Ofer Shezaf
Blogging at http://www.xiom.com

Who can hack a plug?

The InfoSec risks of charging electric cars

About me

<u>What I do for a living?</u>

- Product Manager, Security Solutions, HP ArcSight
- Led security research and product management at Breach Security & HP Fortify

<u>I am passionate about security after hours as well:</u>

- OWASP leader and founder of the Israeli chapter
- Leads the Web Application Firewall Evaluation Criteria project
- Wrote the ModSecurity Core Rule Set
- But I am a defender and not a hacker. I am too old for that. Everything in this presentation is taken from public sources.

Fun fact: the closest airport to my house is in Damascus, Syria

We are in the right city!

Agenda

Plugs	**Why smart charge?**	The electric car and the smart grid
	How to charge smartly?	Architecture and functionality of charge stations
Security	**What can go wrong?**	Vulnerabilities and incidents
	What should we care?	The risk
	What should we do?	Solutions
Philosophy	**Hacking the internet of things**	
	Why doesn't it happen more?	

Smart charging electric cars

Why not just plug to the wall?

Are there plugs on the streets?

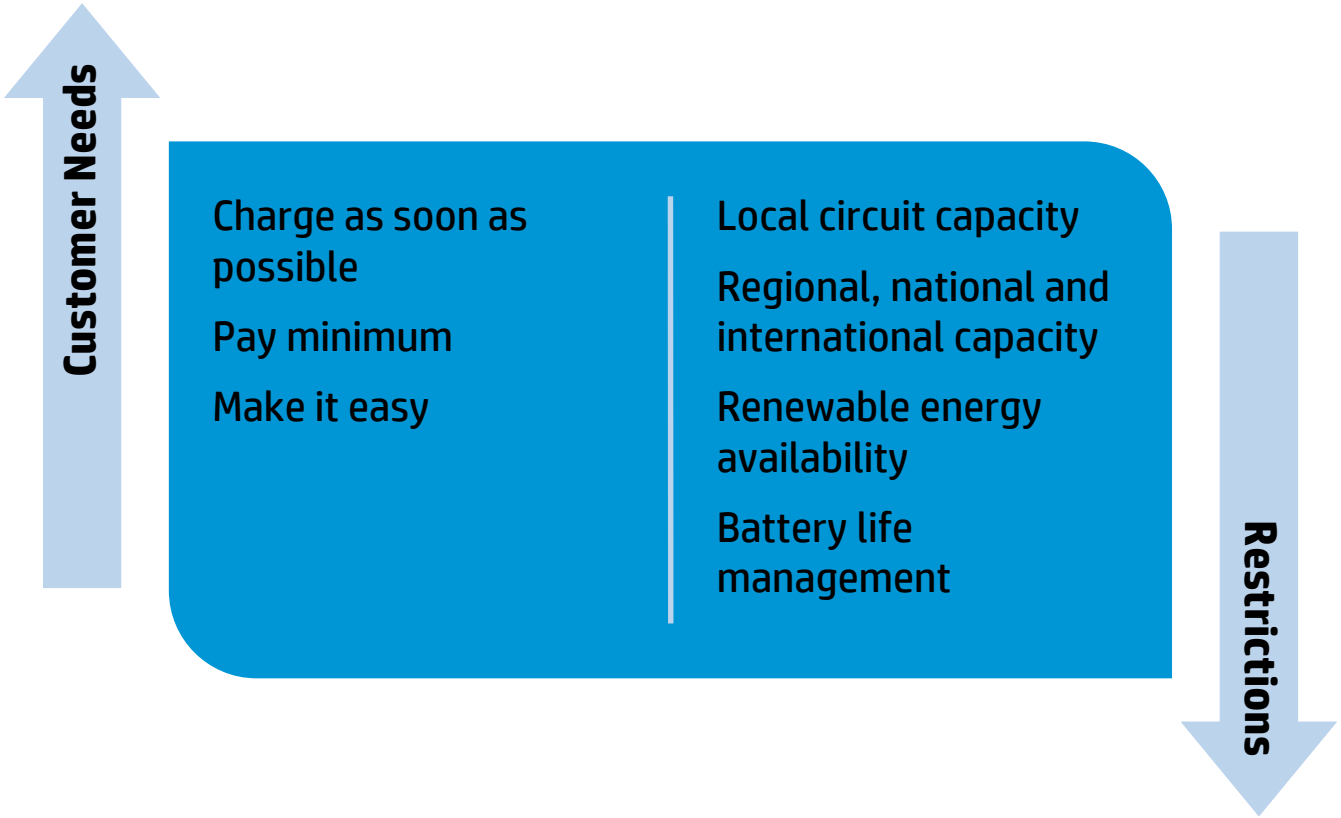
And if there were, who will pay for the power?

Is there enough power for all cars?

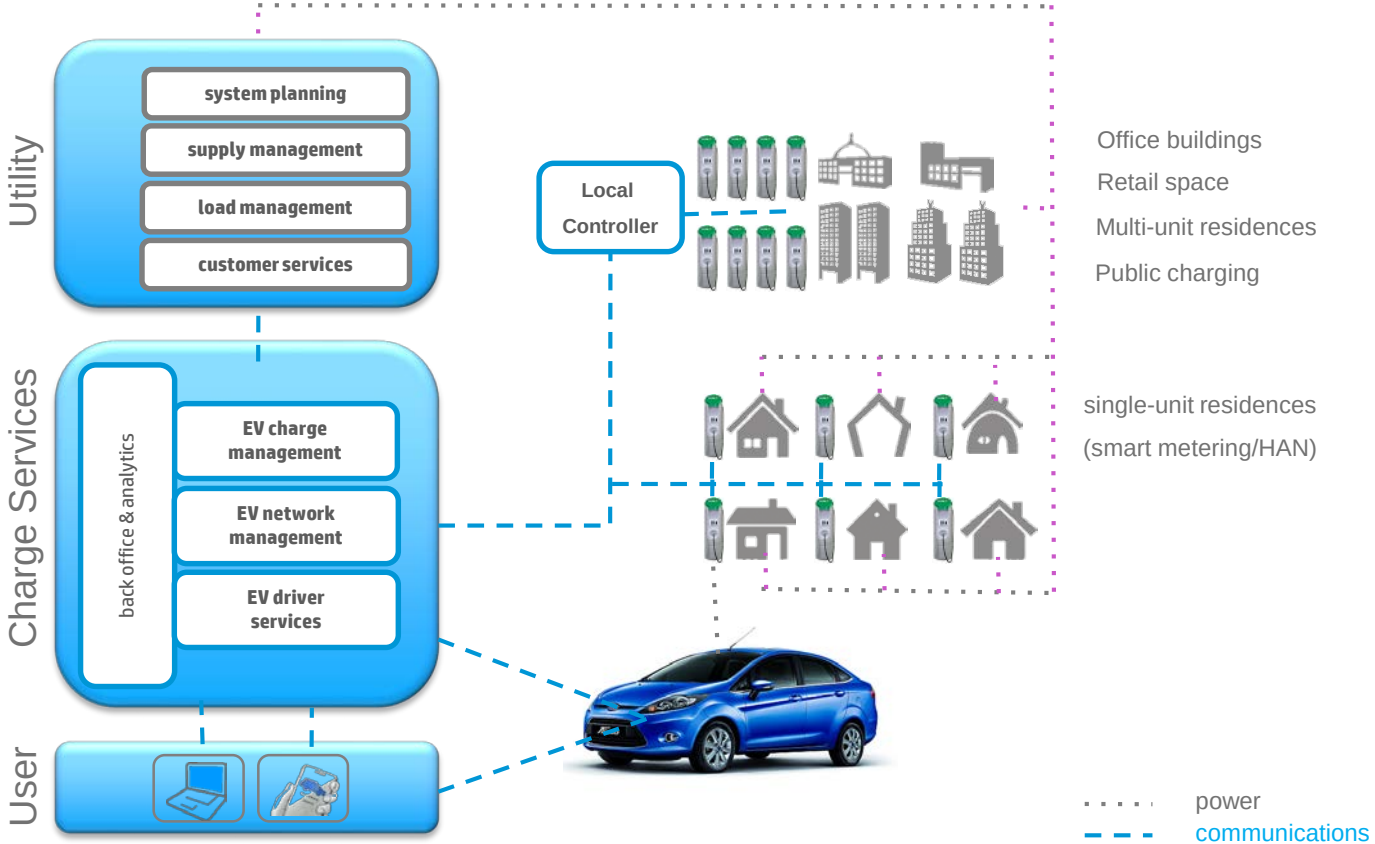
In a building? In the country?

Are electric cars really green?

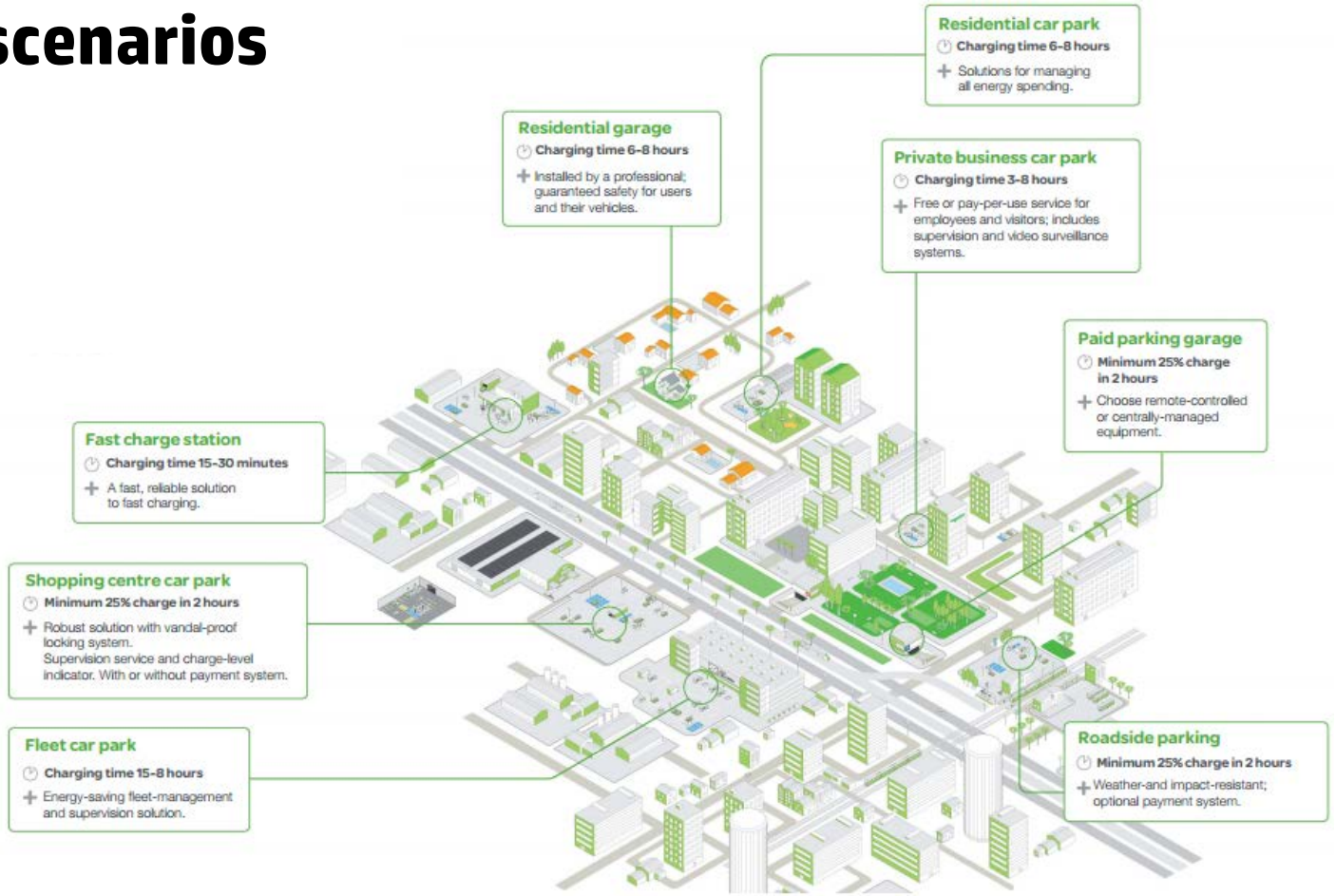
When is renewable energy available?


Customer Needs
Charge as soon as possible
Pay minimum
Make it easy
Local circuit capacity
Regional, national and international capacity
Renewable energy availability
Battery life management
Restrictions

So we need to smart charge

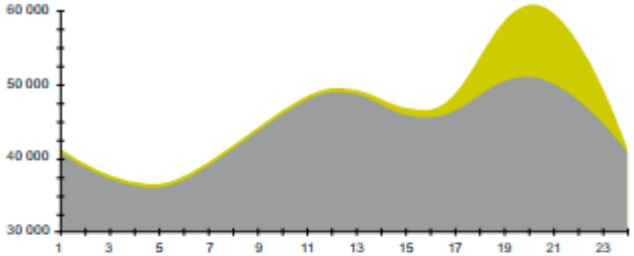


Charge scenarios

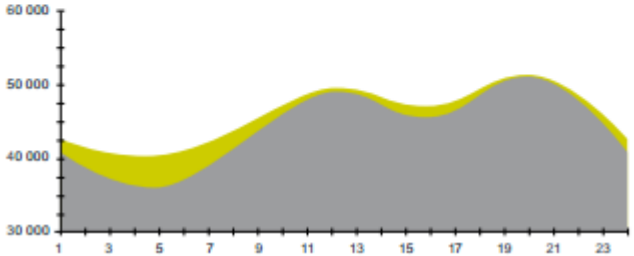


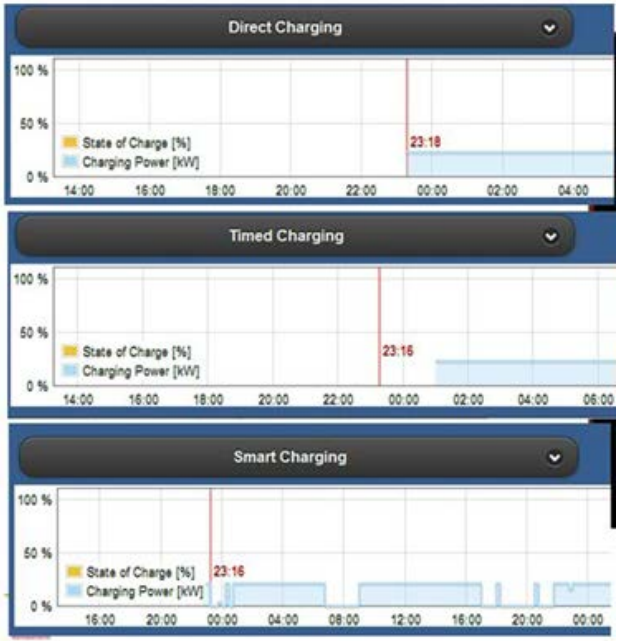
Charge plans

Without smart system



With smart system





Charge stations

A computer on the street

Brushed stainless steel component housing design allows for pedestal or wall mounted installations

Indestructible and identifiable stainless steel component housing

Designed to be safe, secure and meet or exceed all standards for charging station equipment

Durable concrete pedestal prevents the need for concrete bollards, is ADA compliant and is designed for vehicle bumper heights

Eight inch weatherproof, sunlight readable LCD touch screen

Card reader allows multiple types of access

Dual level 2 (208V/30A) charging ability with SAE J1772 connectors

Highly visible coiled cords prevent trip hazards, damage and misplacement of cords

Component by component

Electronics

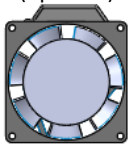
Electrical

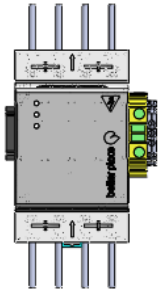
UI – LCD, LEDs, Buzzer

GSM/WiFi/ZigBee/RS

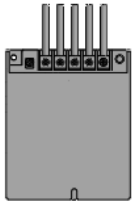
Main PCB

Fan
(optional)

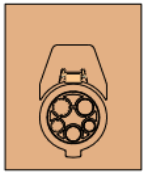




Metering, GND
Terminal, CP
Terminal



PSU,
RCD



Smart
Socket

Actually a network

Architecture	Power	Charging access
Stand-alone	Individual	Open-access

Recommended for:
- Residential use
- Commercial applications for small business, hotel and shopping centre car parks

Architecture	Power	Charging access
Stand-alone	Individual	Open-access

Recommended for:
- Commercial applications such as business, hotel and shopping centre car parks

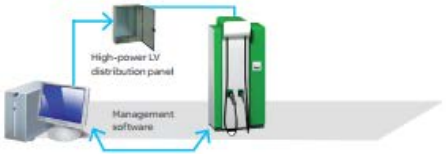
Architecture	Power	Charging access
Multi-point	Managed	Open-access

Recommended for:
- Commercial applications such as vehicle fleet, medium/large sized businesses, hotels and amenity car parks.

Architecture	Power	Charging access
Multi-point	Managed	Restricted-access

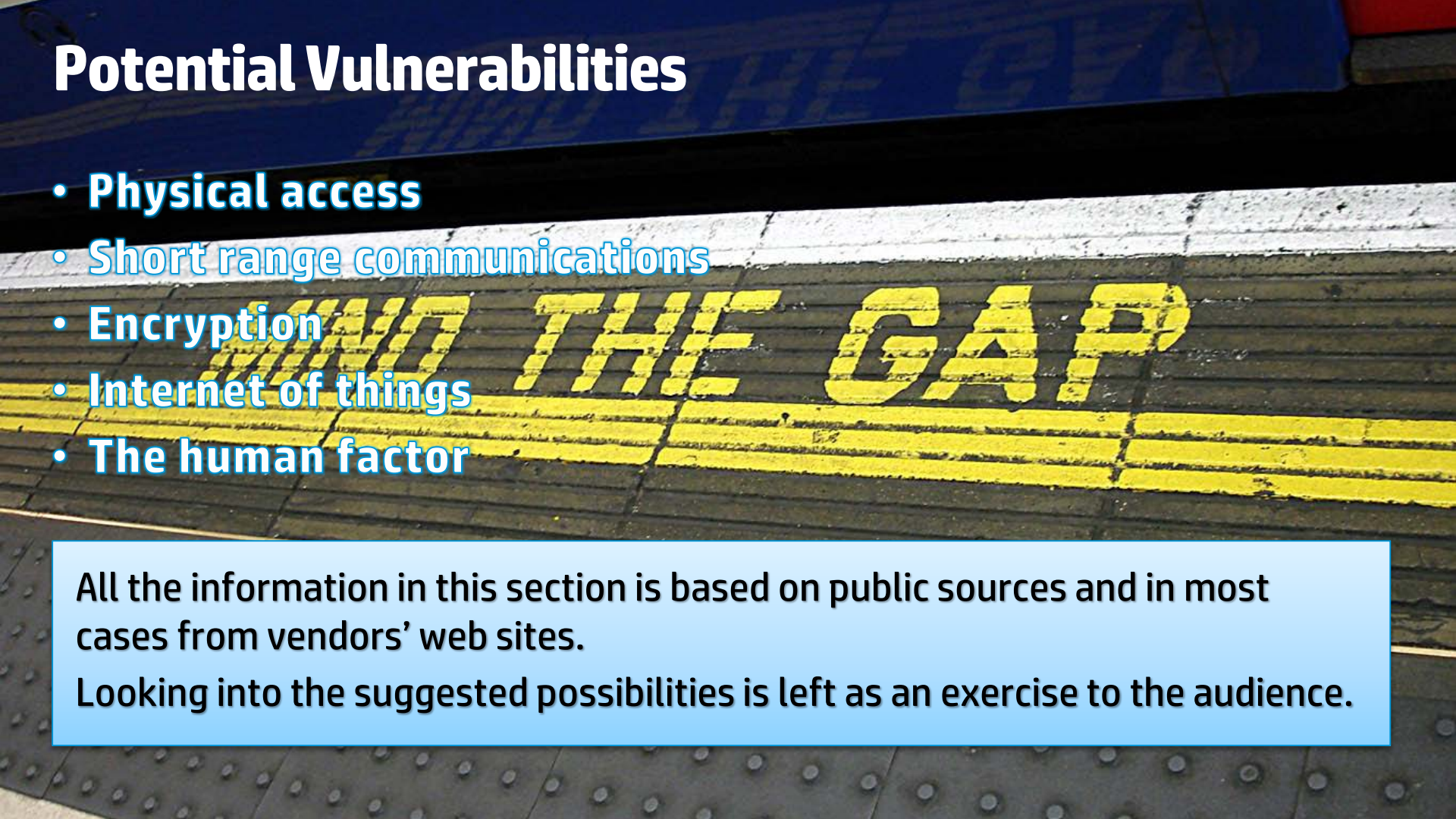
Recommended for:
- Roadside charging application
- Commercial parking garages
- Commercial applications such as vehicle fleet, business, hotel and shopping centre car parks

Architecture	Power	Charging access
Stand-alone	Managed	Restricted-access or pay-per-use



Recommended for:
- Fast charging applications such as motorway service areas, fleet managers and other strategic locations

Potential Vulnerabilities



- Physical access
- Short range communications
- Encryption
- Internet of things
- The human factor

All the information in this section is based on public sources and in most cases from vendors' web sites.

Looking into the suggested possibilities is left as an exercise to the audience.

Physical access

What is it?

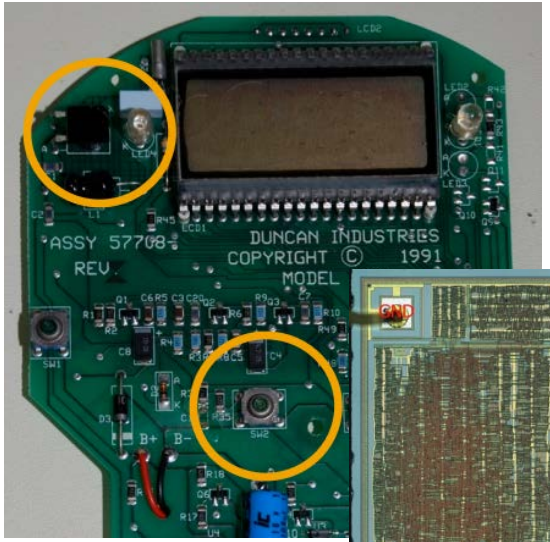
Take apart system to:

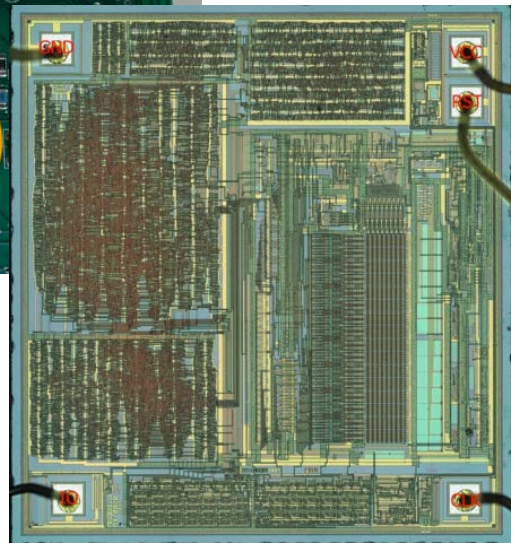
- Determine components
- Extract firmware and EEPROM
- Analyze and debug firmware

Either of the street or purchased from vendor

Potential vulnerabilities:

- Convenient eavesdropping points
- Get encryption keys
- Analyze RFID, car or control center encryption
- Analyze car/control center protocol and determine vulnerabilities





Images:
Grand et al,
Parking meter hacking,
BlackHat 2009

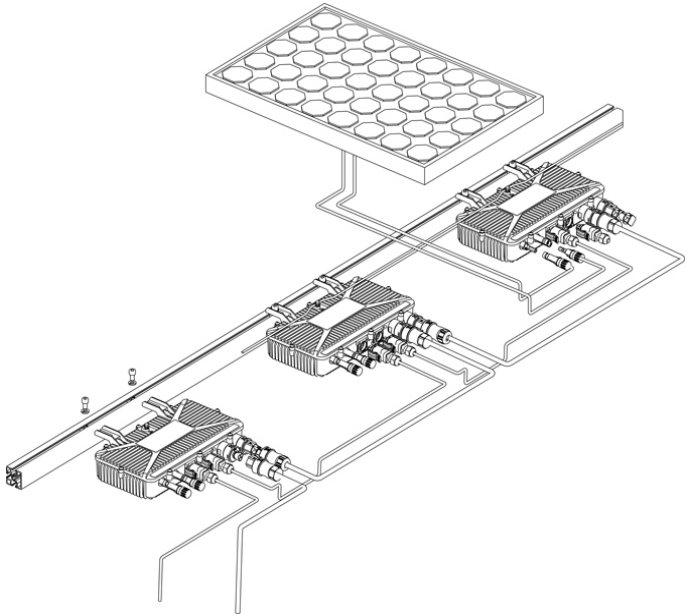
Short range communications: RS-485

What is it?

- Multi-drop serial protocol enables single data cable across all charge stations.
- Very low bandwidth and high latency due to multiplexing and range (100KBs shared by all nodes at 1200m bus)
- ModBus commonly used as data protocol and has no inherent security,

Potential Vulnerabilities

While it all depends on the application, bandwidth and latency limits encryption and makes eavesdropping and man in the middle attacks simple.



Short range communication: RFID

How is it used?

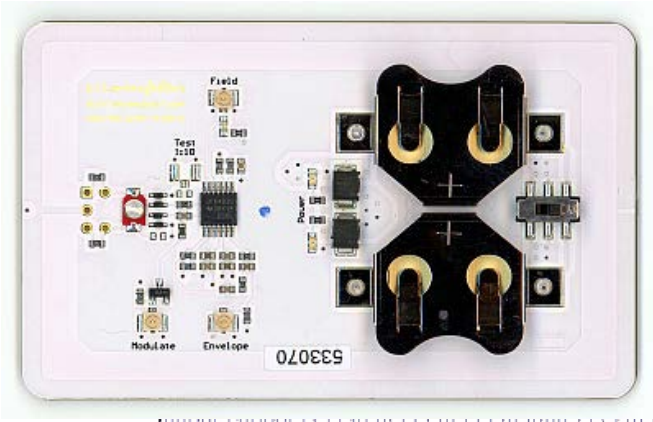
Several standards used

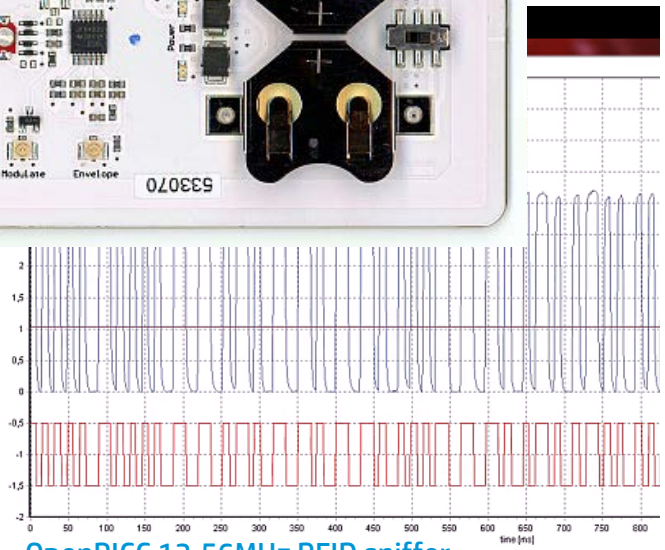
- ISO 14443 can be secured, but is not always.
- ISO 15693 is cheaper and has longer range but provides little security.
- Older 125KHz cards have no security.

Standards do not determine application

Potential vulnerabilities

- **Easy to eavesdrop:** authentication is secured but not identification.
- **Extremely costly to patch**
- **Encryption…** on next slide





OpenPICC 13.56MHz RFID sniffer

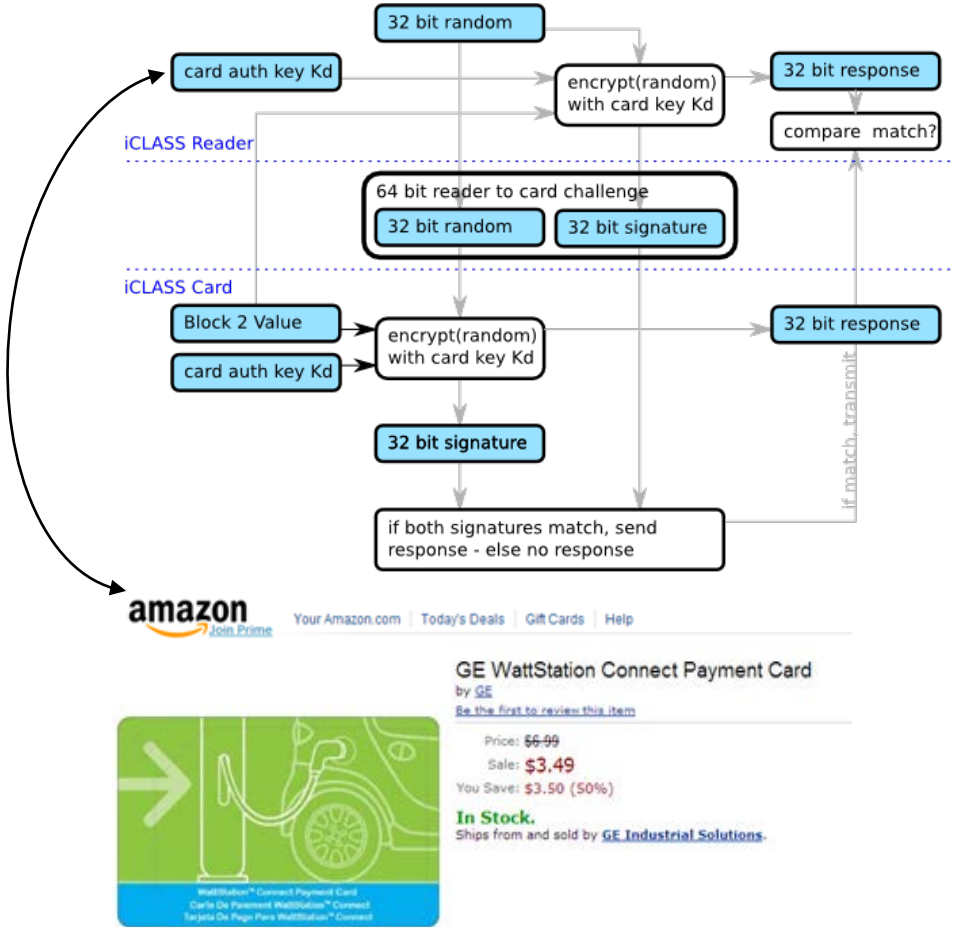
Encryption: RFID

How is it used?

- Application either a stored value or identification
- Commonly employs protected memory using symmetric keys.

Potential vulnerabilities

- **Same symmetric key used for all stations and cards:** does not scale and open to relay and card attacks.
- **Different symmetric keys require connectivity.**
- **Weak cryptography**
- **That is if keys are used…**



Internet of things: protocols

Charge station to central management

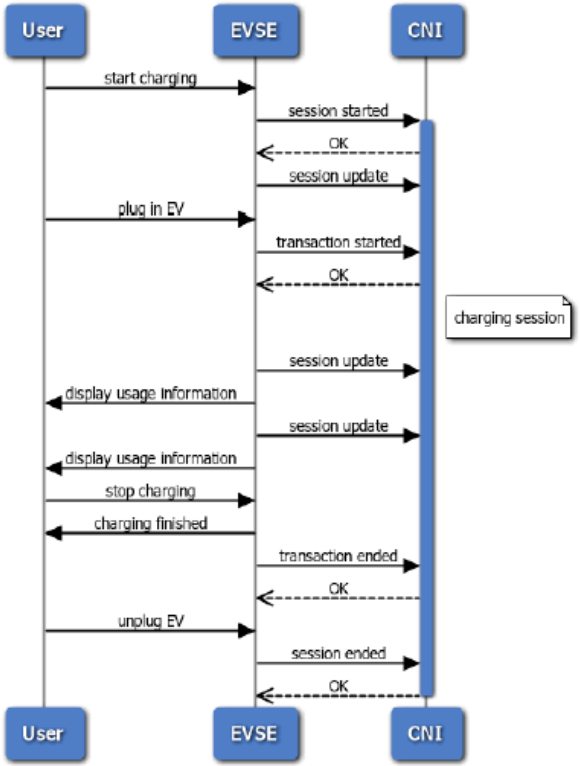
- Identification, starting and stopping a charge transaction
- Reservations
- Maintenance: Setup, heartbeat, Configuration, Firmware Updates, Errors and diagnostics

Car to charge station

- Negotiate current
- Identification

Potential vulnerabilities

- Security by obscurity
- Trust in end points
- SSH and SNMP used extensively for management



Internet of things: web and mobile control

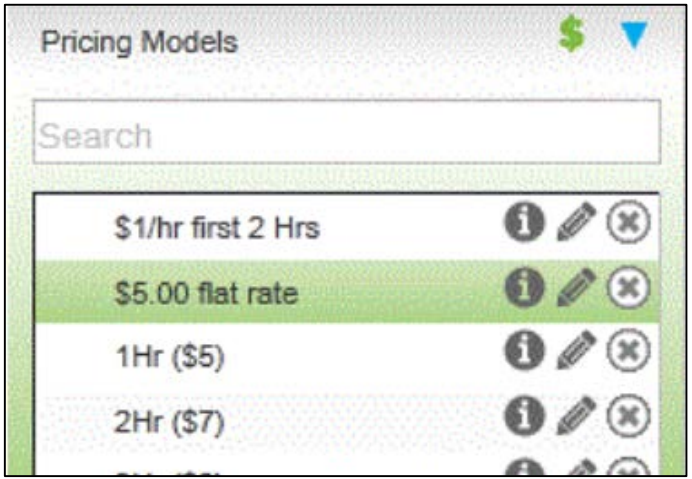
For charge station owners:

- Configure stations (max current allowed…public or not…)
- Set pricing and manage transactions
- Start/stop charging
- Accounts and RFID cards management
- Manager transactions

For drivers:

- Pay and manage payments
- Start/stop charging
- Connect RFID cards

Potential vulnerabilities? Kidding me…



Setting up user credentials for Web Services

Follow these steps to set up your WattStation Connect credentials and start using the Web services:

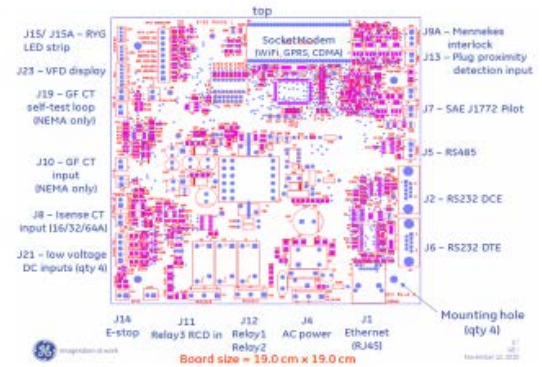
1. Go to www.gewattstation.com
2. Click **Register** to create a new WattStation Connect user account. If you have an existing account, you simply log in with your username and password.

Now you can access all web services provided by WattStation Connect by passing your credentials to each Web service call.

Human factor: deployment and maintenance

Configuring is sometimes as simple as:

- Open the box
- Place a DIP switch to configuration mode
- Connect Ethernet cross cable to the Ethernet port
- Fire a browser and connect to 192.168.2.2
- I wonder what you can get to outside of a browser?



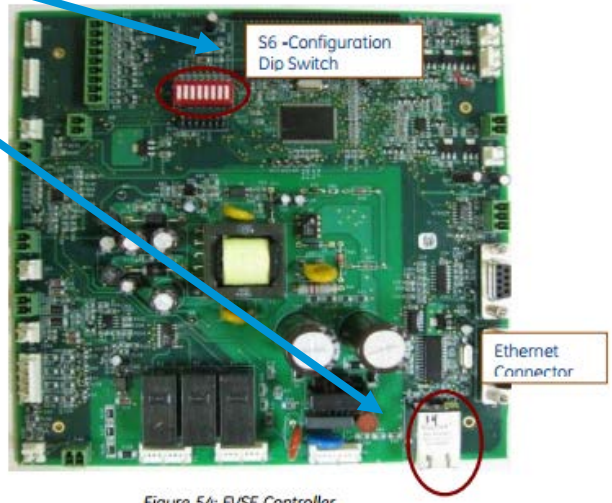


Figure 54: EVSE Controller

Risks & Scenarios

- Denial of (energy) services
- Stealing
- Privacy infringement
- ...and...

As EV charging is still in infancy, to the best of my knowledge no incident have been reported yet. The example below are from similar systems that share many of the components such as :

- Parking meters
- Transportation payment systems

Denial of (charging/power) service

Scenarios:

Large scale or targeted:

- Web/mobile: reservation, stopping charge
- Control center: Massing with charge planning (local of global)
- Charge stations: time bomb in firmware

Imagine no electric car can charge for a day when the are 30% of a national fleet!

Happened before:

- Chicago parking meters meltdown
- Ex-Dealership Employee Uses Internet To Disable 100 Cars

27

Stealing electricity (or money)

A lot of small charges can accumulate

Scenarios:

- RFID fraud: stored value of identity theft
- Communications: Man in the middle
- Protocols: emulating the control center
- Web: refunds, identity theft
- Meter spoofing

Happened before:

- Grand et al, SF parking meter hacking, BlackHat 2009
- Ryan et al, Boston subway hack, Defcon 2008. Faulty cards just now replaced in the Netherlands.

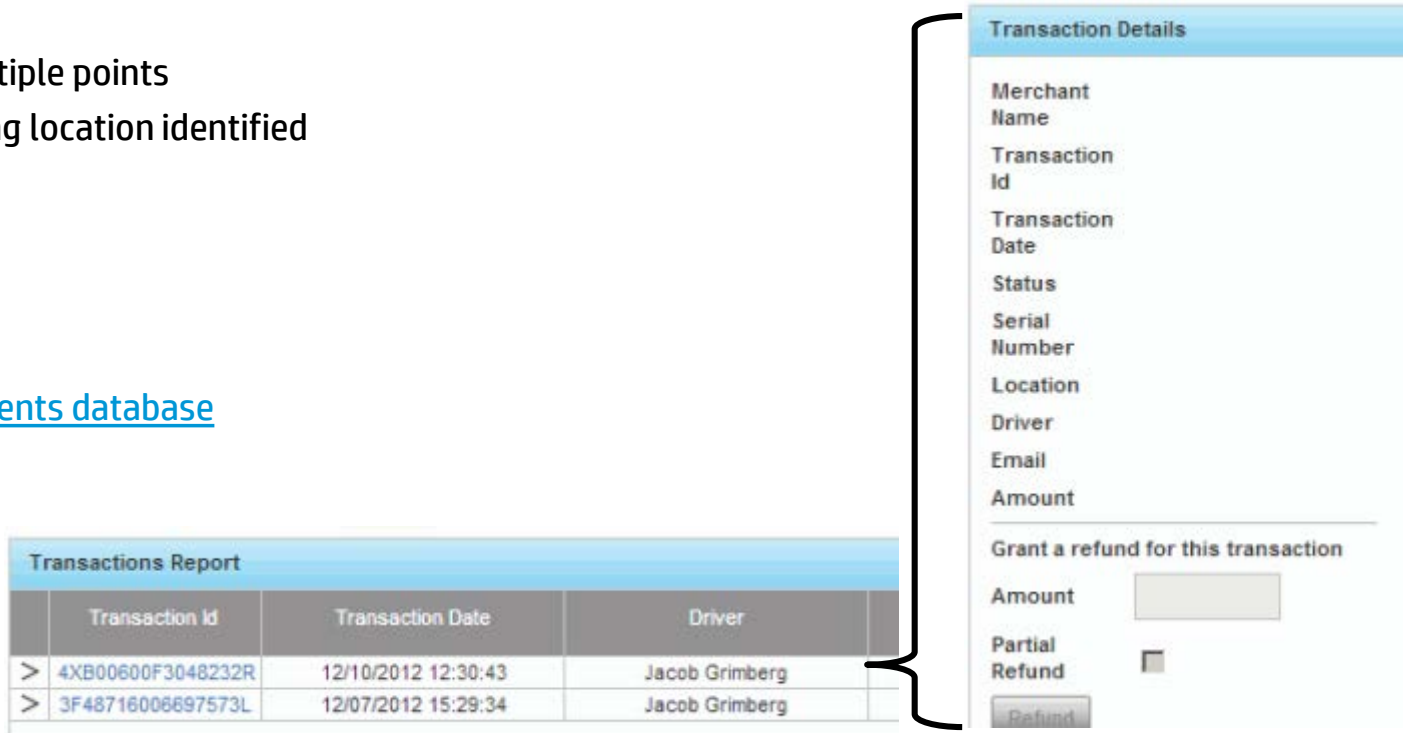
Privacy infringement

Scenarios:

- Eavesdropping at multiple points
- Web/mobile: Retrieving location identified transactions.

Happened before:

- [The web hacking incidents database]



29

Electrocution?

Solutions

Open Standards

Today standards in in infancy and not open enough forcing security by obscurity.

Roaming ?

Direct cloud communications ?

Control Center communications

Application:

- e-Laad OPPC
- ChargePoint Open Charge
- ISO/IEC 15118 (partial)

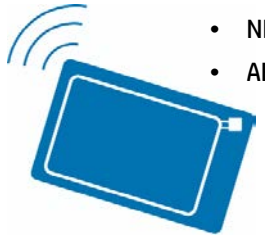
Network: ZigBee

EV 2 CS communication

- ISO/IEC 15118 V2G
- SAE J2293/2836/2847

RFID

- ISO 14443 + PayWave/PayPass ?
- NFC ?
- AES/3DES



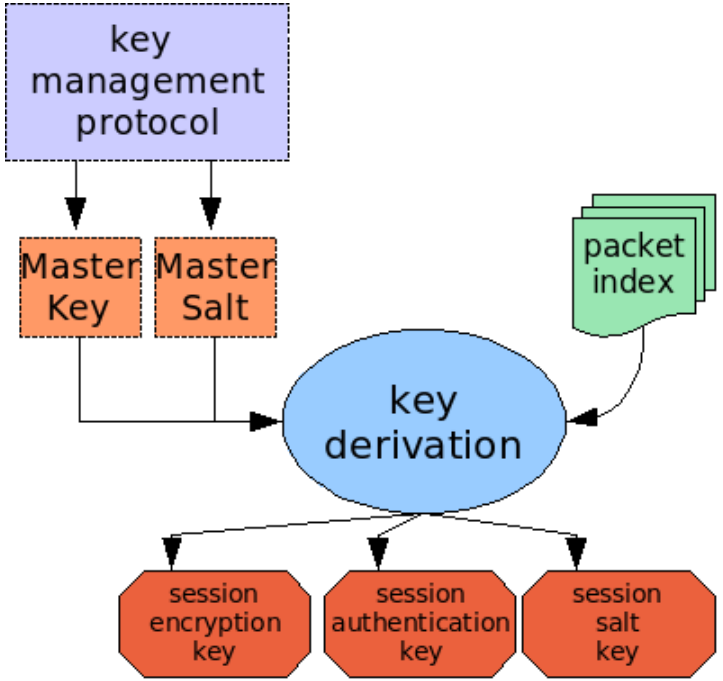
Massive key and password management

Support unique key issuing and revocation

- Public key cryptography where feasible.
- Derived symmetric keys for online systems and management protocols.
- One time maintenance keys or passwords.

Encryption risk management

- Consider insecure offline mode allowing no key in charge station.



Just design (and invest) in security!

The Internet of things

Thoughts about physical hacking

So many frightening talks

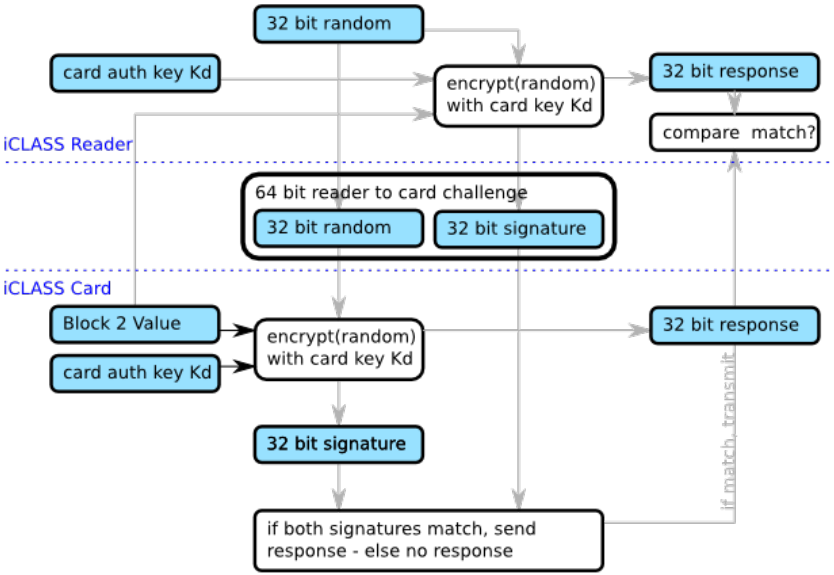
So why no hacks?

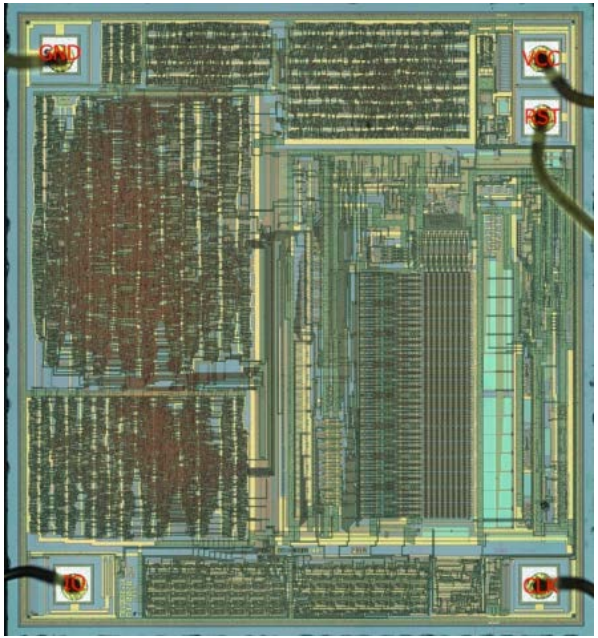
It takes an expert, and not just in hacking

Physical hacking presentation

And not just any security expert

This is as simple at it gets (i.e. just presentation graphics):

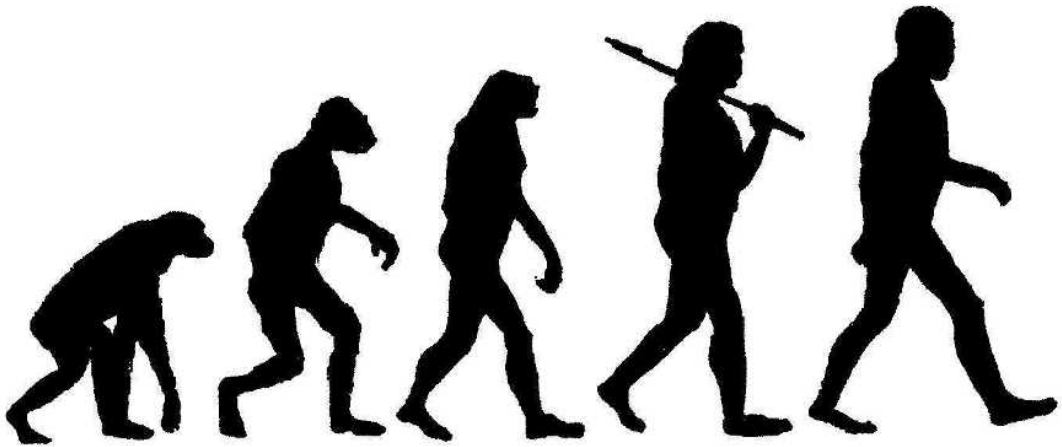





Perceived(?) risks are small
Especially for emerging technologies

Or maybe people are just good?

At least when it gets physical



However:

Risks are aggregative and involve a basic service

Will become an issue when electric cars become a reality

It may be too late by than…

Thank you

Next episode: Hacking cars…

Ofer Shezaf

ofer@shezaf.com