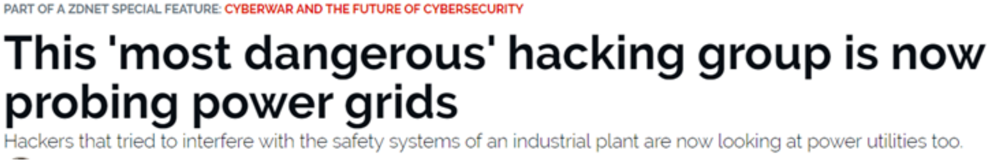
Combating Persistent Cyber Attacks: The Secure Flash-to-Cloud Approach

Naseem Aslam – Sr. Manager Product Marketing, Cypress Semiconductor
Yoni Kahana – VP Customers, NanoLock Security

Security is a Growing Concern

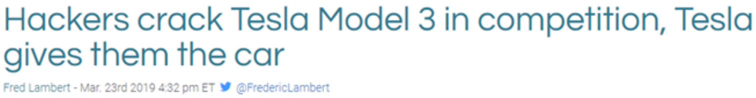


PART OF A ZDNET SPECIAL FEATURE: CYBERWAR AND THE FUTURE OF CYBERSECURITY

This 'most dangerous' hacking group is now probing power grids

Hackers that tried to interfere with the safety systems of an industrial plant are now looking at power utilities too.

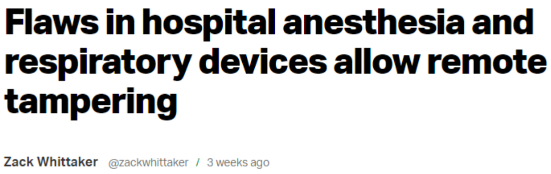
https://www.zdnet.com/article/this-most-dangerous-hacking-group/



Hackers crack Tesla Model 3 in competition, Tesla gives them the car

Fred Lambert - Mar. 23rd 2019 4:32 pm ET @FredericLambert

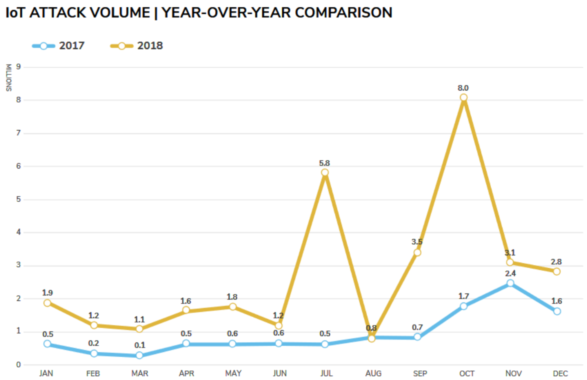
https://electrek.co/2019/03/23/tesla-model-3-hacker-competition-crack/



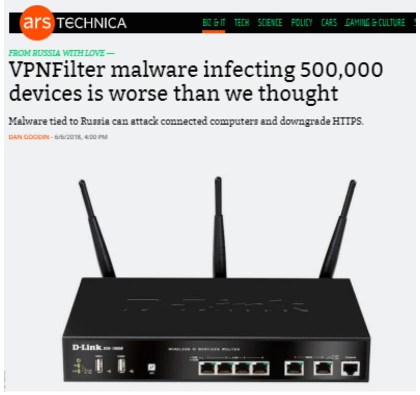
Flaws in hospital anesthesia and respiratory devices allow remote tampering

Zack Whittaker @zackwhittaker / 3 weeks ago

https://techcrunch.com/2019/07/09/flaws-anesthesia-respiratory-devices-tampering/



Source: SonicWall - 2019 Cyber Threat Report



FROM RUSSIA WITH LOVE —

VPNFilter malware infecting 500,000 devices is worse than we thought

Malware tied to Russia can attack connected computers and downgrade HTTPS.

DAN GOODIN - 6/6/2018, 4:00 PM

https://arstechnica.com/information-technology/2018/06/vpnfilter/

Connected systems present expanding security risks, and customers need an end-to-end security solution which includes a secure storage

nanolock

CYPRESS
EMBEDDED IN TOMORROW™

Requirements for Combating Persistent Cyber Attacks

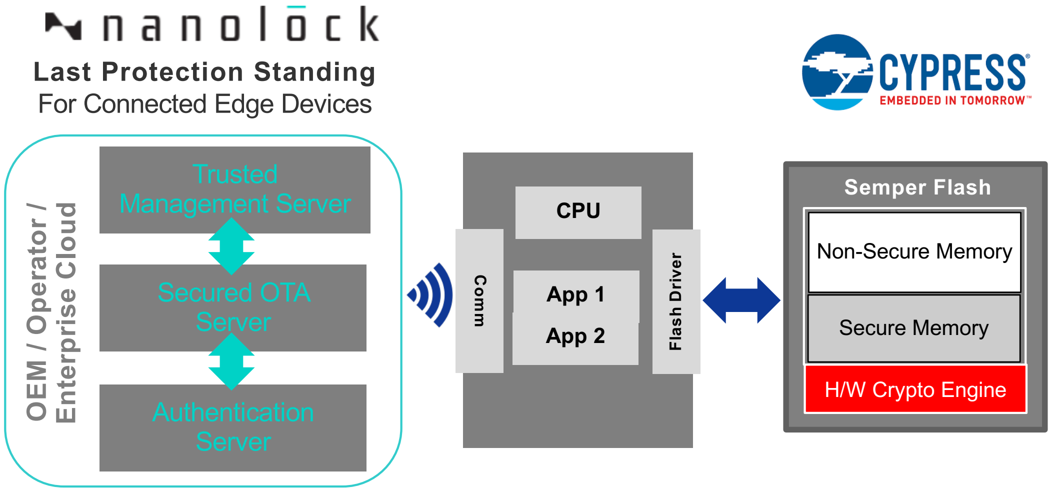
- **Real-time attack prevention of firmware manipulation** & reliable status and alerts
- **Prevent** outsiders, insiders and supply-chain attacks
- **Reliable OTA updates and status** through a root-of-trust
- **Big data analysis - Unique and trusted device analytics** to identify critical patterns and anomalies.

nanolock

CYPRESS
EMBEDDED IN TOMORROW™

Flash-to-Cloud Ironclad Solution

NanoLock + Cypress Ecosystem Partnership



Secure Flash Use Cases

- 🔒 Cryptographically secure storage of code, data, and system secrets (Keys, Certificates)

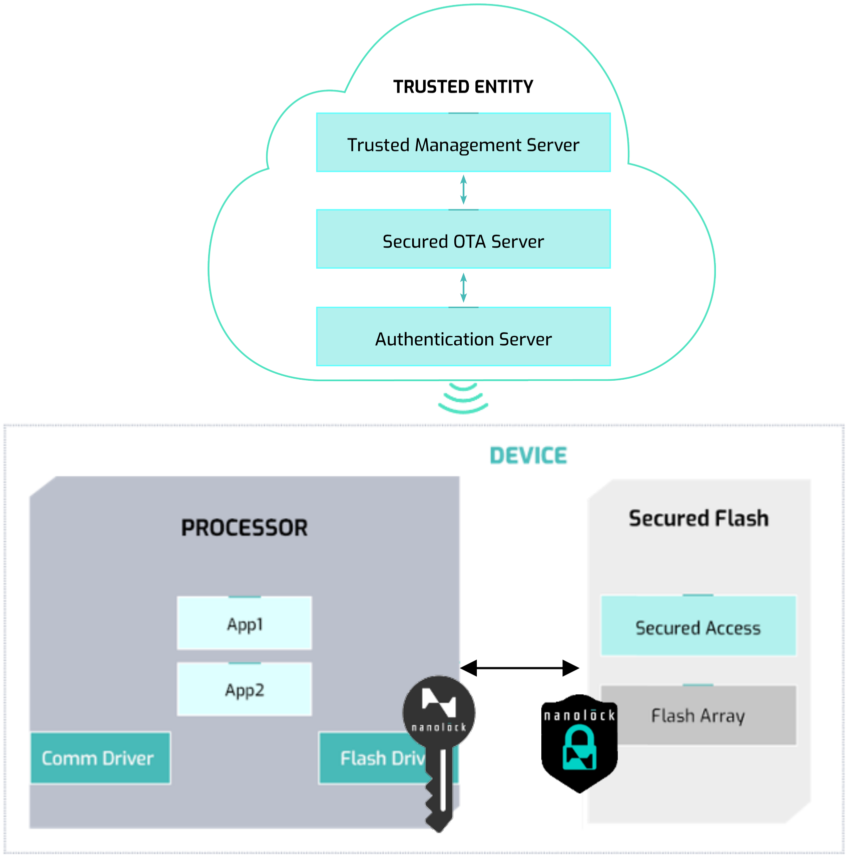
- Firmware over the air (FOTA) update between host, secure storage, and cloud

- Fast Secure boot for firmware authentication, version attestation and rollback protection

- Secure Provisioning in unsecure manufacturing facility and unsecure service center

The Innovation

Move the control from a vulnerable device to a **trusted entity in the customer's cloud**



Managed Flash

Lifetime

Embedded protection

No
additional BoM

zero power / resources /
memory constraints

nanolock

Flash-to-Cloud
Protection

Processor & operating
system agnostic

No performance hit

Wide Range of Applications

Automotive

Smart Cities & Security Cameras

Smart Meters

Connectivity

Flash Memory Summit

Automotive Use-Case

Customers are:
- OEMs
- TierI

- Working with major OEMs and Tier-1 in EU, Japan and USA
- Need to protect from insiders and outsiders
- Customers can enjoy:
  - Device level protection
  - Alerts and inside information on attack vectors
  - Secured updates

nanolock CYPRESS EMBEDDED IN TOMORROW™

Connectivity Use-Case

Customers are:

- Telcos
- Integrators
- Device makers

- Flash-to-Cloud protection stops the attacks even if there is unknown SW bug
- Easy integration with extended capabilities
- The customer can enjoy and present to the market:
  - Device protection
  - Alerts on multiple attacks
  - Operational benefit on versions installed

nanolock

CYPRESS EMBEDDED IN TOMORROW™

NanoLock

Last Protection Standing for Connected Edge Devices

- **Category leading customers** in Japan, Singapore, EU & USA
- **Offices** in Israel, USA & Japan
- **Strong IP** Portfolio

Company of the Year
MWC 2019

NETWORKWORLD FROM IDG

10 Hot IoT security
startups to watch

Startup of the Year
2018 IT World Awards

THANK YOU

Ironclad, Flash-to-Cloud Protection for critical assets