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

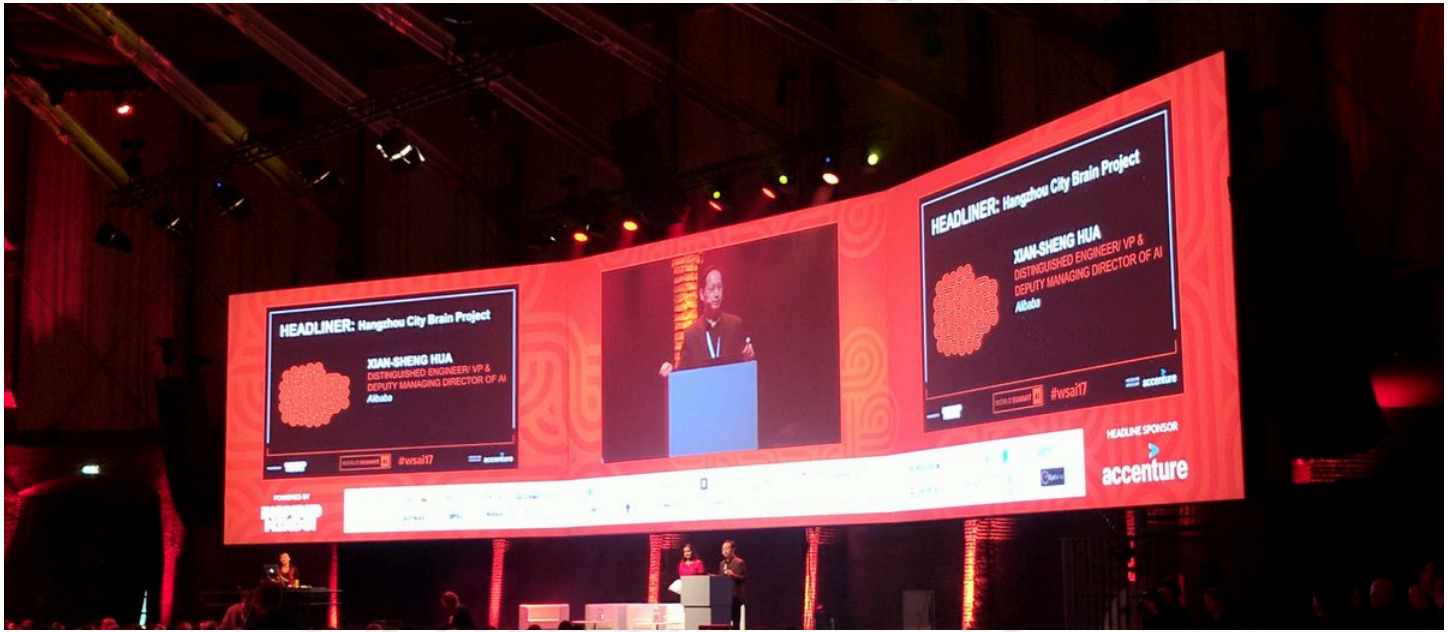
Limited citizen privacy and risk management options

- 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

Texas Department of Transportation

PURCHASE ORDER

Page: 1 of 2

P.O. No: 6013100000025400
Solicitation Number: 0000011599
P.O. Date: 09/21/2015
No Bid Required

To:
OSCS INC
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

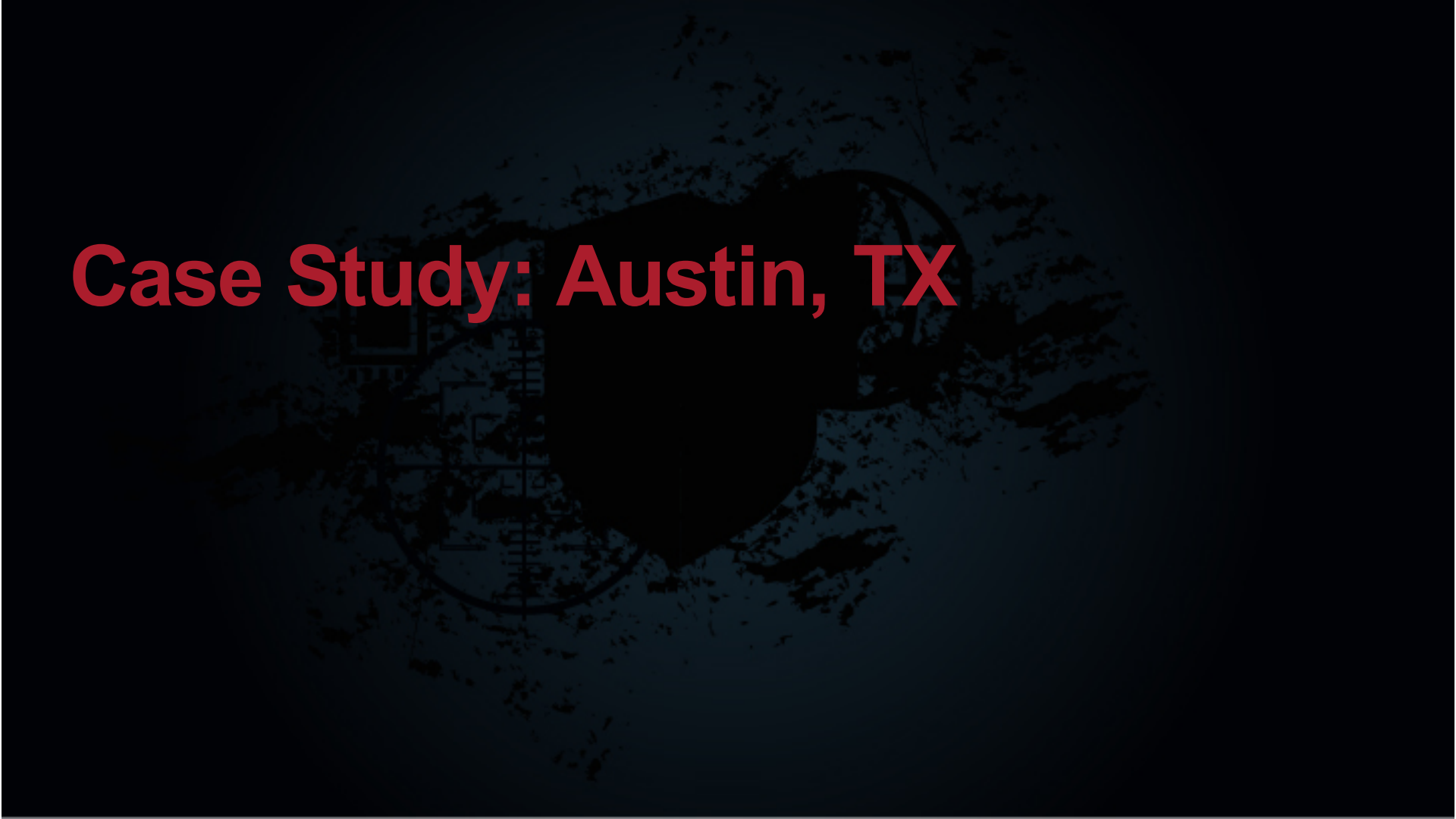
VENDOR ID: 1412129927-*00

BUYER: Nichols, Sheila

Line Item	Item Description	Quantity	Unit	Unit Cost	Extended Cost
	SHIP TO THE FOLLOWING LOCATION UNLESS OTHERWISE NOTED: DALLAS DISTRICT HEADQUARTERS 4777 EAST HIGHWAY 80 MESQUITE TX 75150 United States				
1	**93862000000** **LABORATORY EQUIPMENT AND ACCESSORIES,MAINTENANCE AND REPAIR: FOR GENERAL ANDANALYTICAL RESEARCH USE, NUCLEAR,OPTICAL, PHYSICAL** Promise Date: Sep 21, 2015 **Estimated repairs for Nuclear Gauge Smart Panel, Serial # 22878 - Add a smart panel.**	1.00	EA	$650.00	$650.00

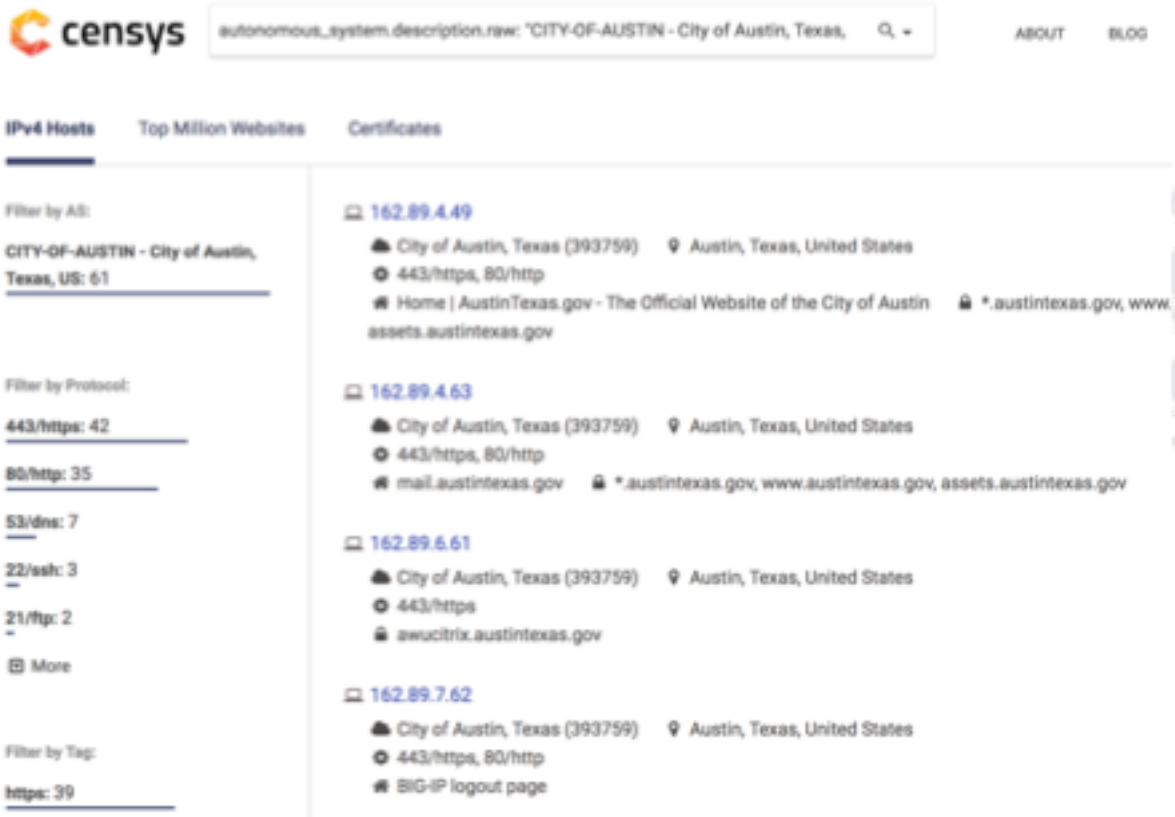
Open Source Application Development Portal (OSADP)

Case Study: Austin, TX



From port scans

From Internet scan data



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

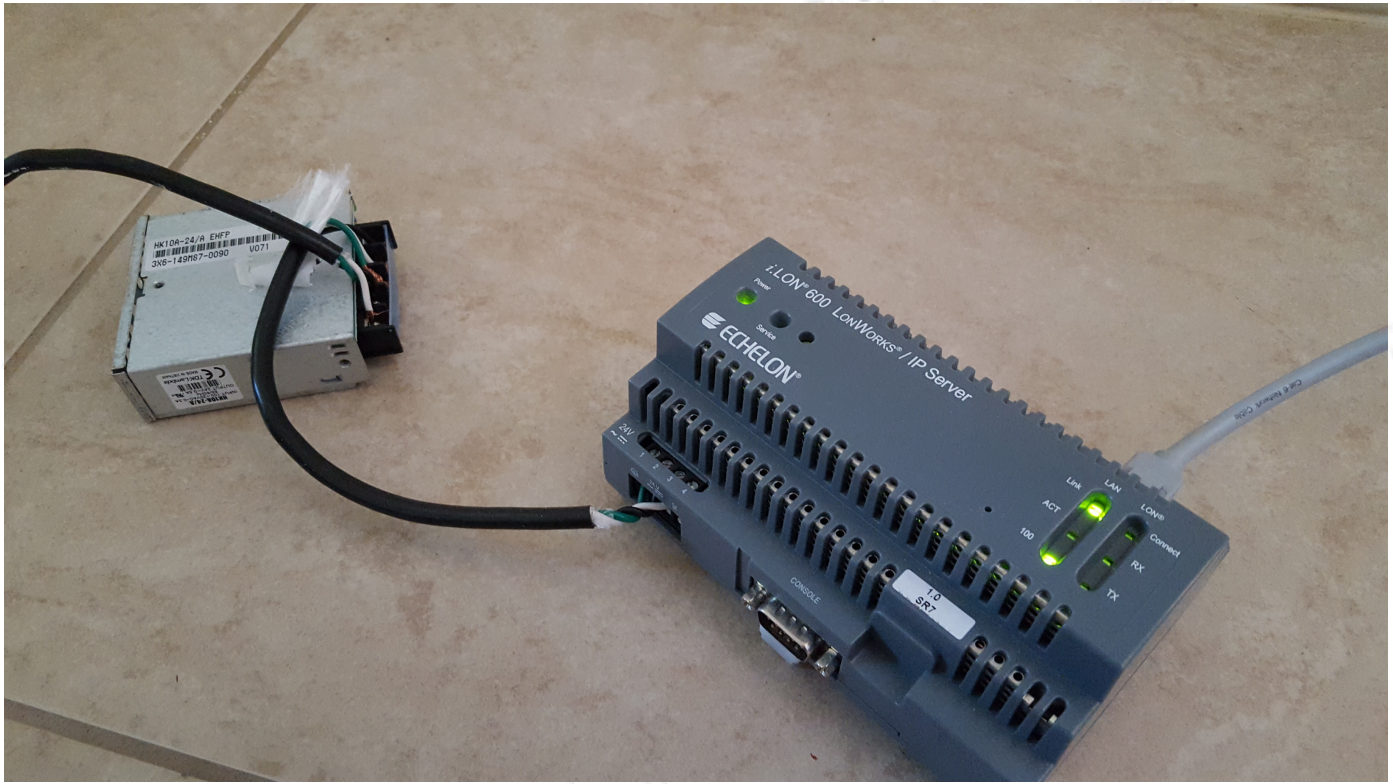
Devices and Vulnerabilities

Echelon i.LON SmartServer and i.LON 600

i.LON: What it does

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

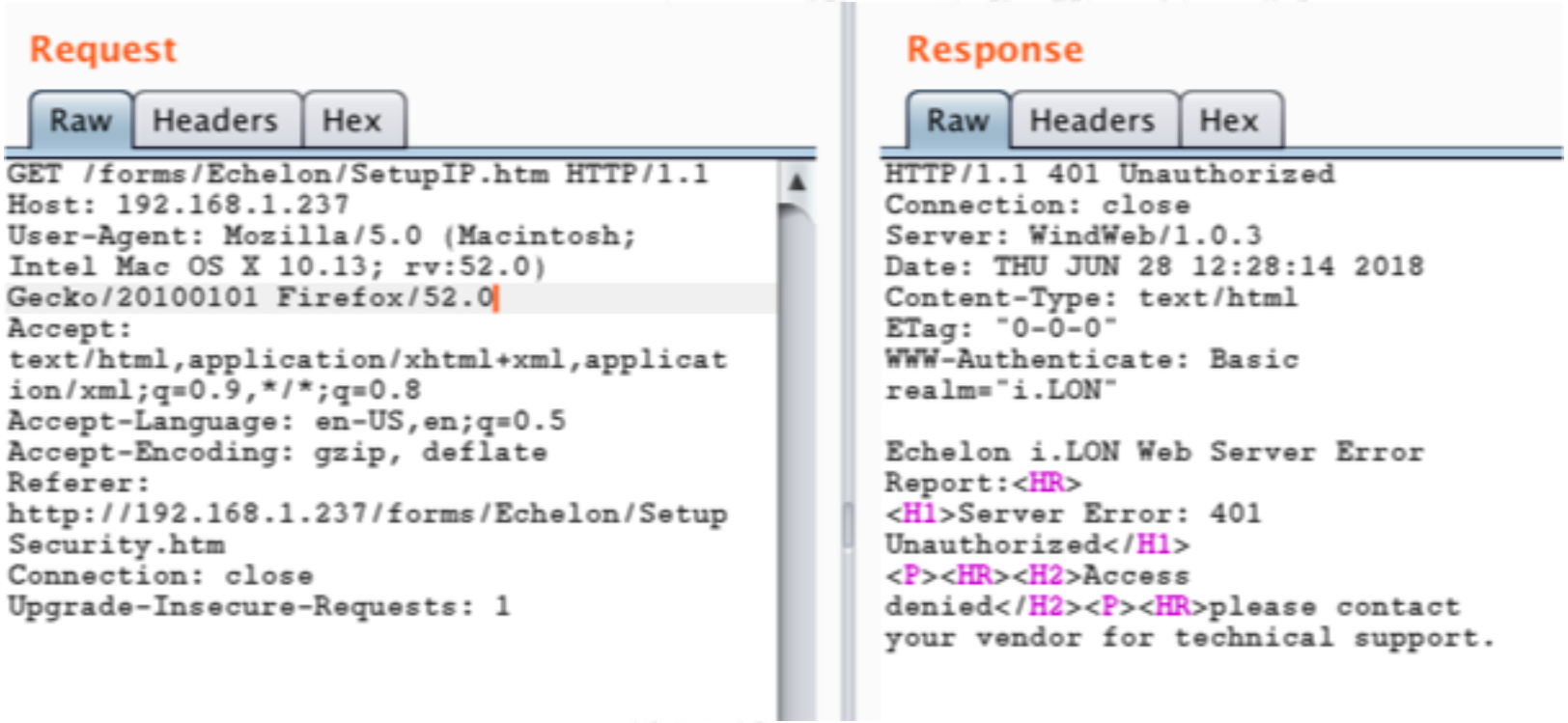
Probably not OSHA-approved



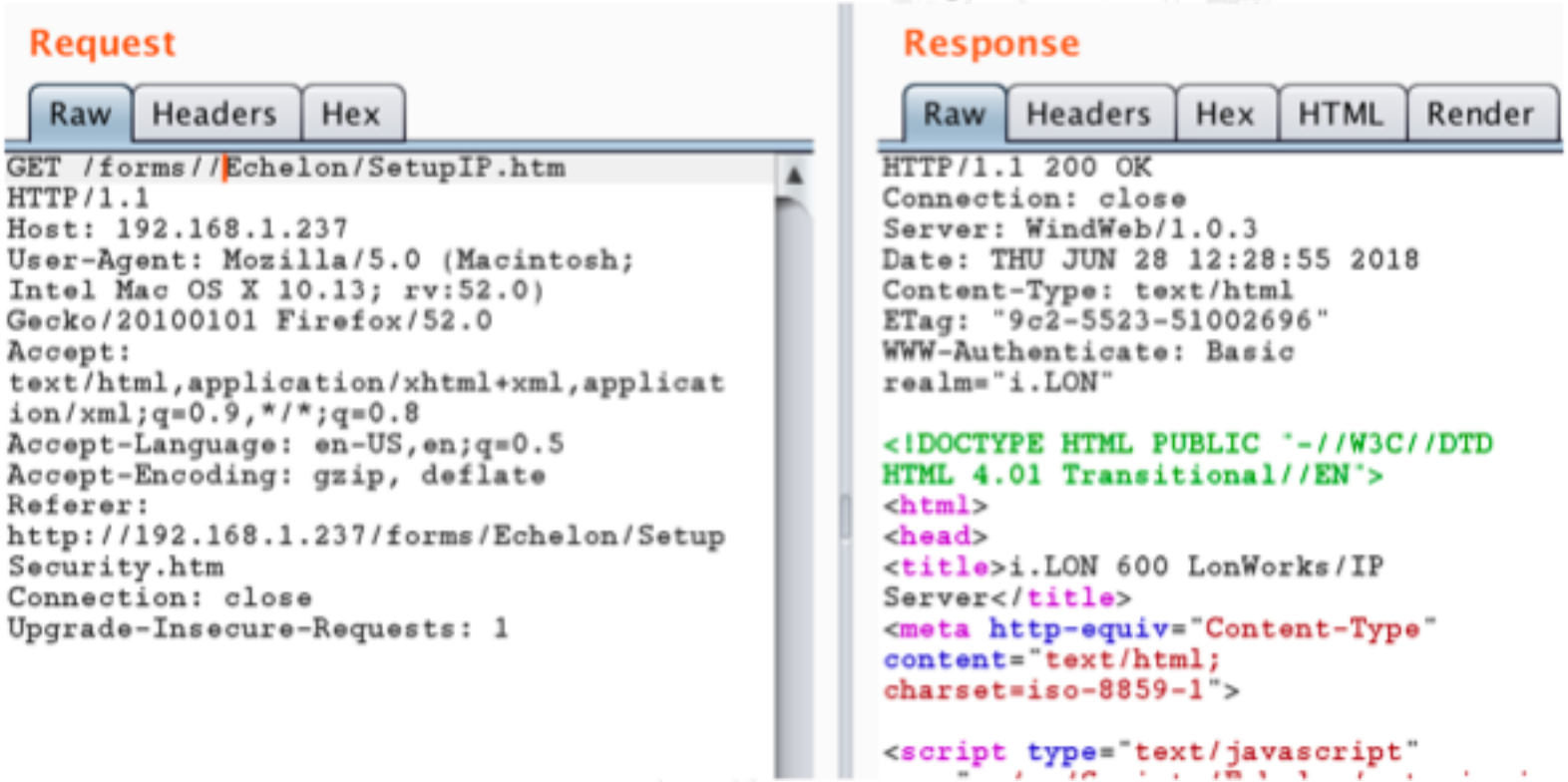
i.LON SmartServer and i.LON 600

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

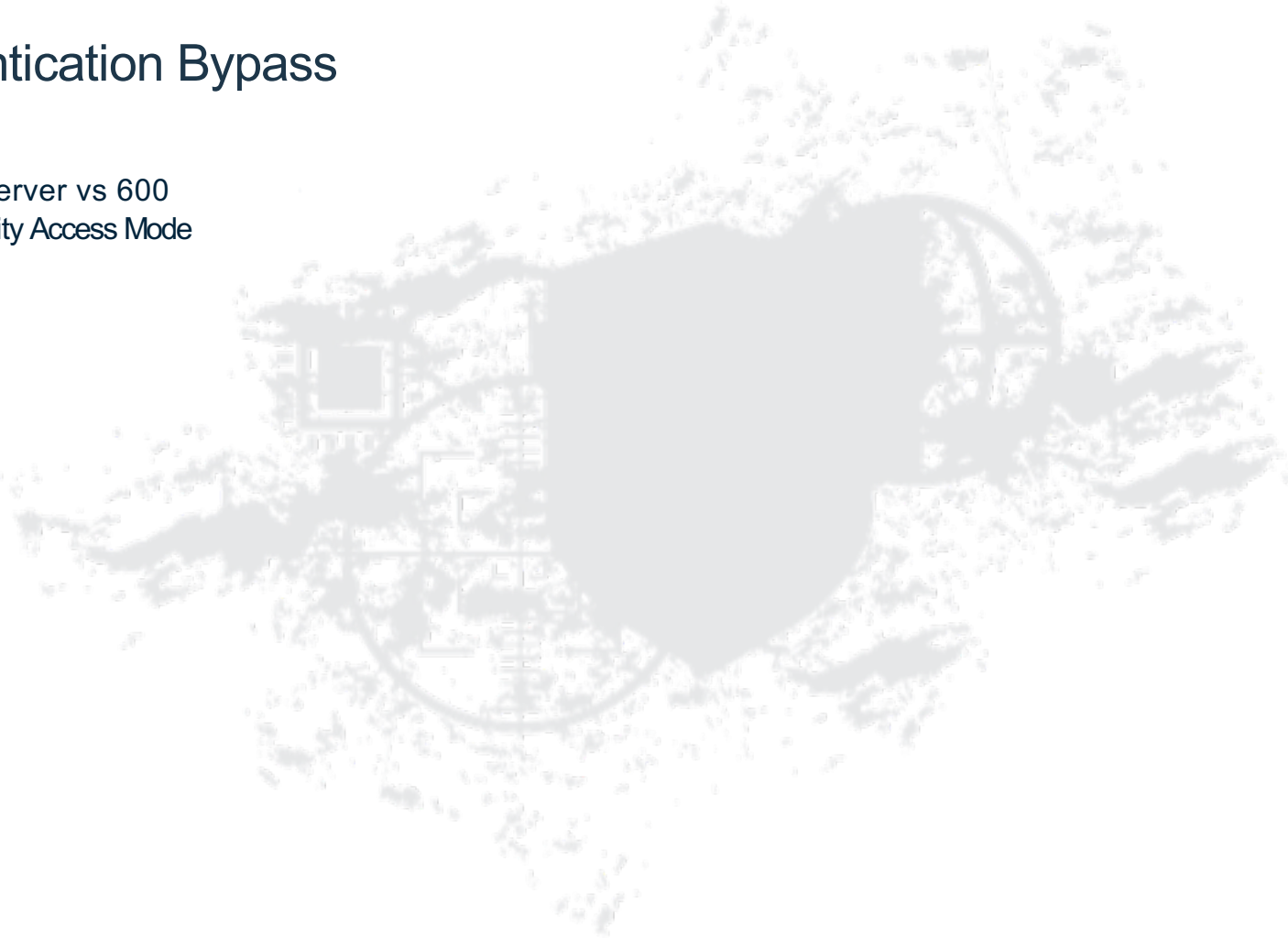


Authentication Bypass



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

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	Track vehicles
Various API key issues	Send false safety messages
XSS	Create traffic
SQLi in API	…or just power it down
Missing authentication	

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

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

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

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

PHP strcmp() weirdness

▲ 74 ▼ 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(6152951945280972069370258312681 4, 6152951945280972000000000000000000) => 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

Missing authentication

Shell command injection

Do bad things

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

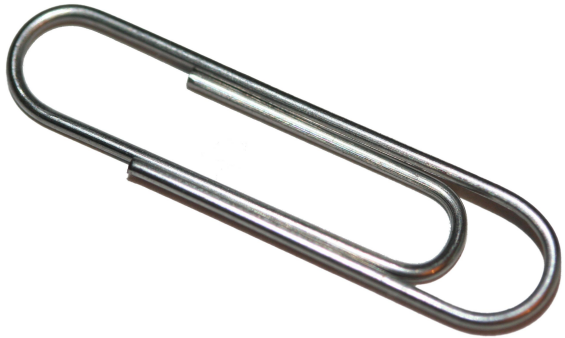
Implications

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
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM