softScheck
we identify vulnerabilities others don't

Internet of (dangerous) Things (IodT)

Thomas Bötner, Prof. Dr. Hartmut Pohl

softScheck GmbH Köln
Büro: Bonnerstr. 108. 53757 Sankt Augustin www. softScheck.com

softScheck
we identify vulnerabilities others don't

Our Services

Application Security

Penetration Testing

Compliance

Research

Threat Modeling

Secure Development

Training

Forensics

© softScheck

softScheck
we identify vulnerabilities others don't

Industries

Automation

Retail

Financial Services

Energy & Water

Automotive

Defense

Entertainment & Gaming

Health

Security

Telecom

Software

Logistics

© softScheck

Cyberspionage

FBI deckt Hackerangriffe auf amerikanisches Wahlsystem auf

Die Wahlsysteme zweier amerikanischer Bundesstaaten waren dem FBI zufolge Ziel von ausgeklügelten Cyber-Attacken. Spuren führen offenbar nach Russland. Die Sorge vor einer Manipulation der Präsidentenwahlen wächst.

30.08.2016

Teilen Twittern Teilen E-mailen

Aktuelle Umfragen

Wahl in Amerika

Wer liegt in den Umfragen vorn?

Quelle: RCP, Stand: 17.08.2016

Demokraten
Hillary Clinton

Republikaner
Donald Trump

145%

Stuxnet: Natanz Uranium Enrichment Facility

Iranian President Mahmoud Ahmadinejad visits the Natanz uranium enrichment facilities, where a “closed” computer network was infected by malware introduced via a small flash drive

Stuxnet-like 'Havex' Malware Strikes European SCADA Systems

Thursday, June 26, 2014 Swati Khandelwal

g+1 124 Share 576 Tweet 304 Reddit 1 Share 44 ShareThis 1124

Supervisory Control and Data Acquisition (SCADA) – Industrial Control Systems (ICS)

YES, WE SCAN!

softScheck
we identify vulnerabilities others don't

Schnüffelcode in Juniper Netzgeräten: Weitere Erkenntnisse und Spekulationen

21.12.2015 15:10 Uhr – Monika Ermert vorlesen

Die Analysen der ScreenOS-Updates fördern vogelwilde Dinge zu Tage. So gab es zwei unabhängige Hintertüren. Die SSH-Backdoor kann dank des veröffentlichten Passworts jeder ausnutzen; die komplexere VPN-Lücke beruht

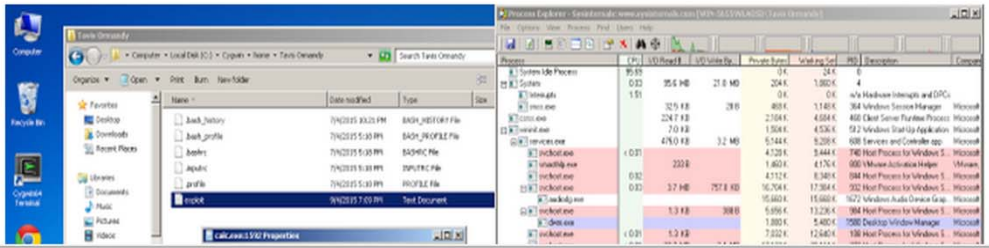
RISK ASSESSMENT / SECURITY & HACKTIVISM

Security wares like Kaspersky AV can make you *more* vulnerable to attacks

Products often open computers to hacks they otherwise wouldn't be vulnerable to.

by **Dan Goodin** - Sep 23, 2015 8:46pm CEST

Share Tweet 103



Alert!

NSA-Exploits: Cisco schließt weitere Einfallstore in Firewalls

22.08.2016 10:23 Uhr – Dennis Schirrmacher vorlesen

Kritische Sicherheitslücken gefährden Systeme, in denen Firewalls von Cisco zum Einsatz kommen. Abgesicherte Versionen sollen Abhilfe schaffen.

© softScheck

Hackerangriffe durch OK

Technische Anlagen "gehackt"

Die meisten der Hacker-Angriffe gehen von organisierten Kriminellen aus

Sabotage übers Netz
Erpresser und Spione hacken Industrieanlagen

Industrieanlagen sind immer häufiger Angriffen von Hackern ausgesetzt, sagt Claudia Eckert, Leiterin des Fraunhofer-Instituts für angewandte und integrierte Sicherheit.

Online-Angebot des Heise-Verlags zu IT-Sicherheitsthemen, hatte sich daraufhin sofort an das BSI gewandt.

Eine App für das iPad reicht für die Steuerung aus

Sicherheitssysteme von Industrieanlagen wie auch kleine Heizanlagen für Einfamilienhäuser ließen sich vielfach über das Internet mit einer iPad-App

In Deutschland gibt es 500 gefährdete Anlagen

Die Internetanbindung von technischen Anlagen macht sie so angreifbar (Beitrag vom 3. Mai 2013)

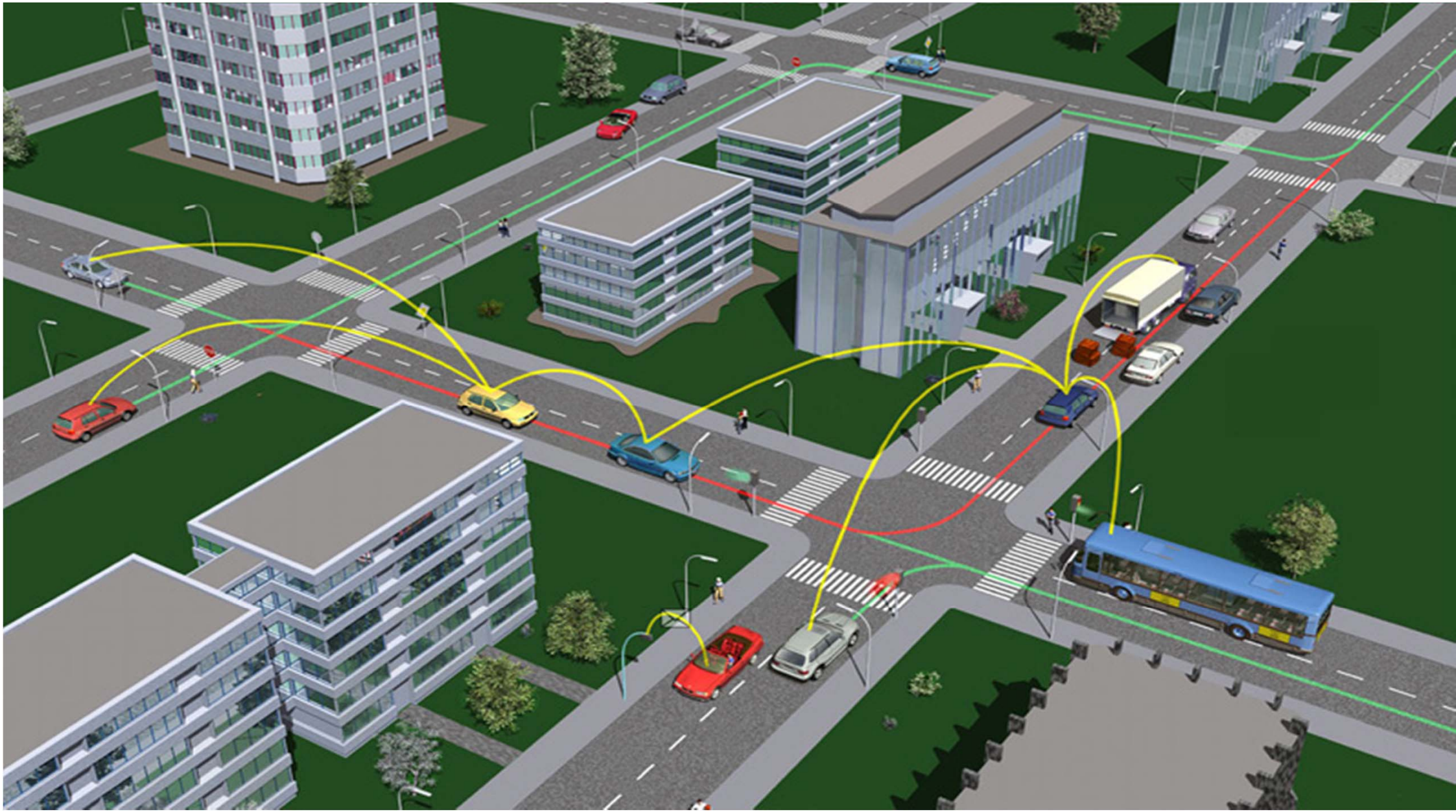
Experten der angesehenen Computerzeitschrift "c't" haben Sicherheitslücken in Steuersystemen von Fabriken, Gefängnissen und Heizkraftwerken entdeckt. Die Anlagen sind durch die Anbindung an das Internet zu verwundbar geworden. Mit wenigen Mausklicks sei es den Hackern gelungen, die Kontrolle einiger solcher Anlagen zu übernehmen, berichtet die Zeitschrift. Plötzlich hätten sie am "virtuellen Schaltpult eines realen Heizkraftwerks" gestanden.

https://www.3sat.de/page/?source=/nano/technik/169524/index.html

© softScheck

softScheck
we identify vulnerabilities others don't

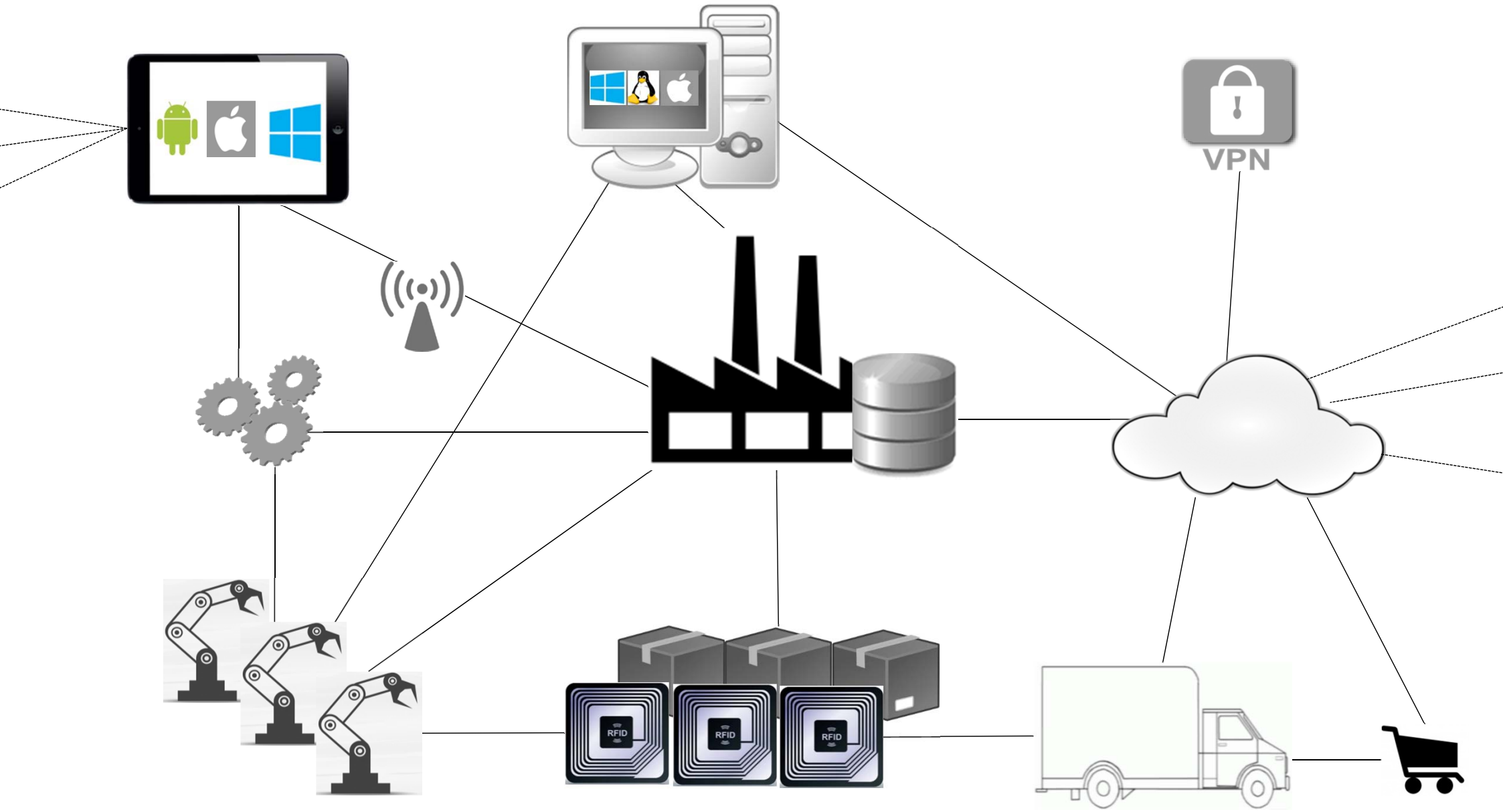
Connected Cars



© softScheck

softScheck
we identify vulnerabilities others don't

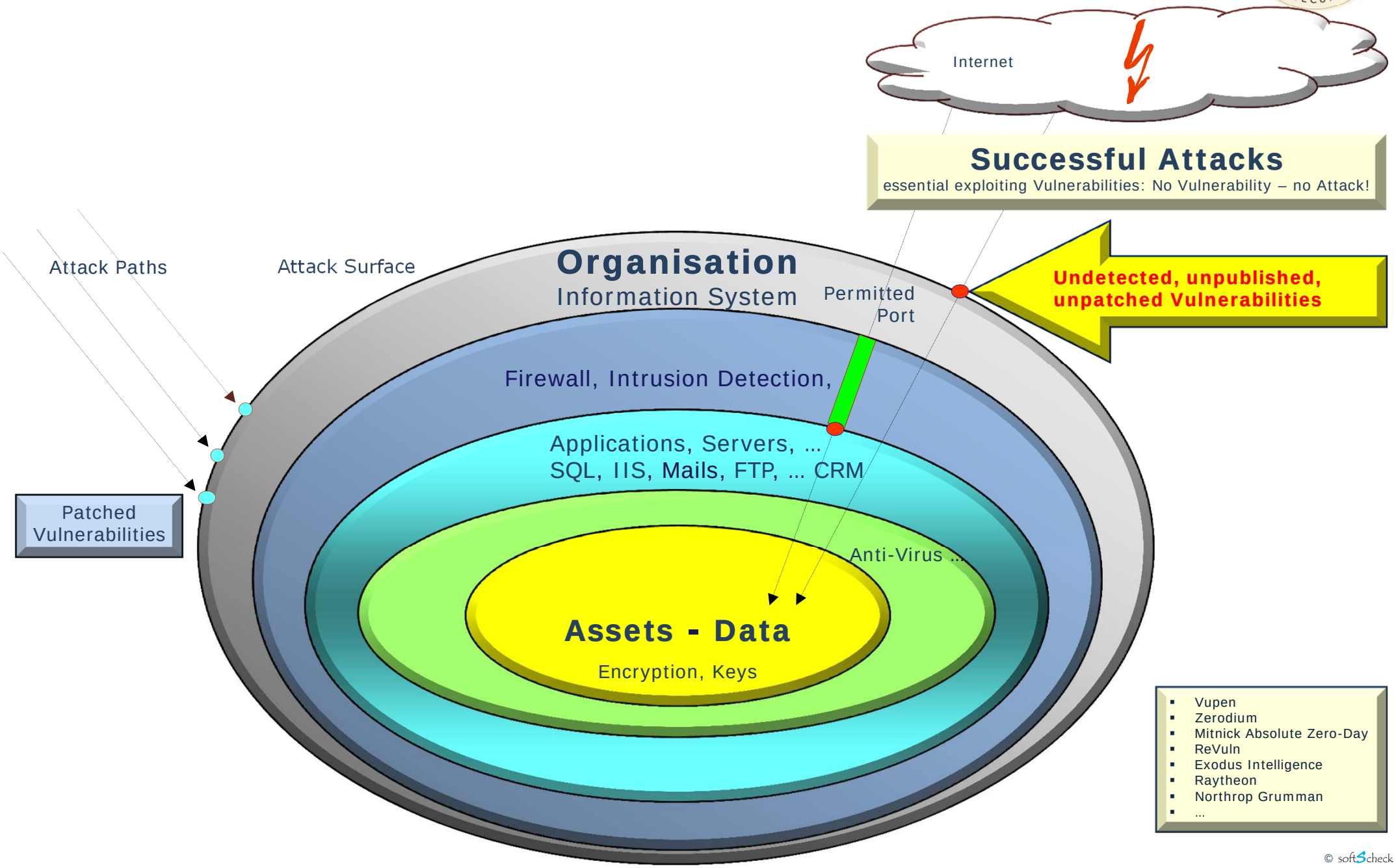
Internet of Things



© softScheck

softScheck
we identify vulnerabilities others don't

No Attack without Vulnerability



- Vupen
- Zerodium
- Mitnick Absolute Zero-Day
- ReVuln
- Exodus Intelligence
- Raytheon
- Northrop Grumman
- ...

© softScheck

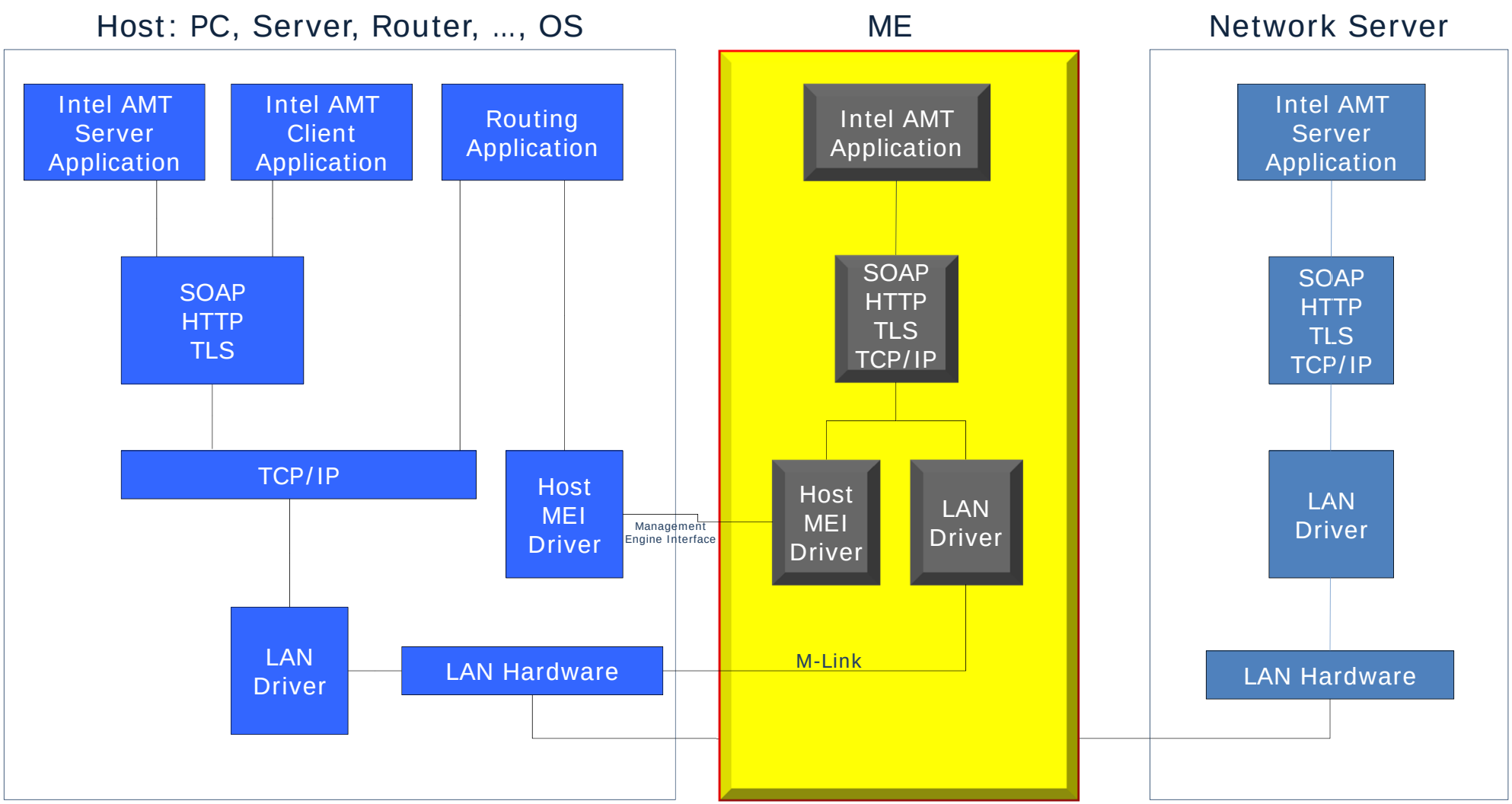
CGC

CYBER

GRAND_CHALLENGE

DARPA

Intel Management Engine: Backdoor



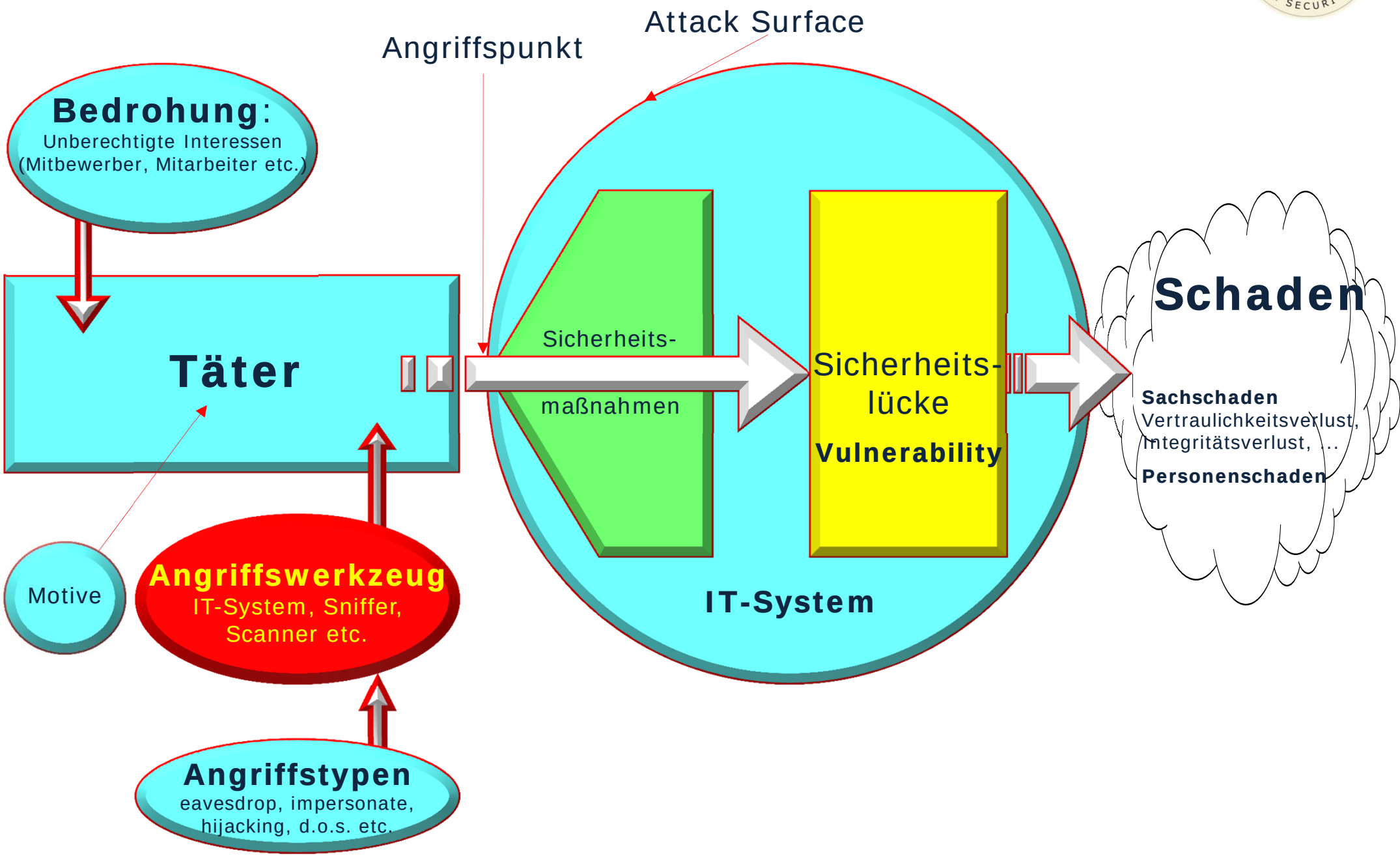
- Intel Management Engine (IME, ME) 32-bit ARC RISC Prozessor - kann auf die gesamte Hardware zugreifen inkl. Haupt- und periphere Speicher, Netzwerk - fest-verdrahtete Software (Firmware).
- ME kommuniziert verschlüsselt via Netzwerkchip - am Betriebssystem vorbei mit dem Internet.
- AMT - Active Management Technology. IPMI - Intelligent Platform Management Interface.

Bild auf Intel-Basis

© softScheck

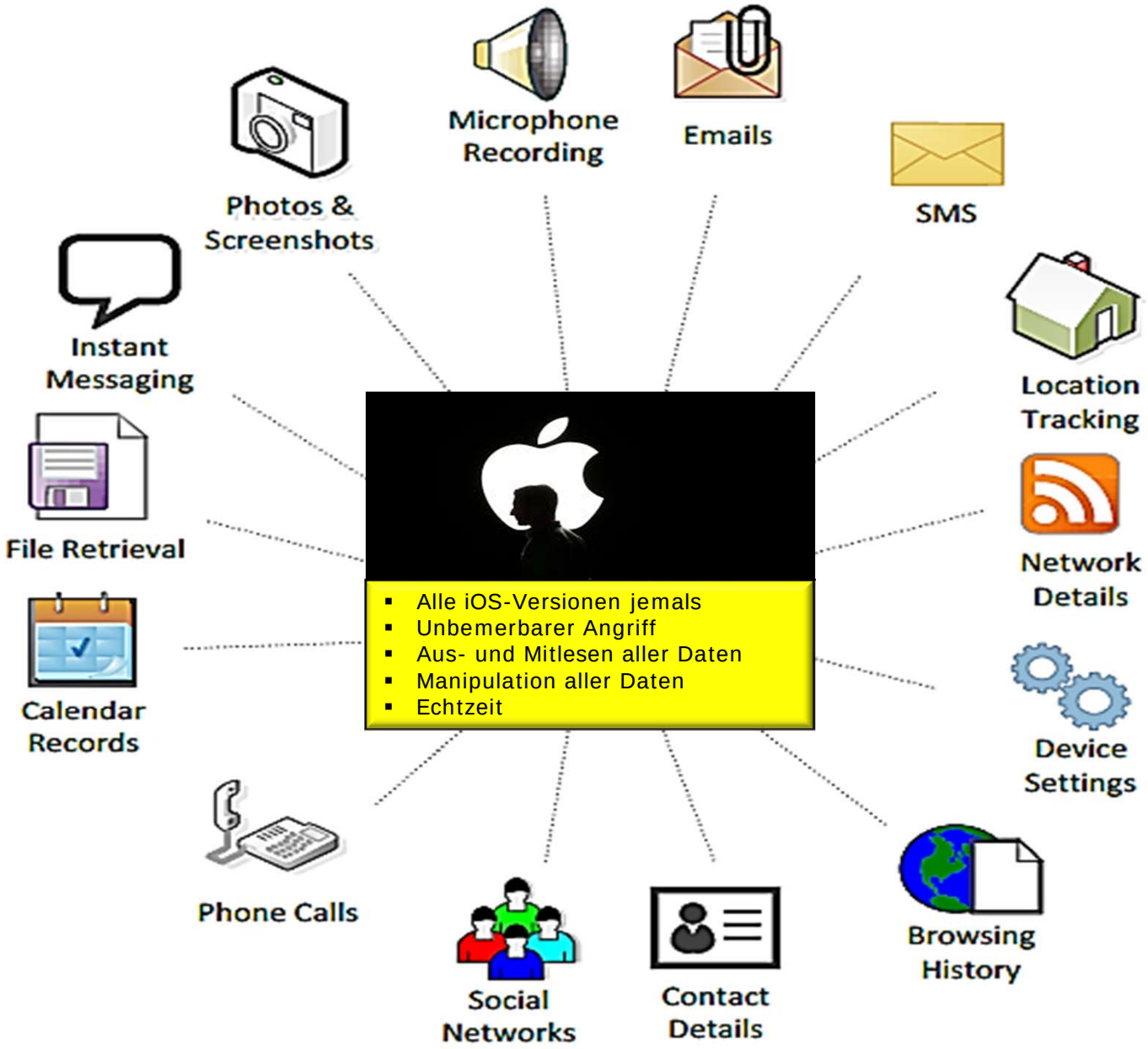
softScheck
we identify vulnerabilities others don't

Generic Attack Model



© softScheck

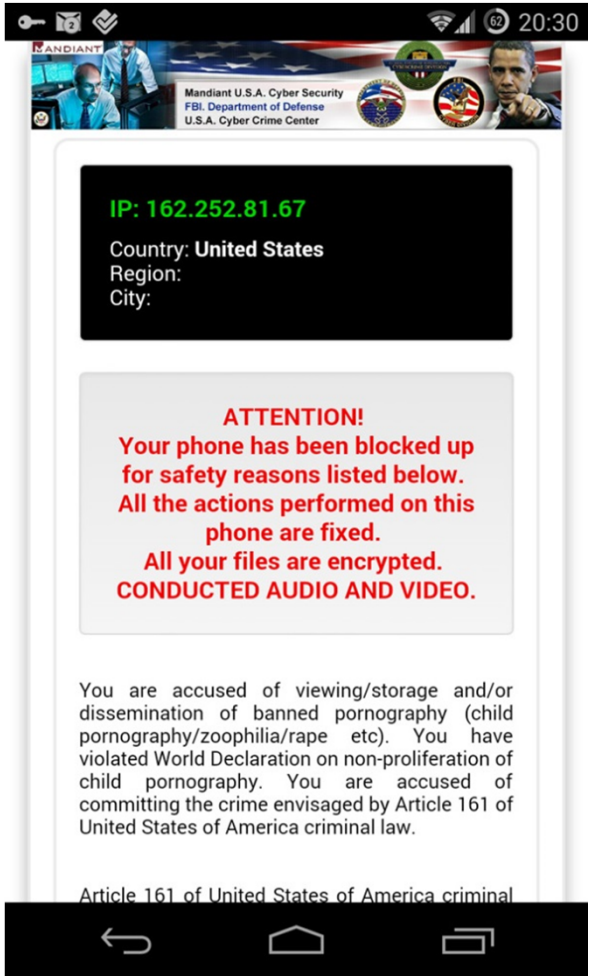
Pegasus Attack on iOS (Apple)



© softScheck

softScheck
we identify vulnerabilities others don't

Ransomware

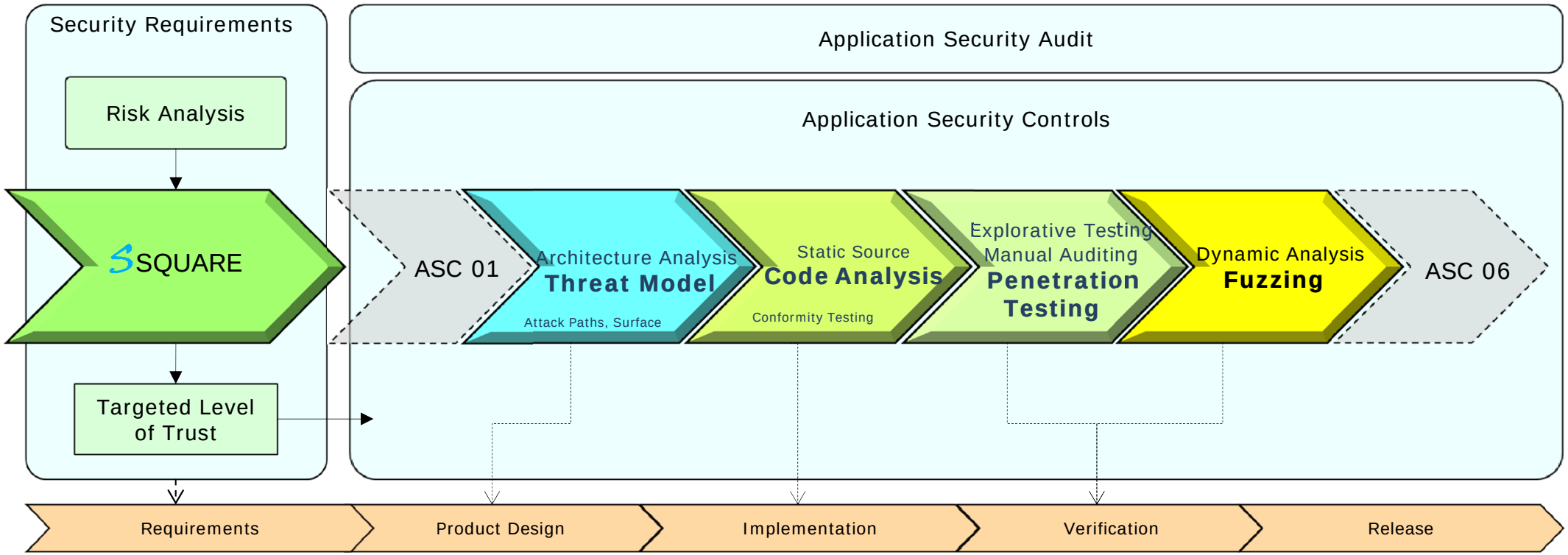


© softScheck

softScheck
we identify vulnerabilities others don't

Application Security Management SASM

ISO 27034 conform Development



© softScheck

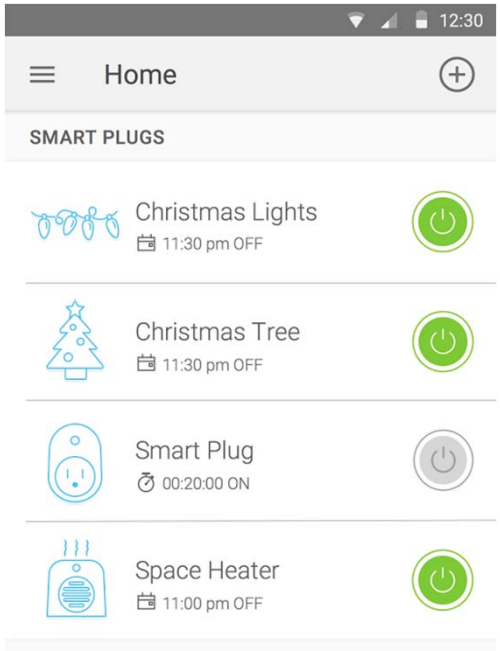
Customer Premises Equipment (CPE)

© softScheck

Internet of (dangerous) Things

Reverse Engineering einer WiFi-Steckdose

- TP-Link HS110 WiFi Smartplug
- Steuerbar mit "Kasa for Mobile" Smartphone-App (iOS, Android)
- TP-Link Cloud-Anbindung



© softScheck

SmartPlug Setup

- SmartPlug startet Access Point (AP) "TP-LINK_Smart Plug_XXXX"

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat
map	00:0A:EB:11:07:02	TP-LINK_Smart Plug_0702		infra	2015-10-19 07:18:13	2016-02-16 21:57:09		37.38174820
map	00:0A:EB:11:07:03	TP-LINK_Smart Plug_0703		infra	2015-10-19 07:18:13	2016-02-16 21:57:09		37.38174820
map	50:C7:BF:00:3A:5A	TP-LINK_Smart Plug_3A5A		infra	2016-04-10 13:48:10	2016-04-10 15:52:42		42.36147690
map	50:C7:BF:00:3E:EF	TP-LINK_Smart Plug_3EEF		infra	2016-05-13 18:52:01	2016-05-13 16:22:10		42.47166443
map	50:C7:BF:00:42:3F	TP-LINK_Smart Plug_423F		infra	2016-03-23 15:38:45	2016-03-26 19:18:18		40.29348755
map	50:C7:BF:00:4C:6B	TP-LINK_Smart Plug_4C6B		infra	2016-04-30 14:55:46	2016-04-30 20:30:08		39.64738083
map	50:C7:BF:02:CE:A6	TP-LINK_Smart Plug_CEA6		infra	1970-01-02 00:50:34	2016-06-09 15:43:02		39.76014328
map	50:C7:BF:00:D7:89	TP-LINK_Smart Plug_D789		infra	2016-03-31 12:52:06	2016-03-31 13:27:18		37.76496124
map	50:C7:BF:00:DD:2A	TP-LINK_Smart Plug_DD2A		infra	2016-04-30 15:09:23	2016-04-30 20:30:08		39.64726639
map	50:C7:BF:00:E8:60	TP-LINK_Smart Plug_E860		infra	2016-03-31 12:49:07	2016-05-05 19:18:08		37.76498413

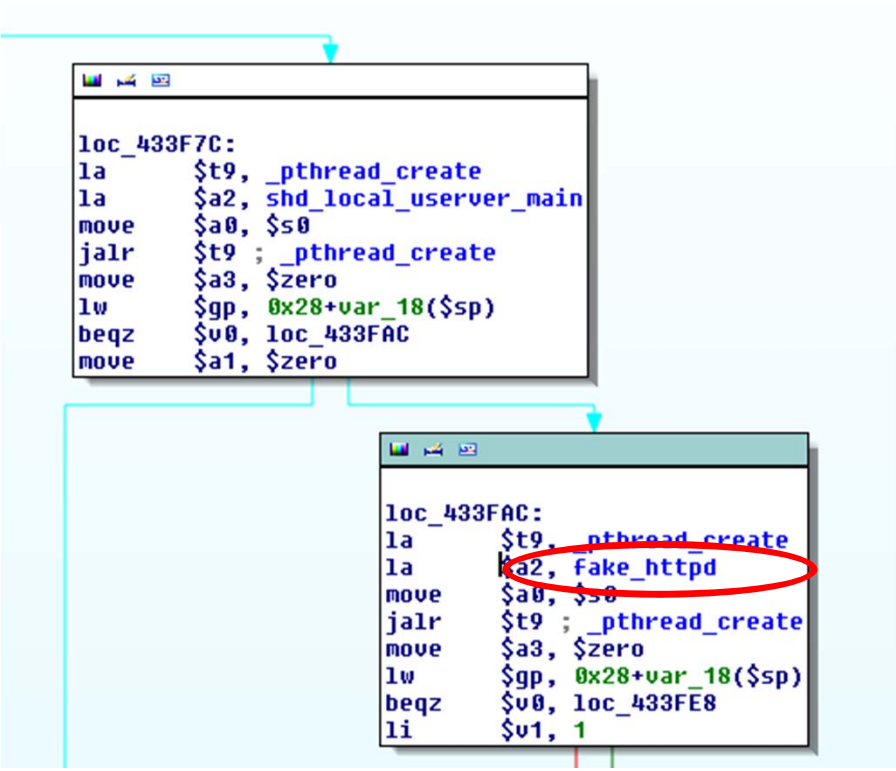
- Kasa App verbindet Smartphone mit dem AP
- App kommuniziert lokal verschlüsselt über TCP Port 9999
- Passwort des Heim-WLANs wird von App an SmartPlug geschickt
- SmartPlug schaltet AP aus und verbindet sich mit Heim-WLAN

© softScheck

Offene Ports

Port	Protocol
80/tcp	HTTP
9999/tcp	TP-Link Smart Home Protocol
1040/udp	TP-Link Device Debug Protocol (TDDP)

- Web-Server ist ein Fake!



© softScheck

Reverse Engineering der Verschlüsselung

CERTIFICATE softScheck SECURITY TESTED

- Jedes Byte XOR mit vorigem Plaintext-Byte
- Erstes Byte XOR -85 (Schlüssel)
- Ver- und Entschlüsselung gleich

```
public static byte[] crypt(byte[] data)
{
    if(data != null && data.length > 0)
    {
        int key = -85;
        for (int i = 0; i < data.length; i++)
        {
            byte b = (byte) (data[i] ^ key);
            key = data[i];
            data[i] = b;
        }
    }
    return data;
}
```

© softScheck

Wireshark Dissector

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.1	192.168.0.100	TP-LINK…	330	9999 → 32855 [PSH, ACK] Seq=1 Ack=1 Win=2896 Len=214 TSval=4294900590 TSecr=1778164

```
▷ Frame 1: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface 0
▷ Radiotap Header v0, Length 26
▷ 802.11 radio information
▷ IEEE 802.11 QoS Data, Flags: ......F.C
▷ Logical-Link Control
▷ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.100
▷ Transmission Control Protocol, Src Port: 9999 (9999), Dst Port: 32855 (32855), Seq: 1, Ack: 1, Len: 214
◢ TP-Link Smart Home, Decrypted TP-Link protocol
    {"cnCloud":{"get_info":{"username":"","server":"devs.tplinkcloud.com","binded":0,"cld_connection":0,"illegalType":-1,"stopConnect":-1,"tcspStatus"
◢ JavaScript Object Notation
  ◢ Object
    ◢ Member Key: "cnCloud"
      ◢ Object
        ◢ Member Key: "get_info"
          ◢ Object
            ▷ Member Key: "username"
            ▷ Member Key: "server"
            ▷ Member Key: "binded"
            ▷ Member Key: "cld_connection"
            ▷ Member Key: "illegalType"
            ▷ Member Key: "stopConnect"
            ▷ Member Key: "tcspStatus"
            ▷ Member Key: "fwDlPage"
            ▷ Member Key: "tcspInfo"
            ▷ Member Key: "fwNotifyType"
            ▷ Member Key: "err_code"
```

© softScheck

TP-Link SmartHome Protokoll

- JSON-basiert
- Beispiel-Befehle:

`{"system":{"get_sysinfo":{}}}`	Systeminfos
`{"system":{"reboot":{"delay":1}}}`	Neustart
`{"system":{"set_relay_state":{"state":1}}}`	Steckdose anschalten
`{"netif":{"get_scaninfo":{"refresh":1}}}`	Nach WLANs scannen
`{"netif":{"set_stainfo":{"ssid":"WiFi","password":"secret", "key_type":3}}}`	Mit WLAN verbinden
`{"cnCloud":{"bind":{"username":"your@email.com","password":"secret"}}}`	In Cloud registrieren
`{"cnCloud":{"unbind":null}}`	Registrierung aufheben

© softScheck

TP-Link SmartHome Protokoll

- time
- emeter (energy meter)
- schedule (scheduled on/off)
- count_down (countdown on/off)
- anti_theft (random scheduled on/off)

© softScheck

Cloud-Kommunikation

- SmartPlug agiert nur als HTTPS-Client
- Regelmäßige TLS-Verbindung zum Cloud-Server
- App schickt JSON-Befehle verpackt mit "method:passthrough"

```
POST /?token=<sessionid> HTTP/1.1
Content-Type: application/json
Host: eu-wap.tplinkcloud.com

{"method":"passthrough", "params":
{"deviceId":"<deviceID>,
"requestData":"{\"system\":{\"get_sysinfo\":null}}"}}
```

- Cloud-Server leitet Befehle an SmartPlug weiter

© softScheck

Offene Ports

Port	Protocol
80/tcp	HTTP
9999/tcp	TP-Link Smart Home Protocol
1040/udp	TP-Link Device Debug Protocol (TDDP)

© softScheck

TP-Link Device Debug Protocol

TDDP Patent

(19) 中华人民共和国国家知识产权局

(12) 发明专利申请

(10) 申请公布号 CN 102096654 A
(43) 申请公布日 2011.06.15

(21) 申请号 201110031593.4

(22) 申请日 2011.01.28

(71) 申请人 深圳市普联技术有限公司
地址 518055 广东省深圳市南山区桃源街道平山大园工业区南区 2 栋 1-6 楼

(72) 发明人 李智威 张向明

(74) 专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文

(51) Int.Cl.
G06F 15/163 (2006.01)

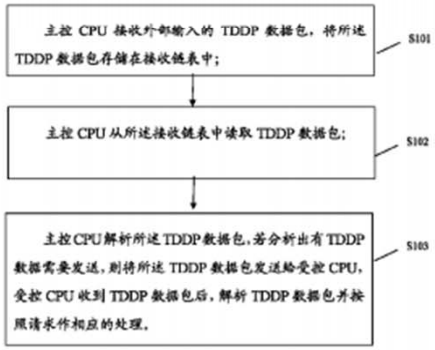
权利要求书 1 页 说明书 7 页 附图 1 页

(54) 发明名称

一种 CPU 之间的数据通信方法、系统及处理器

(57) 摘要

本发明适用于数据通信技术领域，提供了一种 CPU 之间的数据通信方法、系统及处理器。所述方法包括以下步骤：主控 CPU 接收外部输入的 TDDP 数据包，将所述 TDDP 数据包存储在接收链表中；主控 CPU 从所述接收链表中读取 TDDP 数据包；主控 CPU 解析所述 TDDP 数据包，若分析出有 TDDP 数据需要发送，则将所述 TDDP 数据包发送给受控 CPU，受控 CPU 收到 TDDP 数据包后，解析 TDDP 数据包并按照请求作相应的处理。本发明能够实现多 CPU 之间的通信，采用多线程处理上更加快



[0018] TDDP 包的格式如下表所示：

[0019]

TDDP 报头	TDDP 数据

[0020] TDDP 报头格式如下：

[0021]

Ver	Type	Code	ReplyInfo
PktLength			
PktID		SubType	Reserve
Digest[0-3]			
Digest[4-7]			
Digest[8-11]			
Digest[12-15]			

[0022] 各字段的意义如下：

[0023] Ver：TDDP 协议的版本；

© softScheck

TDDP Crypto

```
la      $t9, _strcpy
lui     $s1, 0x5A
move    $a0, $s0
jalr    $t9 ; _strcpy
addiu   $a1, $s1, (aAdmin - 0x5A0000)  # "admin"
lw      $gp, 0x60+var_50($sp)
addiu   $a1, $s1, (aAdmin - 0x5A0000)  # "admin"
la      $t9, _strcat
nop
jalr    $t9 ; _strcat
move    $a0, $s0
lw      $gp, 0x60+var_50($sp)
nop
la      $t9, _strlen
nop
jalr    $t9 ; _strlen
move    $a0, $s0
move    $a2, $v0
addiu   $a0, $sp, 0x60+var_48
jal     md5checksum
move    $a1, $s0
lw      $v0, 0x60+var_44($sp)
lui     $a0, 0x5E
addiu   $v1, $a0, (dword_5E3E00 - 0x5E0000)
sw      $v0, (byte_5E3E04 - 0x5E3E00)($v1)
li      $v0, 1
sw      $v0, (dword_60D9C8 - 0x610000)($s2)
lw      $v0, 0x60+var_48($sp)
lw      $gp, 0x60+var_50($sp)
sw      $v0, dword_5E3E00
```

DES Key = md5(username + password)[:16]

© softScheck

Demo

© softScheck

softScheck
we identify vulnerabilities others don't

Fork us on GitHub: https://github.com/softScheck/tplink-smartplug

Prof. Dr. Hartmut Pohl

Hartmut.Pohl@softScheck.com

Thomas Bötner

Thomas.Boetner@softScheck.com

softScheck GmbH Köln
Büro: Bonnerstr. 108. 53757 Sankt Augustin www. softScheck.com +49 (2241) 255 43 – 12

© softScheck