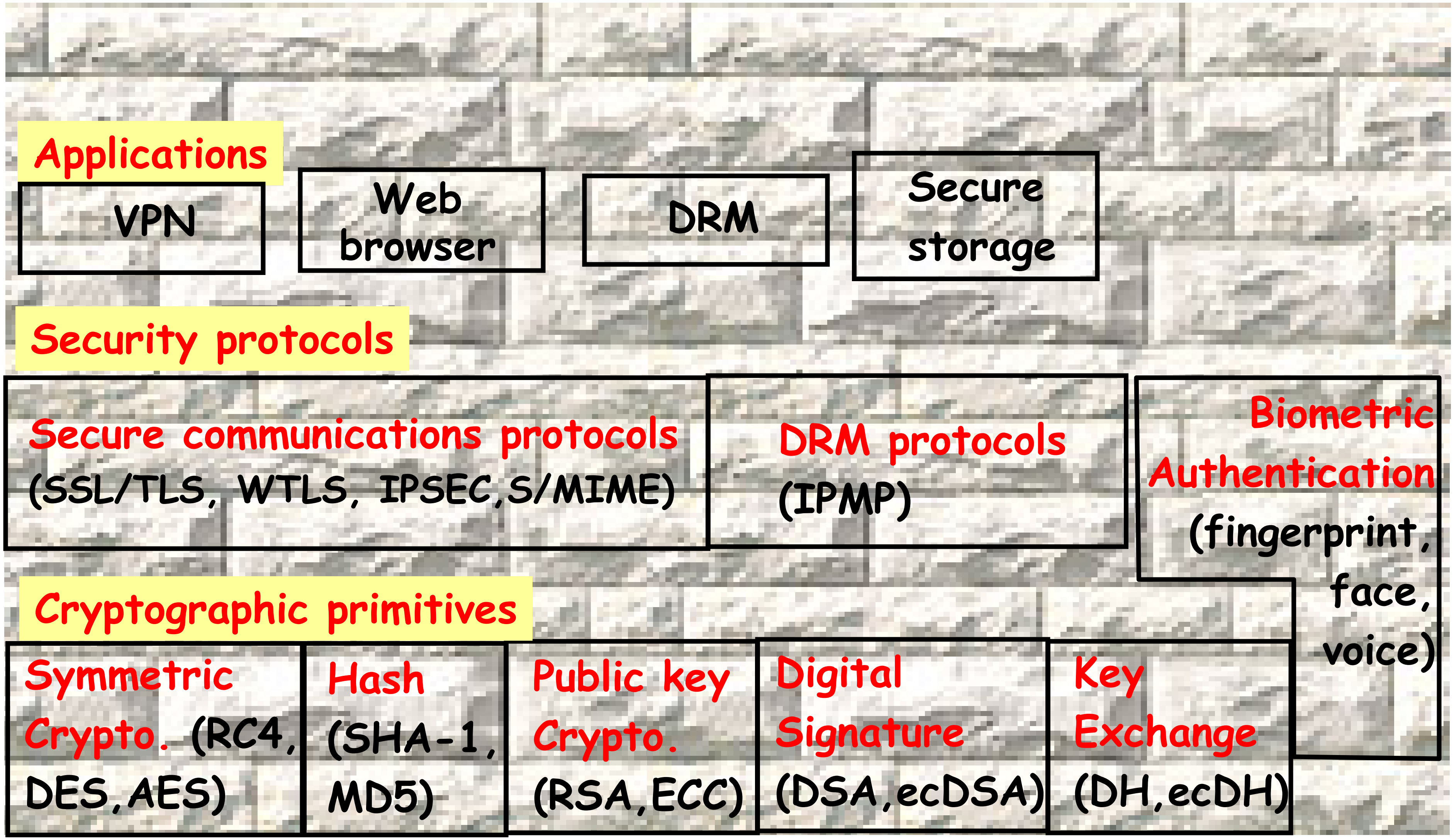
- Content security, digital rights management

- Secure end-to-end communications
- Non-repudiation

- Secure network access
- Fraudulent service usage

- Intellectual property protection

Functional Security Measures



Applications

VPN

Web browser

DRM

Secure storage

Security protocols

Secure communications protocols (SSL/TLS, WTLS, IPSEC,S/MIME)

DRM protocols (IPMP)

Biometric Authentication (fingerprint, face, voice)

Cryptographic primitives

Symmetric Crypto. (RC4, DES,AES)

Hash (SHA-1, MD5)

Public key Crypto. (RSA,ECC)

Digital Signature (DSA,ecDSA)

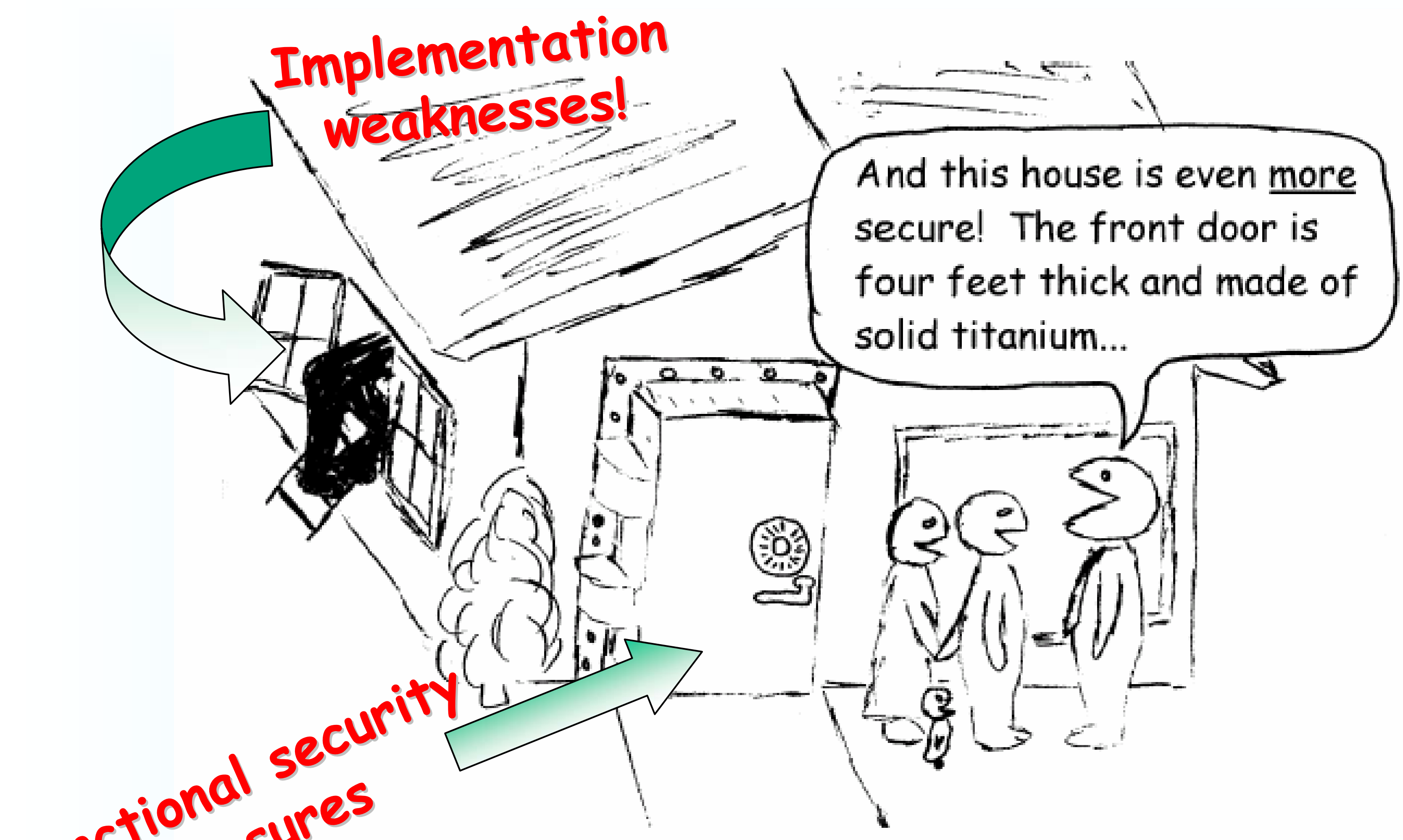
Key Exchange (DH,ecDH)

Security Challenges for an SOC Designer

- **Assurance gap**
  - Gap between sound functional measures and a secure implementation
- **Security processing gap** *
  - Disparity between processing requirements and capabilities
- **Battery gap** *
  - Energy requirements for security related functionality

* Please refer to the Appendix for quantitative illustrations

Assurance Gap

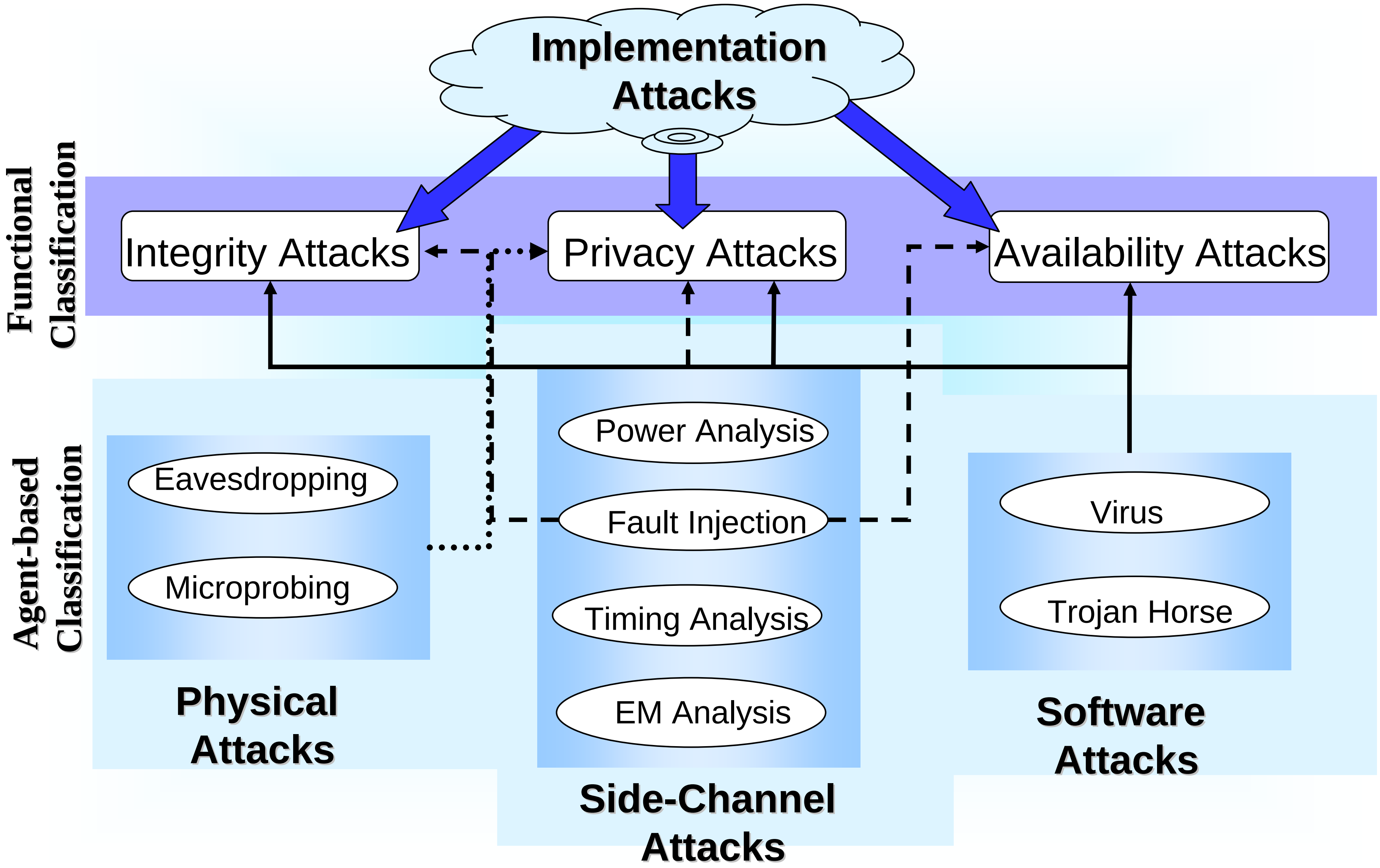

And this house is even more secure! The front door is four feet thick and made of solid titanium...

Implementation weaknesses!

Functional security measures

Cartoon courtesy: Paul Kocher

"Implementation" Attacks



Approaches to addressing the security gaps

- **Software**
  - SW certificates
  - Encrypted SW execution
  - OS and language-based techniques for isolation
  - Tools that check code for vulnerabilities
- **Architecture**
  - Security-enhanced embedded processors
    - ARM TrustZone, AEGIS (MIT), XOM (Stanford)
    - Co-processors for crypto.
    - Trusted Computing Platforms (TCPA, NGSCB)
  - Secure SoCs
    - TI OMAP, NEC M
- **Logic-level**
  - Minimize side-chan
    of data
- **Circuit, Layout, packa**
  - Randomizing layout
  - Scrambling bus lines
  - Sensors to detect environment variations or package removal

- **One shoe does not fit all!**
- **Security solutions strongly tied to the SOC architecture, resource constraints, attack model, ….and the bottomline**

Case Study: MOSES (Security Architecture of NEC's MP211 mobile phone SoC)

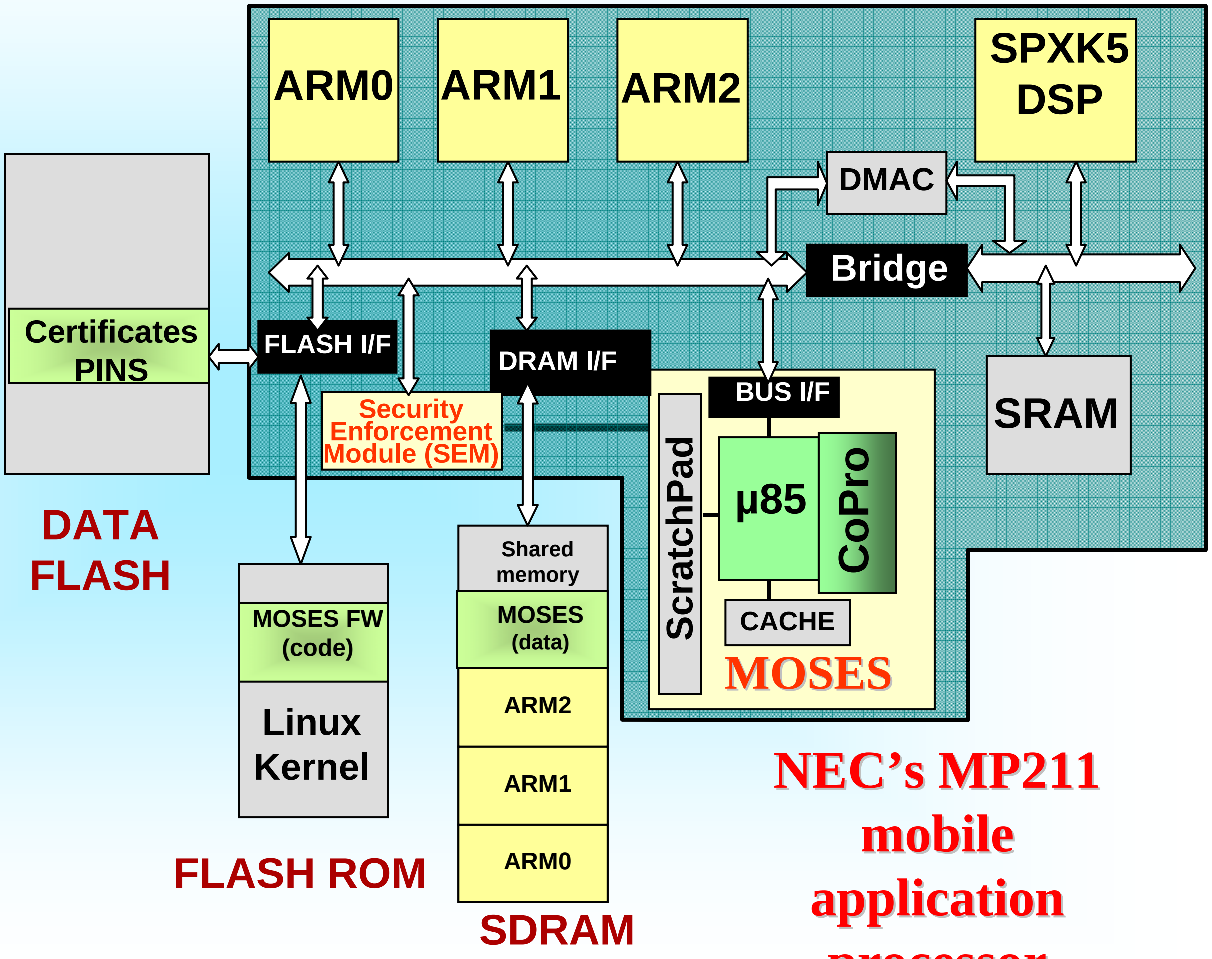
Joint work with:
A. Raghunathan, M. Sankaradass, S. T. Chakradhar
NEC Labs America
H. Nakajima, T. Hasegawa, S. Ueno
NEC Electronics Corp.

Objectives/Requirements

- **Mobile phone will be used to run applications such as secure browsing, VPN, DRM players, etc.**
  - Must support SSL, IPSec, OMA DRM 2.0
  - Must meet performance and power targets
  - Solution must be flexible
    - Security protocols/cryptographic algorithms may change
  - Provide protection to any sensitive data or cryptographic keys against common attacks

MOSES : MObile SEcurity processing System

- First fully programmable mobile security engine
  - Custom instruction set extensions provide > 10X security processing speedup
  - Novel SW architecture for true protocol-level acceleration and multiprocessor systems
  - Secure boot and run-time memory protection prevents software (virus) and physical (code modification) attacks

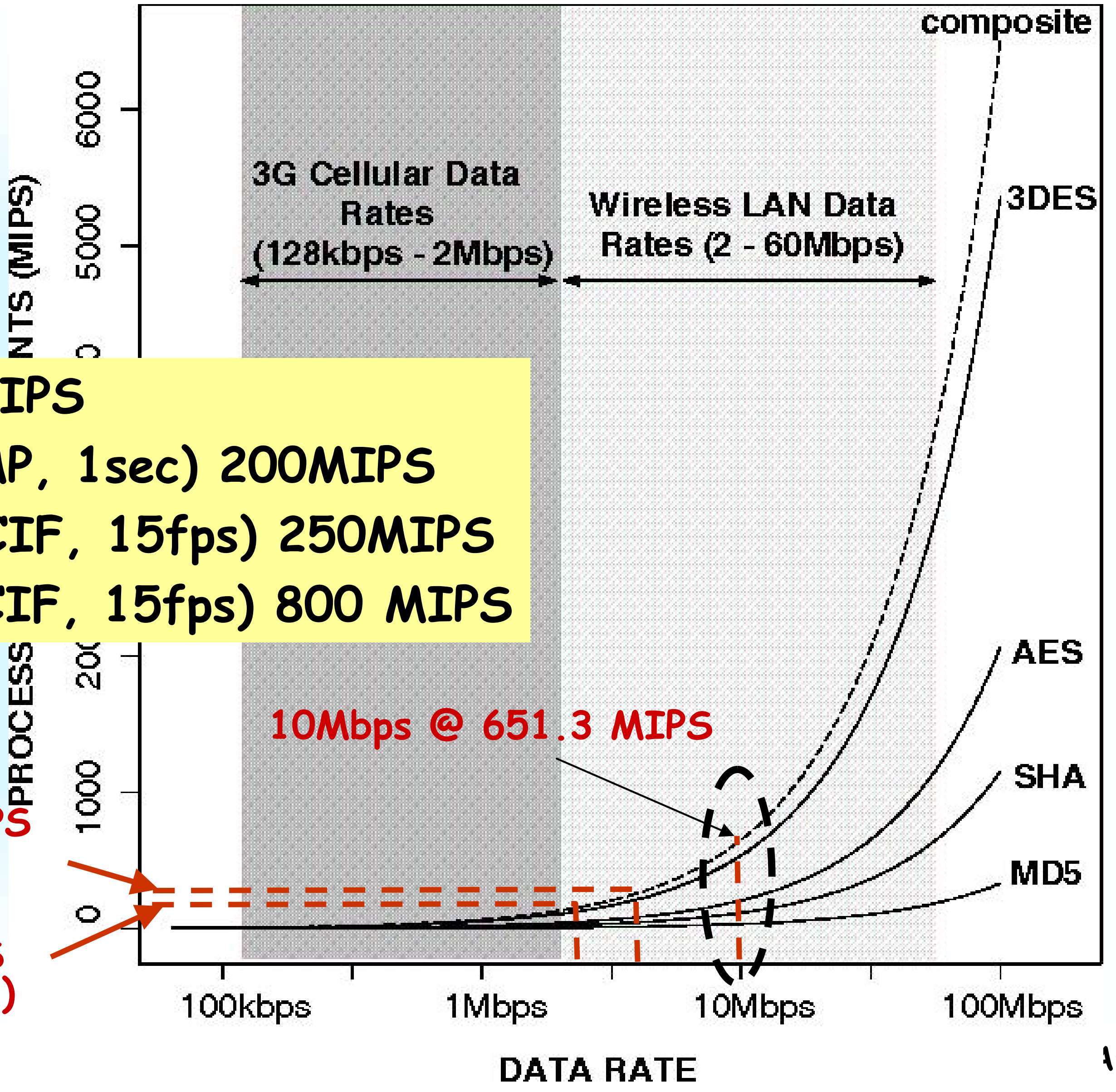


NEC's MP211 mobile application processor

Thank you.

Computation Requirements for Cryptography : Symmetric Encryption & Hashing

MIPS requirements for symmetric encryption and hash algorithms



10Mbps @ 651.3 MIPS

MP3 dec 50MIPS

JPEG enc (2MP, 1sec) 200MIPS

MPEG4 dec (CIF, 15fps) 250MIPS

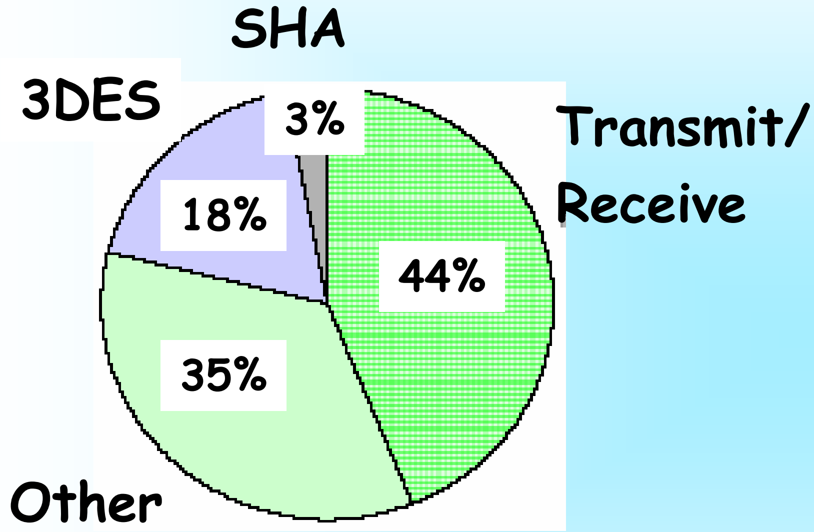
MPEG4 enc (CIF, 15fps) 800 MIPS

3.8 Mbps@ 250MIPS (~XScale 400MHz)

2.3 Mbps@150MIPS (~SA-1100 206MHz)

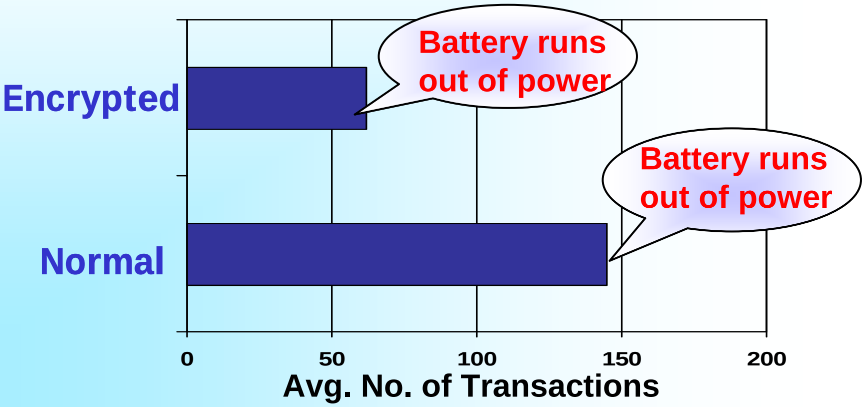
Battery Requirements for Security

- Additional computation & communication drains energy



IPSec on a Symbol PPT2800 Pocket PC

Source: Mishra et. al., ICC 2002



Secure data collection on a wireless sensor node

Mobile Node

- Motorola DragonBall MC68328
- Sensoria WINS NG RF Subsystem (10 Kbps, 10mW power)
- Sensoria WINS NG Battery Pack (7.2 V supplying 26 kJ)

Source: NAI Labs

REFERENCES

Survey Papers:
****

- S. Ravi, A. Raghunathan, S. Hattangady, and J.-J Quisquater, "Emerging Challenges in Designing Secure Mobile Appliances" in *Ambient Intelligence: Impact on Embedded System Design* , Kluwer Academic Publishers, November 2003
- S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady, "Security in Embedded Systems: Design Challenges" in *ACM Transactions on Embedded Computing Systems: Special Issue on Embedded Systems and Security* , 2004
- S. Ravi, A. Raghunathan and S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," *IEEE* Intl. Conf. on VLSI Design, Jan. 2004.
- P. Kocher, R. Lee, G. McGraw, A. Raghunathan and S. Ravi, "Security as a New Dimension in Embedded System Design," ACM/IEEE Design Automation Conference (DAC), June 2004.

Books:
******

- W. Stallings, Cryptography and Network Security: Principles and Practice. Prentice Hall, 1998.
- B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley, 1996.
- G. Hoglund and G. McGraw, Exploiting Software: How to Break Code, Addison-Wesley, 2004.
- W. Rankl and W. Effing, Smart Card Handbook. John Wiley and Sons.
- R. Anderson, Security Engineering - a Guide to Building Dependable Distributed Systems, John Wiley, 2001