TeleTrusT
Pioneers in IT security.

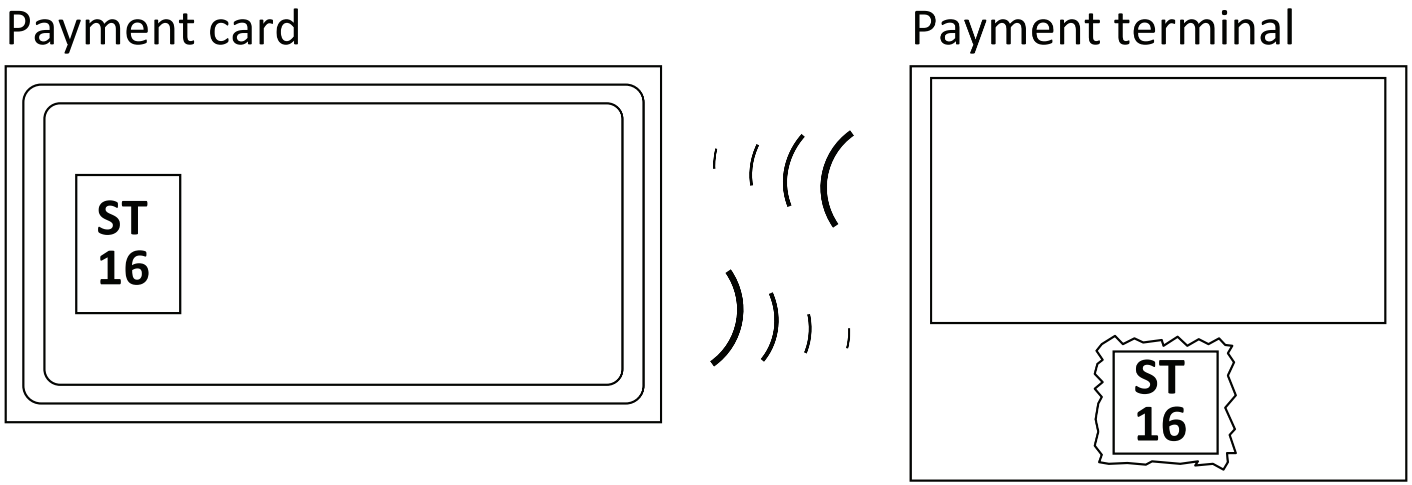
TeleTrusT-Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 31.05.2011

Dr. Karsten Nohl
Security Research Labs
Die Hackerperspektive auf Meterintelligenz

Technology risks vary widely with use case

Example: Nationwide micro-payment scheme

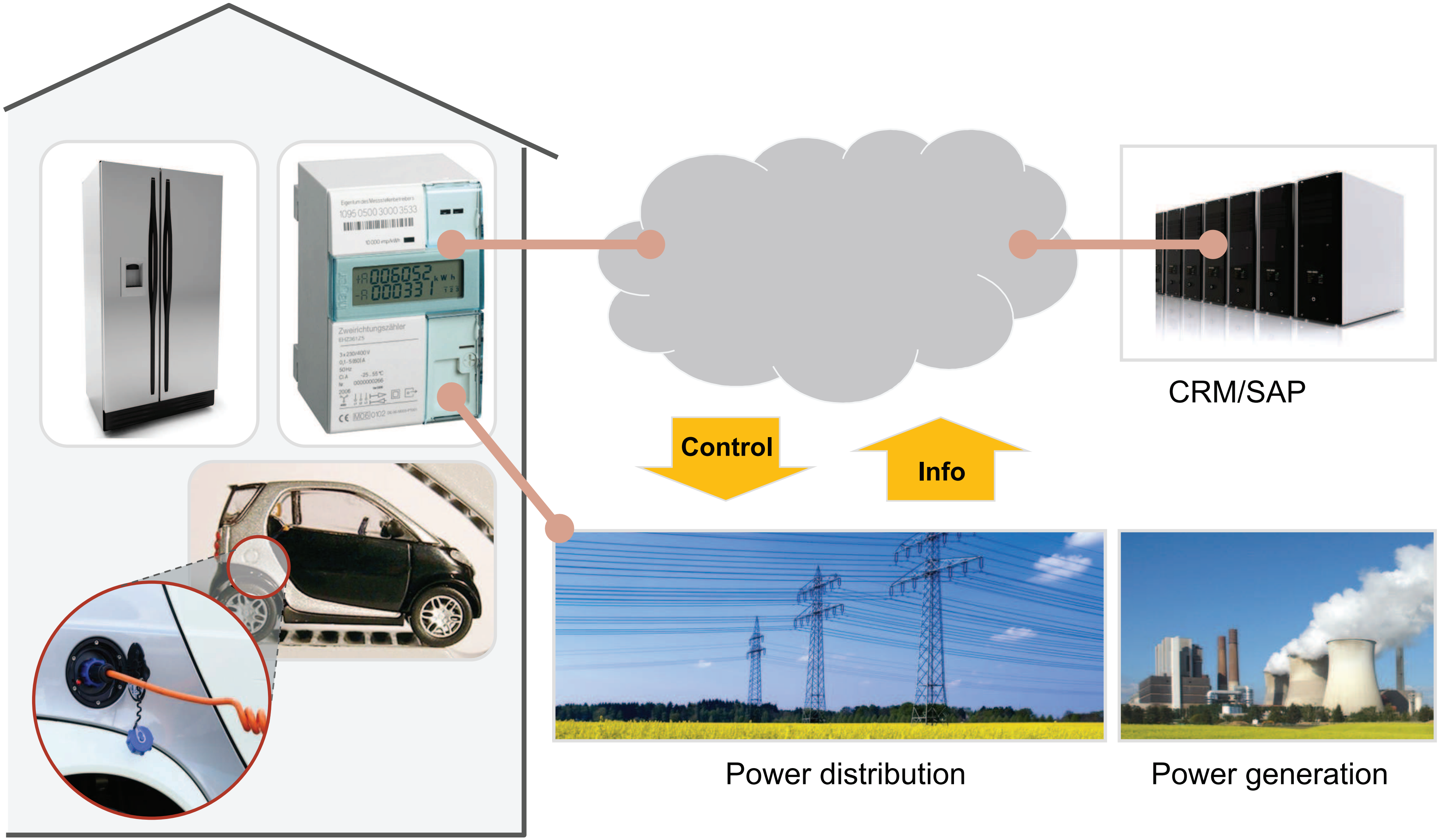


Extracting secret keys allows cloning **one card**

Extracting secret keys allows cloning **all cards**

Same protection, different security level

The intelligent power grid interconnects critical infrastructure, customer data and electronics



CRM/SAP

Control

Info

Power distribution

Power generation

Smart meters can be abused for smart grid attacks or in committing fraud

Scenario	Finding	Attack effort
1 **Switch-off meters with virus**	Switch-off is not currently implemented in German meters	N/A
2 **Attack backend or smart home**	**Possible** through emulating meter or changing firmware	2 weeks, simple tools
3 **Alter measurements**	**Possible** through emulating meter, changing firmware, or altering internal traffic	1 week, simple tools

Two weeks of analysis create various attacks

	Prepare analysis	Document functionality	Extract software	Reengineer metering logic	Create exploit
Analysis step	▪ Create safe test setup ▪ Document + circumvent intrusion detection ▪ Find datasheets	▪ Create Circuit diagram ▪ Sniff data from internal interfaces	▪ Find debug interface ▪ Read out firmware	▪ Create emulator for firmware ▪ Disassemble code	▪ Weaponize knowlege
Abuse potential	▪ Operate meter outside of its intended environment	▪ Decode or inject data on unencrypted interfaces; change measurements	▪ Find software bugs (potential goal: smart meter virus) ▪ Decrypt encrypted traffic	▪ Spoof arbitrary traffic to back-end and home automation	▪ Crash smart grid and smart home components ▪ Distribute viruses

Analysis process takes less than two weeks for current meters

Mitigations: best-practice protection measures should meters

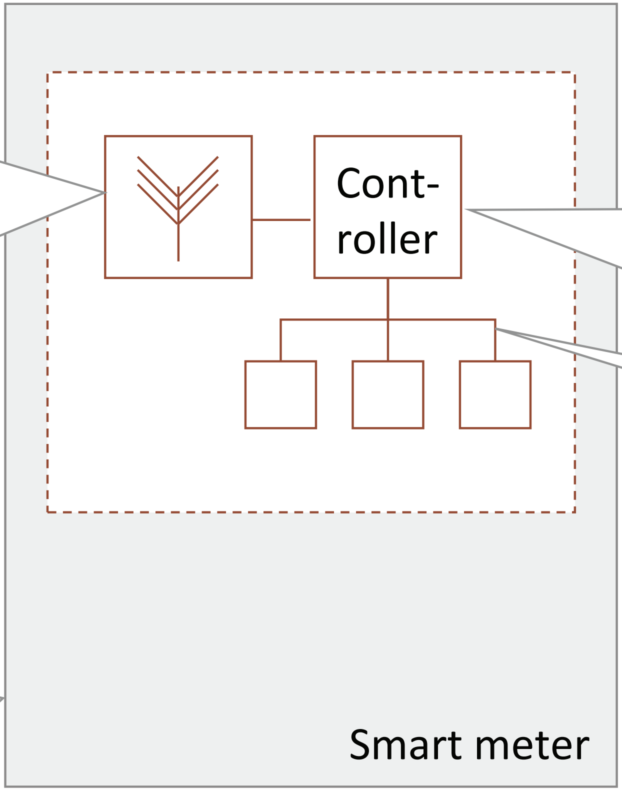
Protection measures already found in modern **cell phones, set-top boxes, and femto cells**

Protect external data

- Encrypt communication
- Sign data with unique secret key
- Prohibit meter-to-meter communication

Intrusion detection

- Enforce reporting
- Add light sensors



Protect firmware

- Deactivate JTAG
- Use secure chip
- Encrypt firmware images

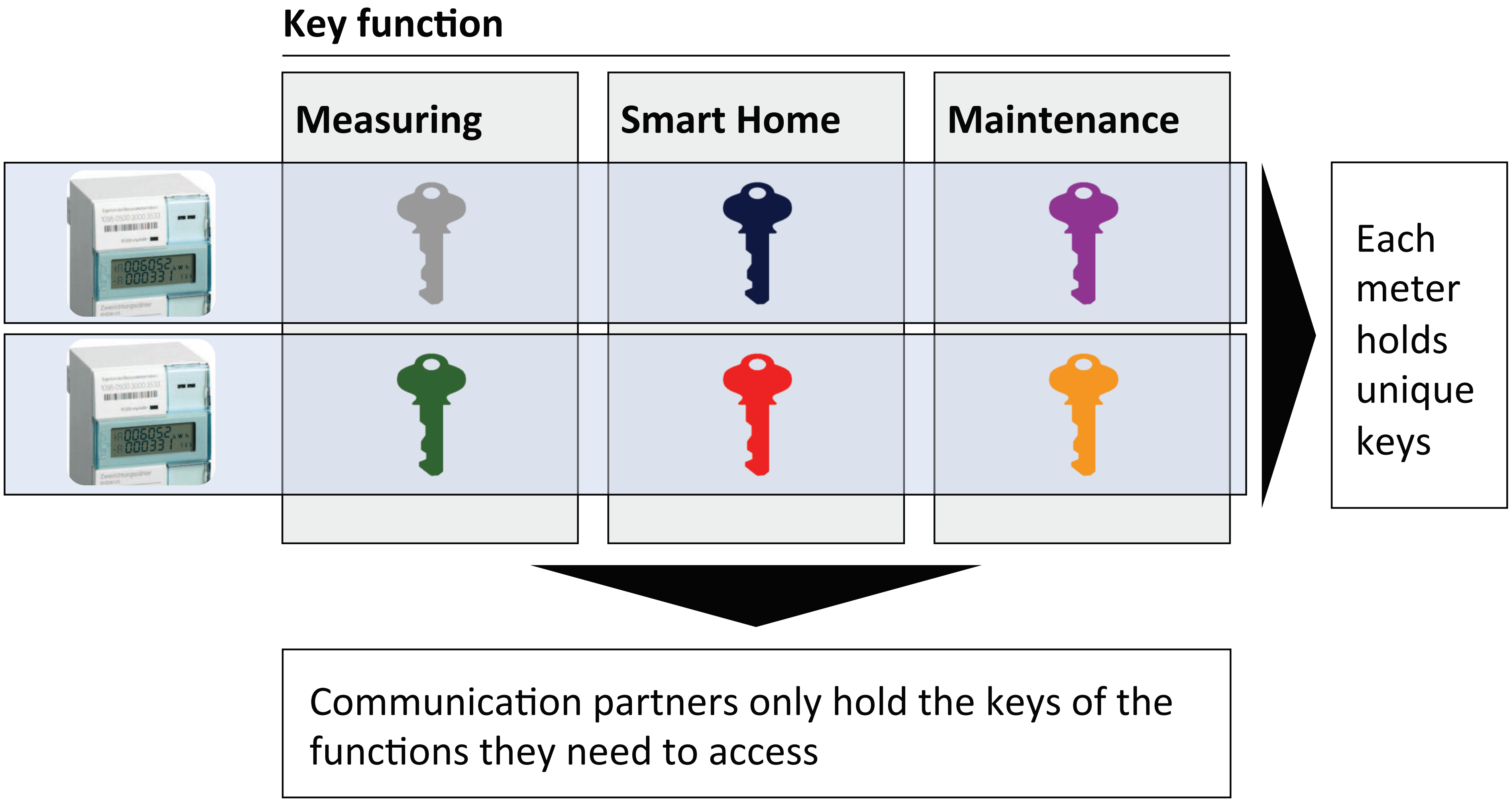
Protect internal data

- Encrypt protocols
- Sign data

The smart grid threat model should be extended to cover all realistic hackers

	Threat level 1: Script kiddy	**Threat level 2: Chip hacker**	**Threat level 3: Well-funded agency**
Abilities and motivation	Able to use standard hacker tools; interested in individual fraud or vandalism	Able to find new vulnerabilities in software and hardware; interested in organized fraud or exposure of vulnerabilities	Capable of funding research; determined to hurt companies or nations
Attacks currently possible	Emulate being a meter: a) Save money b) Decode, understand, emulate application-layer control data (ie, DoS neighbors) c) Find software bugs (ie, spread local worm)	• Emulate smart devices to save cost or confuse network • Adopt and spread publicized worms	• Exploit smart grid distribution layer through smart meters • Gain access to billing or power plant systems • Develop and spread global worm
Attack cost	< $5,000	< $50,000	< $100,000
Best practice target	$50,000	$200,000	$500,000

Key distribution should follow ‘need-to-know’ philosophy to limit attack surface



Key function

Measuring

Smart Home

Maintenance

Each meter holds unique keys

Communication partners only hold the keys of the functions they need to access

Questions?

SECURITY
RESEARCH
LABS

Karsten Nohl
nohl@srlabs.de