



eMemory

eMemory Security Solutions for IoT Applications

eMemory

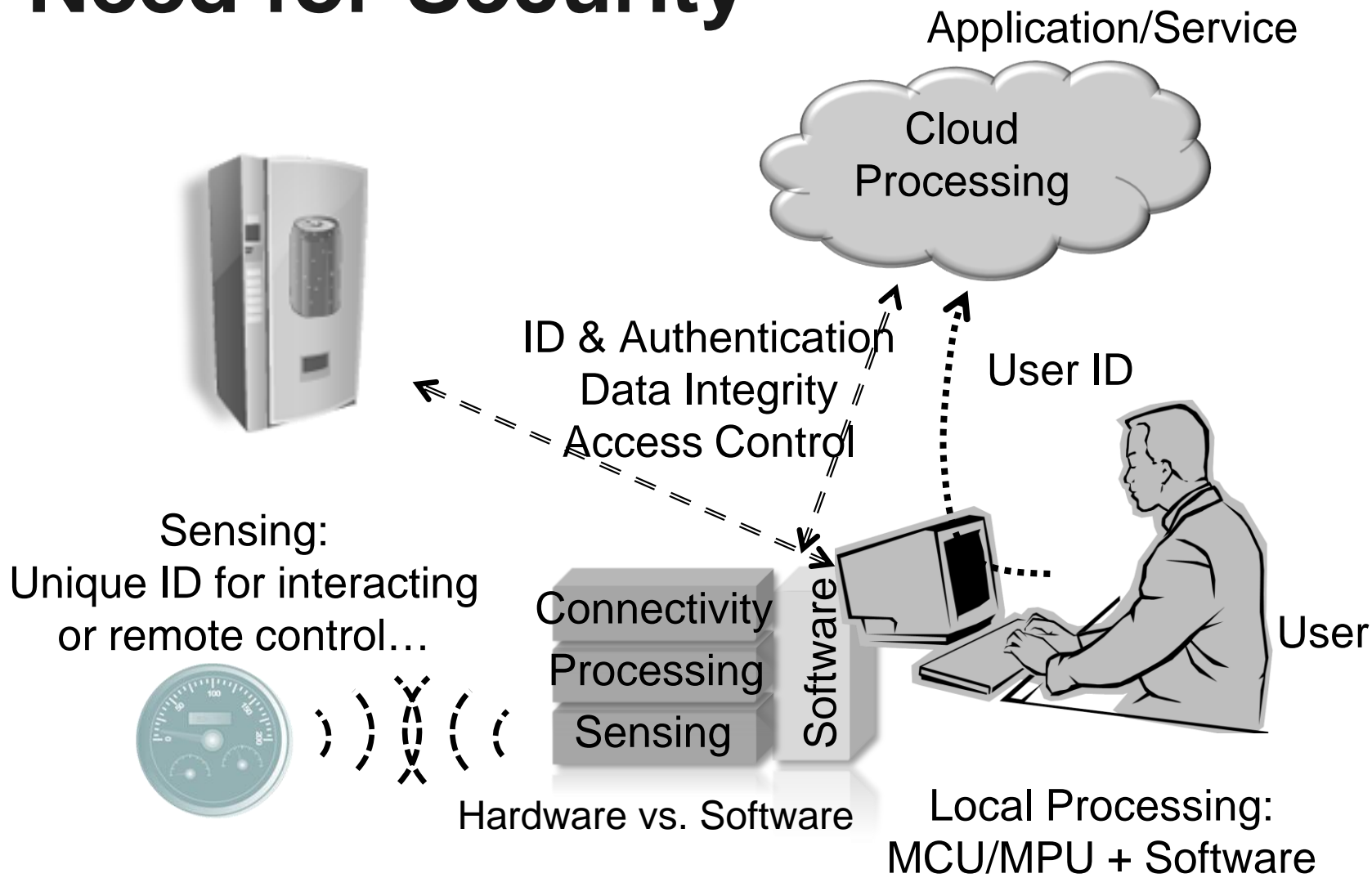
Apr 28, 2015

IPR Notice

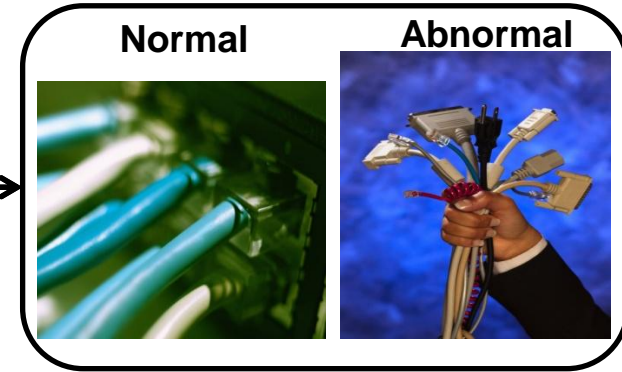
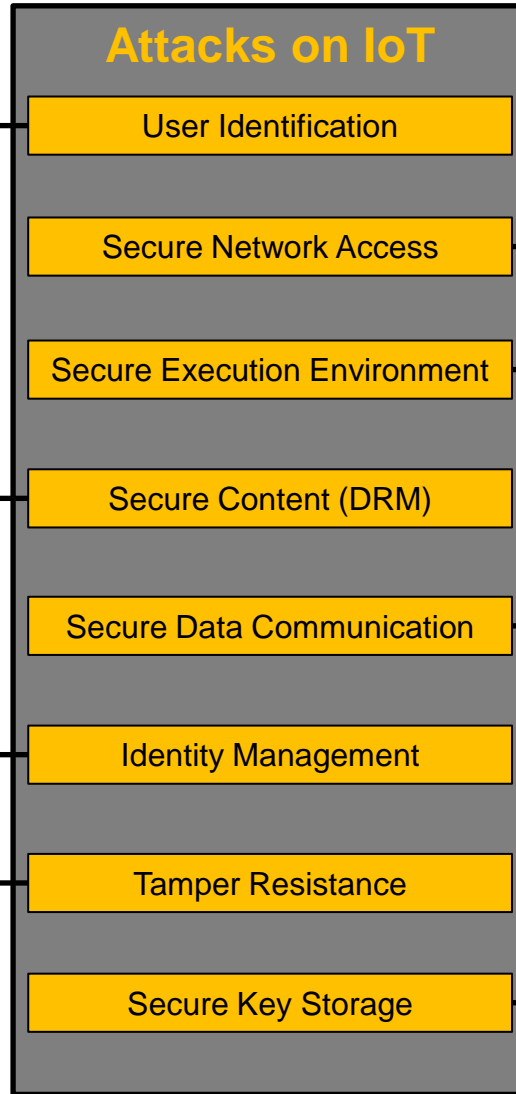
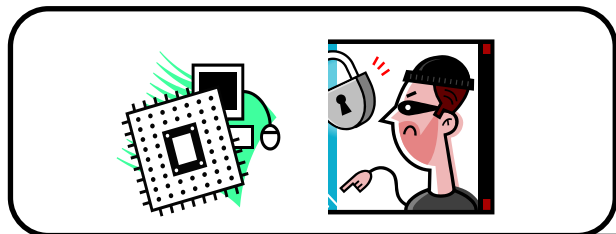
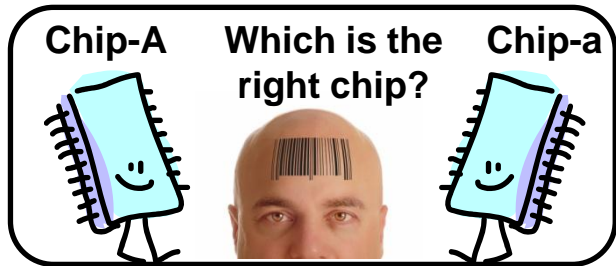
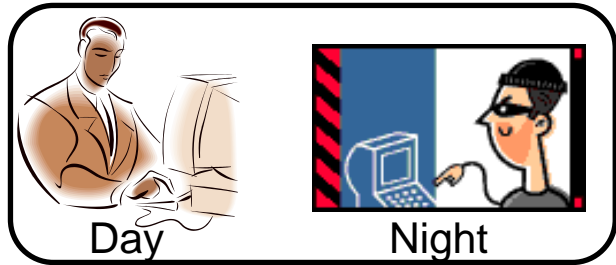
All rights contained in this information, the text, images or other files herein, including but not limited its ownership and intellectual property rights, are reserved by eMemory. This information contains privileged and confidential information and shall not be disclosed, copied, distributed, reproduced or used in whole or in part without prior written permission of eMemory Technology Inc..

eMemory, NeoBit, NeoFuse, NeoFlash, NeoEE and NeoMTP are all trademarks and/or service marks of eMemory in Taiwan and/or in other countries.

Need for Security



Attacks on IoT



Low Cost Hardware-Key for Mass IoT Market

Whole System Security

Enhance

Most complex algorithm + longest password

General chip with common interface & circuit

How to add security level with lowest hardware cost?

Use “Invisible Hardware Key” inside to activate IC when power on

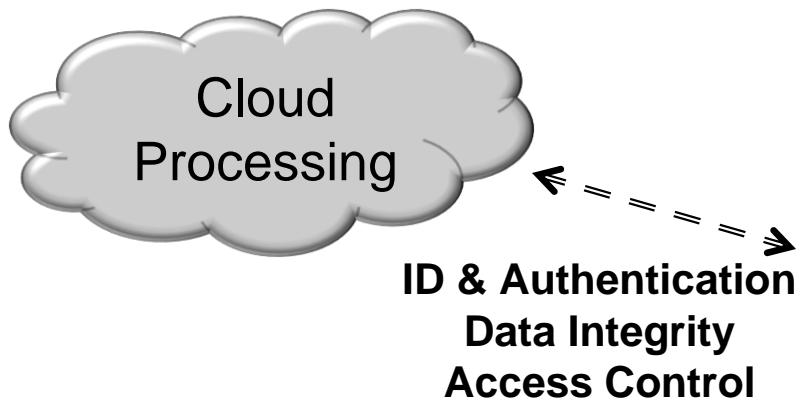
Prevent non-authorized or counterfeit chip to enhance security level of whole system

Demand of Security Key

- **Security for System & Internet Link**
 - › Authentication and secure communication
- **Security for Hardware & Software Link**
 - › Hardware/Software authentication and protection from cloning
- **Security for IC Authorization**
 - › Secret security key to protect hardware from cloning

Security with eMemory IPs

Security for System Service



Hardware-Software/Firmware Lock



Hardware Protection Invisible Key for Anti-Cloning

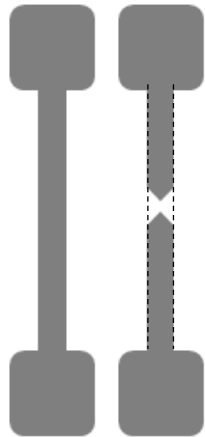


Security IP/Code by
Authorized Use

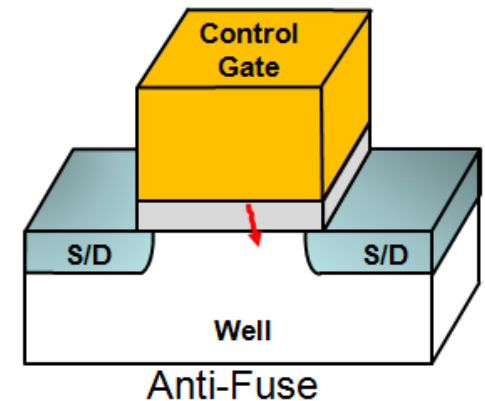
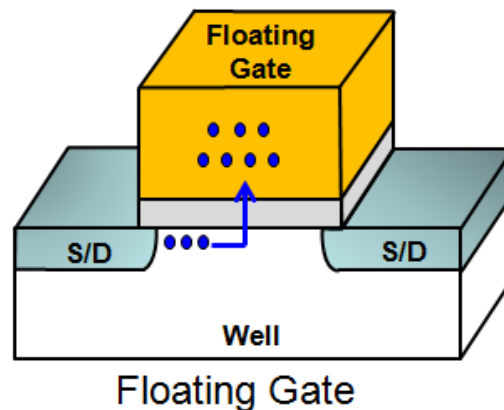
Invisibility for Security

- Provide “Invisible Hardware Key” for invisible storage.
- Prevent reverse-engineering to detect content of security key.
- Protect firmware and hardware of ICs from pirating.
- Extend & protect customer’s business.

eFuse Key: Data is easily observed



Invisible Hardware Key : Data is hard to be detected



Advantages of eMemory Technology

- **Invisible Storage**

- › Using best NVM technology for “Invisible Hardware Key”

- **Small IP area**

- › Easily placed in unused space of SoC design

- **Widespread availability**

- › OTP IP has been deployed in 18 foundries & 250+ process

- **Widest utilization**

- › Over 9 million wafers with eMemory IP inside.

- **Customized design**

- › Best customized design service for special “key” demand.

- › Over 850+ OTP IP adopted for customer’s special demand.

Summary

- **To take the lead in the IoT market, the data security of IC hardware and firmware is crucial.**
- **eMemory's Logic NVM IPs use floating-gate and anti-fuse structures to prevent reverse-engineering; effectively protect data from detection and interpolation**
- **eMemory's customized OTP IPs for security key storage can satisfy security demand of IoT products; the system security level will be greatly enhanced at minimum cost.**
- **eMemory is the best security key provider based on its industry-leading availability in worldwide foundries**

The background of the slide is filled with a pattern of white wireframe cubes. Some cubes are arranged in a diagonal line from the top-left towards the bottom-right, while others are scattered randomly across the white background.

eMemory

Embedded Wisely, Embedded Widely