The Risks of Huawei Risk Mitigation

Sophia d'Antoine
Perri Adams

Who are we?

Sophia D'Antoine

@calaquendi44

Perri Adams

@perribus

A Tale of Risk and Mitigation

THE CRM APPROACH

Composite Risk Management

“injure or kill personnel, damage or destroy equipment, or otherwise impact mission effectiveness.”

Identify Hazards

- Mission complexity
- Enemy threat
- Weather
- Soldier fatigue
- Geographic obstacles
- Etc.

Assess Risk

How do the potential benefits outweigh the cost

Develop Controls

- Benefit: how much do the controls reduce risk?
- Cost: how much do the controls cost?

Application to US Critical Infrastructure

1998 **Critical Infrastructure Assurance Office (CIAO)** created by Presidential Directive in 1998

2014 NIST releases **Framework for Improving Critical Infrastructure Cybersecurity** Version 1.0

2018 **John S. McCain National Defense Authorization Act (NDAA)** - NDAA for FY2019

- ➔ Senate version: Blocks lifting export denial order (ZTE)
- ➔ Final version: Provision banning federal purchase of telecommunications equipment from certain vendors citing *security concerns*
  - ◆ Huawei & ZTE singled out
  - ◆ Huawei currently suing over this NDAA
- ➔ Any surveillance equipment for the purposes of national security
  - ◆ Dahua Technology, Hytera, and Hikvision

Critical Infrastructure: 5G

- New generation of critical communications infrastructure
- Requires 5G capable equipment
  - **Base Stations**
- 5 Suppliers:
  - **Ericsson** (Sweden), **Huawei** (China), and **Nokia** (Finland)
  - Samsung (South Korea) and ZTE (China) make up smaller market share
  - Other companies develop additional equipment e.g. Cisco (American)
- Governments assess **national security risks** of suppliers
  - Governments oversee supplier bidding process
  - Establish security requirements, possibly ban certain suppliers

1-800-HUAWEIBLING
1-800-HUAWEIBLING
1-800-HUAWEIBLING
1-800-HUAWEIBLING
1-800-HUAWEIBLING
1-800-HUAWEIBLING
1-800-HUAWEIBLING

Huawei

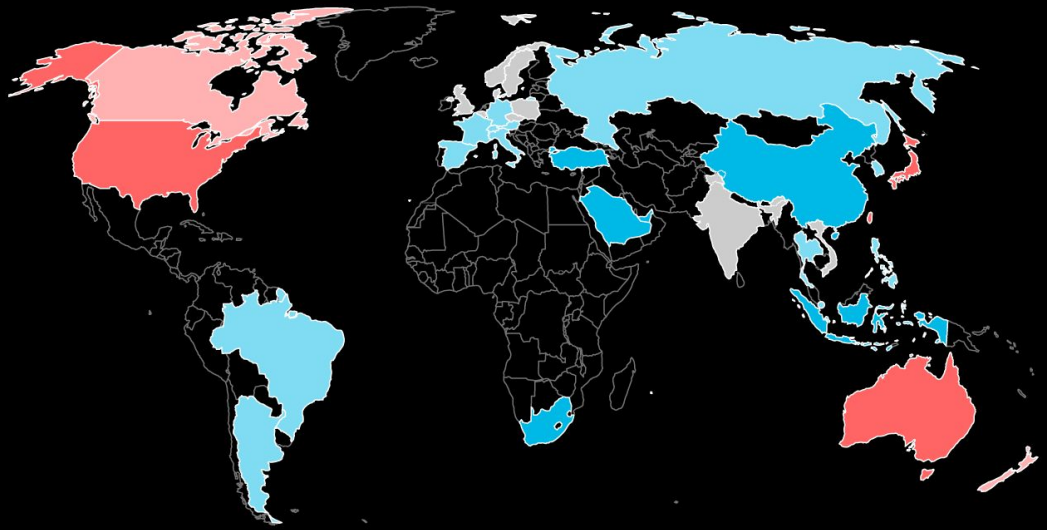
- Sells telecommunications equipment and consumer electronics
- Beat Apple to become 2nd largest phone manufacturer globally
- Subsidized by Chinese Government
- **Cheapest** base stations (30% below competitors)

Headquarters in Schenzen, China

The Huawei Barometer

Countries that have banned Huawei make up nearly a third of the world's GDP

Stance on Huawei	Percentage of World GDP
Ban in effect Australia, Japan, Taiwan and U.S.	32.6%
Likely to ban Canada and New Zealand	2.3%
On the fence Belgium, Czech Rep., Denmark, India, Norway, Poland, Sweden, U.K. and Vietnam	9.9%
Unlikely to ban Argentina, Austria, Brazil, France, Germany, Italy, Philippines, Russia, Singapore, South Korea, Spain, Switzerland and Thailand	21.6%
Embracing Huawei China, Indonesia, Saudi Arabia, South Africa, Turkey and UAE	19.8%



Sources: International Monetary Fund GDP data for 2018; Bloomberg

Bloomberg

March 2019

Huawei Debate

Mug of MSS Tears

The Huawei Debate

National Security

- Chinese companies beholden to Government
- Chinese Gov't can compel Huawei to backdoor devices, steal data, etc.
    - Allow China's Ministry of Public Security to access all networks and data?
        - National Intelligence Law (2017) "Regulation on Internet Security Supervision and Inspection by Public Security Organs" (2019)
        - Huawei Technologies USA, Inc. refuted before the FCC, May 2019
        - (公安机关互联网安全监督检查规定)

Geopolitics & Cost

- Cheaper equipment
- Avoiding tensions with China
    - China views bans as "protectionism" disguised as national security
    - Countries depend economically on China
    - China increasingly powerful global player

Five Eyes Divided

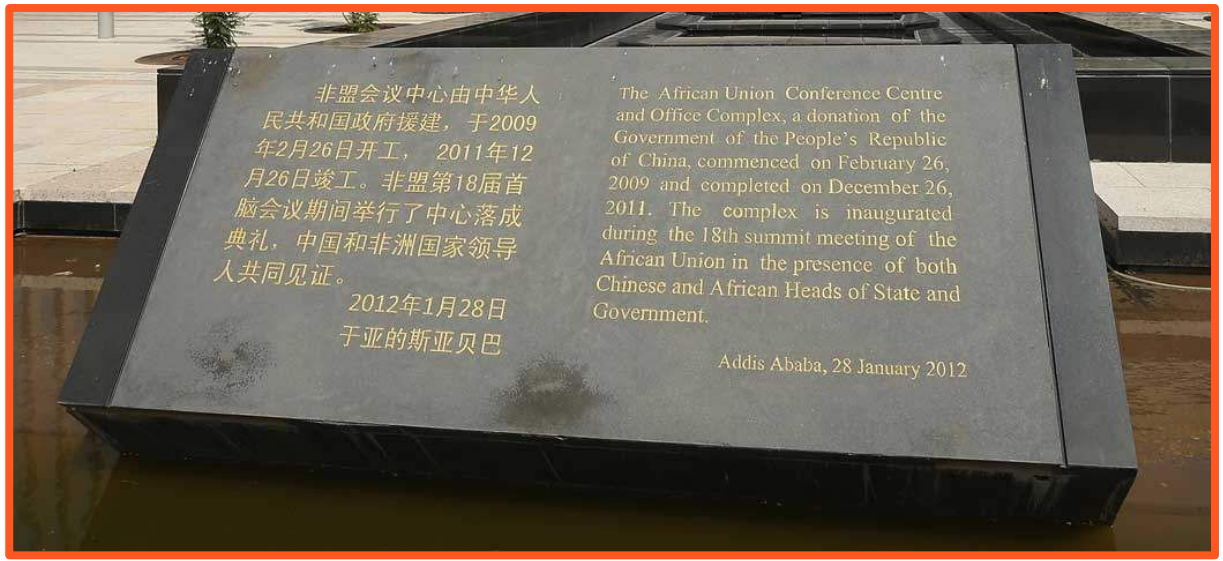
- Australia and US leading the charge to ban Huawei equipment
  - US led global pressure campaign against allies use of equipment
- Britain considering allowing “non-core” Huawei equipment
- New Zealand undecided, may use British model
- Canada postponing decision until after election
  - Fate of Canadian detainees in China undecided
    - Chinese response to Canada arresting Huawei CFO (daughter of founder) at US request
  - Huawei already ingrained in Canadian networks and 5G research

European Disunity

- EU refused to issue a blanket ban against Huawei
  - Going against US pressure
- Many countries following Britain's lead
- German infighting
  - Merkel refused to ban Huawei
  - German Spy Chief warned against Huawei
  - MPs pushing to let legislature decide
- Nokia and Ericsson are both European companies
- Poland torn between US allyship against Russia and economic ties to China

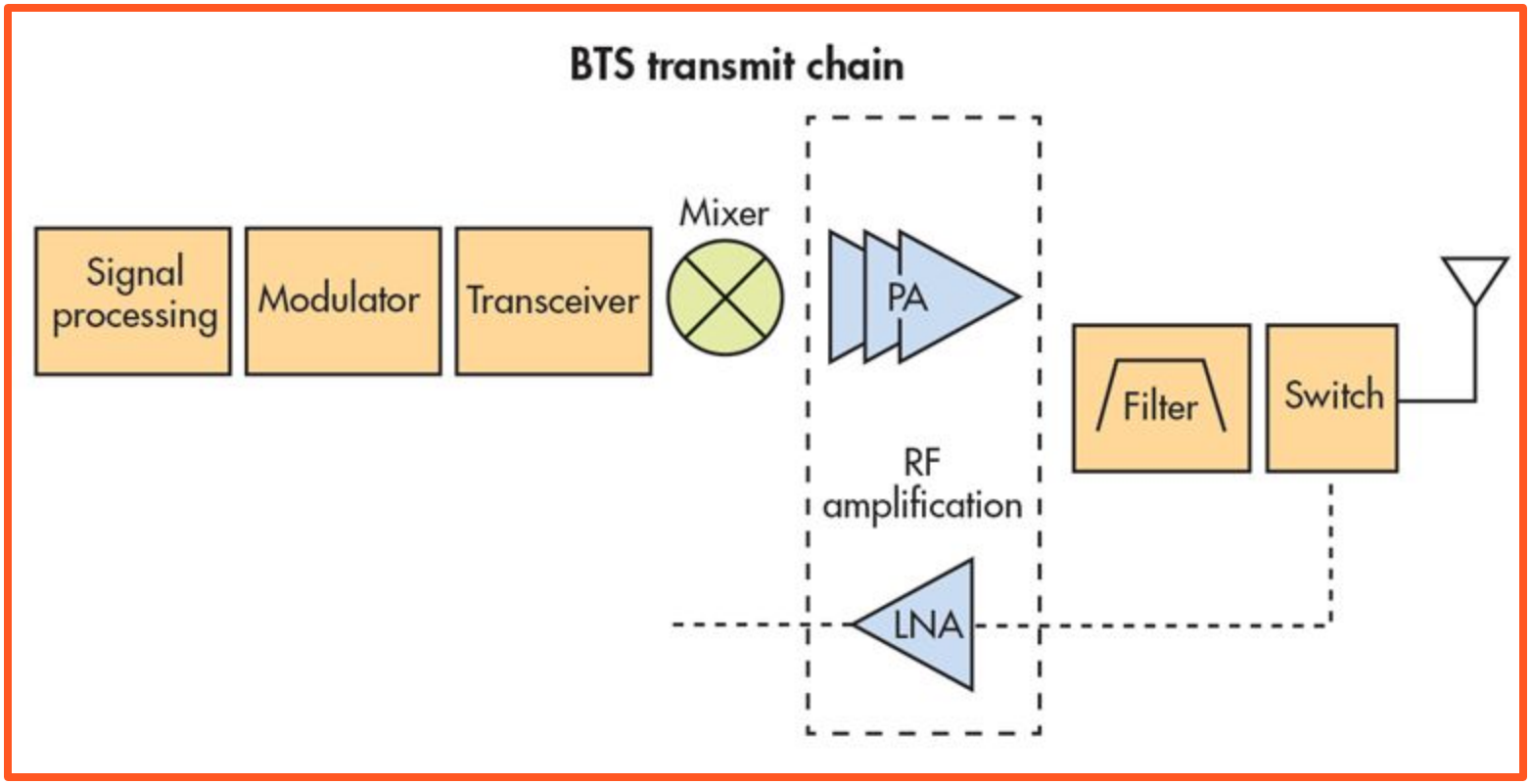
Huawei in Developing Economies

- Huawei is cheap, China offers subsidies
- Developing economies risk relationship with China & losing Chinese investment
- Mexico has banned Huawei near the US border, but not farther south
- African Union
  - Chinese funded new HQ
  - Huawei caught exfiltrating data
  - AU doesn't want to risk relationship w/ China



What is 5G


5G


BTS transmit chain
Signal processing
Modulator
Transceiver
Mixer
PA
Filter
Switch
RF amplification
LNA

What is 5G?

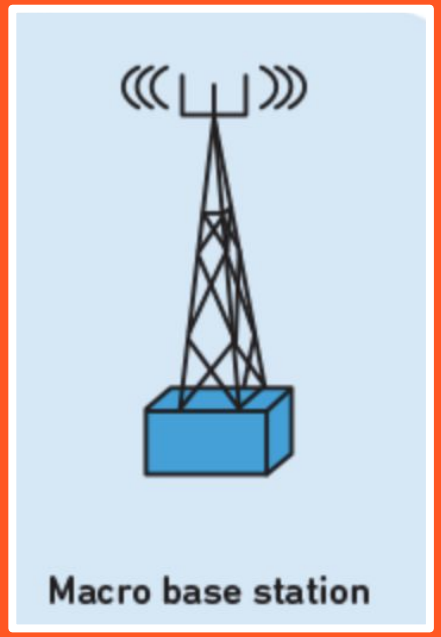
- Millimeter wavelength technology (30 and 300 gigahertz)
- Higher frequency means higher bandwidth, but shorter range
  - Wireless modem or phone will need to be close to a base station
- Latency: 1ms compared to 4G's 70ms
- Installation: Historically tall towers, "small cells" installed to existing polls, buildings

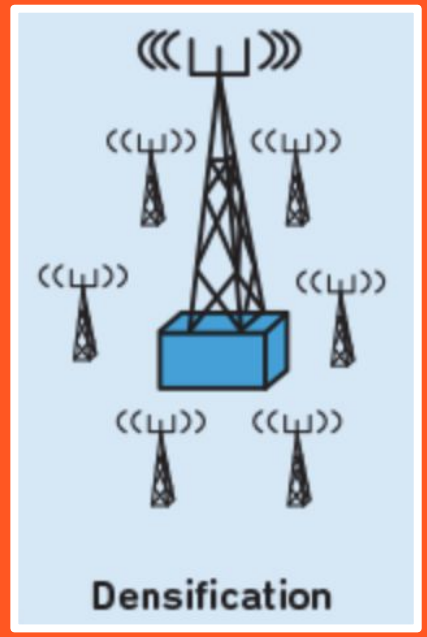
TLDR many more base stations

5G Improvements

- **Speed:** carrier aggregation
- **Compression:** higher-order modulation
- **Capacity:** spectrum expansion
  - add shared/unlicensed spectrum to the available 40-plus licensed bands
- **Coverage Efficiency:** full-dimension MIMO
  - azimuth and elevation beamforming
  - Sub-6 GHz (3.5GHz) Spectrum required for national coverage to offset mmWave shortcomings
    - IntelSat currently sits on this spectrum
- **IoT Capability:** Intended to connect to millions of IoT devices

More Base Stations





5G Small Cells/ Macro BTS

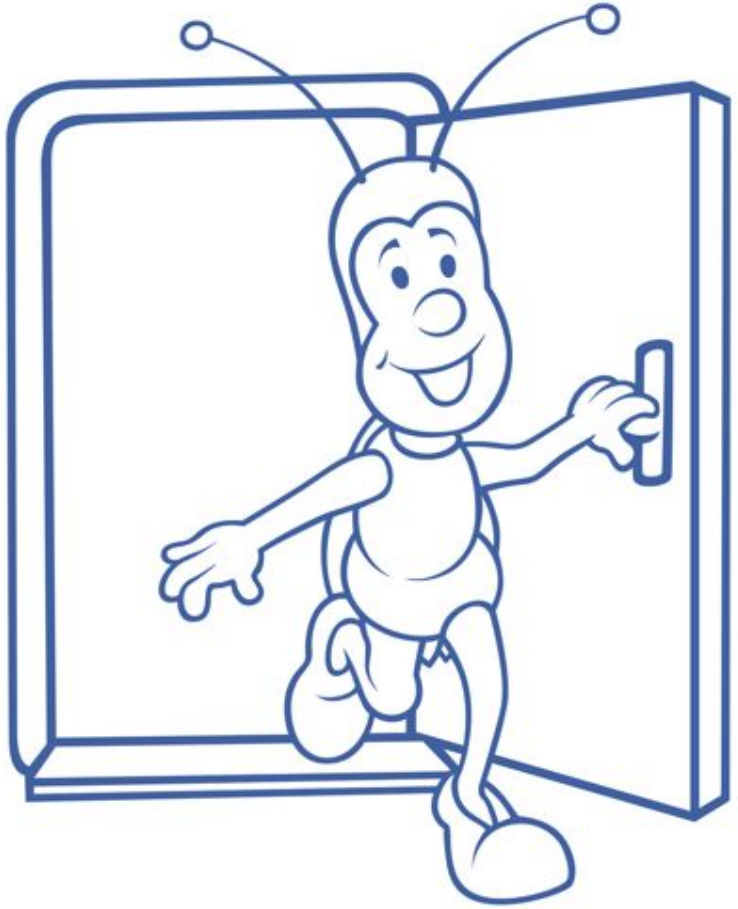
- Base Stations
- Contain each containing many support devices and monitoring sensors
- Management systems hosted in the cloud
- Remotely managed!
  - Many listening services with features 
- Embedded device (IoT) with firmware which is reflashed and updated... like a router!

Nokia's AirScale BTS

Risks

Huawei Base Stations: Access

- China backdoors their own device
- Bug-door
- Remote update introduces a security critical change
- Federation of telecommunication infrastructure
- Difficult to enforce data regulations



Huawei Base Stations: Consequences

- Intelligence collection
- Critical infrastructure - Could knock out service
- Pivot for other malicious activity
- Obscure attribution efforts
- Economic: Artificial prices force competitors out of business
- IoT Devices: Not just handheld devices, millions of IoT devices will be connected

5G is technically about fast speeds and almost zero latency, at a global level represents political dominance and economic might

Huawei Base Stations: Long Term

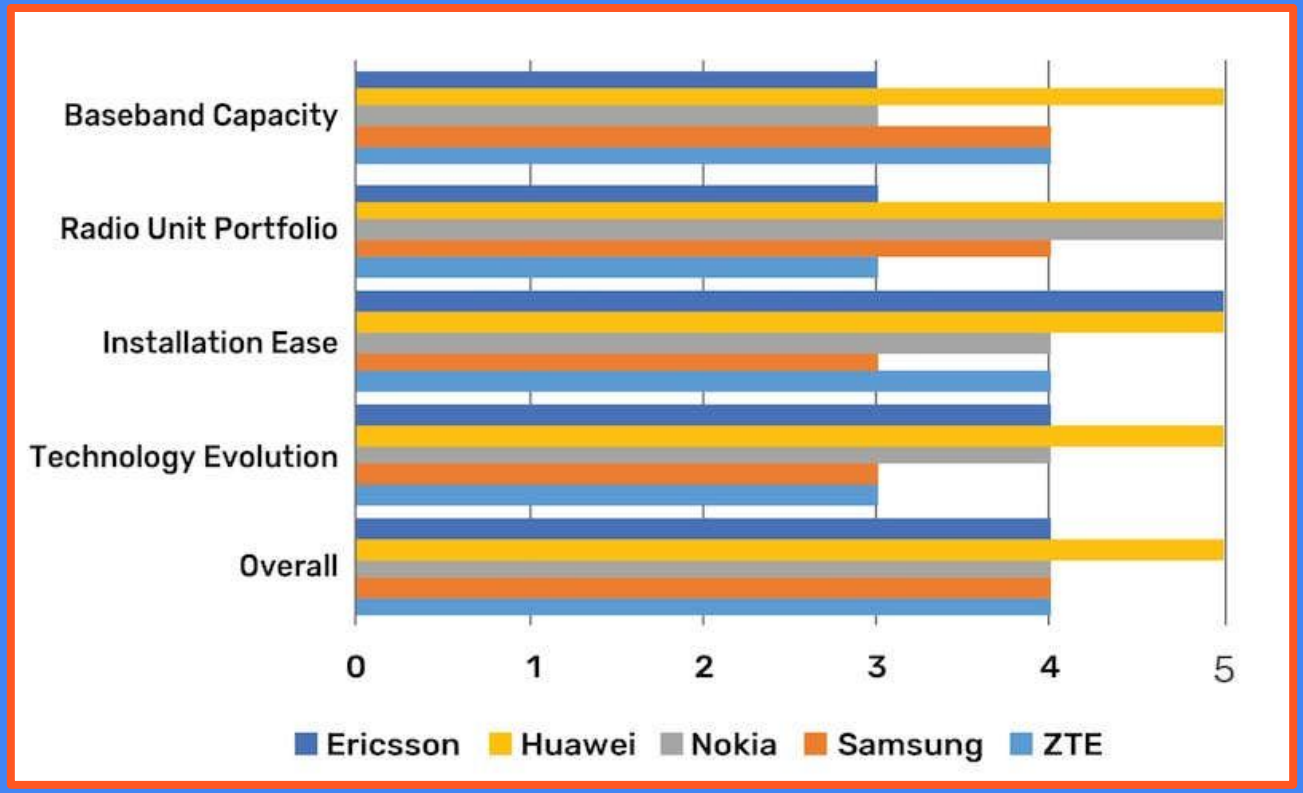
- These devices would be embedded in our networks for decades
- Networks in rural areas depend on access to cheap equipment which is **replaced** less often
- 5G designed to bring connectivity to **IoT devices**

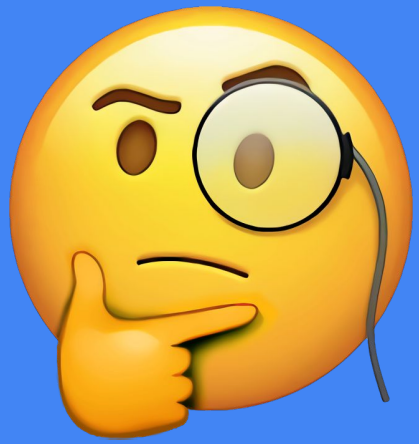
Argument for Huawei

Huawei Base Stations: Pros

- 30% cheaper than market
- Consolidated solution, works out of box
    - Nokia requires purchase of multiple parts
    - Installation is time consuming
    - US companies still waiting on FCC auctions and mmWave technology to get cheaper

Comparison June 2019





Proposed Risks

- Security Concerns can be Mitigated?
- Lawfare “Huawei and Managing 5G Risk”
- Risks Outlined
  - Vulnerabilities in Huawei devices have been found
  - Fail to patch in timely manner
  - Updates introduce uncertainty
  - Huawei is subject to Chinese law requiring Chinese organizations or citizens to “support, assist, and cooperate with state intelligence work.”
  - Solution: Assume network is compromised
- Use CIA Triad

https://www.lawfareblog.com/huawei-and-managing-5g-risk

Proposed Mitigations

- **(C) Confidentiality & (I) Integrity**
  - Use of VPN's and end-to-end encryption
  - Assume insecure channel
- **(A) Availability**
  - Nothing stops vendor from turning off service
  - Backup equipment from different vendor

https://www.lawfareblog.com/huawei-and-managing-5g-risk

Why These Mitigations Fail

- **(C) Confidentiality & (I) Integrity**
  - Encryption doesn't solve confidentiality
  - Metadata is useful
  - Loss of integrity is still possible even in encrypted data
  - Why give adversary such a large foothold?
- **(A) Availability**
  - Do we have a trusted in-house vendor?
  - If so why not just use them?
- Properly configured, encrypted channels would be dependent on each device on the network
  - Transmits cost to the consumer (iPhone vs. Samsung)
  - Network segmentation for critical comm's

https://www.lawfareblog.com/huawei-and-managing-5g-risk

Strategy: UK Proposed Mitigations

Assume Chinese state could compel anyone in China to do anything

- Code and device review
- No use of the equipment in sensitive networks
- Have enhanced monitoring
- Architect the networks to be resilient to exploitation
- Keep more risky vendors out of sensitive functions (i.e. lawful intercept)
- Every chunk of the network should have multiple vendors, noting there'll be exceptions due to practicalities

https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

Strategy: GCHQ Huawei Report

- Huawei Cyber Security Evaluation Centre (HCSEC) running for 9 years
- “HCSEC’s work has continued to identify concerning issues in Huawei’s approach to software development”
- Huawei has made no material progress on issues raised in 2018
  - No reliable patches!
- Limited assurance that long-term technical risks can be managed
- HCSEC believes it cannot appropriately risk-manage future products
- Intentional software failures
- TLDR: Security risks cannot be managed

Strategy: GCHQ Huawei Report

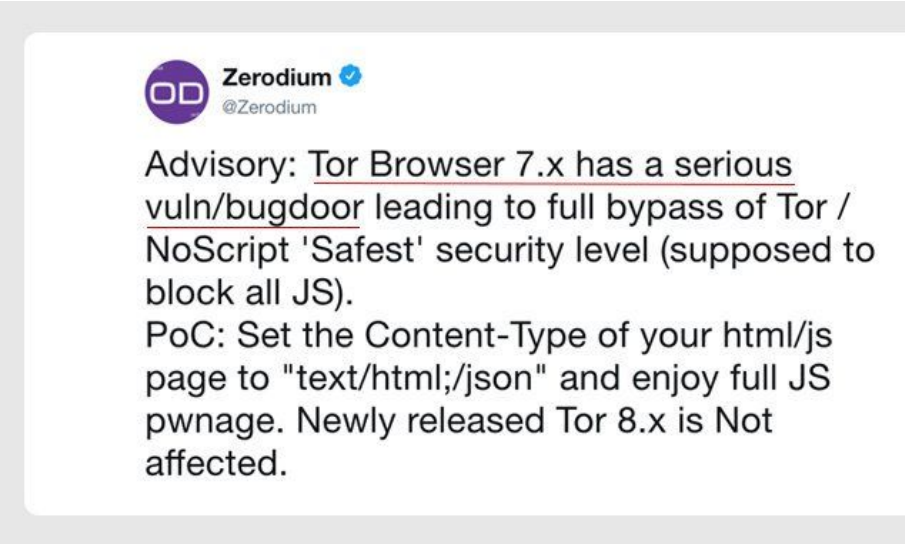
3.38 Analysis of relevant source code worryingly identified a number pre-processor directives of the form “#define SAFE_LIBRARY_memcpy(dest, destMax, src, count) memcpy(dest, src, count)”, which redefine a safe function to an unsafe one, effectively removing any benefit of the work done to remove the unsafe functions in the source code. There are also directives which force unsafe use of potentially safe functions, for example of the form “#define ANOTHER_MEMCPY(dest,src,size) memcpy_s((dest),(size),(src),(size))”.

Strategy: GCHQ Huawei Report

3.33 The report analysed the use of the commonly used and well maintained open source component OpenSSL. OpenSSL is often security critical and processes untrusted data from the network and so it is important that the component is kept up to date. In the first version of the software, there were 70 full copies of 4 different OpenSSL versions, ranging from 0.9.8 to 1.0.2k (including one from a vendor SDK) with partial copies of 14 versions, ranging from 0.9.7d to 1.0.2k, those partial copies numbering 304. Fragments of 10 versions, ranging from 0.9.6 to 1.0.2k, were also found across the codebase, with these normally being small sets of files that had been copied to import some particular functionality. There were also a large number of files, again spread across the codebase, that had started life in the OpenSSL library and had been modified by Huawei.

Bug Doors & Easy Exploitation

- Intentionally writing unsafe code
- Vulnerability is trivial to exploit
- Can be written off as a “mistake”
- No repercussions if patch introduces another bug
- Would appease Chinese state while bypassing Western review boards



Not Just Your Average Junk Device

- Issues like Telnet ports being left open are commonplace in IoT devices
- So are bad coding practices, undocumented/messy build chains, etc.

However

- Huawei is **exceptionally bad**
- Other devices aren't made by companies who are beholden to the Chinese Government

Source Code Review Fails

- The UK received uncompilable source code
- ***No*** guarantees that a binary or firmware blob running on purchased hardware matches source code
- Reversing firmware off the devices is time consuming but more accurate

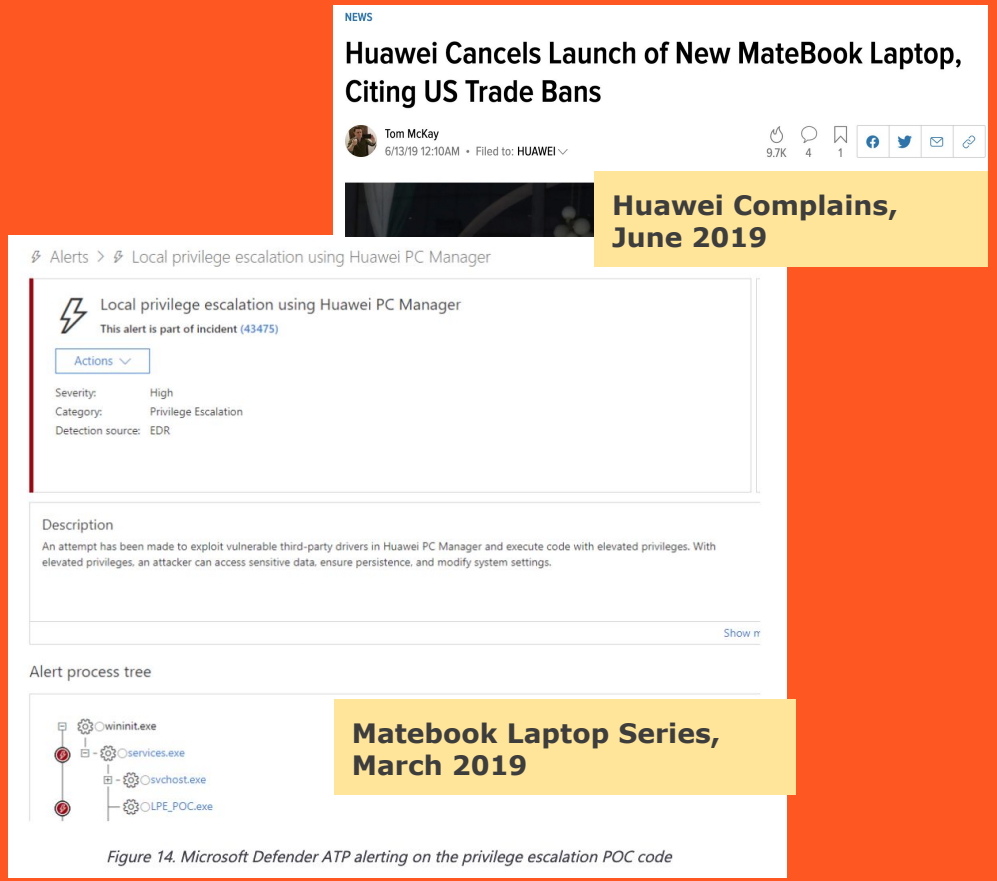


Figure 14. Microsoft Defender ATP alerting on the privilege escalation POC code

https://arstechnica.com/gadgets/2019/03/how-microsoft-found-a-huawei-driver-that-opened-systems-up-to-attack/

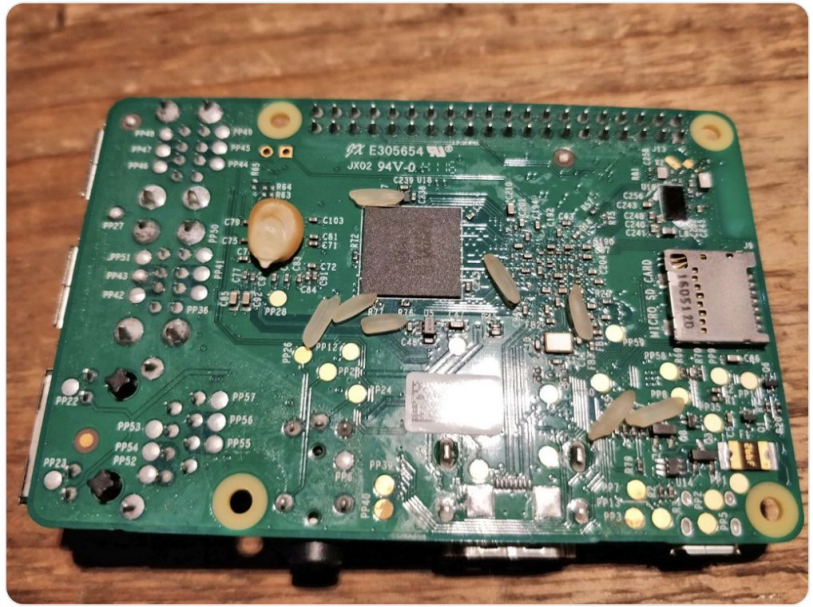
Hardware Backdoors

- As we learned from the SuperMicro case these are very hard to prove
- A true hardware backdoor is undetectable from factory swapping a cheap part
- If you control hardware fabrication you control the device

joernchen
@joernchen

Follow

Found some Chinese and one US backdoor on my raspi.



9:52 AM - 27 Oct 2018

237 Retweets **854** Likes

35 237 854

Unbounded Software Updates

- Operation ShadowHammer 2019
- Mystery why limited payload execution to 600+ ASUS victims
- Mystery where the victims MAC addresses collected from
- ShadowPad is one of the largest known supply-chain attacks, 2017
- Server management software product

MOTHERBOARD
TECH BY VICE

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

The Taiwan-based tech giant ASUS is believed to have pushed the malware to hundreds of thousands of customers through its trusted automatic software update tool after attackers compromised the company's server and used it to push the malware to machines.

By **Kim Zetter**

Mar 25 2019, 9:00am Share Tweet

IMAGE: SHUTTERSTOCK

TakeAways

- Risk mitigation is not only impossible but ridiculous
- Example of broader supply chain risk and global economy
- Policy decisions of this calibre **NEED** to be informed with a **COMPLETE** understanding of technical issues
- Mixing trade with national security
  - Not to be confused with bargaining chips
  - Undercuts the meaning of the ban
  - Protectionism in disguise

Case Study: Voting Infrastructure