IoT and Silicon Security

Dissecting a real life IoT attack

Asaf Shen, VP Secure Devices, Emerging Businesses Group, Arm

The Architects of Global Possibilities

The global leader in the development of licensable technology

- R&D outsourcing for semiconductor companies

Focused on freedom and flexibility to innovate

- Technology reused across multiple applications

With a partnership based culture & business model

- Licensees take advantage of learnings from a uniquely collaborative ecosystem

1,650+
licenses, growing by >100 every year

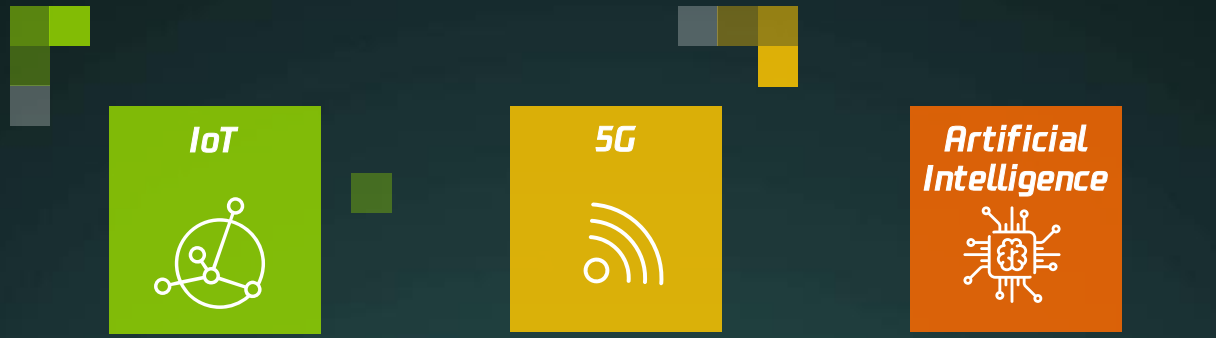
138bn+
Arm-based chips shipped to-date

6.2bn
Arm-based chips shipped in Q3 FY2018

525+ Licensees
Industry leaders and high-growth start-ups; chip companies and OEMs

The Fifth Wave of computing

Data-driven computing era



Generating data

Transporting data

Processing data

The Internet of Things

A ‘hyper-connected’ world of devices

Now

3+ billion Smartphones

2 billion Personal computers

8.4 billion IoT devices

Future

1 trillion

Connected devices by 2035

Source: Gartner, Statista, Strategy Analytics, Arm Estimates

Delivers Value Through Digital Transformation

Productivity gains – automation, sensor driven insights, smart manufacturing

New business models – from a 'product sale' to 'as a Service' revenue

Enhanced customer experience – access to real-time data, agile support

The Value of this Digital Transformation:

$11 Trillion

Global economic value of IoT by 2025*

*McKinsey Global Institute, 2017

The Complexity of IoT

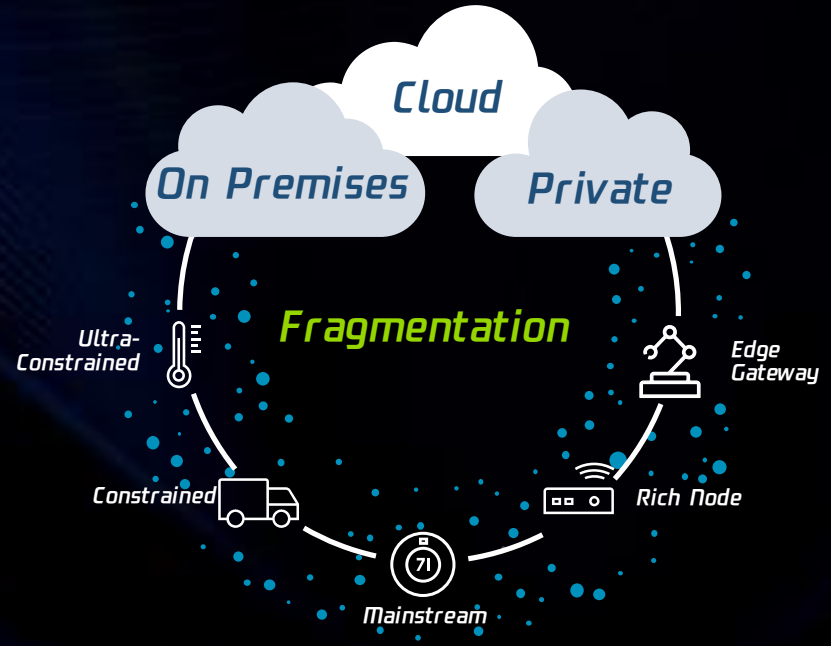
Security

Connect

Provision

Manage

Develop devices



IoT's Commercial Challenges

Investment return

What is the value of data to my business?

Security concerns

Can the data be trusted?
Does it make me vulnerable?

Interoperability hurdles

What is required to integrate IoT with current systems?

Network infrastructure

Is the network architected to cope with 1 trillion connected devices?

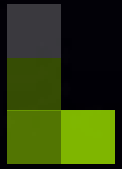
Arm's Approach to IoT

Enable Choice, Underpinned by Trust

The Cost of Security Inaction is Significant

>300%

Increase in malware loaded onto IoT devices[2]



29%

Increase in industrial control system vulnerabilities[1]

600%

Increase in IoT device attacks[1]

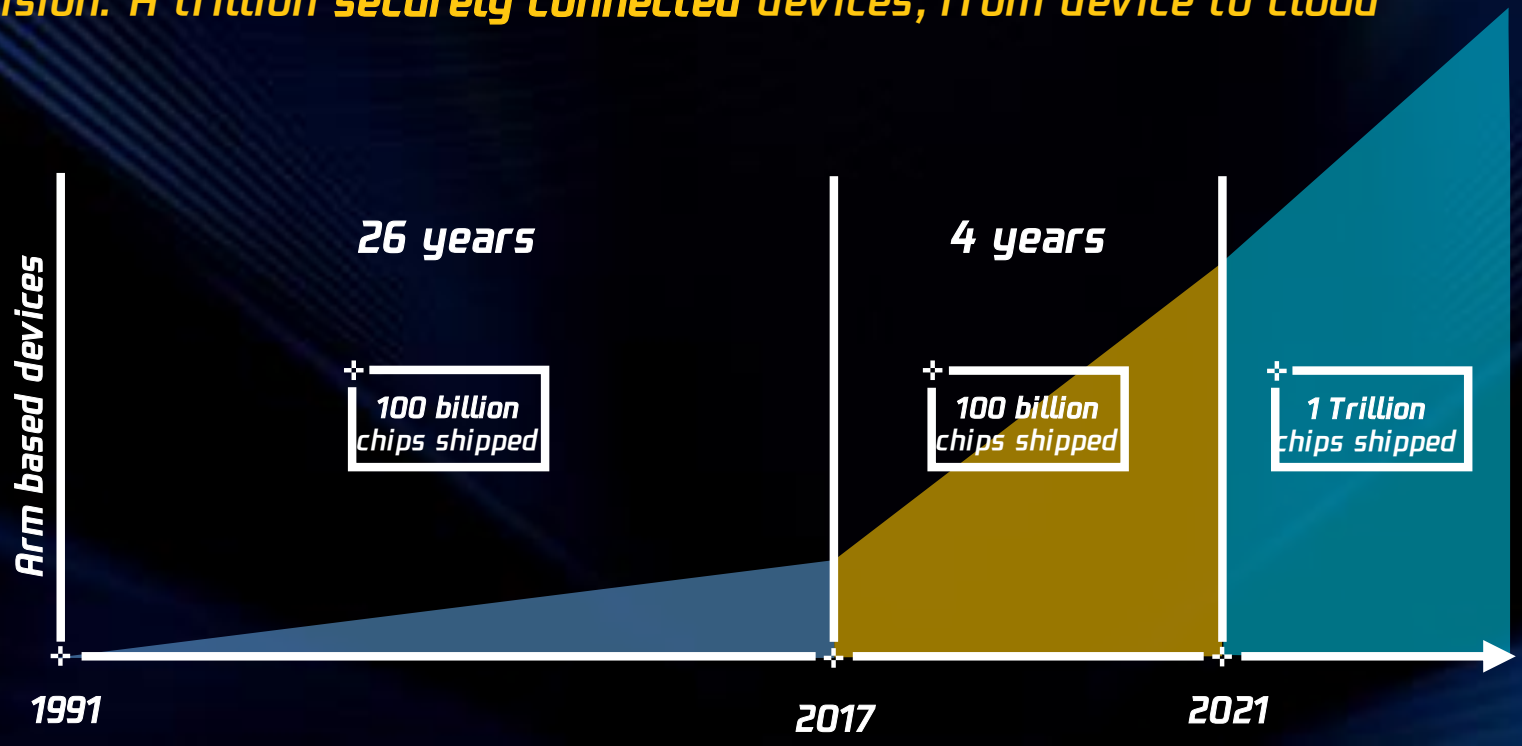
$6 trillion

Cost of damage related to cybercrime by 2021[3]

1 – Symantec Internet Security Threat Report 2018
2 – Kaspersky Labs, New Trends in the World of IoT Threats 2018
3 – Annual Cyber Crime Report, Cyber Security Ventures 2019

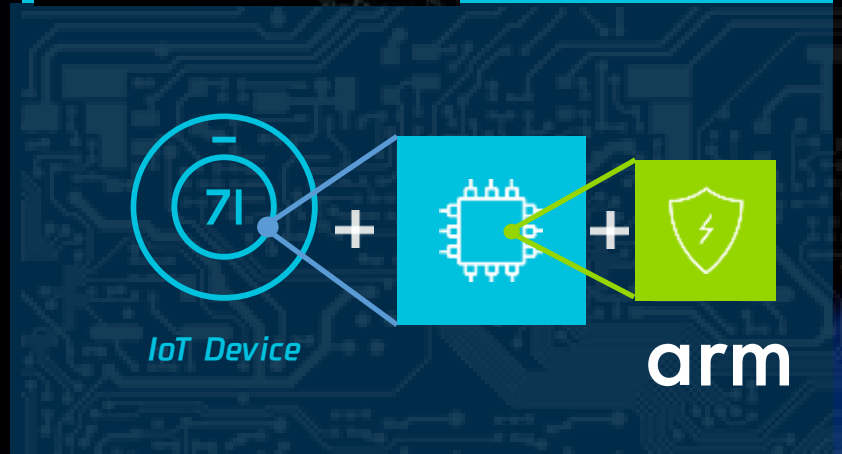
The Road Ahead is Exciting··· and Scary···

*Arm vision: A trillion **securely connected** devices, from device to cloud*



Arm's Security Vision

- Security needs to be built from the ground up… and at the core of every device
- No single point of ownership, whole IoT value chain needs to share the responsibility
- Simple and seamless integration of security from foundational architecture to cloud service is key



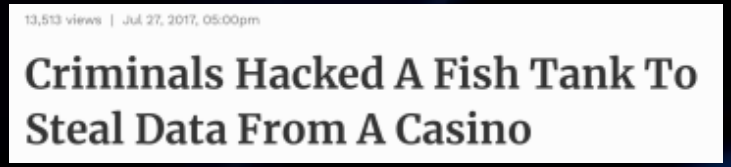
Plenty of Vulnerabilities and Exploits to Choose From…

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

On October 12, 2016, a massive distributed denial of service (DDoS) attack **left much of the internet inaccessible on the U.S. east coast.** The attack, which authorities initially feared was the work of a hostile nation-state, was in fact the work of the Mirai botnet. This attack, which initially had much less grand

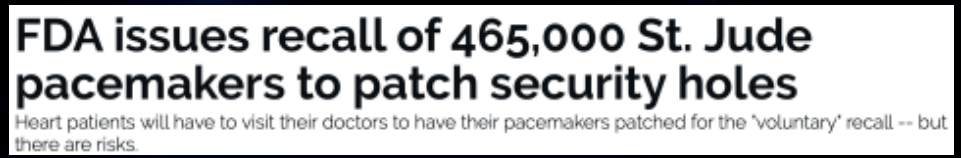
BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking

September 12, 2017 Swati Khandelwal



13,513 views | Jul 27, 2017, 05:00pm

Criminals Hacked A Fish Tank To Steal Data From A Casino



FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

A DEEP FLAW IN YOUR CAR LETS HACKERS SHUT DOWN SAFETY FEATURES

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

https://eprint.iacr.org/2016/1047.pdf

Scenario

IoT devices infect each other with a worm that rapidly spreads over large areas (depending on critical mass).

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Impact

Starts with infecting a single street lamp with a worm.

The worm spreads to wider network of street lamps.

Enables an attacker to control and abuse city lights and perform massive DDOS attack.

Interesting note: In Paris (~105 Sq.Km), critical mass is fewer than 15,000 randomly selected smart street lamps

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

How did attackers gain control of an already installed lamp?

"We overcame the first problem by discovering and exploiting a major bug in the implementation of the Touchlink part of the ZigBee Light Link protocol…."

How did attackers perform an un-authorized over-the-air firmware update?

"…They found out that all lamps (from the same product type) were using the same global AES-CCM key for the firmware update process."

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

How was the global AES-CCM key compromised?

"… using novel side channel attacks…… a side channel attack to extract the global AES-CCM key (for each device type) that manufacturer uses to encrypt and authenticate new firmware"

"…Once we obtained these secret values, we could create any new firmware and upload it into any… lamp"

Interesting note: The equipment used in the SCA attack costs just a few $100

Security Issues Demonstrated in This Attack…

Protocol implementation bug in the Zigbee light link was not revealed in protocol validation…

Usage of symmetric keys shared within a large class of devices

- A Zigbee light link master key, used by all Zigbee light link certified products for "commissioning" (initial delivery of a network key)
- A key for firmware update is shared across all devices of a certain type

Not protecting these keys very well…

- Zigbee light link master key leaked long ago…
- The firmware update key was extracted through a side channel attack

Platform Security Architecture

A framework for building secure devices – openly published

Asset Tracker TMSA

Smart Water Meter TMSA

Network Camera TMSA

Analyze

Threat models & security analyses

Architect

Hardware & firmware architect specifications

Implement

Firmware source code

Certify

Independently tested

psacertified™

www.arm.com/psa-resources

A Plethora of Threats

side channel attack to expose the FW update key

Physical

- Non-invasive: e.g. clock or power glitch or SCA
- Invasive: package removal, e.g. microprobe station FIB

Communications

- Man-in-the-middle
- Weak RNG
- Code vulnerabilities

Shared keys for large class of devices

Zigbee touchlink implementation bug

Software

- ROP, e.g. buffer overflows
- Interrupts
- Malware

Zigbee light link master key leak

Lifecycle

- Code downgrade
- Change of ownership or environment
- Unauthorized overproduction

System Security: You're Only as Strong as Your Weakest Link

The attack surface is growing

Attacks are becoming easier

The risk is only increasing

Hardest

Easiest

The Fourth PSA Stage: Certification

Analyze

Threat models & security analyses

Architect

Hardware & firmware architect specifications

Implement

Firmware source code

Certify

Independently tested

psacertified™

riscure
Challenge your security

UL

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

PROVE & RUN

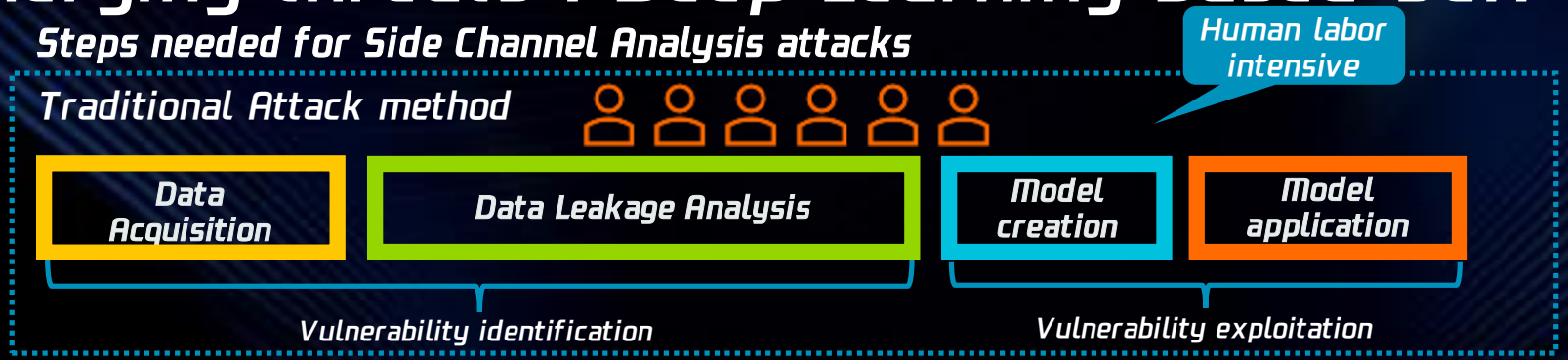
arm

brightsight®
the number one security lab in the world

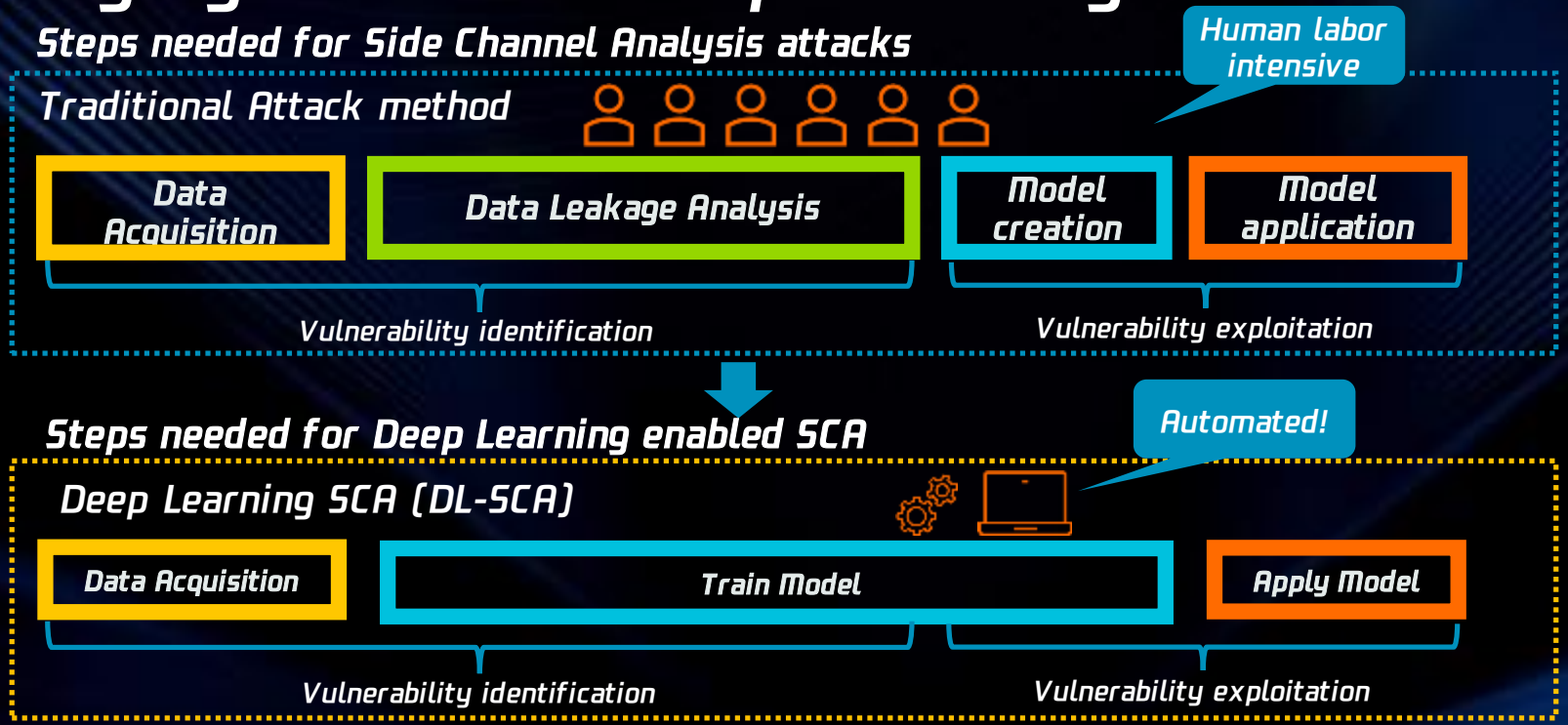
www.arm.com/psa-resources

Emerging threats : Deep Learning based SCA

Steps needed for Side Channel Analysis attacks



Emerging threats : Deep Learning based SCA



Deep Learning and SCA - Summary of the Threat

DL-SCA is rapidly approaching weapon grade

DL-SCA will become dominant tool for attackers.

Traditional mitigations might fall short to protect against DL-SCA.

DL-SCA "Push-button Attack" scenario is optimistic at this point

SCA still requires a lot of expertise and background knowledge. Experience of the user is still essential.

Deep learning is computationally intense technique.

Connecting Chip-to-Cloud Securely

System-level solutions to simplify IoT development and deployment

Secure | Scalable | Configurable | Power efficient | Consistent

Energy efficient processing, with right-fit security

Secure devices - trusted data, secure identity

Secure, open OS - designed ground-up for IoT

Device, connectivity & data management


THANKS
TENCENT SECURITY CONFERENCE 2019