MIDC·2018

小米IoT安全峰会

岂止于逻辑攻击

Beyond logical attacks

Markus Hinkelmann 博士

首席安全技术专家

NXP Semiconductors

个人简介
About me

- SE密码算法首席安全架构师

  Lead Security Architect for Secure Element Crypto SW

- JHAS主要成员——SoC安全子系统工作组主席

  Member of JHAS (Security IC evaluation harmonization group) Chair for SoC secure subsystem working group

- 计算机科学/数据安全博士

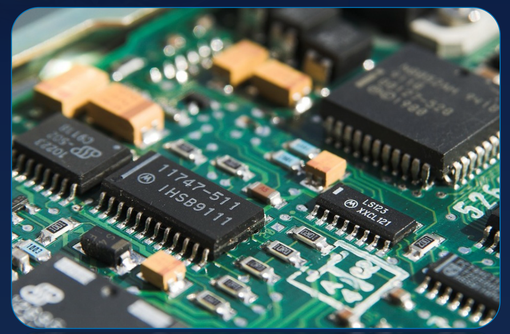
  PhD in Computer Science / Data Security

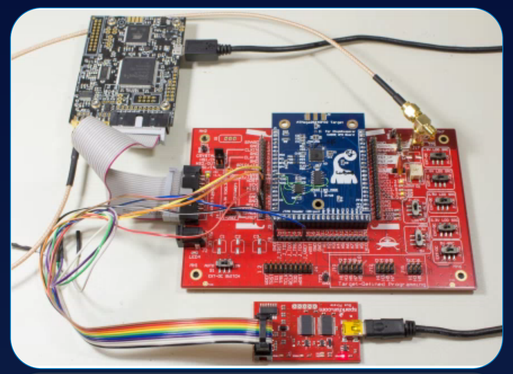
什么是“逻辑攻击”?
What’s a ‘logical’ attack?

0101101000110111010100110100110

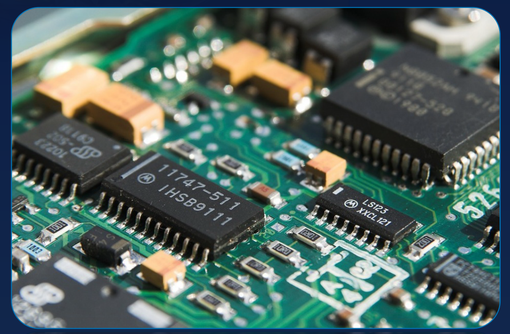
岂止是“逻辑”攻击?
What’s beyond ‘logical’ attacks?

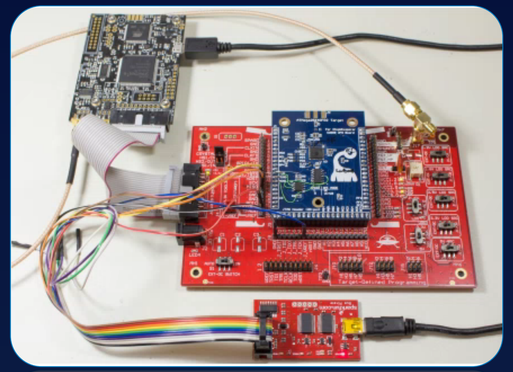
岂止是“逻辑”攻击?
What’s beyond ‘logical’ attacks?



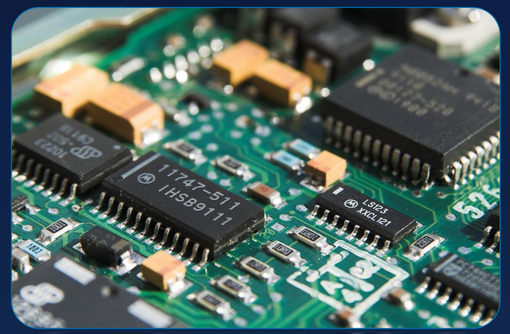


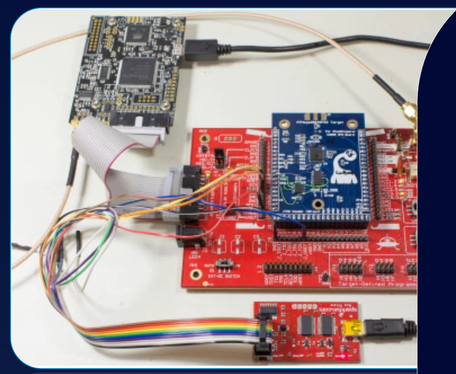
什么攻击与IoT相关?
What attacks are relevant for IoT?





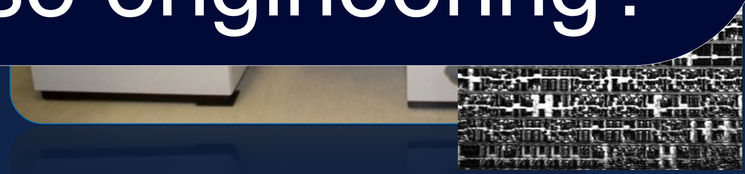
什么攻击与IoT相关?
What attacks are relevant for IoT?



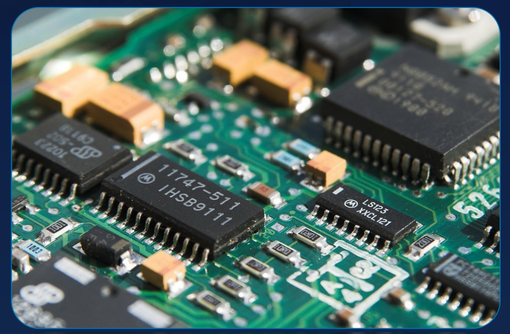


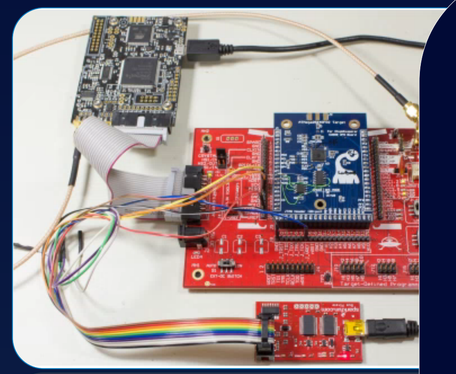
PCB级别操纵，FLASH读取，逆向工程?

PCB level manipulation, flash readout, reverse engineering?



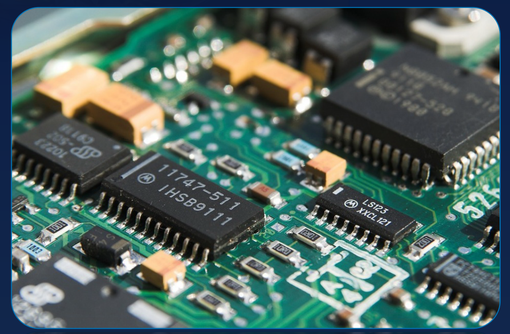
什么攻击与IoT相关?
What attacks are relevant for IoT?

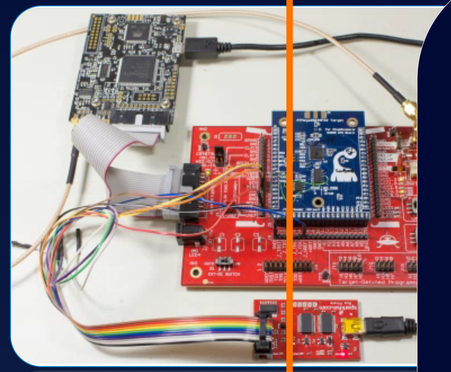




安全单元（SE）相关的
全部攻击范围?
Full attack scope
relevant for
secure elements?

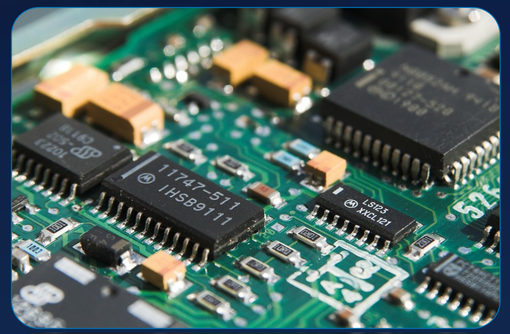
什么攻击与IoT相关?
What attacks are relevant for IoT?

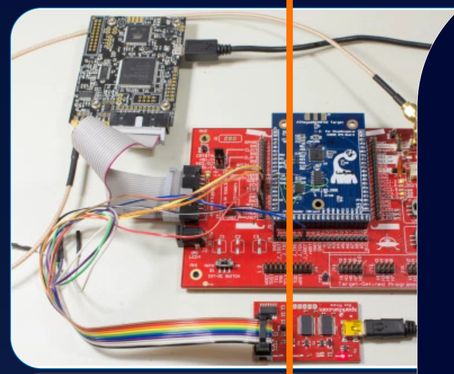




在这之间还有什么?
Something in between?

什么攻击与IoT相关?
What attacks are relevant for IoT?





Good question

需要基于 资产价值+攻击风险/难度 进行考虑depends on asset value + attack risk/effort.

侧信道攻击案例告诉我们，它同样可以用于攻击IoT产品

Let’s look at

side channel analyis examples that seem feasible for IoT

利用RSA算法实现弱点进行简单电磁分析攻击
Exploitation of an RSA vulnerability by Simple EM analysis

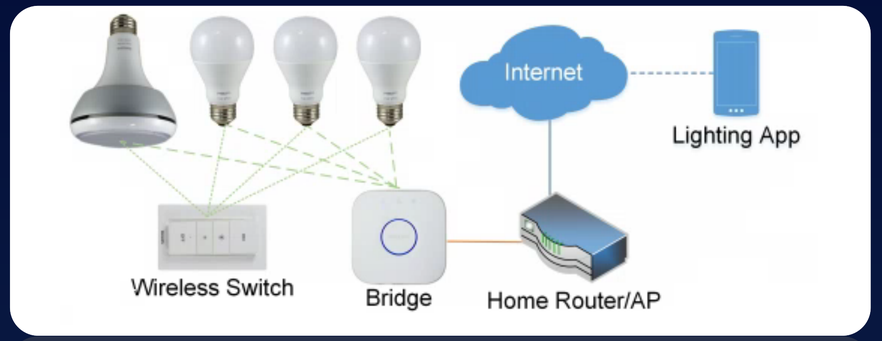
- 电磁分析 – 利用设备运行时对外的电磁辐射进行侧信道攻击
  EM analysis - side channel attack using electromagnatic emanation of a device
- 简单 – 只需要单个运算产生的电磁辐射数据
  Simple - requires data from a single execution only

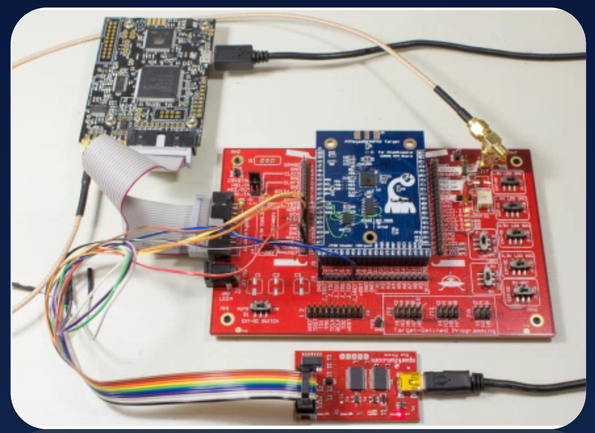
- 目标: 存储在一部有漏洞的安卓手机上的RSA私钥
  Target: RSA private key on a vulnerable Android smartphone
  (例如：用于认证、会话建立、支付等e.g. used for authentication / session establishment / payment / etc.)
- 不需要拆开设备！No device opening required!
- 不需要复杂的攻击设备。No sophisticated equipment needed.
- 仅需要 <1分钟就可以破解密钥。 Exploitation<1min including brute force.

‘IoT Goes Nuclear – Creating a ZigBee Chain Reaction’

在Philips Hue 智能灯上进行的规模攻击

Scalable attack on Philips Hue smart lamps





http://iotworm.eyalro.net/

第一步Step 1

使用价值350美元的Chipwhisper Lite平台提取OTA固件更新密钥（AES-CCM）

The 350US$ Chipwhisperer Lite platform was used to extract the OTA firmware update key (AES-CCM)

糟糕的设计Very unfortunate choice:

同一型号的灯泡使用相同的密钥

Every bulb of a certain model used the same key...

第二步Step 2

Zigbee协议的一个实现上的漏洞（临近性检查）是允许等泊与个人局域网分离。我们可以利用这个漏洞和第一步的成果，在400米以外就可以给灯泡安装带有木马的固件。

An implementation bug in the Zigbee protocol (proximitiy check) allowed to disassociate the lamps from their PANs and use the FW update key from step 1 to install the attack FW from up to 400m away

= 链式反应 chain reaction

AI

- 我们可以看到AI（例如深度学习）正在简化攻击步骤。
  We see that AI (e.g. Deep Learning) simplifies attack steps.

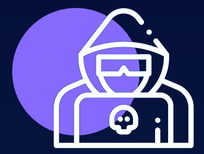
- AI正在逐步减少对攻击专家的需求。
  AI has the potential to remove the need for attack experts.

- 提高攻击的可行性，降低攻击成本。
  AI increases attack feasibility, reduces attack costs.

2017 网络攻击急剧升级 & 新形式攻击

2017 Dramatic uptick in cyberattacks & new aggressive types of attacks

每**40秒**就会有
一个勒索软件攻击企业
Ransomware hits
businesses every
40 seconds

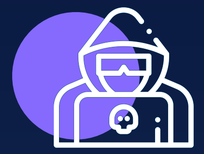


企业平均需要
~197天 才能侦破
It takes most
businesses **~197 days**
to detect a breach

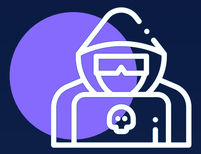
FBI：俄罗斯黑客可以访问
全球超过50万个网关
FBI: Russian hackers
have access to over
500 K gateways globally

新的远程物理攻击：
new remote physical
attacks:
Rowhammer and
Nethammer

每天有
100万
新的恶意文件产生
There are **1M** new
malicious files daily



每秒可以侦测到**5个**
恶意软件变体
5 new malware variants
are discovered
every second



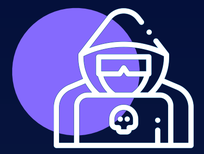
每小时有**超过100个**未知的恶
意软件攻击
Over 100 unknown malware
attacks hit on
organizations every hour

18个新的漏洞变种
18 new variants
of Spectre and Meltdown
vulnerabilities

2017 网络攻击急剧升级 & 新形式攻击

2017 Dramatic uptick in cyberattacks & new aggressive types of attacks

每**40秒**就会有
一个勒索软件攻击企业
Ransomware hits
businesses every
40 seconds



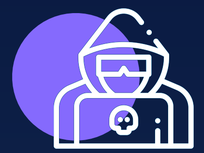
企业平均需要
~197天 才能侦破
It takes most
businesses **~197 day**
to detect a breach

FBI：俄罗斯黑客可以访问

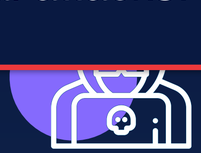
物理攻击并不仅仅发生在本地。
Physical is
not necessarily equal to
Local attacks!

新的远程物理攻击：
new remote physical
attacks:
Rowhammer and
Nethammer

每天有
100万
新的恶意文件产生
There are **1M** new
malicious files daily



每秒可以侦测到**5个**
恶意软件变体
5 new malware variants
are discovered
every second



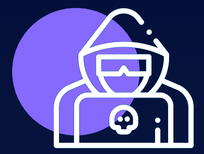
每小时有**超过100个**未知的恶
意软件攻击
Over 100 unknown malware
attacks hit on
organizations every hour

18个新的漏洞变种
18 new variants
of Spectre and Meltdown
vulnerabilities

2017 网络攻击急剧升级 & 新形式攻击

2017 Dramatic uptick in cyberattacks & new aggressive types of attacks

每**40秒**就会有
一个勒索软件攻击企业
Ransomware hits
businesses every
40 seconds

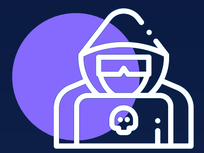


企业平均需要
~197天 才能侦破
It takes most
businesses **~197 days**
to detect a breach

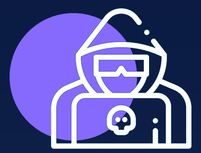
FBI：俄罗斯黑客可以访问
全球超过50万个网关
FBI: Russian hackers
have access to over
500 K gateways globally

新的远程物理攻击：
new remote physical
attacks:
Rowhammer and
Nethammer

每天有
100万
新的恶意文件产生
There are **1M** new
malicious files daily



每秒可以侦测到**5个**
恶意软件变体
5 new malware variants
are discovered
every second



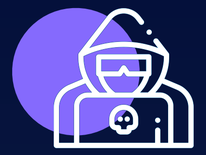
每小时有**超过100个**未知的恶
意软件攻击
Over 100 unknown malware
attacks hit on
organizations every hour

18个新的漏洞变种
18 new variants
of Spectre and Meltdown
vulnerabilities

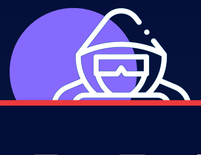
2017 网络攻击急剧升级 & 新形式攻击

2017 Dramatic uptick in cyberattacks & new aggressive types of attacks

每**40秒**就会有
一个勒索软件攻击企业
Ransomware hits
businesses every
40 seconds



企业平均需要
~197天 才能侦破
It takes most
businesses **~197 days**
to detect a breach

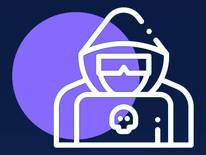


截至11月18日：Nov 18：

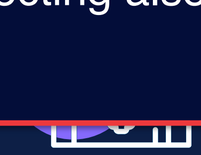
7个新的Meltdown变体已经影响
到ARM安全
7 new Meltdown variants
affecting also ARM

的远程物理攻击：
v remote physical
attacks:
owhammer and
Nethammer

每天有
100万
新的恶意文件产生
There are **1M** new
malicious files daily



每秒可以侦测到**5个**
恶意软件变体
5 new malware variants
are discovered
every second



每小时有**超过100个**未知的恶
意软件攻击
Over 100 unknown malware
attacks hit on
organizations every hour

18个新的漏洞变种
18 new variants
of Spectre and Meltdown
vulnerabilities

总结 Conclusion

- IoT安全绝不仅仅是“逻辑”安全
  IoT security is much more than ‘logical’ protection.
- 通过远程或本地的方式对硬件的攻击往往使“更大规模”的攻击成为可能
  Remote and local HW attacks are often enabling further attacks that ‘scale’.
- AI可以使侧信道攻击和错误注入攻击更为有效，而且不再依赖于攻击专家
  AI can amplify side channel and fault attacks and remove need for experts.

- “逻辑”攻击只是第一波。NXP不局限于此，防患于未然，研发出更为安全的芯片产品。
  ‘Logical’ attacks is just the first wave. NXP is looking beyond that and is creating products to withstand the waves to come.
- 让我们共同努力，共创更为安全的未来！
  Let’s work together.

谢谢