Trust & the Internet of Things

Cmd + Click to open video in a new tab

That was a replay attack.

feature :)

That was a ~~replay attack~~.

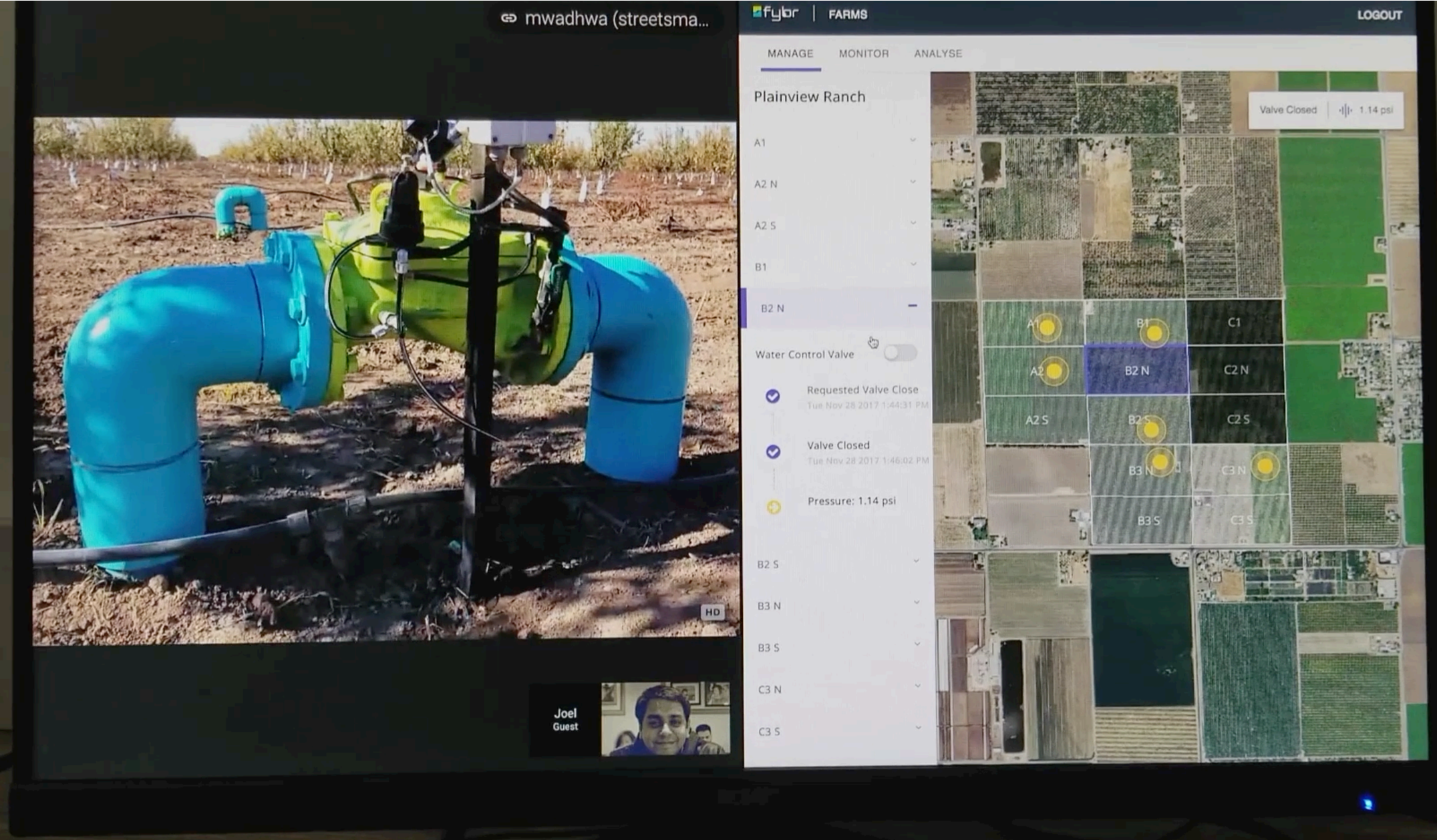
From the vendor's website:
"works with over 99% of garage door and gate opening systems"

feature :)

That was a ~~replay attack~~.

If you were building a system to log entry and exit from this garage, who sent that open command, the remote, the car or an attacker?

IoT is now mission-critical.



Cmd + Click to open video in a new tab

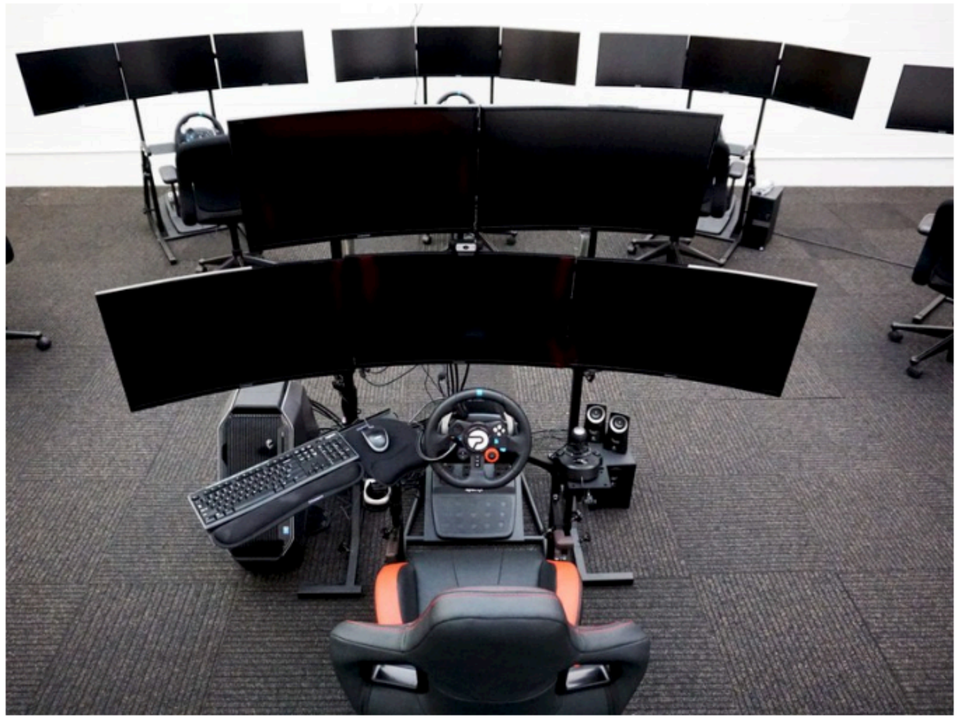
The farmer must always be able to trust data from sensors/controllers in the fields.

The remote driver must always be able to trust the data from the sensors/controllers in the car.

WIRED SUBSCRIBE

ALEX DAVIES TRANSPORTATION 02.01.18 07:00 AM

SELF-DRIVING CARS HAVE A SECRET WEAPON: REMOTE CONTROL



Phantom Auto plans to establish call centers where a few humans will keep watch over a fleet of someone else's robocars. If one gets in trouble, a human can use a steering wheel and pedal combo to do whatever needs doing. PHANTOM AUTO

Such mission critical applications are not viable unless the confidence in the source and integrity of data is extremely high.

Trust begins with knowing the source of a piece of data and being able to verify that the data, you would base your decisions on, is exactly what that source sent.

Majority of currently deployed IoT devices are not trustworthy.

Deloitte. Insights | Industries | Topics | Economics | Multimedia | Deloitte Review | Regions | Search

Article

January 21, 2016

The power is on: How IoT technology is driving energy innovation

The Internet of Things in the electric power industry

Rob Young John McCue Christian Grant

As conservation efforts and alternative energy ramp up, electric utilities can no longer count on customers using more and more power. How to survive? With a new focus on efficiency and cost control, based on technology—particularly Internet of Things applications.

27TH USENIX SECURITY SYMPOSIUM

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

Authors:
Saleh Soltan, Prateek Mittal, and H. Vincent Poor, *Princeton University*

Abstract:
We demonstrate that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid. In particular, we reveal a new class of potential attacks on power grids called the Manipulation of demand via IoT (MadIoT) attacks that can leverage such a botnet in order to manipulate the power demand in the grid. We study five variations of the MadIoT attacks and evaluate their effectiveness via state-of-the-art simulators on real-world power grid models. These simulation results demonstrate that the MadIoT attacks can result in local power outages and in the worst cases, large-scale blackouts. Moreover, we show that these attacks can rather be used to increase the operating cost of the grid to benefit a few utilities in the electricity market. This work sheds light upon the interdependency between the vulnerability of the IoT and that of the other networks such as the power grid whose security requires attention from both the systems security

Make a contribution | Subscribe | Search jobs | Sign in

The Guardian

News | Opinion | Sport | Culture | Lifestyle

US | World | Environment | Soccer | US midterms 2018 | Business | Tech | Science

Smart homes

Smart electricity meters can be dangerously insecure, warns expert

Hackers can cause fraud, explosions and house fires, and utility companies should do more to protect consumers, conference told

McAfee Together is power. | Securing Tomorrow. Today.

McAfee ATR Team Discovers New IoT Vulnerability in Wemo Insight Smart Plugs

By Gary Davis on Aug 21, 2018

From connected baby monitors to smart speakers — IoT devices are becoming commonplace in modern homes. Their convenience and ease of use make them seem like the perfect gadgets for the whole family, but their poor security standards also make them conveniently flawed for someone else: cybercriminals. As a matter of fact, our McAfee Labs Advanced Threat Research team has uncovered a flaw in one of these IoT devices: the Wemo Insight Smart Plug, which is a Wi-Fi–connected electric outlet.

SMART HOME

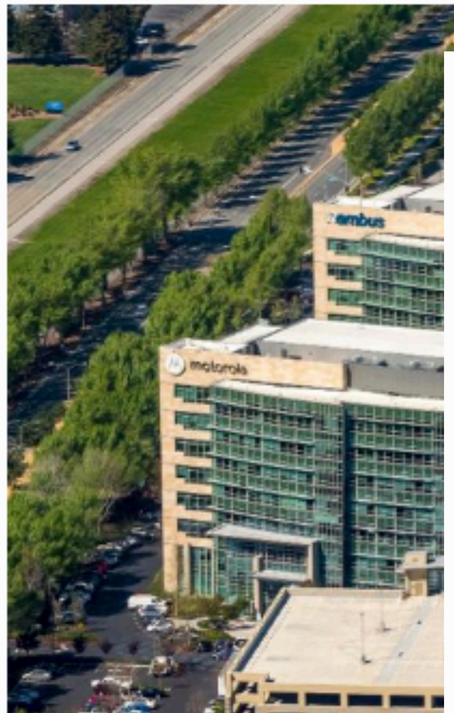
Here's what happened when someone hacked the August Smart Lock

Worried about smart lock security? A recent vulnerability shows that smart lock makers still have a lot to learn.

BY MEGAN WOLLERTON | AUGUST 25, 2016 5:00 AM PDT

Google's Doors Hacked By Own Employee

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.



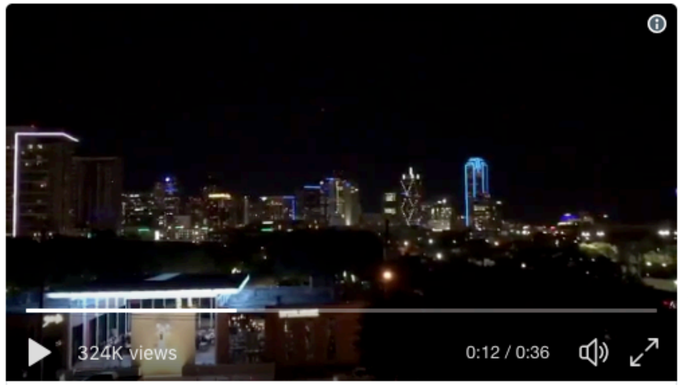
Last summer, when Tomaschik looked at the encrypted messages the Software House devices (called iStar Ultra and IP-ACM) were sending across the Google network, he discovered they were non-random; encrypted messages should always look random if they're properly protected. He was intrigued and digging deeper discovered a "hardcoded" encryption key was used by all Software House devices. That meant he could effectively replicate the key and forge commands, such as those asking a door to unlock. Or he could simply replay legitimate unlocking commands, which had much the

The Washington Post
Democracy Dies in Darkness

The Intersect

Someone hacked every tornado siren in Dallas. It was loud.

By **Avi Selk**
April 9, 2017

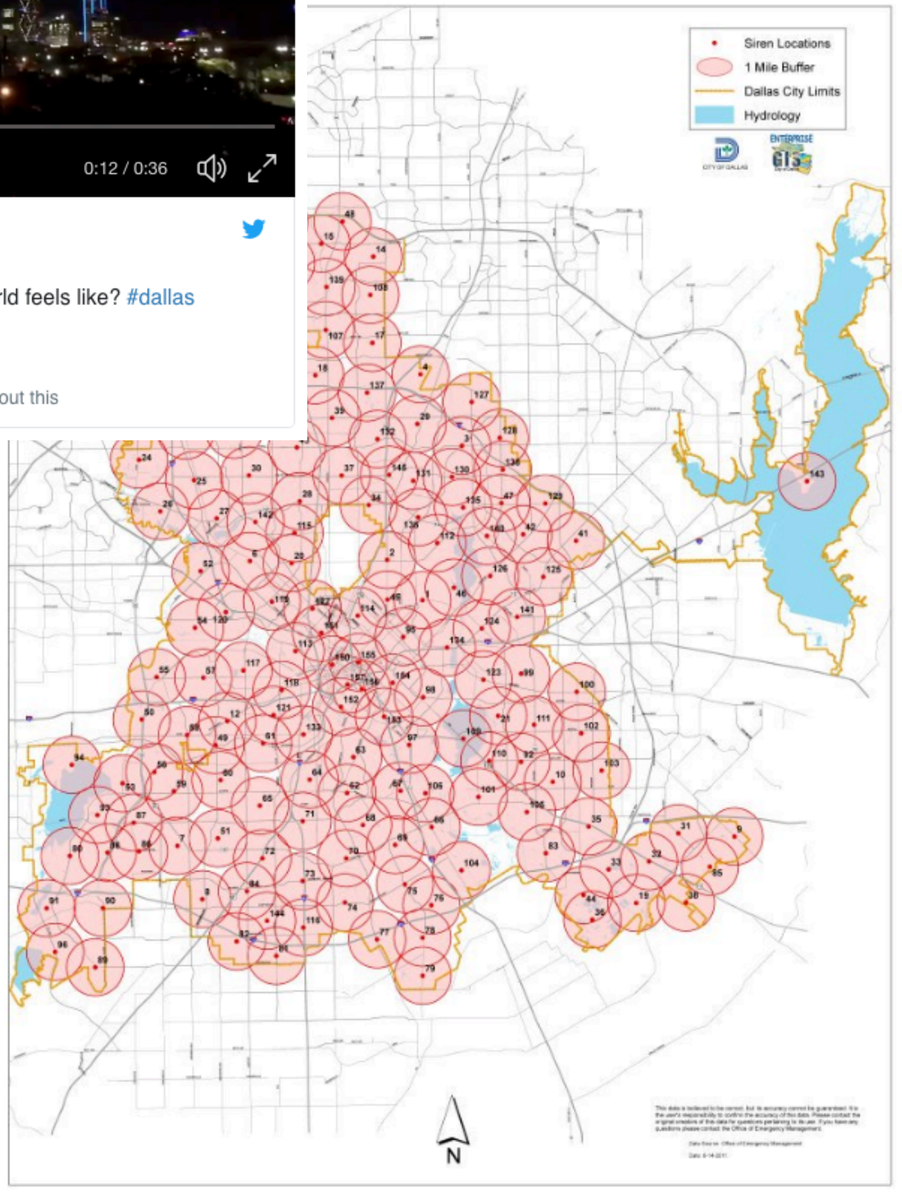


ManicPixieDreamGay
@deadlyblonde

Ever wonder what the end of the world feels like? #dallas #sirens

10:10 PM - Apr 7, 2017 · Dallas, TX

♡ 2,485 💬 2,120 people are talking about this



NEWS APR 2017

Culprit broadcast signal that triggered Dallas' emergency sirens Friday night

Robert Wilonsky, City Columnist

It is becoming easier, cheaper, lucrative and attractive to attack IoT.

Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

RECORDED FUTURE BLOG

Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018

By Priscilla Moriuchi and Sanil Chohan on April 5, 2018

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 10.20.17 05:45 PM

THE REAPER IOT BOTNET HAS ALREADY INFECTED A MILLION NETWORKS

7 Variants (So Far) of Mirai

Mirai is an example of the newest trend in rapidly evolving, constantly improving malware. These seven variants show how threat actors are making bad malware worse.

root xc3511	user user	guest 12345	root ikwb
root vizxv	admin (none)	admin1 password	root dreambox
root admin	root pass	administrator 1234	root user
admin admin	admin admin1234	666666 666666	root realtek
root 888888	root 1111	888888 888888	root 00000000
root xmhdipc	admin smcadmin	ubnt ubnt	admin 1111111
root default	admin 1111	root klv1234	admin 1234
root juantech	root 666666	root Zte521	admin 12345
root 123456	root password	root hi3518	admin 54321
root 54321	root 1234	root jvbzd	admin 123456
support support	root klv123	root anko	admin 7ujMko0admin
root (none)	Administrator admin	root zlxx.	admin 1234
admin password	service service	root 7ujMko0vizxv	admin pass
root root	supervisor supervisor	root 7ujMko0admin	admin meinsm
root 12345	guest guest	root system	tech tech

> ***MIRAI was able to infect over 600,000 IoT devices by simply exploiting a set of 64 well-known default IoT login/password combinations.***

From July to September 2017, SecurityScorecard identified 34,062 IPv4 addresses on the public internet that showed symptoms expected from an embedded device infected with the Mirai IoT malware. This contrasts with 184,258 IPv4 addresses of IoT devices infected with Mirai IoT malware from August 1, 2016, to July 31, 2017.

MOTHERBOARD Moveable Hacking Environment

NEWS | By Lorenzo Franceschi-Bicchierai | Aug 7 2016, 7:00am

Hackers Make the First-Ever Ransomware for Smart Thermostats

White hat hackers have made the first proof of concept for malware that locks a smart thermostat and demands a ransom.

WIRED The Untold Story of NotPetya, the Most Devastating Cyberattack in SIGN IN | SUBSCRIBE

MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Victoria

Traffic cameras in Victoria infected by WannaCry ransomware

State government says 55 cameras were affected after a contractor introduced the virus to the system by mistake

CSO FROM IDG INSIDER Sign In | Register

Report: IoT is the next frontier for ransomware

The growth of the Internet of Things will offer new ransomware opportunities for cybercriminals, according to a report released Thursday by Symantec

THE COST OF NOTPETYA

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

$188,000,000

Snack company Mondelez (parent company of Nabisco and Cadbury)

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$10 BILLION

Total damages from NotPetya,

ANDY GREENBERG SECURITY 09.10.18 01:00 PM

HACKERS CAN STEAL A TESLA MODEL S IN SECONDS BY CLONING ITS KEY FOB

work, the KU Leuven team discovered in the summer of 2017 that the Tesla Model S keyless entry system, built by a manufacturer called Pektron, used only a weak 40-bit cipher to encrypt those key fob codes.

The researchers believe their attack might also work against cars sold by McLaren and Karma and motorcycles sold by Triumph, which also use Pektron's key fob system.

NEWS | By Lorenzo Franceschi-Bicchierai | Jun 4 2015, 11:01am

This Kids' Toy Can Hack Garage Doors in Seconds

Open Sesame!

All it takes to hack and open some remotely-controlled garage doors is a slightly modified pink texting toy—and less than ten seconds.

Regulation will get stringent.

TC

California passes law that bans default passwords in connected devices

Zack Whittaker @zackwhittaker / 3 weeks ago Comment

MANAGE

What does the GDPR mean for IoT?

Intelligent Machines

For safety's sake, we must slow innovation in internet-connected things

That's the view of security expert Bruce Schneier, who fears lives will be lost in a cyber disaster unless governments act swiftly.

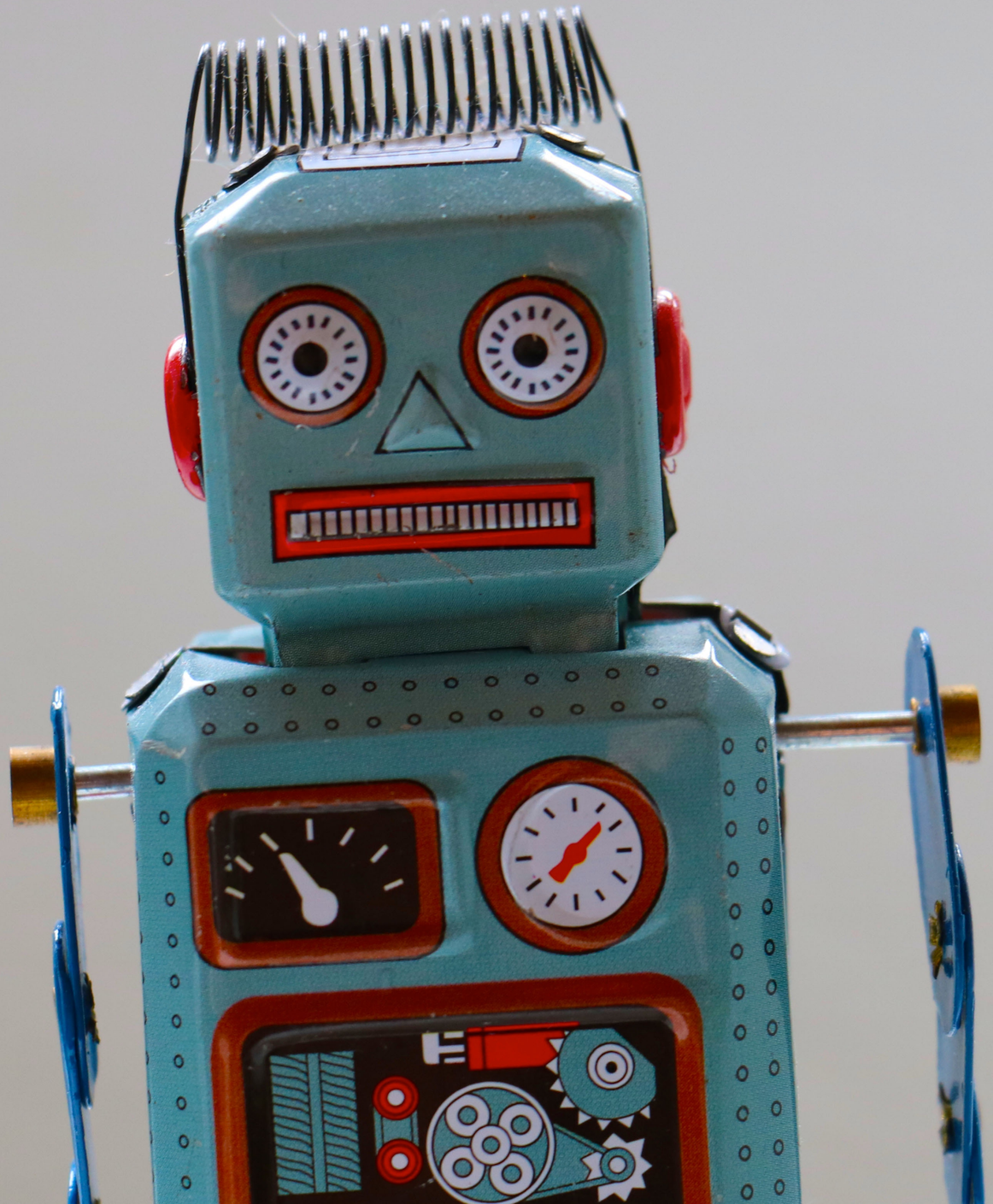
by Martin Giles September 6, 2018

AN RONG XU

How can we build a reliable and trustworthy IoT for our customers?

Trust begins with knowing the source of a piece of data and being able to verify that the data, you would base your decisions on, is exactly what that source sent.

Who am I?



Machine identity is hard.

- Every device, among billions, must be uniquely identifiable.
- Every device must have unique cryptographic keys that it can use to sign all data it produces.
- These cryptographic keys must be stored in secure hardware, like a TPM, that can run cryptographic operations in hardware. This way the secret keys never leave the hardware and cannot be stolen remotely using firmware vulnerabilities.
- There should be a record of exactly what hardware makes up a specific device.
- There should be a record of exactly what firmware is installed in a device and signed acknowledgments for every firmware update that is applied.
- Every message from a device must be cryptographically signed.

And a lot more.

We, the IoT community, must work together to drastically simplify device identity provisioning and management.

Several parties are involved in the life of a device.

The designer, contract manufacturers, component manufactures, shipping companies, auditors, warehousing, retail, installers, owner, end user, 2nd-hand user and more.

SEMICONDUCTOR ENGINEERING

"Complexity is one dimension of the challenge," said Marc Canel, vice president of security systems and technologies at Arm. "There is a layering of technologies, from the physical IP, in which the key that will make the root of trust is embedded, all the way up to the application and everything in between. There also is complexity in the processes to build all of these things, to provision them, to load the code and to load the keys. One of the big challenges is there is no standardization across the overall IoT world."

Blockchain

A decentralized system that combines techniques from the fields of cryptography, economics and distributed systems to enable trust amongst several parties.

Immutable, digitally signed, verifiable attestations about the life of a device.

We can then answer ...

- Was the device made by a reputable manufacturer?
- Does the device have hardware based cryptography and secure key storage?
- Does the device have unique identity and cryptographic keys?
- Has the device been audited by a security auditing firm? Is there a signed audit proof?
- Are there any known vulnerabilities for the device hardware/software?
- Does the device produce signed data and signed firmware acknowledgements?
- Does the device have the latest firmware?
- Who installed the device? Who provisioned the device?

etc.

This auditable, signed history of a device that no one party can manipulate becomes the foundation of trust in data from that device.

We can use it to derive a trust score.

On this foundation of identity
and trust, we can build …

Safe, mutually signed and
acknowledged firmware updates.

Secure, automated device on-boarding.

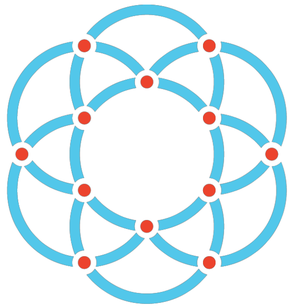
Reliable, mission critical applications.

Interoperability Protocols.

Machine to Machine realtime transactions and micro-payments.

Crypto-economic incentives and disincentives.

Autonomous Systems.



Ockam

Mrinal Wadhwa
Co-Founder & CTO

ockam.network

@mrinal