A Cyber-Resilient ICS through Diversified Redundancy and Intrusion Detection

- Keynote Speaker Presentation -

Charles Kim, Ph.D.
Professor

Electrical Engineering and Computer Science
Howard University
Washington DC
USA
ckim@howard.edu

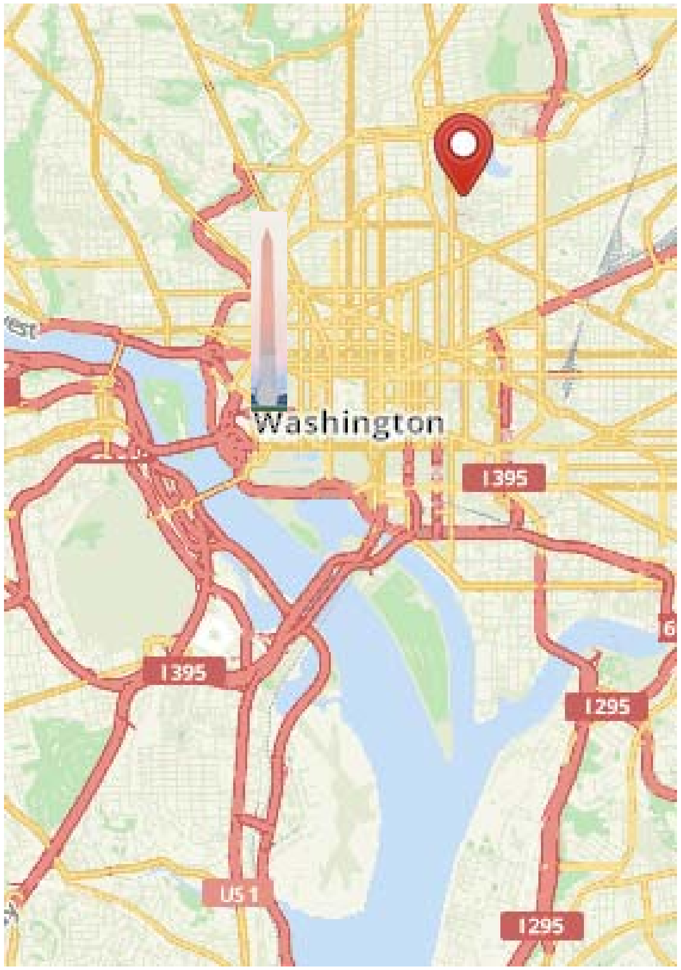
IEEE Advancing Technology for Humanity WCICSS

WCICSS - 2017
World Congress on Industrial Control Systems Security
December 11-14, 2017 | University of Cambridge, UK

Where is Howard?

HOWARD UNIVERSITY 1867

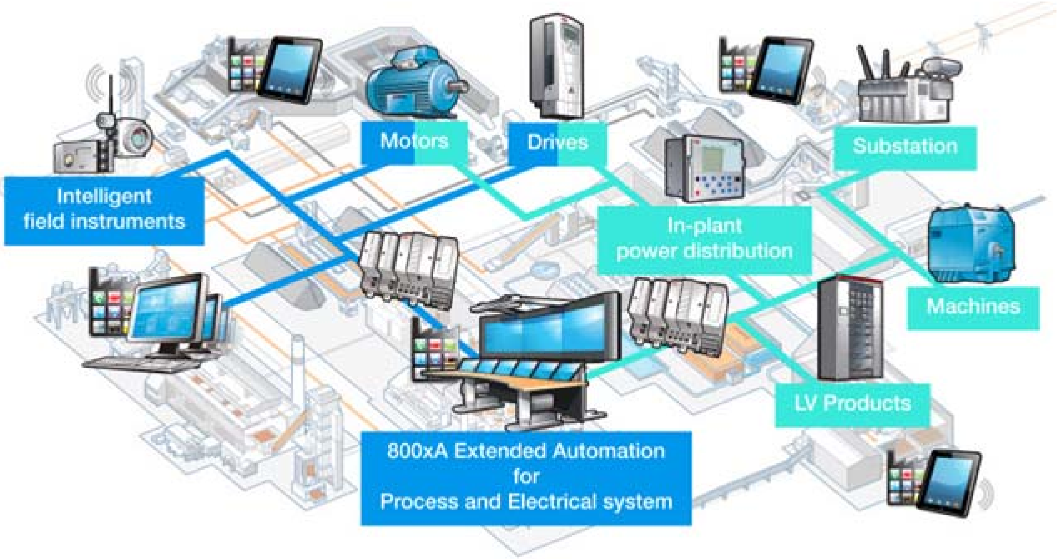
- Founded in 1867
- Private University
- 10,000 students



Howard University: The Founders Library at Upper Quad, looking toward the Washington Monument and Old Post Office, Spring 2000.

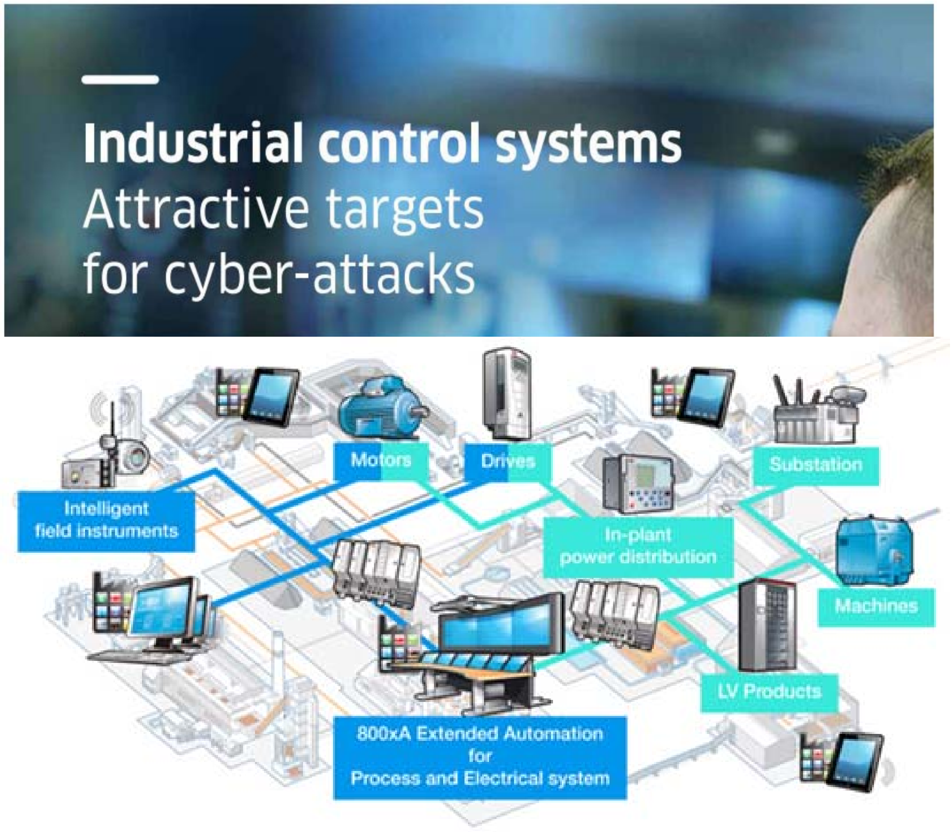
Table of Contents

- Background – Cyber Vulnerabilities in Industrial Control Systems (ICS)
- New Control System Architecture
  - Diversified Redundancy
- Incorporation of Intrusion Detection
- Validation Experimentation
- Conclusions


Motors
Drives
Substation
Intelligent field instruments
In-plant power distribution
Machines
LV Products
800xA Extended Automation for Process and Electrical system

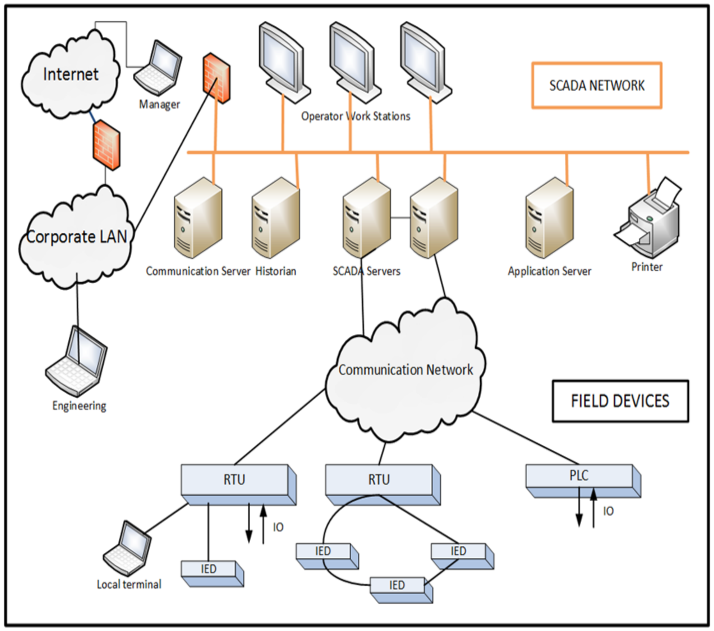
Introduction

- Enhanced use of networked (intelligent/smart) devices
- cyber security vulnerabilities exploited by hackers.
- IT side security technique: Not adequate for the attacks specific to control system networks.
- Intrinsic weakness of the communication protocols used by (legacy) control networks and devices.


Industrial control systems
Attractive targets
for cyber-attacks
Intelligent field instruments
Motors
Drives
Substation
In-plant power distribution
Machines
LV Products
800xA Extended Automation for Process and Electrical system

Cyber Vulnerability in Industrial Control Systems (ICS)

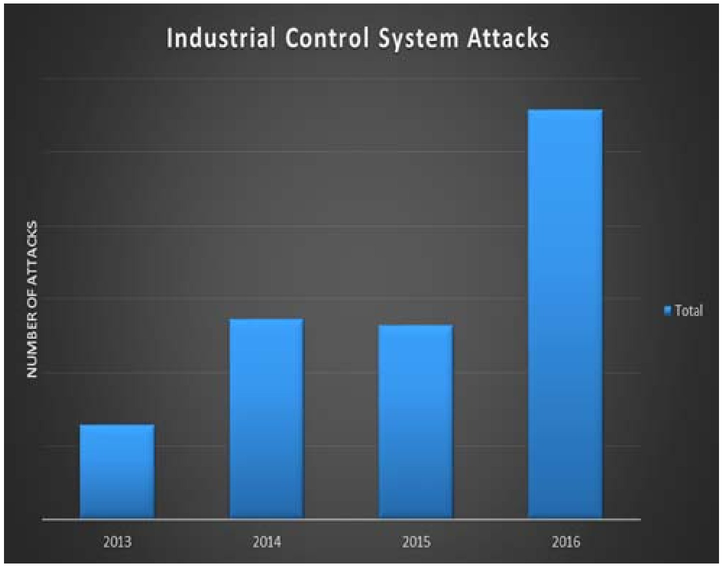
- Connected Control Systems
  - No longer stand-alone: “no air-gap”
  - Connected to corporate network via Internet– open connectivity
  - Resulted in increase in
    - Security vulnerability
    - Unauthorized access and intrusion
    - Malicious code manipulation



- Exploitation
  - Cyber security threats on ICS are ever increasing
  - Legacy systems developed for pre-Internet era are vulnerable to cyber attacks
- Ukraine (2015) – 1st Successful cyber attack on a power system

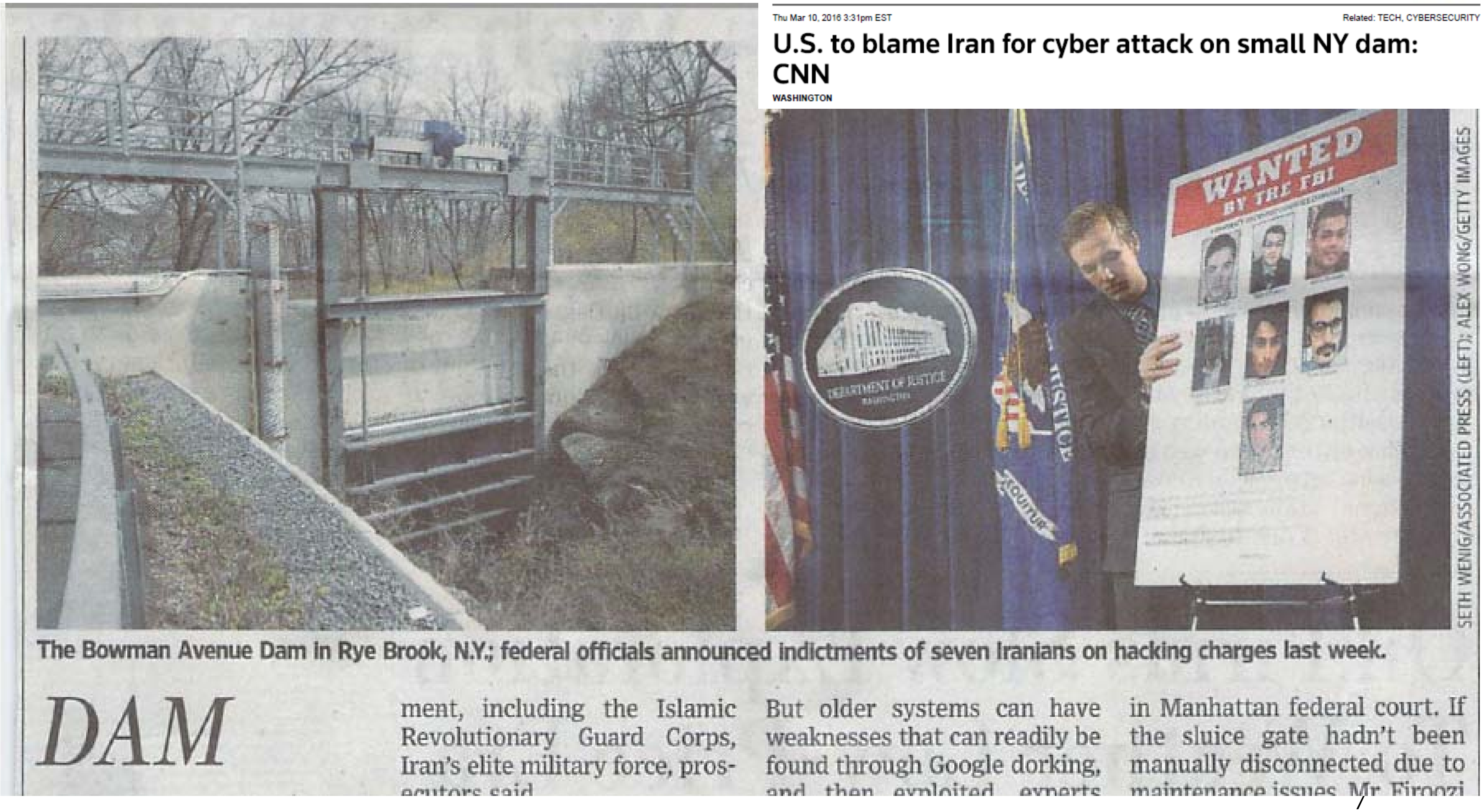
Cyber attacks on ICS

- 2010 – Stuxnet – Nuclear Plant
- 2011 – Duqu – Malware for ICS attacks (similar to Stuxnet)
- 2012 – Black Energy – Targets ICS running GE products
- 2014 – Havex – Remote access attacks in the energy sector
- 2015 – Attack on Ukraine Power System
- 2016 – Attack on Ukraine Military Artillery



Cyber Vulnerability in ICS

- Bowman Avenue Dam, Rye Brook, NY. 2013
- Used the technique to identify an unprotected computer that controlled sluice gates and other functions



Thu Mar 10, 2016 3:31pm EST

Related: TECH, CYBERSECURITY

U.S. to blame Iran for cyber attack on small NY dam: CNN

WASHINGTON

WANTED BY THE FBI
DEPARTMENT OF JUSTICE
SETH WENIG/ASSOCIATED PRESS (LEFT); ALEX WONG/GETTY IMAGES

The Bowman Avenue Dam in Rye Brook, N.Y.; federal officials announced indictments of seven Iranians on hacking charges last week.

DAM

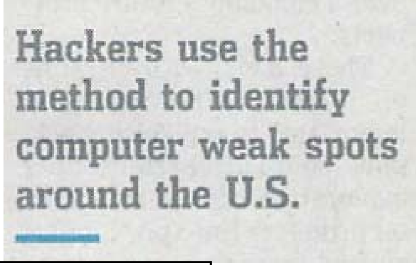
ment, including the Islamic Revolutionary Guard Corps, Iran's elite military force, prosecutors said.

But older systems can have weaknesses that can readily be found through Google dorking, and then exploited experts

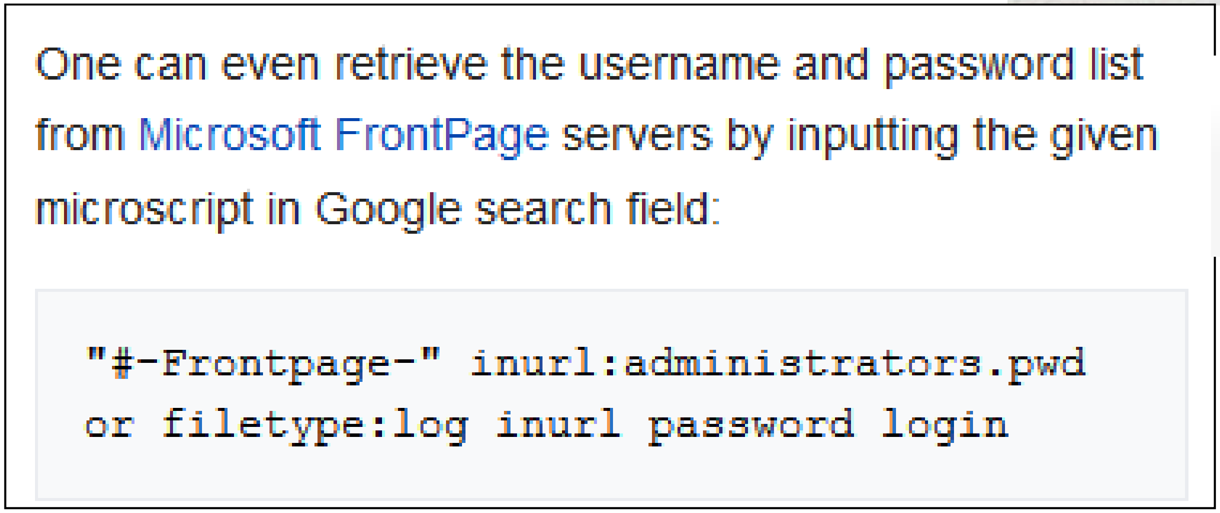
in Manhattan federal court. If the sluice gate hadn't been manually disconnected due to maintenance issues Mr Firoozi

Cyber Vulnerability in ICS

- Google Search Process
- “Google Dorking”

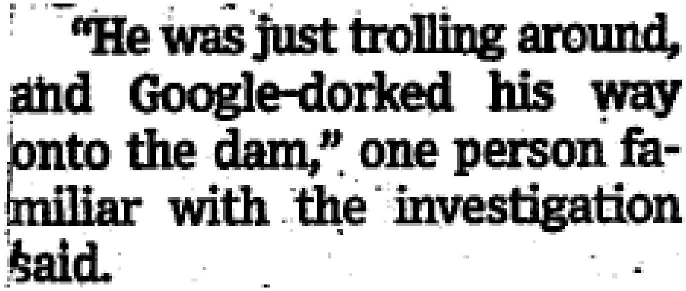


Hackers use the method to identify computer weak spots around the U.S.

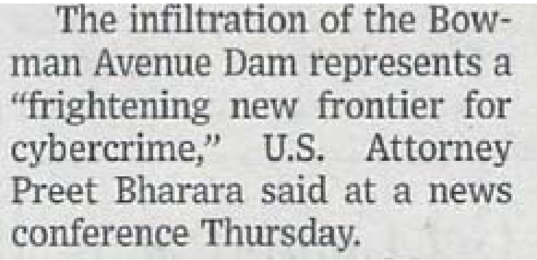


One can even retrieve the username and password list from Microsoft FrontPage servers by inputting the given microscript in Google search field:

```
"#-Frontpage-" inurl:administrators.pwd
or filetype:log inurl password login
```

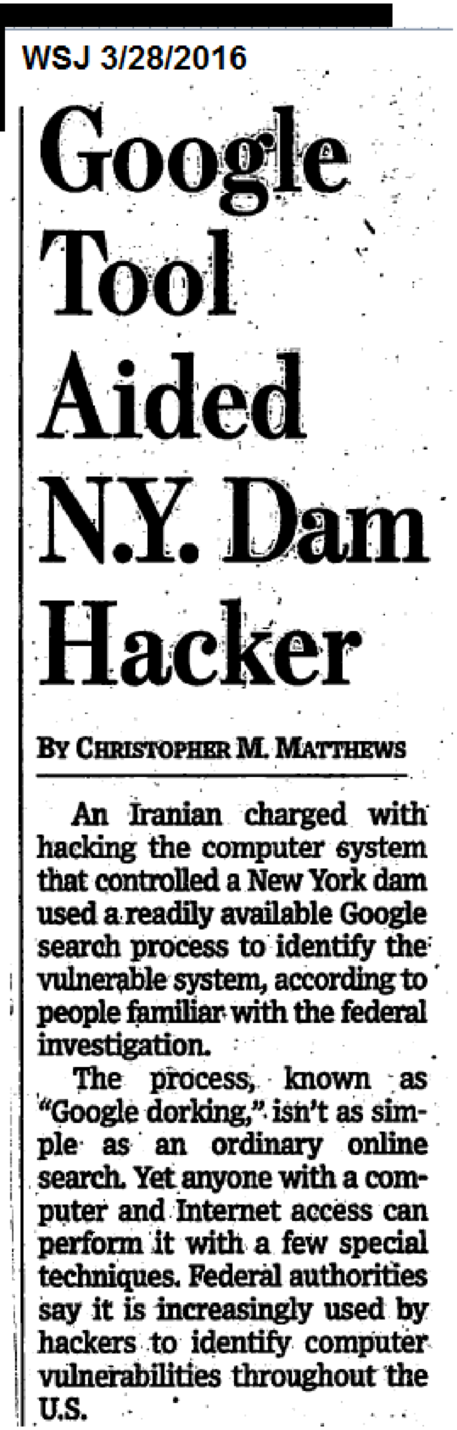


“He was just trolling around, and Google-dorked his way onto the dam,” one person familiar with the investigation said.



The infiltration of the Bowman Avenue Dam represents a “frightening new frontier for cybercrime,” U.S. Attorney Preet Bharara said at a news conference Thursday.

- Point: Any tool can be used to hack



WSJ 3/28/2016

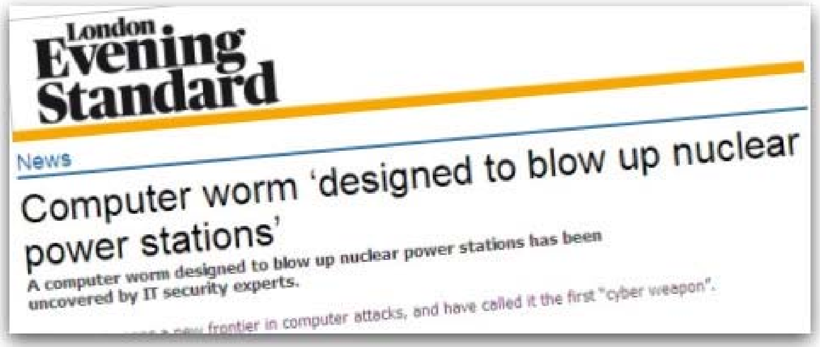
Google Tool Aided N.Y. Dam Hacker

By Christopher M. Matthews

An Iranian charged with hacking the computer system that controlled a New York dam used a readily available Google search process to identify the vulnerable system, according to people familiar with the federal investigation.

The process, known as “Google dorking,” isn’t as simple as an ordinary online search. Yet anyone with a computer and Internet access can perform it with a few special techniques. Federal authorities say it is increasingly used by hackers to identify computer vulnerabilities throughout the U.S.

Cyber Vulnerability in ICS - Stuxnet at Natanz



London Evening Standard

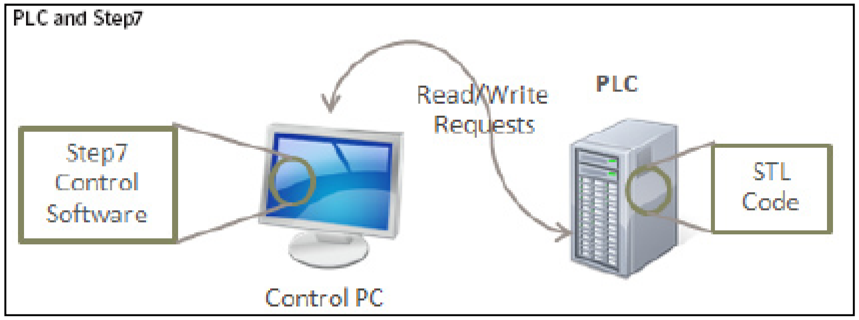
News

Computer worm 'designed to blow up nuclear power stations'

A computer worm designed to blow up nuclear power stations has been uncovered by IT security experts.

a new frontier in computer attacks, and have called it the first "cyber weapon".

Turkey
Tabriz
Turkmenistan
Ashgabat
Adana
Aleppo
Icel
Mosul
Arbil
Tehran
Mashhad
Homs
Syria
prus
Lebanon
Baghdad
Isfahan
Af
Iraq
Amman
Jordan
Iran
Israel
Basrah
Shiraz
Kuwait



PLC and Step7

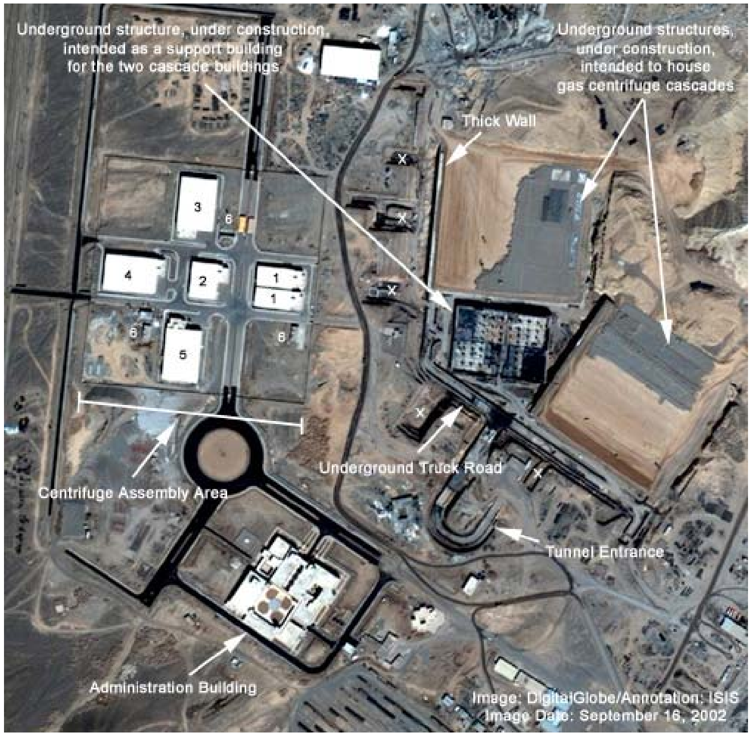
Step7 Control Software

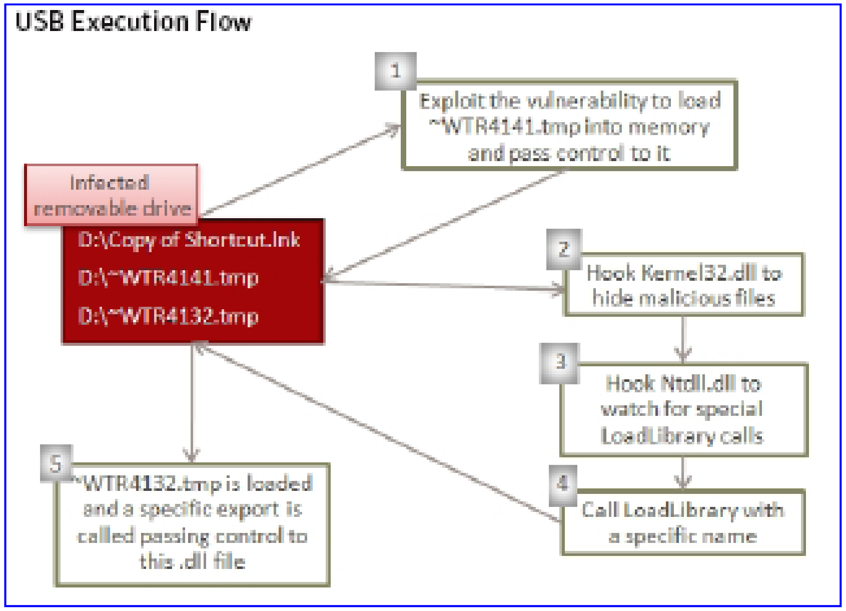
Read/Write Requests

PLC

STL Code

Control PC


Underground structure, under construction, intended as a support building for the two cascade buildings
Underground structures, under construction, intended to house gas centrifuge cascades
Thick Wall
X
3
6
4
2
1
1
6
5
8
Underground Truck Road
Centrifuge Assembly Area
Tunnel Entrance
Administration Building
Image: DigitalGlobe/Annotation: ISIS
Image Date: September 16, 2002



USB Execution Flow

Infected removable drive

D:\Copy of Shortcut.lnk
D:\~WTR4141.tmp
D:\~WTR4132.tmp

1 Exploit the vulnerability to load ~WTR4141.tmp into memory and pass control to it

2 Hook Kernel32.dll to hide malicious files

3 Hook Ntdll.dll to watch for special LoadLibrary calls

4 Call LoadLibrary with a specific name

5 ~WTR4132.tmp is loaded and a specific export is called passing control to this .dll file

- Zero-Day Vulnerability: We know only what we know.

Ukraine Grid Outage – Dec 23, 2015

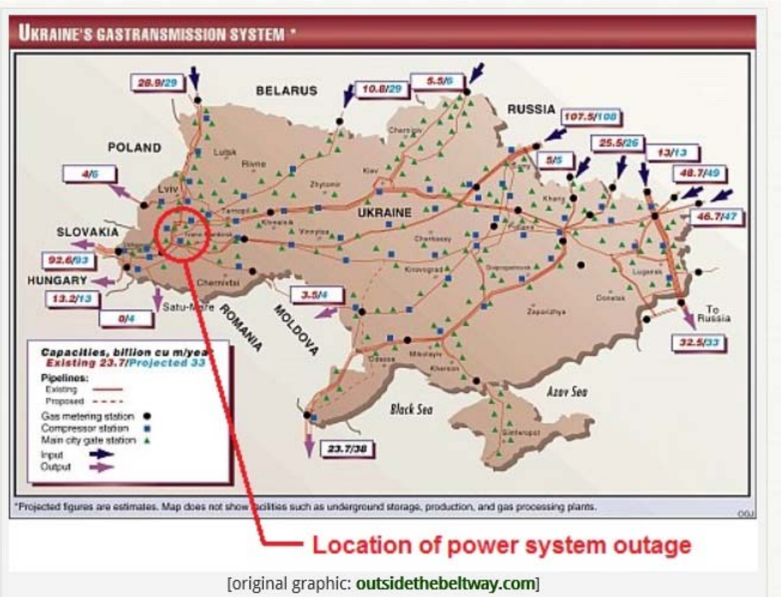
Thu Feb 25, 2016 6:52pm EST

Related: WORLD, TECH, CYBERSECURITY

U.S. government concludes cyber attack caused Ukraine power outage

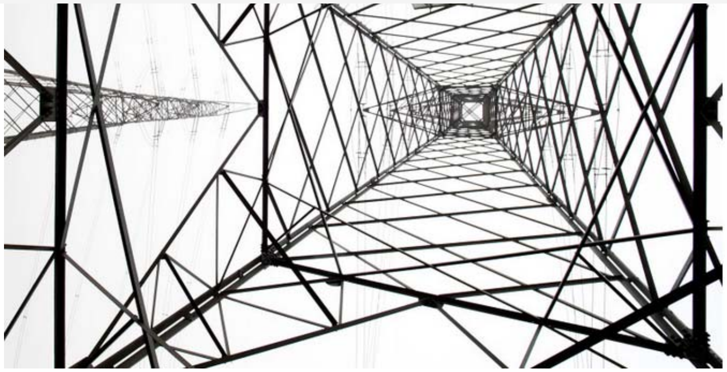
WASHINGTON | BY DUSTIN VOLZ

- US DHS assessment: Interview with 6 Ukrainian organizations affected by the blackout
- DHS: “the December power outage in Ukraine affecting 225,000 customers is the result of a cyber attack” →the first U. S. government recognized blackout caused by a malicious hack
- First known successful cyber intrusion to knock a power grid offline
- Believed to be staged by a Russian hacking group known as “Sandworm”

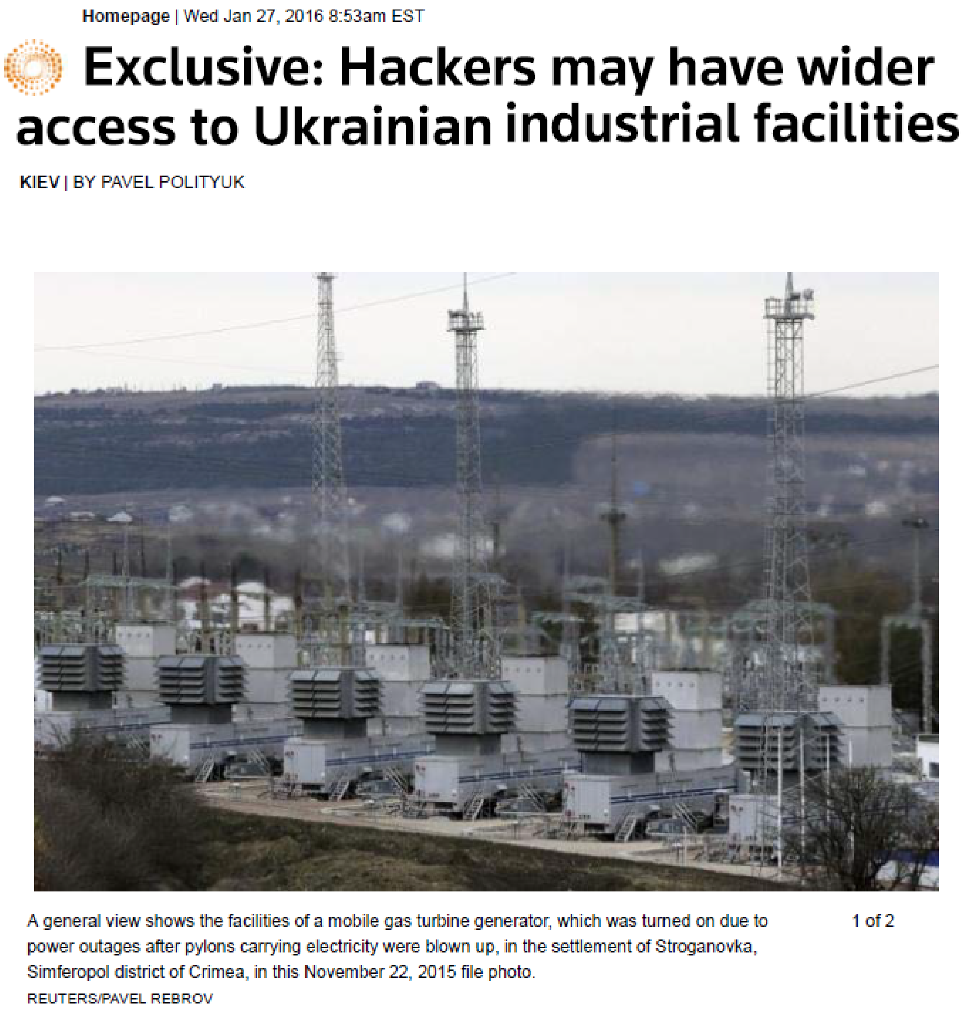

UKRAINE'S GASTRANSMISSION SYSTEM *
BELARUS
RUSSIA
POLAND
SLOVAKIA
HUNGARY
ROMANIA
MOLDOVA
UKRAINE
Black Sea
Azov Sea
To Russia
Capacities, billion cu m/year
Existing 23.7/Projected 33
Pipelines:
Existing
Proposed
Gas metering station
Compressor station
Main city gate station
Input
Output
*Projected figures are estimates. Map does not show facilities such as underground storage, production, and gas processing plants.

Location of power system outage

[original graphic: outsidethebeltway.com]



Ukraine Grid Attack



Homepage | Wed Jan 27, 2016 8:53am EST

Exclusive: Hackers may have wider access to Ukrainian industrial facilities

KIEV | BY PAVEL POLITYUK

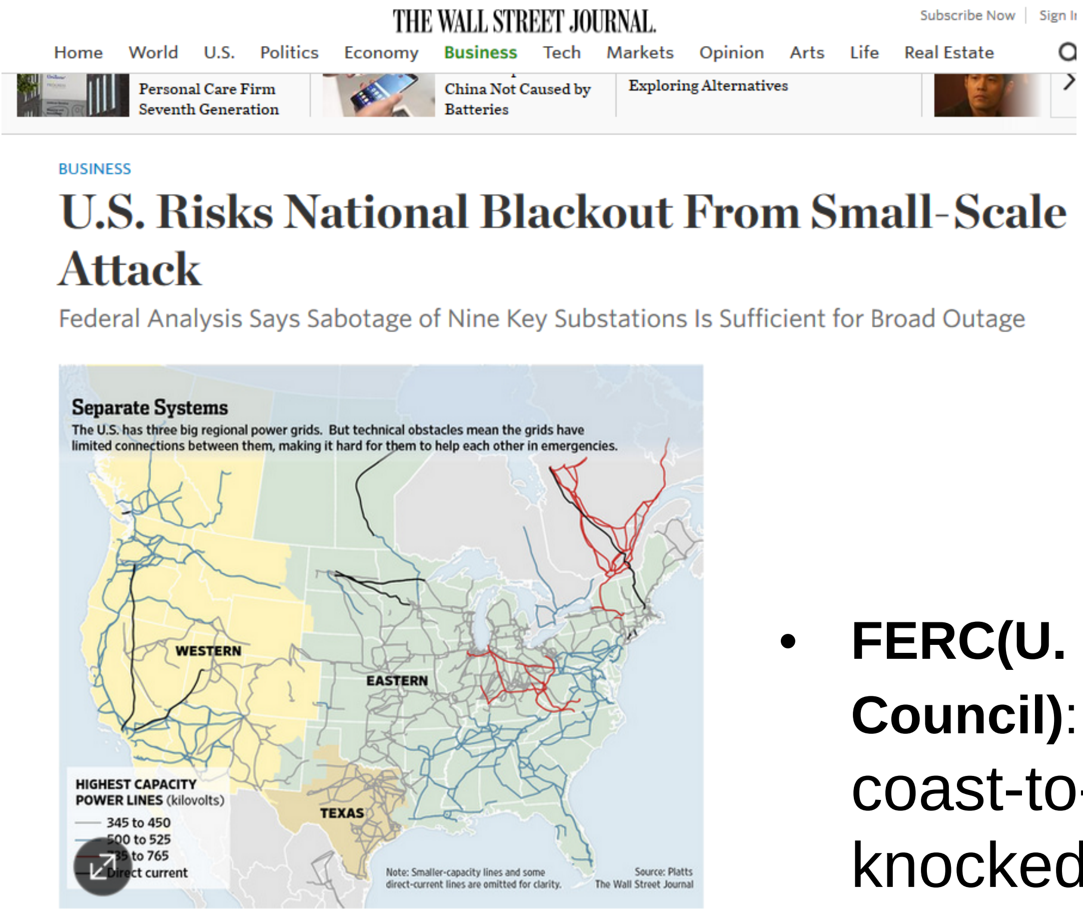
A general view shows the facilities of a mobile gas turbine generator, which was turned on due to power outages after pylons carrying electricity were blown up, in the settlement of Stroganovka, Simferopol district of Crimea, in this November 22, 2015 file photo.

1 of 2

REUTERS/PAVEL REBROV

- Affected by a lesser attack in **October**
- **A similar type of malware** has been identified as far back as **July** by an anti-virus software company
- Attackers must **have known what software was installed** – by emails to workers with infected Word or Excel
- Lesson: **Difficulties and Uncertainties**

U. S. Grid Outage Risk



THE WALL STREET JOURNAL.

Subscribe Now | Sign In

BUSINESS

U.S. Risks National Blackout From Small-Scale Attack

Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage

Separate Systems

The U.S. has three big regional power grids. But technical obstacles mean the grids have limited connections between them, making it hard for them to help each other in emergencies.

Note: Smaller-capacity lines and some direct-current lines are omitted for clarity.

Source: Platts
The Wall Street Journal

PHOTO ILLUSTRATION BY THE DAILY BEAST

'TIME IS RUNNING OUT'

U.S. Power Companies Warned 'Nightmare' Cyber Weapon Already Causing Blackouts

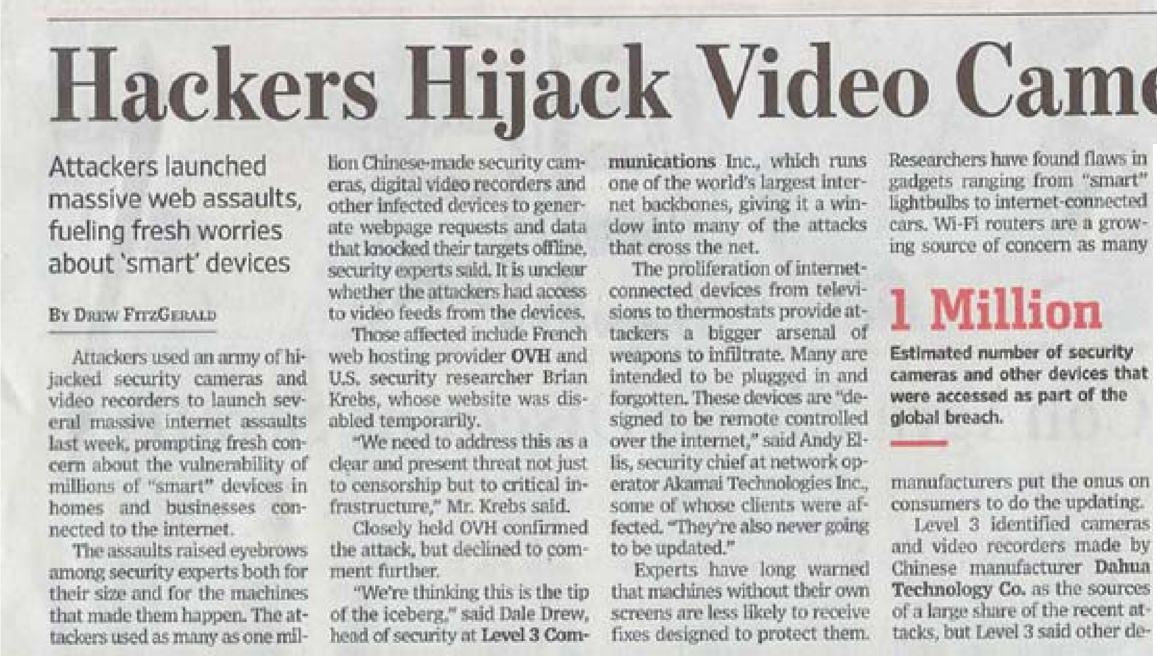
The first hack was small, cutting power to part of Kiev. But security experts now warn that was just the start—the malware is a genuine cyber weapon that threatens the U.S.

KEVIN POULSEN 06.12.17 9:00 AM ET

- **FERC(U. S. Federal Electric Reliability Council)**: “The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day”.

How to protect US (and your) grid against hackers?

IoT Vulnerabilities



Hackers Hijack Video Cameras

Attackers launched massive web assaults, fueling fresh worries about 'smart' devices

By Drew FitzGerald

Attackers used an army of hijacked security cameras and video recorders to launch several massive internet assaults last week, prompting fresh concern about the vulnerability of millions of "smart" devices in homes and businesses connected to the internet.

The assaults raised eyebrows among security experts both for their size and for the machines that made them happen. The attackers used as many as one million Chinese-made security cameras, digital video recorders and other infected devices to generate webpage requests and data that knocked their targets offline, security experts said. It is unclear whether the attackers had access to video feeds from the devices.

Those affected include French web hosting provider **OVH** and U.S. security researcher Brian Krebs, whose website was disabled temporarily.

"We need to address this as a clear and present threat not just to censorship but to critical infrastructure," Mr. Krebs said.

Closely held OVH confirmed the attack, but declined to comment further.

"We're thinking this is the tip of the iceberg," said Dale Drew, head of security at **Level 3 Communications** Inc., which runs one of the world's largest internet backbones, giving it a window into many of the attacks that cross the net.

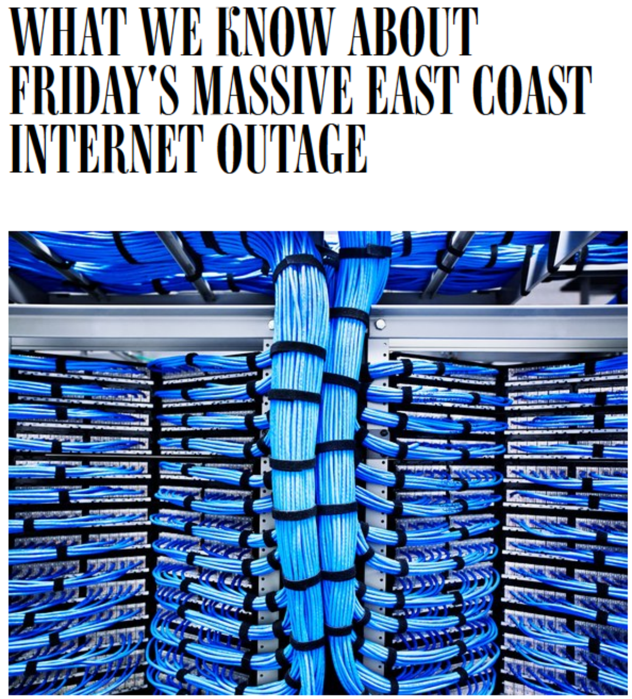
The proliferation of internet-connected devices from televisions to thermostats provide attackers a bigger arsenal of weapons to infiltrate. Many are intended to be plugged in and forgotten. These devices are "designed to be remote controlled over the internet," said Andy Ellis, security chief at network operator Akamai Technologies Inc., some of whose clients were affected. "They're also never going to be updated."

Experts have long warned that machines without their own screens are less likely to receive fixes designed to protect them. Researchers have found flaws in gadgets ranging from "smart" lightbulbs to internet-connected cars. Wi-Fi routers are a growing source of concern as many manufacturers put the onus on consumers to do the updating.

Level 3 identified cameras and video recorders made by Chinese manufacturer **Dahua Technology Co.** as the sources of a large share of the recent attacks, but Level 3 said other de-

1 Million

Estimated number of security cameras and other devices that were accessed as part of the global breach.

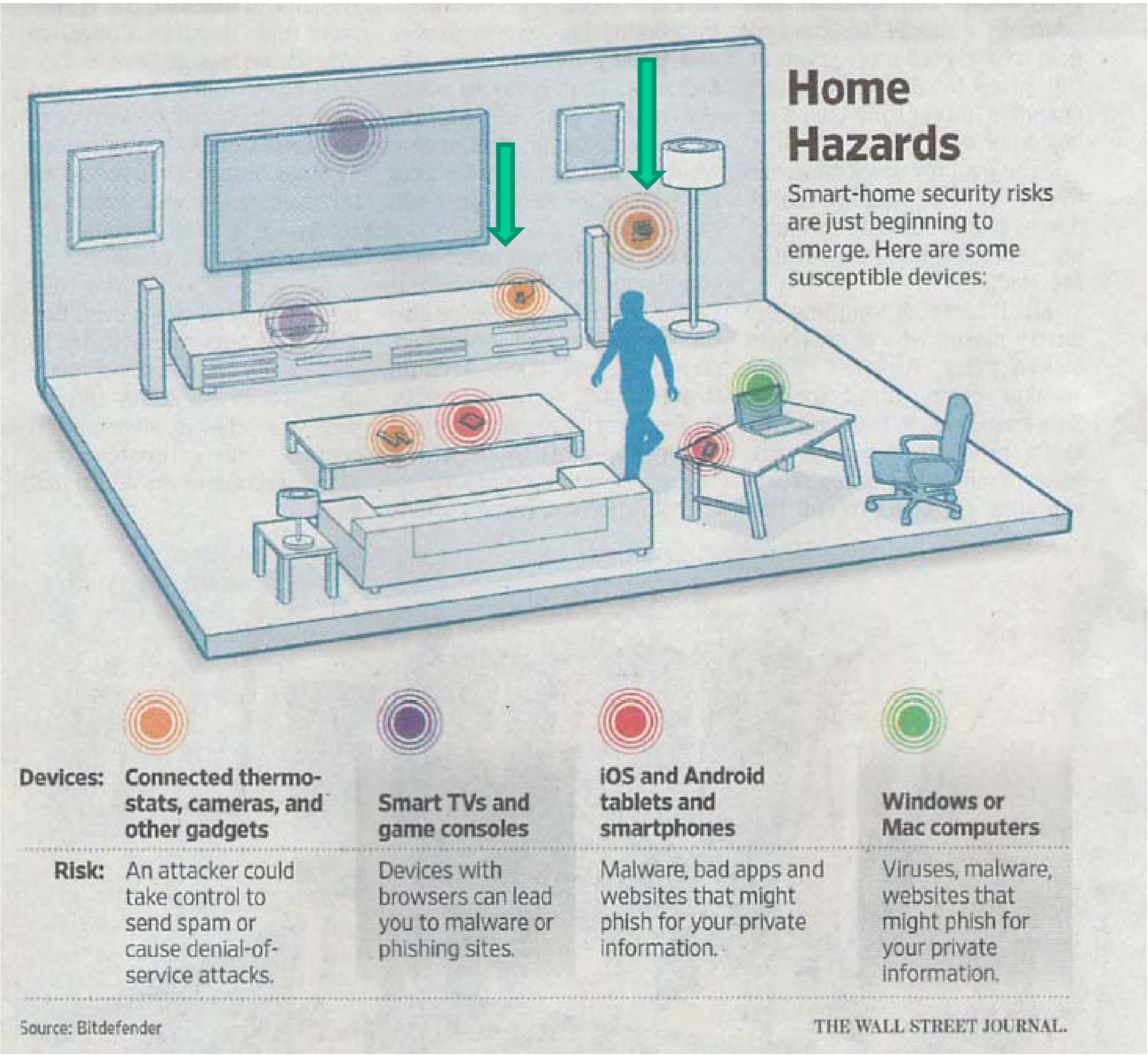


WHAT WE KNOW ABOUT FRIDAY'S MASSIVE EAST COAST INTERNET OUTAGE

- Botnet Attack
  - Web cams: password vulnerability etc.
- Victims
  - Dyn – internet infrastructure company (New Hampshire)
  - Internet Directory service shut down

Your AC and Security Camera may be controlled by someone else

- Susceptible devices
- Thermostats and cameras



Home Hazards

Smart-home security risks are just beginning to emerge. Here are some susceptible devices:

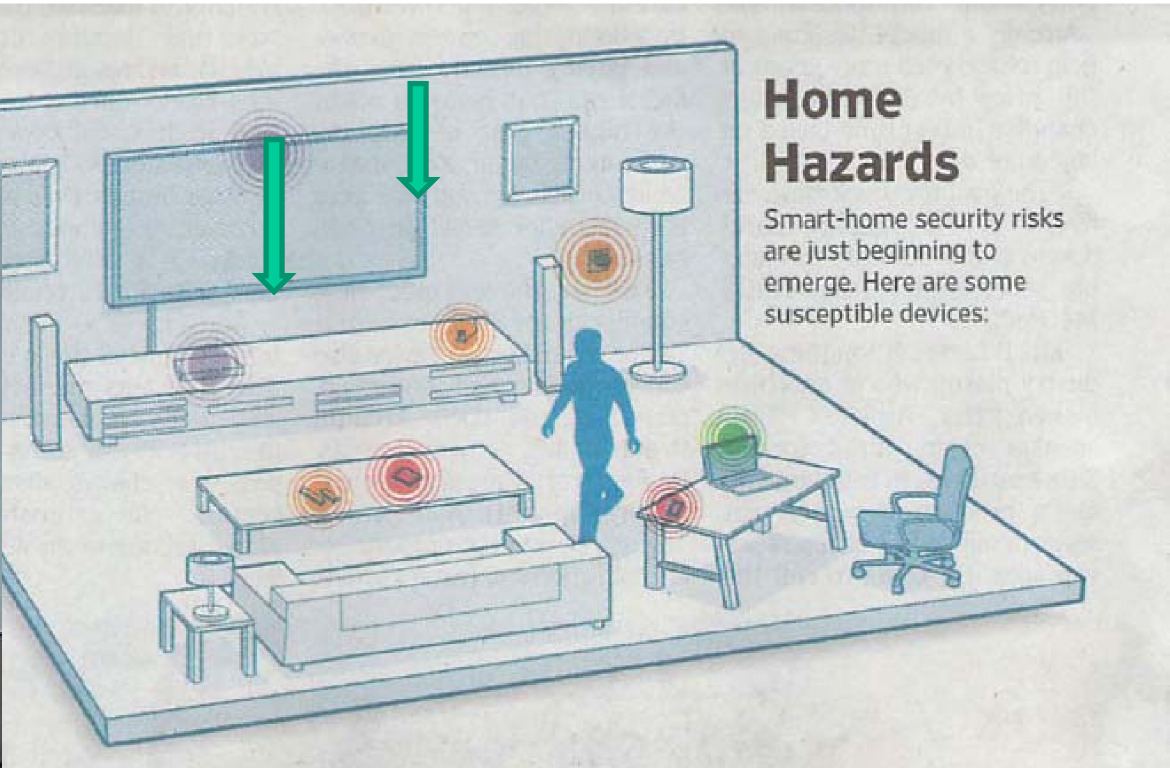
	🟠	🟣	🔴	🟢
Devices:	**Connected thermostats, cameras, and other gadgets**	**Smart TVs and game consoles**	**iOS and Android tablets and smartphones**	**Windows or Mac computers**
Risk:	An attacker could take control to send spam or cause denial-of-service attacks.	Devices with browsers can lead you to malware or phishing sites.	Malware, bad apps and websites that might phish for your private information.	Viruses, malware, websites that might phish for your private information.

Source: Bitdefender

THE WALL STREET JOURNAL.

Your refrigerator may be controlled by someone else

- Smart appliances



Home Hazards

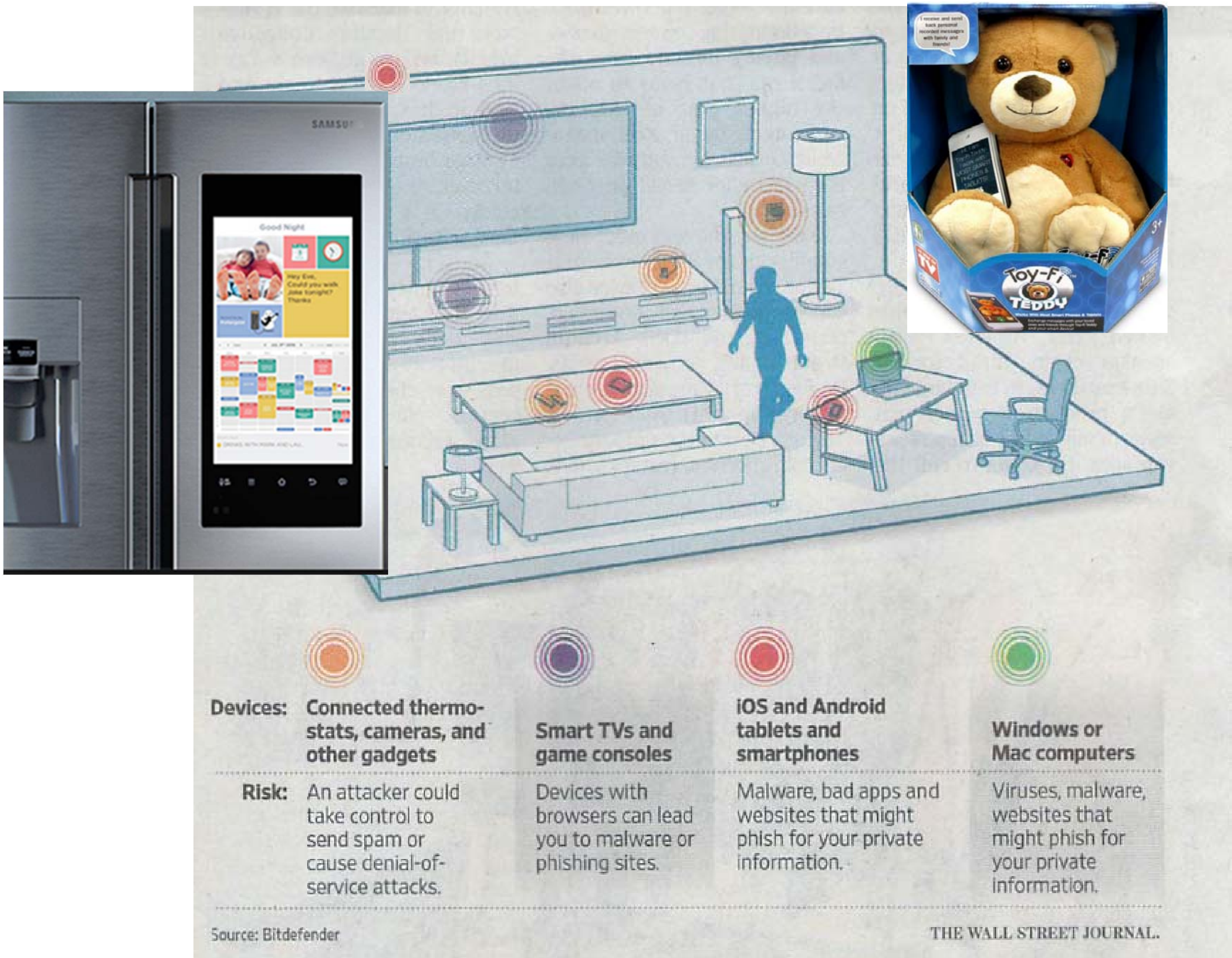
Smart-home security risks are just beginning to emerge. Here are some susceptible devices:

Devices:	**Connected thermostats, cameras, and other gadgets**	**Smart TVs and game consoles**	**iOS and Android tablets and smartphones**	**Windows or Mac computers**
Risk:	An attacker could take control to send spam or cause denial-of-service attacks.	Devices with browsers can lead you to malware or phishing sites.	Malware, bad apps and websites that might phish for your private information.	Viruses, malware, websites that might phish for your private information.

Source: Bitdefender

THE WALL STREET JOURNAL.

Your kid’s toy may be controlled by someone else



Devices:	Connected thermostats, cameras, and other gadgets	Smart TVs and game consoles	iOS and Android tablets and smartphones	Windows or Mac computers
Risk:	An attacker could take control to send spam or cause denial-of-service attacks.	Devices with browsers can lead you to malware or phishing sites.	Malware, bad apps and websites that might phish for your private information.	Viruses, malware, websites that might phish for your private information.

Source: Bitdefender

THE WALL STREET JOURNAL.

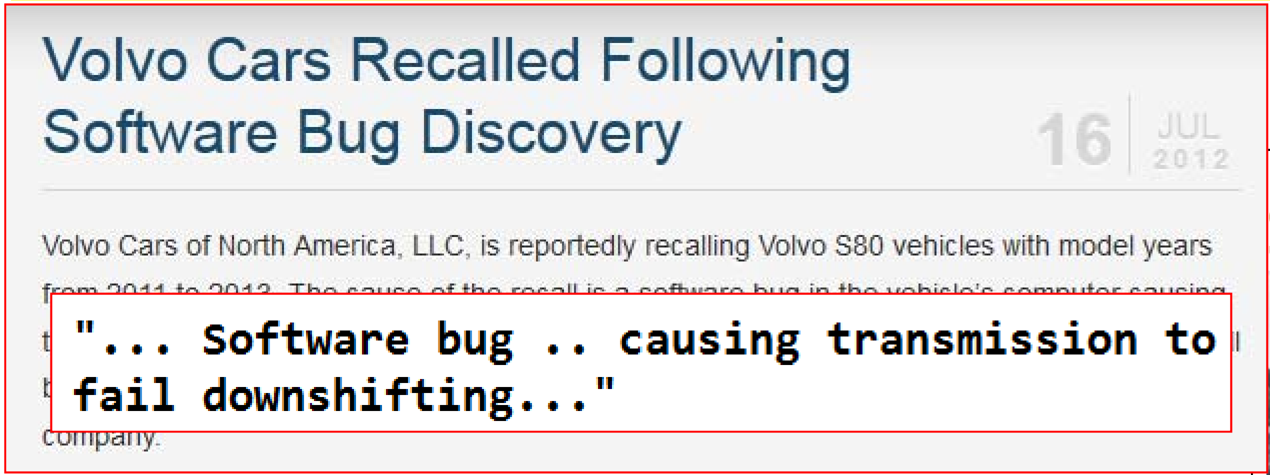
- Smart toys

How hackers gain access

- Hacker’s 6 Steps - According to National Center of Cybersecurity
  1. Gain authorities of system manager through **social engineering and spy emails**
  2. Remote entry to network through VPN (virtual private network), VNC (virtual network computing), and others
  3. **Scan** Intranet to know Operating Systems and terminals
  4. **Copy malware** files to one of the network computers to spread to other computers in the intranet
  5. Operate malware and worm software remotely using Group Policy or System Center Configuration Manager
  6. **Damage**: Deletion of Data, Destroy OS and Software Configuration, Encrypt Data

In addition, Software Faults

"... software failure has led to expensive and embarrassing recalls...."



Volvo Cars Recalled Following Software Bug Discovery

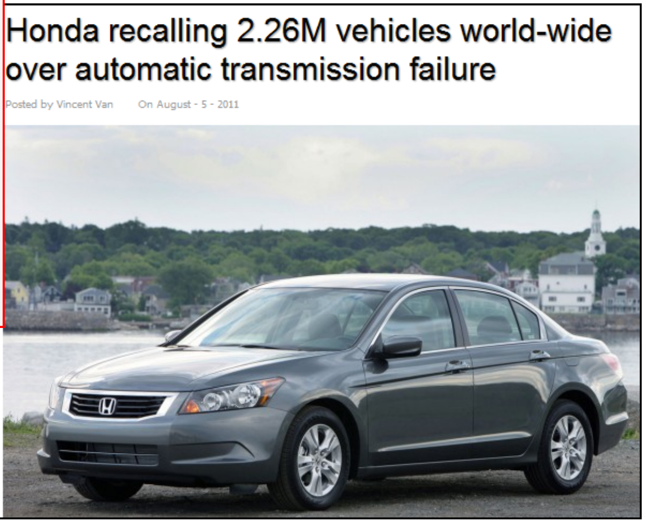
16 JUL 2012

Volvo Cars of North America, LLC, is reportedly recalling Volvo S80 vehicles with model years from 2011 to 2013. The cause of the recall is a software bug in the vehicle's computer causing t

b

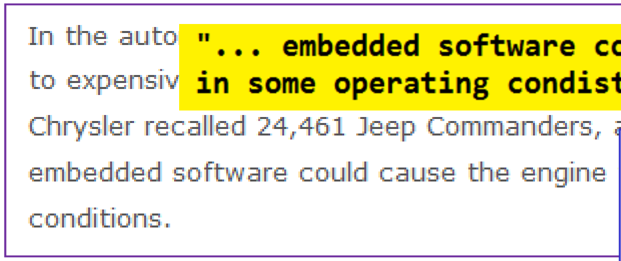
company.

"... Software bug .. causing transmission to fail downshifting..."



Honda recalling 2.26M vehicles world-wide over automatic transmission failure

Posted by Vincent Van   On August - 5 - 2011



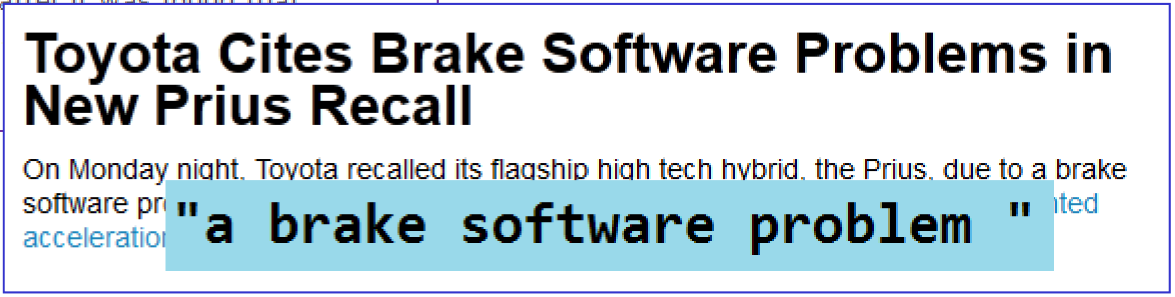
In the auto

to expensiv

Chrysler recalled 24,461 Jeep Commanders, after it was found that embedded software could cause the engine

conditions.

"... embedded software could cause engine to stall in some operating condistions."



Toyota Cites Brake Software Problems in New Prius Recall

On Monday night, Toyota recalled its flagship high tech hybrid, the Prius, due to a brake software pr

nted

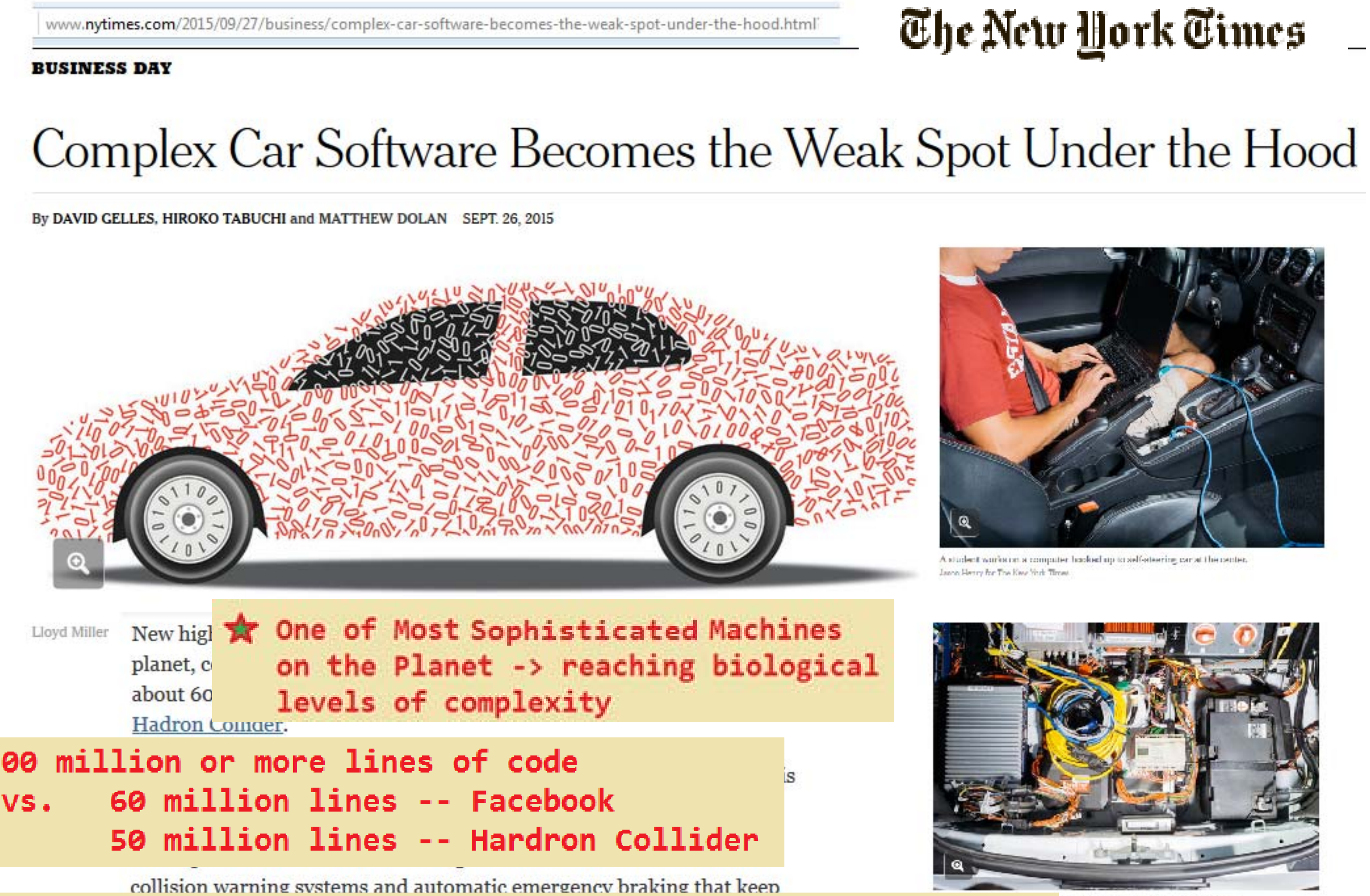
acceleratio

"a brake software problem "

Complexity and software-related problems

More Complex Than a Fighter Jet

2,000 Components
30,000 Parts
10 millision lines
of code



www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html

The New York Times

BUSINESS DAY

Complex Car Software Becomes the Weak Spot Under the Hood

By DAVID GELLES, HIROKO TABUCHI and MATTHEW DOLAN SEPT. 26, 2015

A student works on a computer hooked up to self-steering car at the center.
Jason Henry for The New York Times

Lloyd Miller

New higl
planet, c
about 60
Hadron Collider.

is

collision warning systems and automatic emergency braking that keep

e trunk of one of the self-steering vehicles.

★ One of Most Sophisticated Machines
on the Planet -> reaching biological
levels of complexity

☆ 100 million or more lines of code
(vs. 60 million lines -- Facebook
50 million lines -- Hardron Collider

★ Benefits

Faults, Failures, and

★ New Opportunities for Malevolence

Software - Curse of Flexibility

- Easy change of computer function by easy change of software – **flexible, quick and with low cost → error introduction, complexity**

Mechanical Construction

-Governed by mechanical limit

-Laws of dynamics

-Nature imposes discipline

-Control Complexity

Software Construction

-No physical limitation

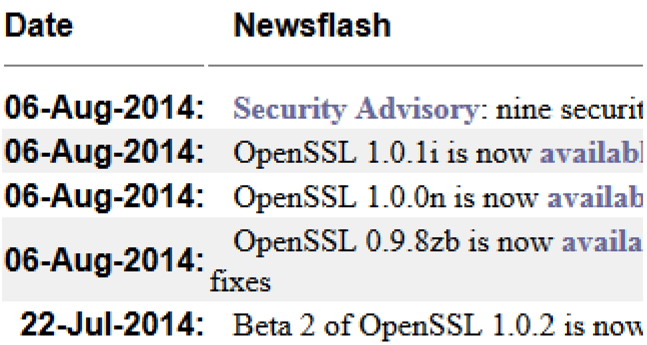
-Enormously complex design

-Premature construction before full understanding

- **Success and Partial success**
  - **S/W:**
    - Difficult to build one that works under all conditions
    - Possible to build one that works 90% of the time
  - **Aircraft:**
    - Almost impossible to build a plane that flies 90% of the time

Hidden Bugs in Trusted Software

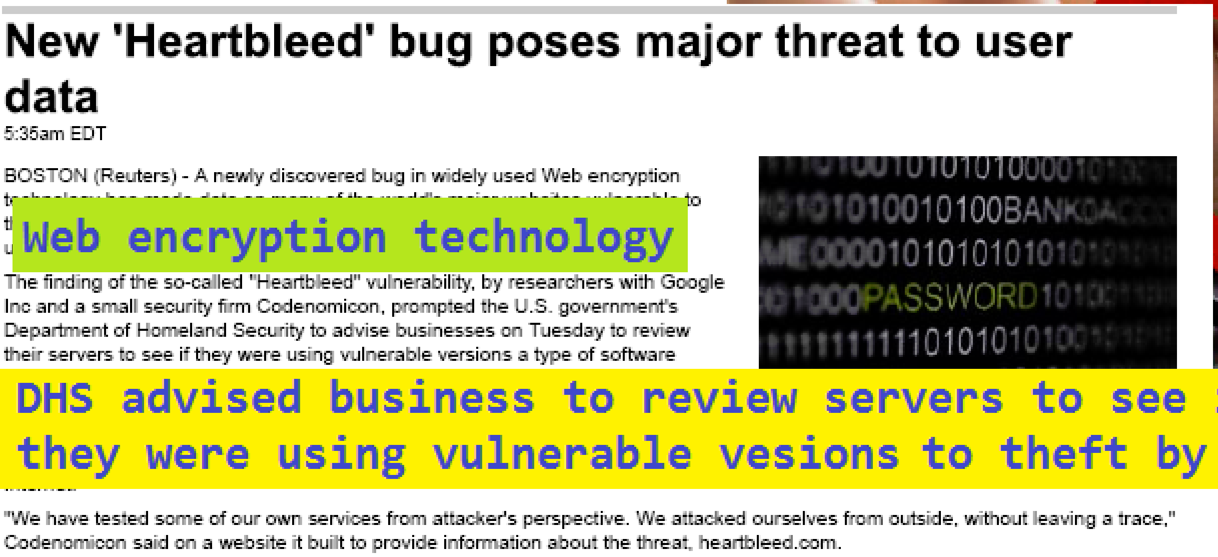
OpenSSL Project: (Secure Sockets Layer) + (Transport Layer Security)



Date	Newsflash
06-Aug-2014:	Security Advisory: nine securit
06-Aug-2014:	OpenSSL 1.0.1i is now availabl
06-Aug-2014:	OpenSSL 1.0.0n is now availab
06-Aug-2014:	OpenSSL 0.9.8zb is now availa fixes
22-Jul-2014:	Beta 2 of OpenSSL 1.0.2 is now

Heartbleed Bug: What is it, Who is handling our security

Heartbleed Bug has raised eyebrows of all the users across the globe and security advocates and surprisingly, only a few people are handling our internet security.



New 'Heartbleed' bug poses major threat to user data

5:35am EDT

BOSTON (Reuters) - A newly discovered bug in widely used Web encryption technology has made data on many of the world's major websites vulnerable to

Web encryption technology

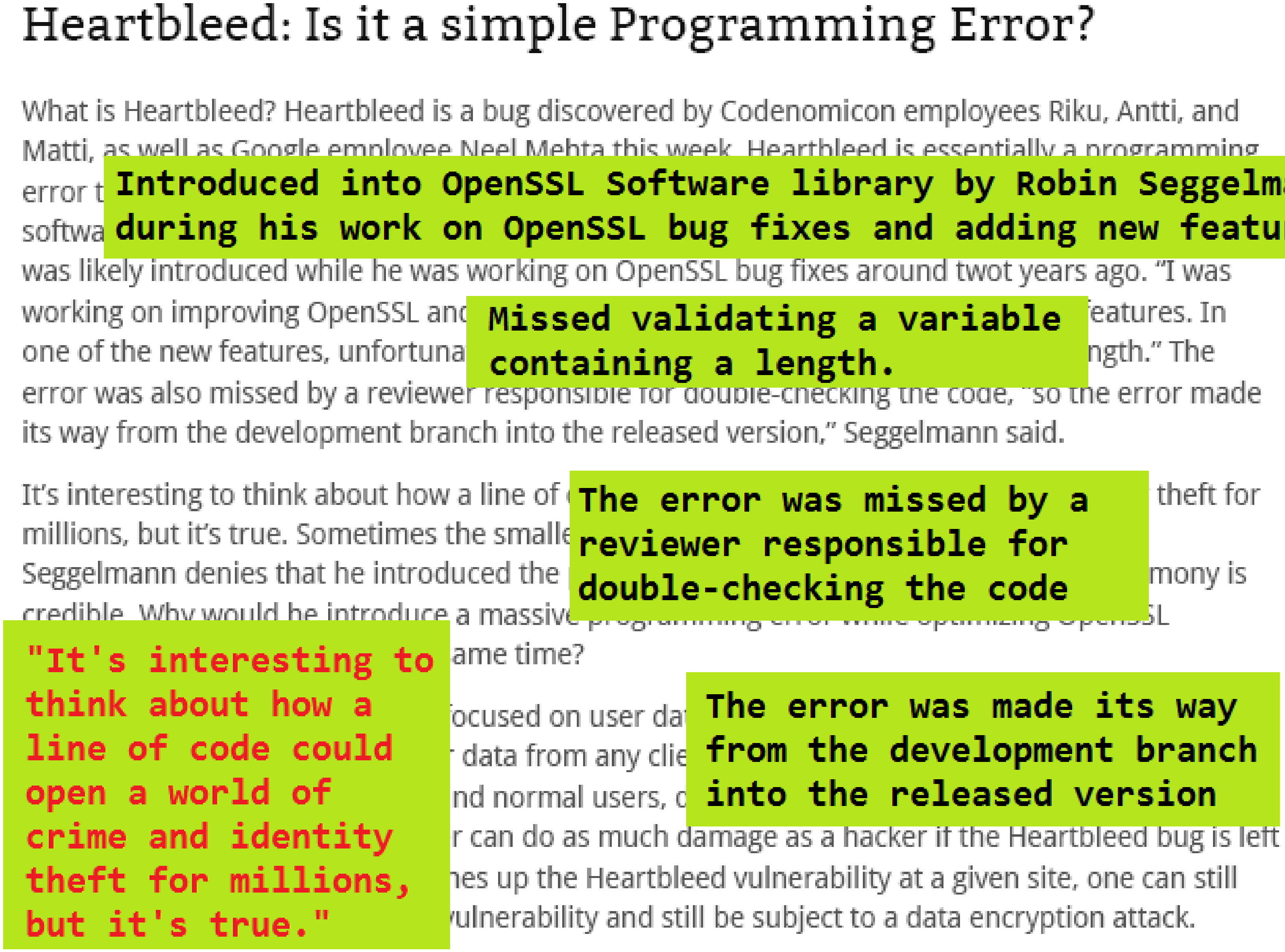
The finding of the so-called "Heartbleed" vulnerability, by researchers with Google Inc and a small security firm Codenomicon, prompted the U.S. government's Department of Homeland Security to advise businesses on Tuesday to review their servers to see if they were using vulnerable versions a type of software

DHS advised business to review servers to see if they were using vulnerable vesions to theft by hackers

"We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace," Codenomicon said on a website it built to provide information about the threat, heartbleed.com.

Deidre Richardson | On 19, Apr 2014

How errors were inserted



Heartbleed: Is it a simple Programming Error?

What is Heartbleed? Heartbleed is a bug discovered by Codenomicon employees Riku, Antti, and Matti, as well as Google employee Neel Mehta this week. Heartbleed is essentially a programming error t

softwa

was likely introduced while he was working on OpenSSL bug fixes around twot years ago. "I was working on improving OpenSSL and

eatures. In one of the new features, unfortuna

ngth." The error was also missed by a reviewer responsible for double-checking the code, "so the error made its way from the development branch into the released version," Seggelmann said.

It's interesting to think about how a line of

theft for millions, but it's true. Sometimes the smalle

Seggelmann denies that he introduced the

mony is credible. Why would he introduce a massive programming error while optimizing OpenSSL

ame time?

ocused on user da

data from any clie

nd normal users, c

r can do as much damage as a hacker if the Heartbleed bug is left

es up the Heartbleed vulnerability at a given site, one can still

ulnerability and still be subject to a data encryption attack.

Introduced into OpenSSL Software library by Robin Seggelmann during his work on OpenSSL bug fixes and adding new features.

Missed validating a variable containing a length.

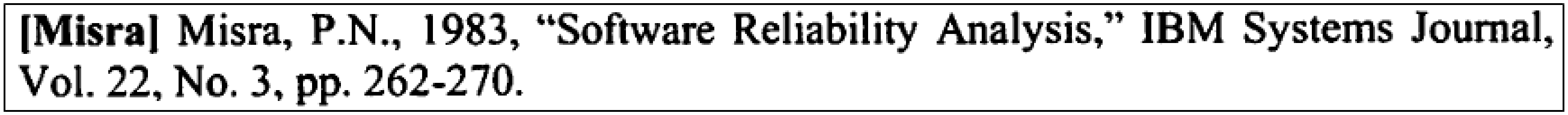
The error was missed by a reviewer responsible for double-checking the code

"It's interesting to think about how a line of code could open a world of crime and identity theft for millions, but it's true."

The error was made its way from the development branch into the released version

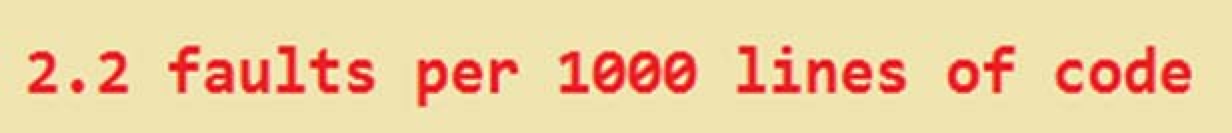
Software Failure and Quantification

- **Can software failure be quantified?**
  - **Fault Density**
    - “Software fault density”: the number of faults per unit of program size: # of faults per lines of code
    - Empirical study with previous software projects



[Misra] Misra, P.N., 1983, “Software Reliability Analysis,” IBM Systems Journal, Vol. 22, No. 3, pp. 262-270.

- **Finding**

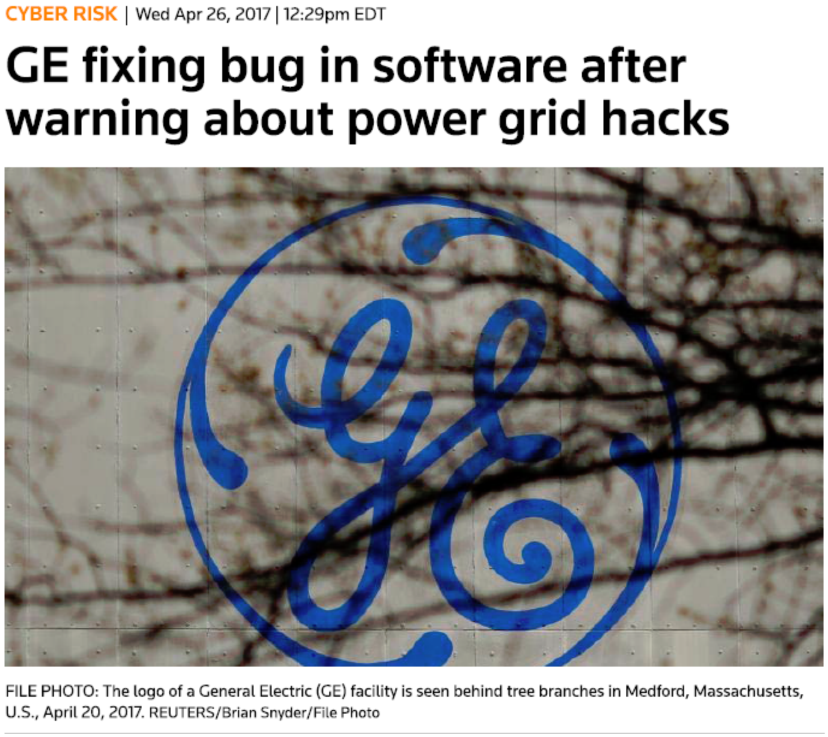


2.2 faults per 1000 lines of code

- **Implication:**
  - A practical reality is that operational software developed using contemporary practices tends to exhibit a fault density of **2.2x10^{-3}** faults per line
    - A software program must somehow be **inherently faulted** !!! ????

Protective Relay S/W Vulnerability

- A bug in software used to control the flow of electricity in a utility's power system: Identified in a Black Hat Conference
- Remote control of GE protection relays – "old GE relays introduced in the 1990s"
- Patches for 5 of 6 models affected by the vulnerabilities



CYBER RISK | Wed Apr 26, 2017 | 12:29pm EDT

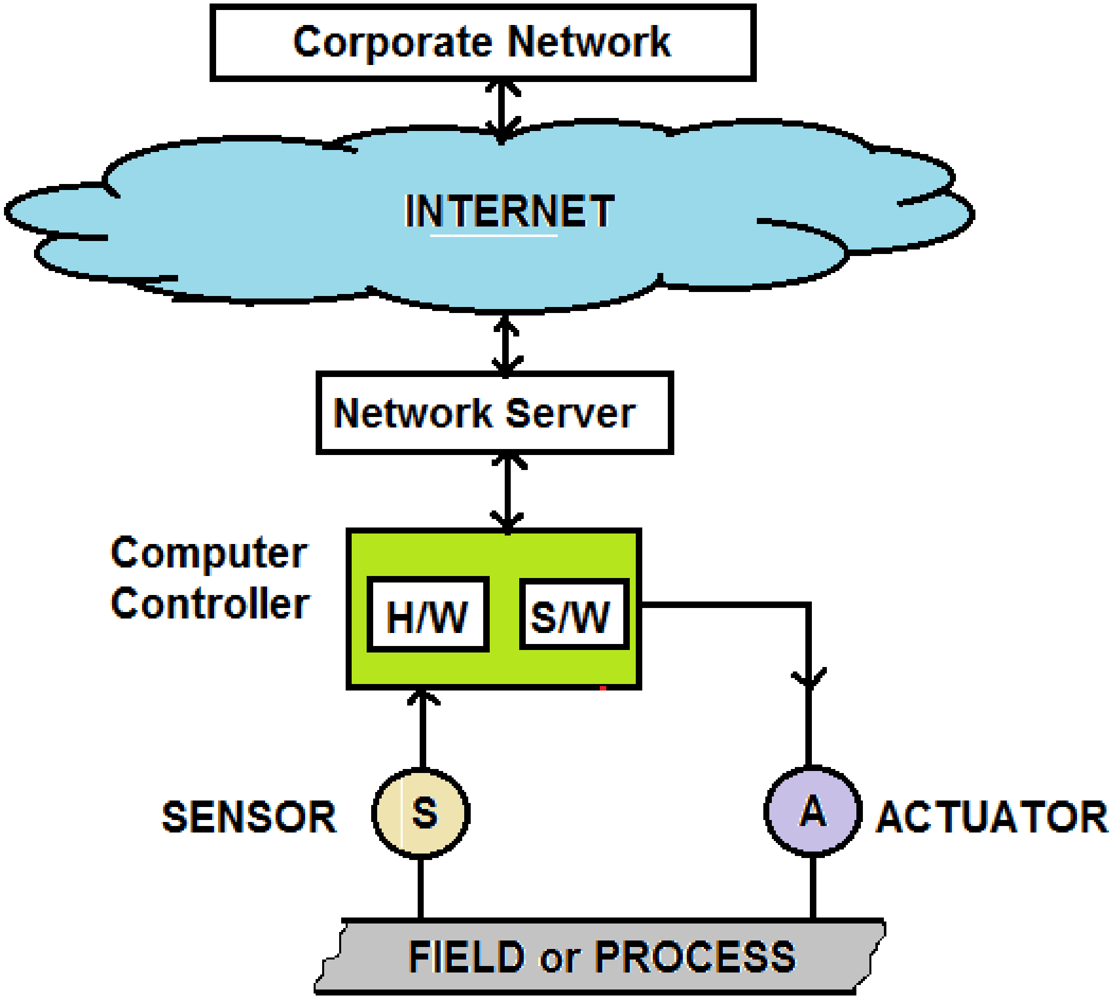
GE fixing bug in software after warning about power grid hacks

FILE PHOTO: The logo of a General Electric (GE) facility is seen behind tree branches in Medford, Massachusetts, U.S., April 20, 2017. REUTERS/Brian Snyder/File Photo

Present Approaches for ICS Hardening

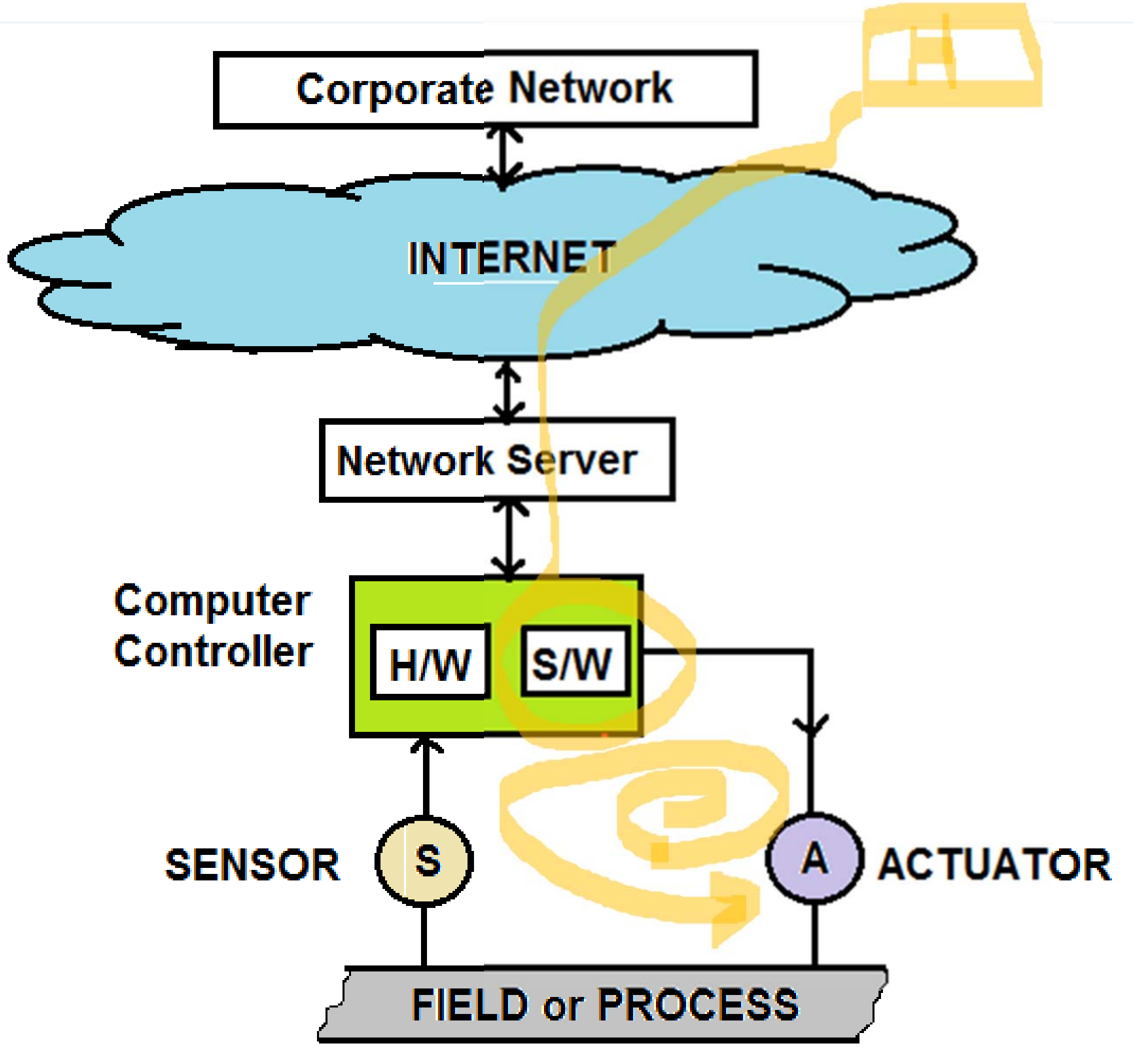
- Basis - Cyber Security for IT systems
- Strategies and tools for
  - Anomaly detection
  - Intrusion detection
  - Network access behavior analysis
  - Mitigation Strategy
- Problems
  - May block some known attacks and attack vectors
  - Post-mortem approach after damages have been done
  - No attack-proof
  - Exploitable vulnerabilities in ICS are real and, not addressed timely, cause **serious impacts to public safety and critical infrastructure**

Existing Control System [simple model]



- Sensors
- Actuators
- Enterprise network

Existing Control System [simple model]

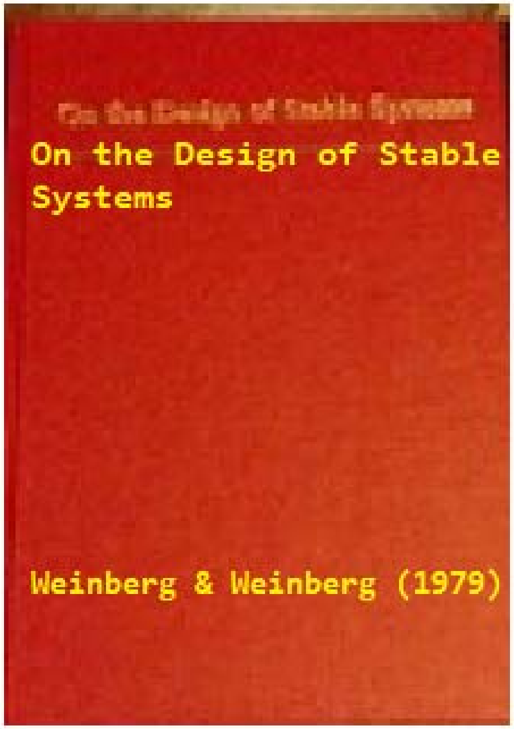


- Hacker may access to the controller and manipulate the S/W

Toward Cyber-Resilient ICS

- Cyber Insensitive
  - Operation Basis
- Hardware Redundancy
  - Supplementary control part (for “Safe-Mode”)
  - Unidirectional Communication for Situation alert
- Working under Compromised Situation
  - Fail-Safe or Fail-Operate
  - Resilience
- “Broken Part” Assumption

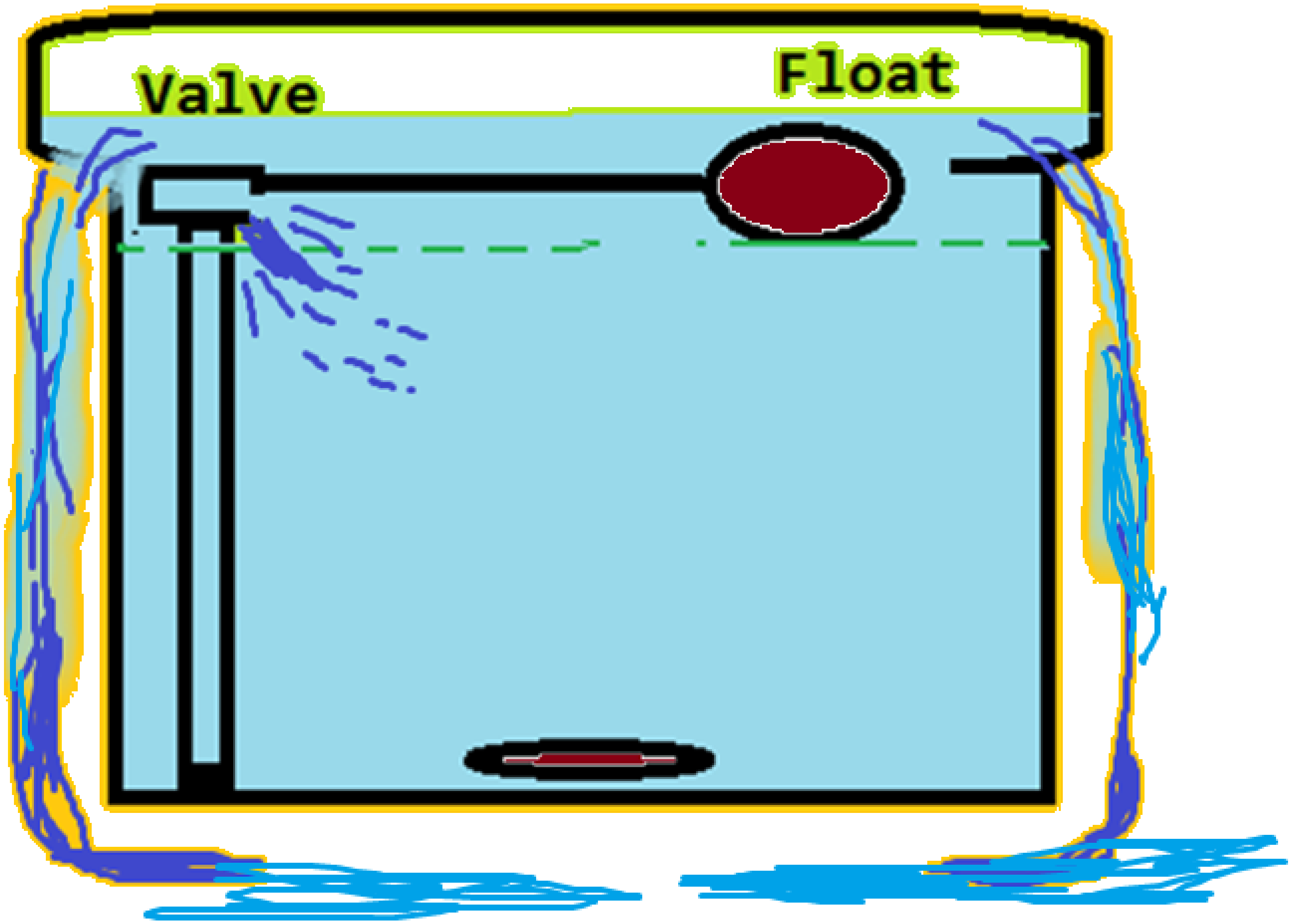
System Regulator Under the “Broken System” Assumption


On the Design of Stable Systems
On the Design of Stable Systems
Weinberg & Weinberg (1979)

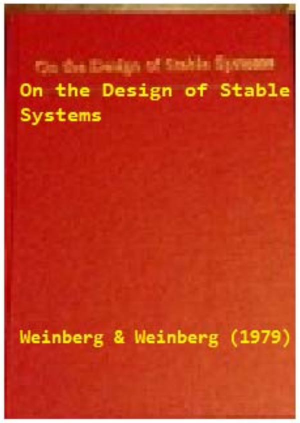
- Old Toilet Age
- Flooded floor every morning
- After moping, a toilet appears trouble-free during the day
- Flooded floor again the next morning

System Regulator Under the “Broken System” Assumption

- Busy Time – Flushes before water level goes above
- Night Hours – the effect of Valve Failure is realized



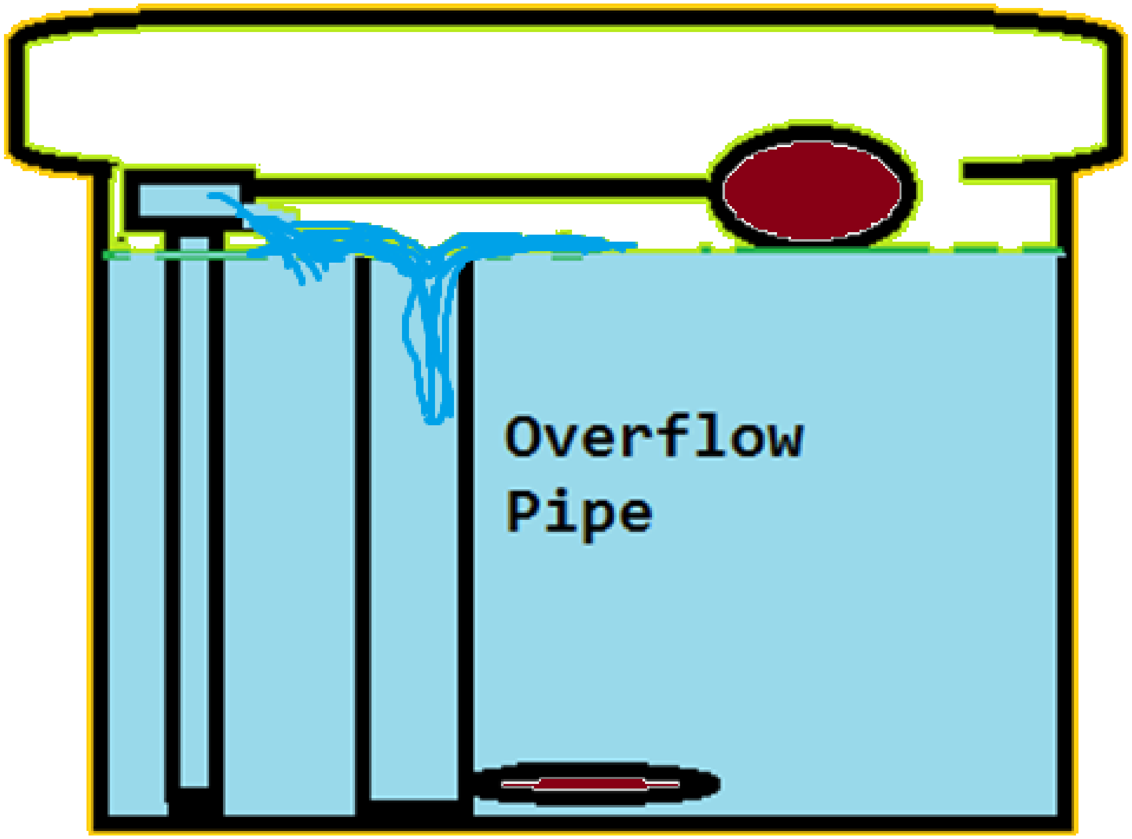
System Regulator Under the “Broken System” Assumption



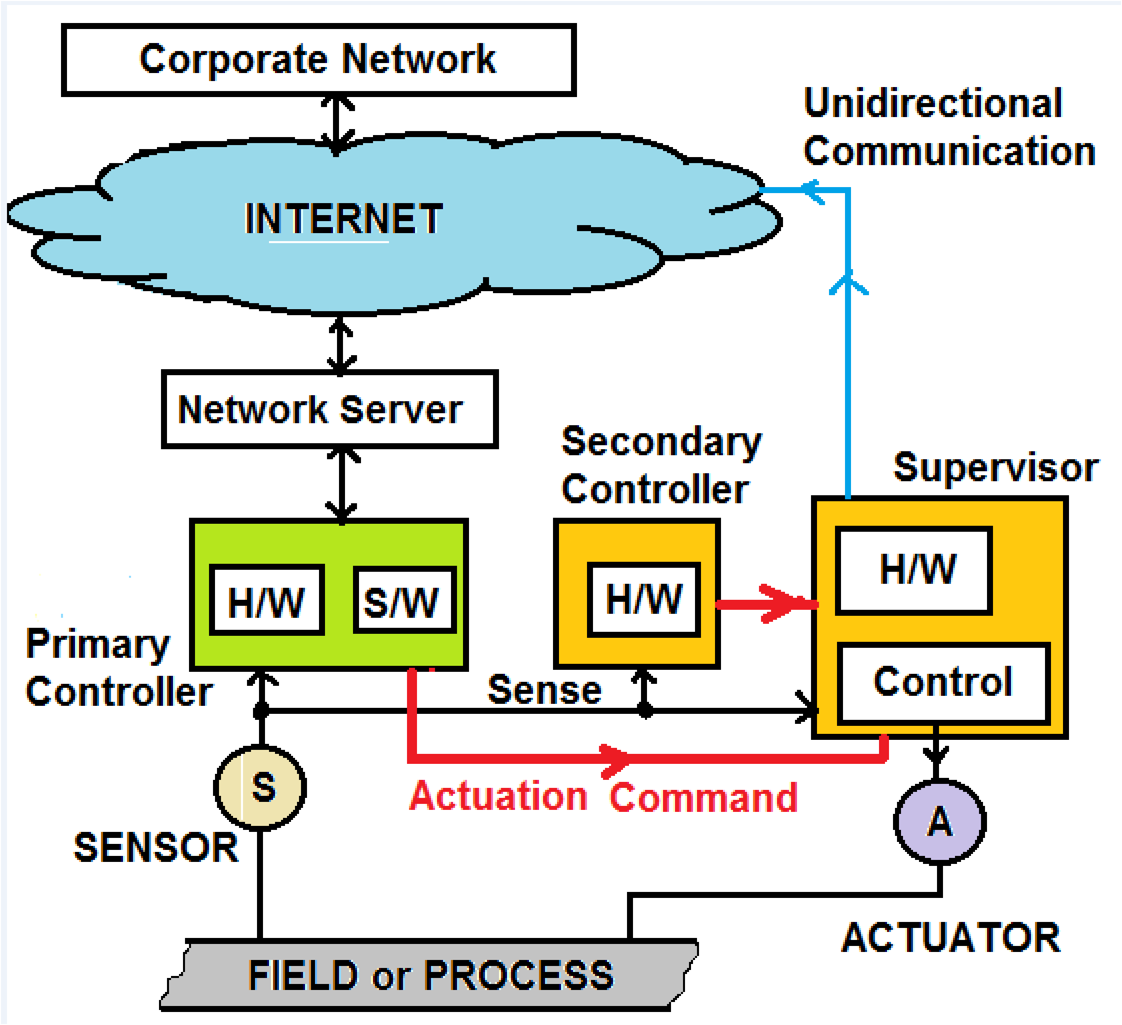
On the Design of Stable Systems

Weinberg & Weinberg (1979)

- How to design a toilet under the assumption that the gasket on the valve will eventually wear out?



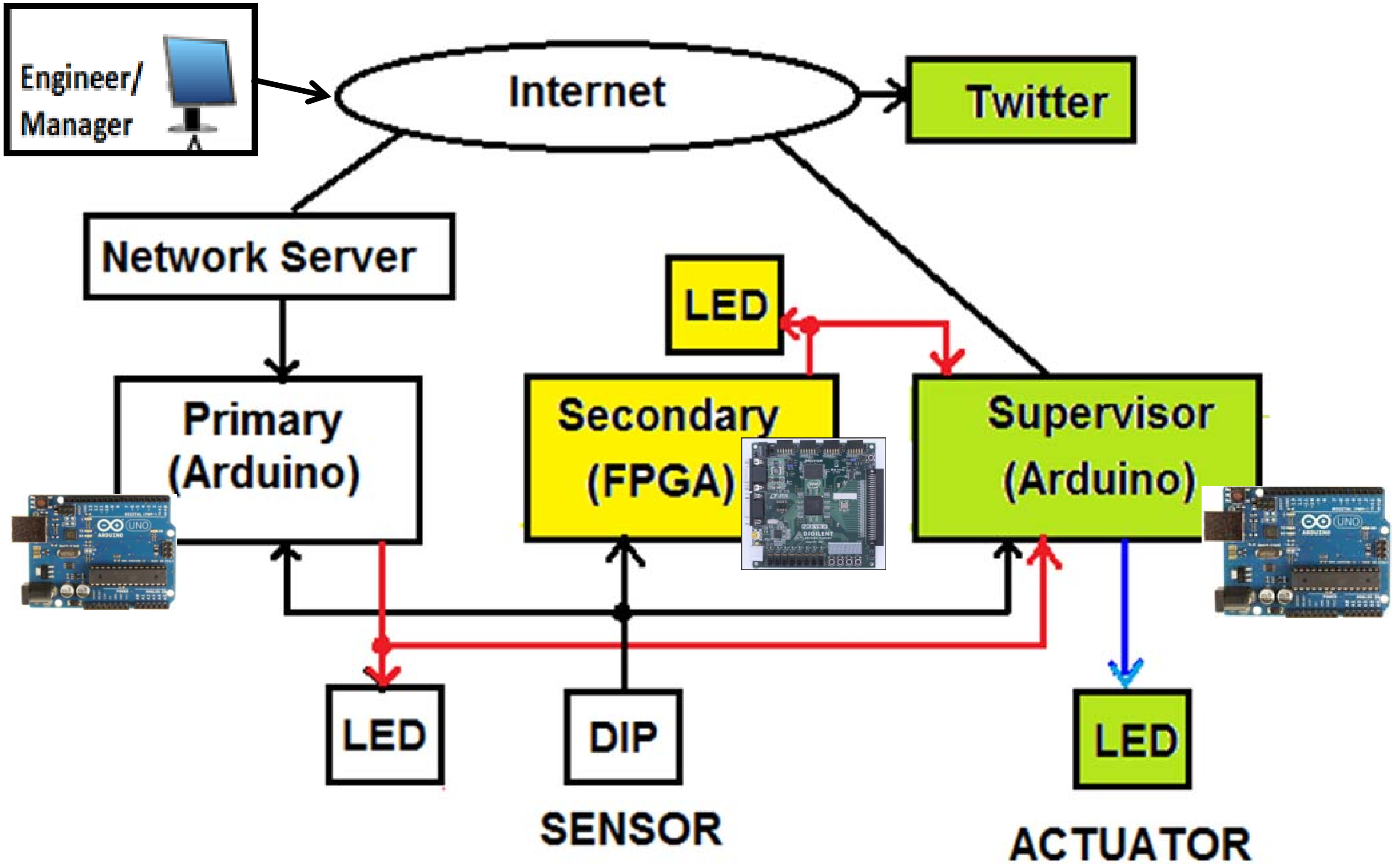
Architecture of Diversified Redundant Control System



- Network connected **Primary Controller**
- Isolated **Secondary Controller** – full duplication or a part for “safe mode”
- **Supervisor** for Operation-Basis Supervision
- Unidirectional Reporting
- Cyber-Robust for
  - Common Virus
  - Man-in-the-middle attack
  - Stuxnet-like Worm

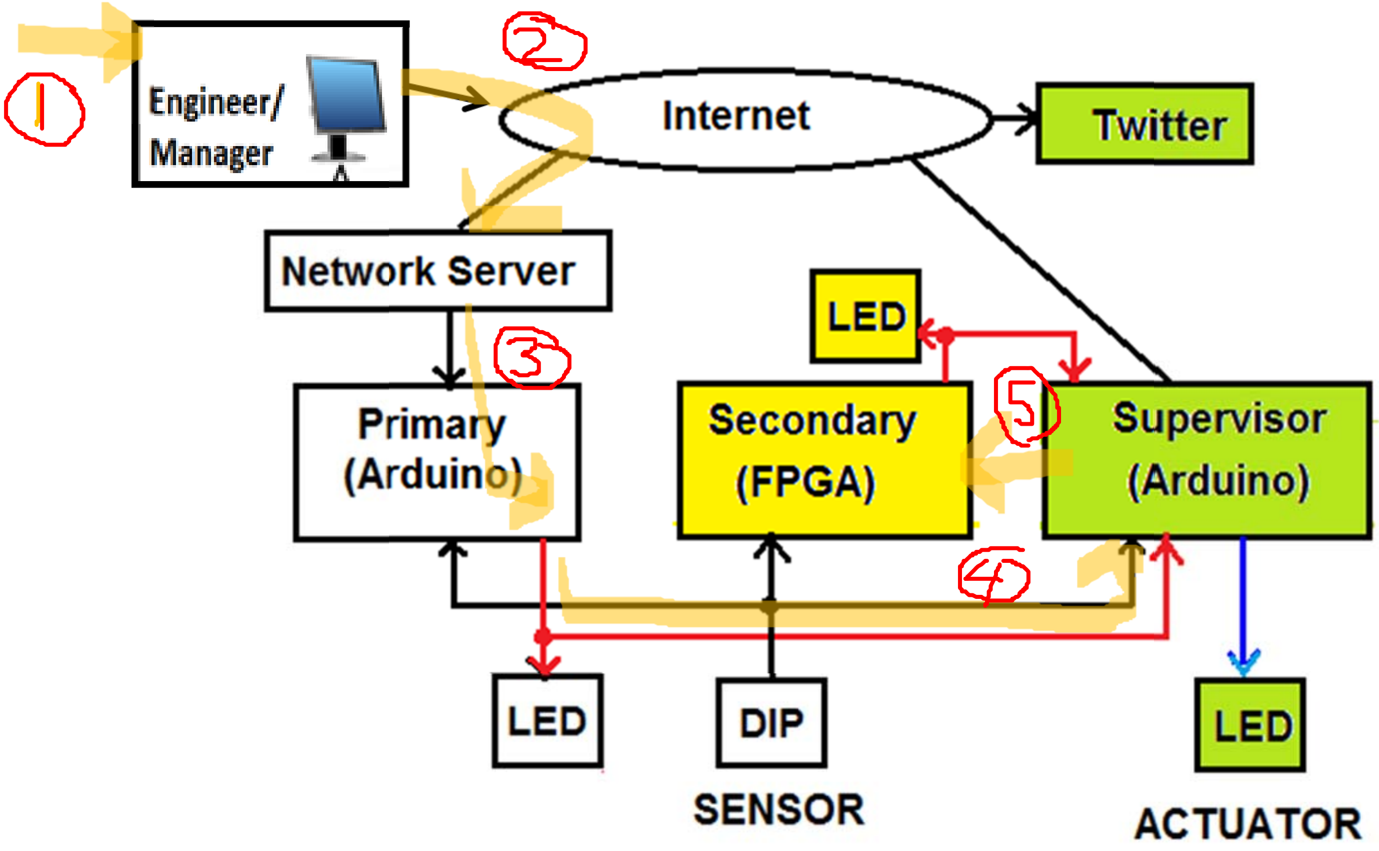
Validation in Lab Experimentation

- Network Server: Internet Connected Laptop with IP 10.232.100.114
- Supervisor holds an operational data(base) in it
- Simple code: Read the DIP position and Send out corresponding LED on/off

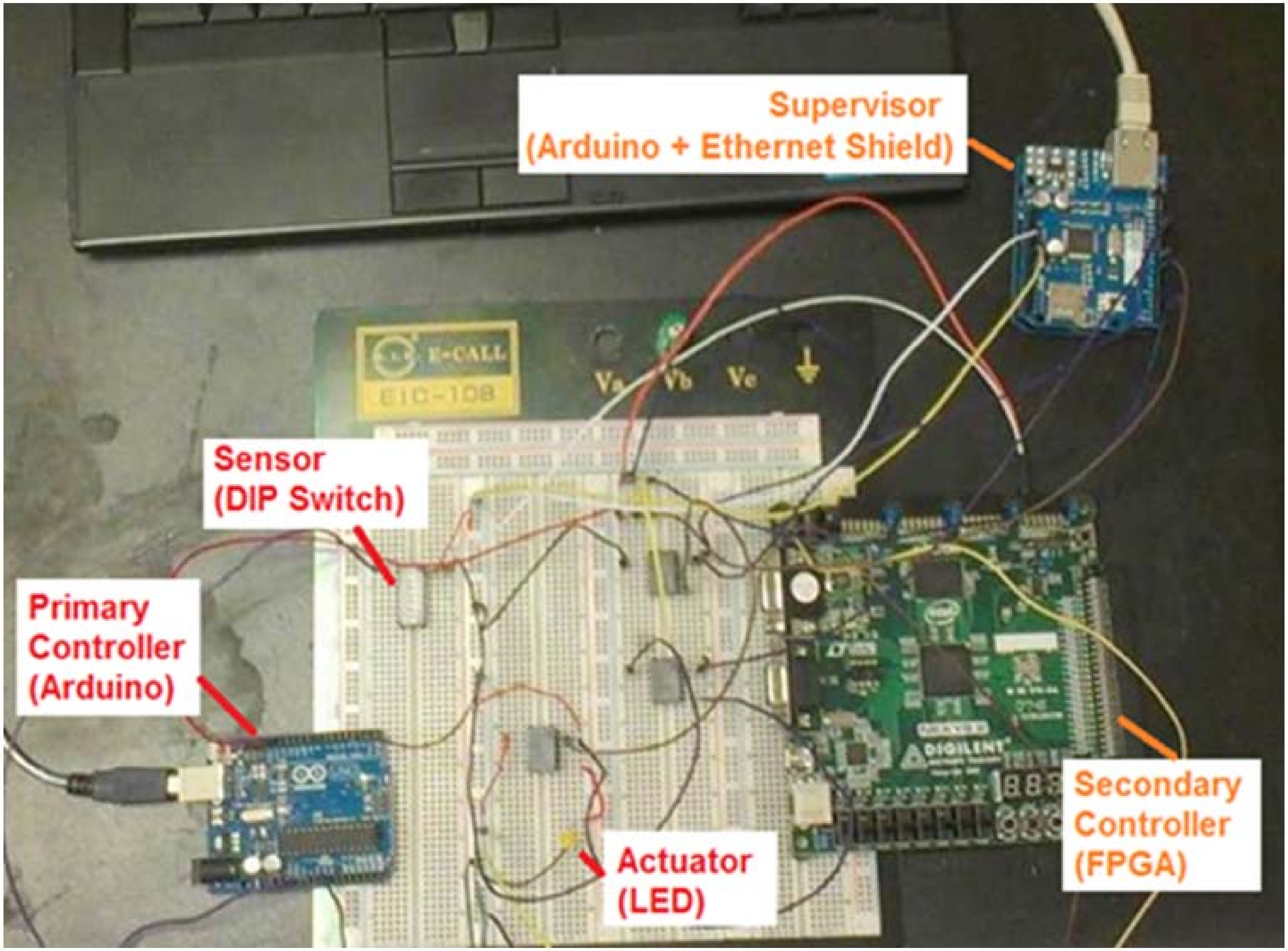


Validation in Lab Experimentation – Attack/Response Scenario

- (1) Engineer/Manager Credentials Stolen
- (2) Remote Access to the Network Server
- (3) Access to the Primary Controller →Malicious Code Change
- (4) Supervisor Notices Operation Change
- (5) Transfer Control to the Secondary Controller



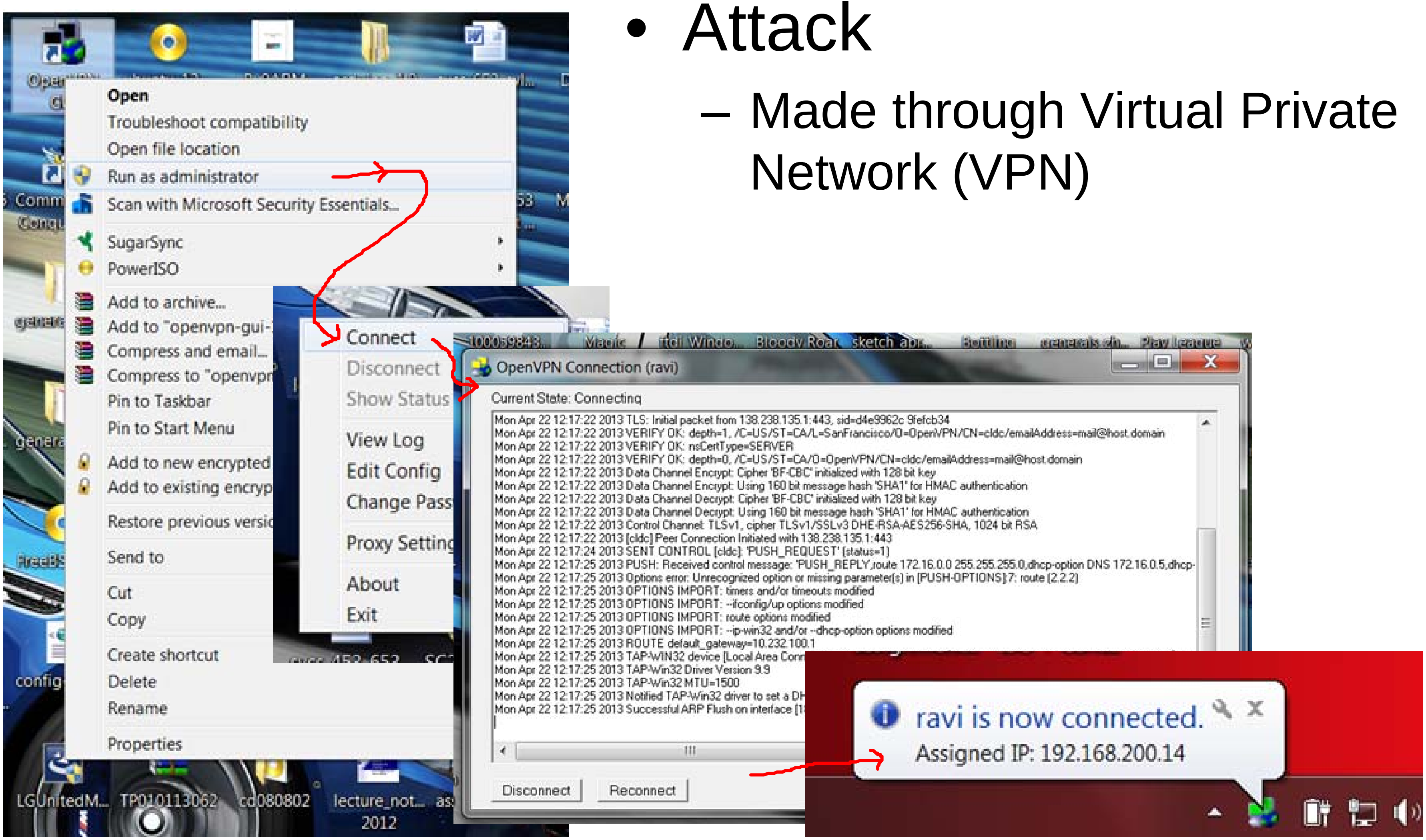
Validation in Lab Experimentation



Validation in Lab Experimentation

Open VPN

- Attack
  - Made through Virtual Private Network (VPN)



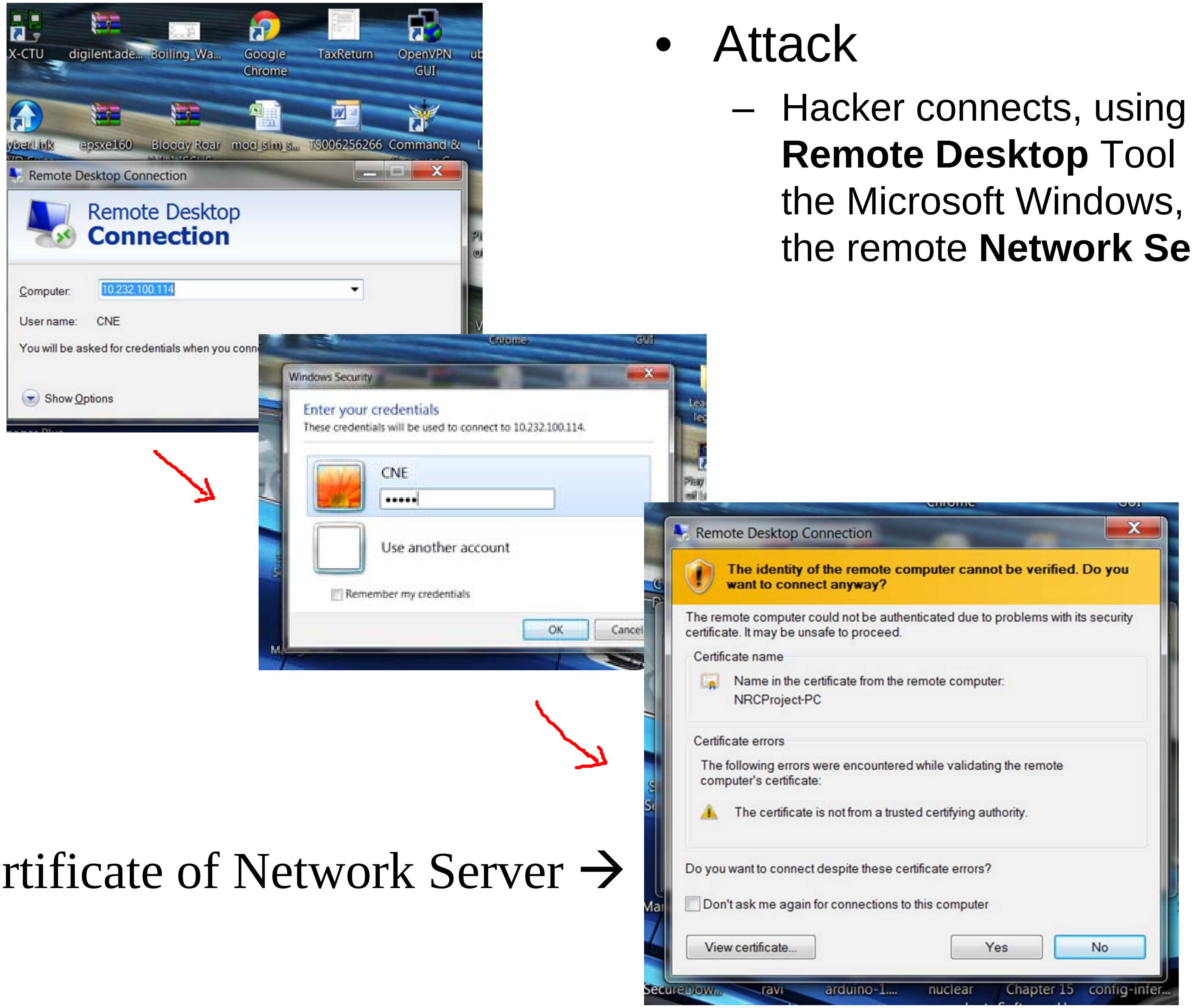
Current State: Connecting

```
Mon Apr 22 12:17:22 2013 TLS: Initial packet from 138.238.135.1:443, sid=d4e9962c 9fefcb34
Mon Apr 22 12:17:22 2013 VERIFY OK: depth=1, /C=US/ST=CA/L=SanFrancisco/O=OpenVPN/CN=cldc/emailAddress=mail@host.domain
Mon Apr 22 12:17:22 2013 VERIFY OK: nsCertType=SERVER
Mon Apr 22 12:17:22 2013 VERIFY OK: depth=0, /C=US/ST=CA/O=OpenVPN/CN=cldc/emailAddress=mail@host.domain
Mon Apr 22 12:17:22 2013 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Apr 22 12:17:22 2013 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Apr 22 12:17:22 2013 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Apr 22 12:17:22 2013 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Apr 22 12:17:22 2013 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Mon Apr 22 12:17:22 2013 [cldc] Peer Connection Initiated with 138.238.135.1:443
Mon Apr 22 12:17:24 2013 SENT CONTROL [cldc]: 'PUSH_REQUEST' (status=1)
Mon Apr 22 12:17:25 2013 PUSH: Received control message: 'PUSH_REPLY,route 172.16.0.0 255.255.255.0,dhcp-option DNS 172.16.0.5,dhcp-
Mon Apr 22 12:17:25 2013 Options error: Unrecognized option or missing parameter(s) in [PUSH-OPTIONS]:7: route (2.2.2)
Mon Apr 22 12:17:25 2013 OPTIONS IMPORT: timers and/or timeouts modified
Mon Apr 22 12:17:25 2013 OPTIONS IMPORT: --ifconfig/up options modified
Mon Apr 22 12:17:25 2013 OPTIONS IMPORT: route options modified
Mon Apr 22 12:17:25 2013 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Mon Apr 22 12:17:25 2013 ROUTE default_gateway=10.232.100.1
Mon Apr 22 12:17:25 2013 TAP-WIN32 device [Local Area Conn
Mon Apr 22 12:17:25 2013 TAP-Win32 Driver Version 9.9
Mon Apr 22 12:17:25 2013 TAP-Win32 MTU=1500
Mon Apr 22 12:17:25 2013 Notified TAP-Win32 driver to set a DH
Mon Apr 22 12:17:25 2013 Successful ARP Flush on interface [1
```

ravi is now connected.
Assigned IP: 192.168.200.14

Validation in Lab Experimentation

- Attack
  - Hacker connects, using **Remote Desktop** Tool of the Microsoft Windows, to the remote **Network Server**



Remote Desktop Connection

Computer: 10.232.100.114

User name: CNE

You will be asked for credentials when you conn

Windows Security

Enter your credentials

These credentials will be used to connect to 10.232.100.114.

CNE

•••••

Use another account

□ Remember my credentials

Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer: NRCProject-PC

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

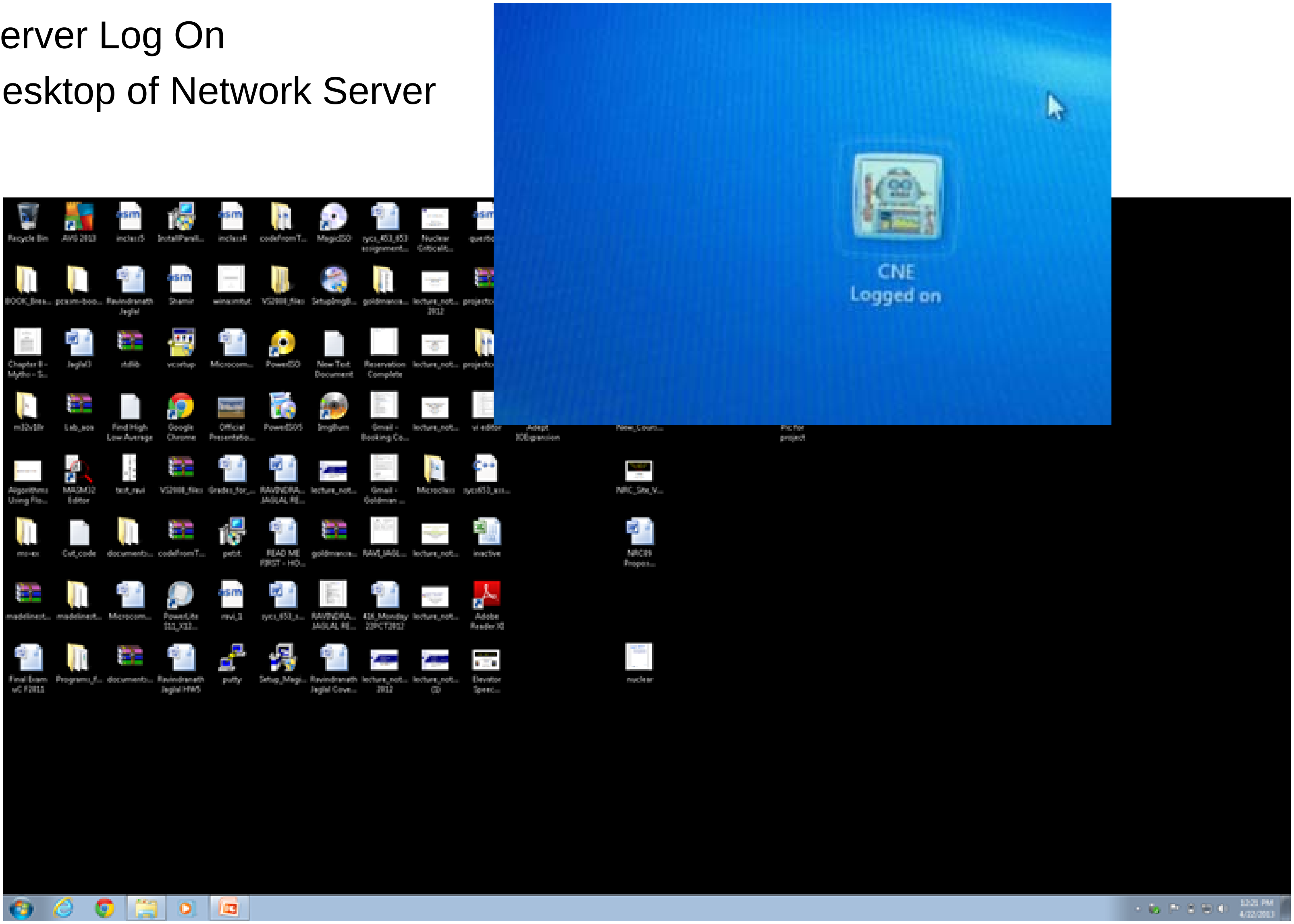
Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

Certificate of Network Server →

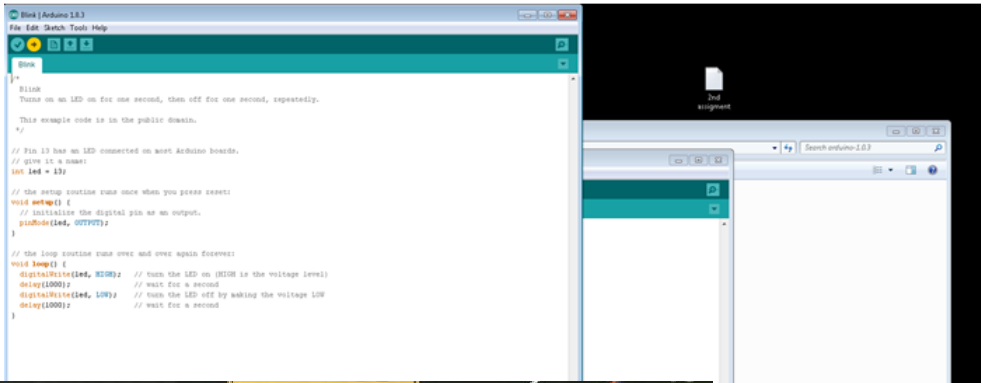
Validation in Lab Experimentation

- Server Log On
- Desktop of Network Server

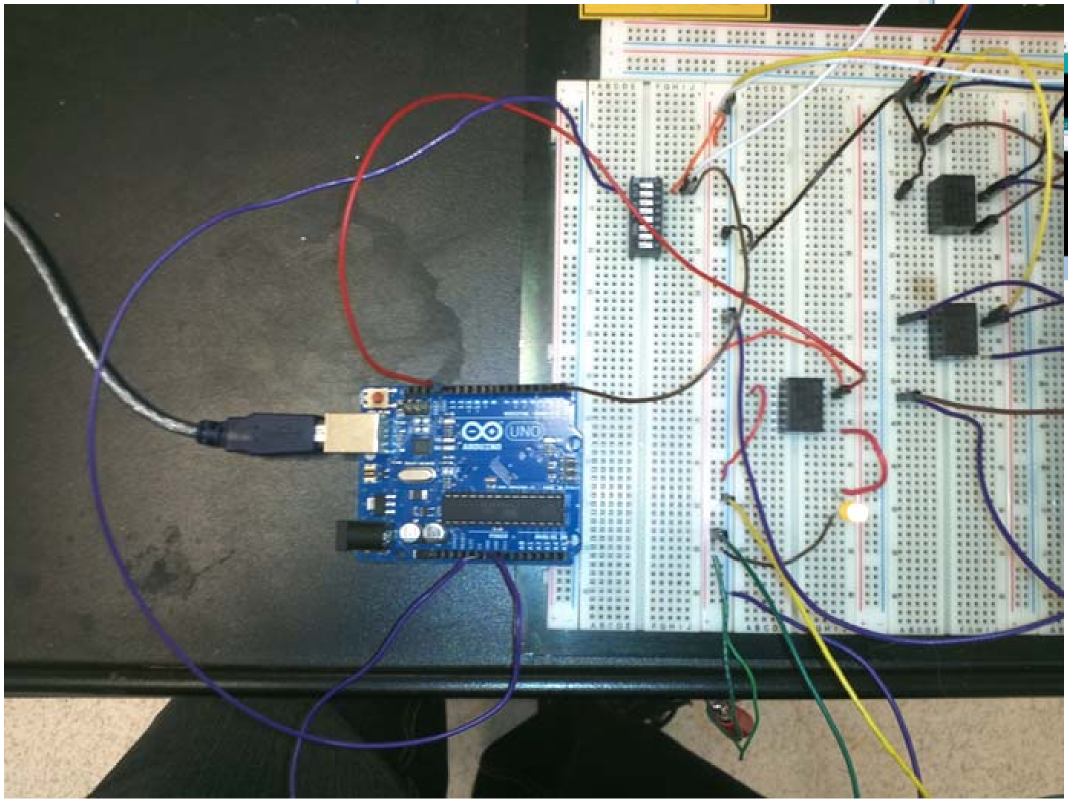


Validation in Lab Experimentation

- Code Change
- Upload the Revised Code
- Run to code



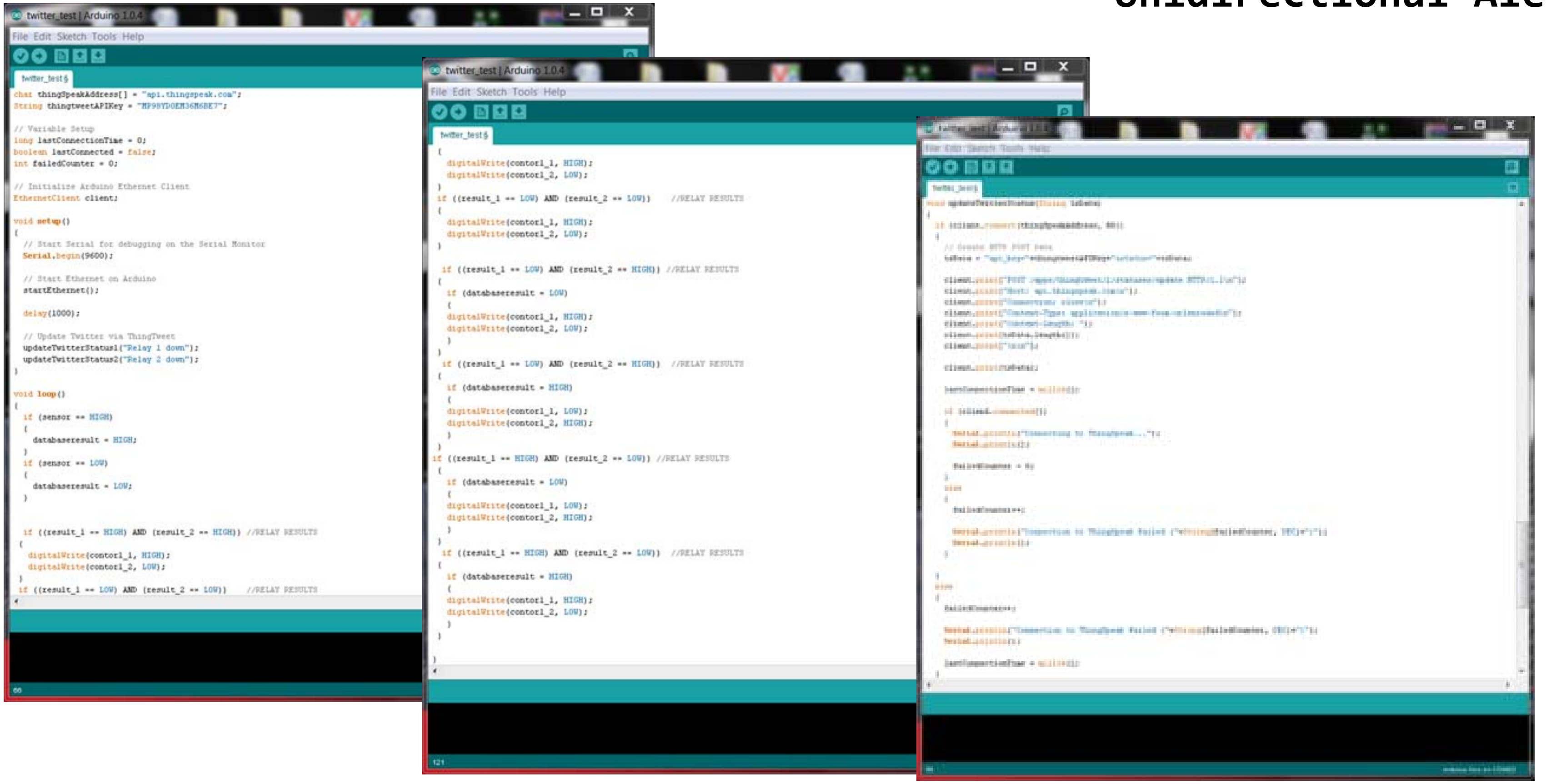
```
/*
  Blink
  Turns on an LED on for one second, then off for one second, repeatedly.

  This example code is in the public domain.
 */

// Pin 13 has an LED connected on most Arduino boards.
// give it a name:
int led = 13;

// the setup routine runs once when you press reset:
void setup() {
  // initialize the digital pin as an output.
  pinMode(led, OUTPUT);
}

// the loop routine runs over and over again forever:
void loop() {
  digitalWrite(led, HIGH);   // turn the LED on (HIGH is the voltage level)
  delay(1000);               // wait for a second
  digitalWrite(led, LOW);    // turn the LED off by making the voltage LOW
  delay(1000);               // wait for a second
}
```



Validation in Lab Experimentation – New Architecture

Supervisor's Action:

(1) Operation-Action mismatch recognized
(2) Control Transfer to Secondary Controller
(3) Twitter Message -- Simulation of Unidirectional Alert



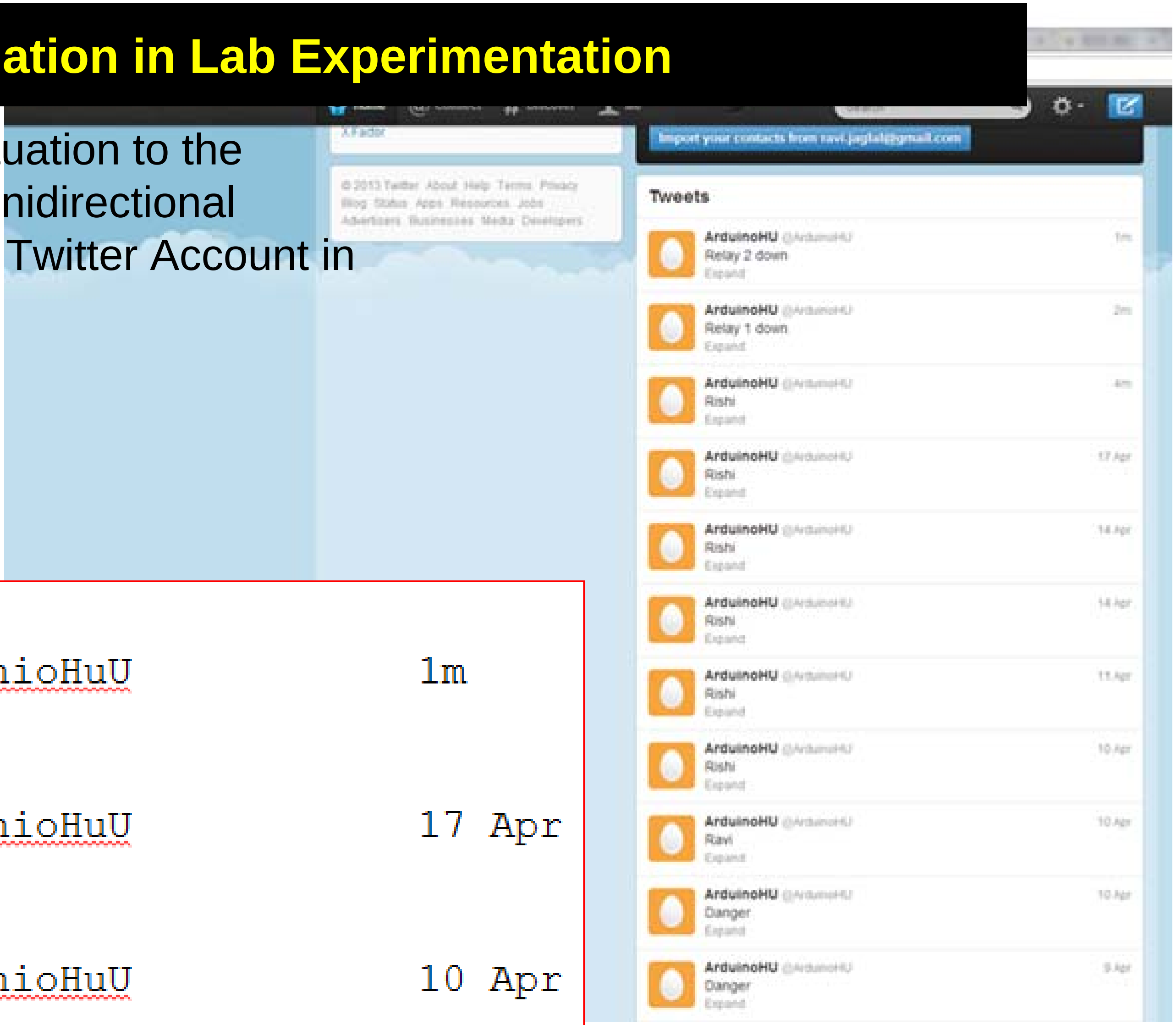
```
char thingSpeakAddress[] = "api.thingspeak.com";
String thingtweetAPIKey = "MP98YD0EM36M6BE7";

// Variable Setup
long lastConnectionTime = 0;
boolean lastConnected = false;
int failedCounter = 0;

// Initialize Arduino Ethernet Client
EthernetClient client;

void setup()
{
  // Start Serial for debugging on the Serial Monitor
  Serial.begin(9600);

  // Start Ethernet on Arduino
  startEthernet();

  delay(1000);

  // Update Twitter via ThingTweet
  updateTwitterStatus1("Relay 1 down");
  updateTwitterStatus2("Relay 2 down");
}

void loop()
{
  if (sensor == HIGH)
  {
    databaseresult = HIGH;
  }
  if (sensor == LOW)
  {
    databaseresult = LOW;
  }


  if ((result_1 == HIGH) AND (result_2 == HIGH)) //RELAY RESULTS
 {
   digitalWrite(contorl_1, HIGH);
   digitalWrite(contorl_2, LOW);
 }
 if ((result_1 == LOW) AND (result_2 == LOW))    //RELAY RESULTS
```

```
 {
   digitalWrite(contorl_1, HIGH);
   digitalWrite(contorl_2, LOW);
 }
 if ((result_1 == LOW) AND (result_2 == LOW))    //RELAY RESULTS
 {
   digitalWrite(contorl_1, HIGH);
   digitalWrite(contorl_2, LOW);
 }

  if ((result_1 == LOW) AND (result_2 == HIGH)) //RELAY RESULTS
 {
   if (databaseresult = LOW)
   {
   digitalWrite(contorl_1, HIGH);
   digitalWrite(contorl_2, LOW);
   }
 }
  if ((result_1 == LOW) AND (result_2 == HIGH))  //RELAY RESULTS
 {
   if (databaseresult = HIGH)
   {
   digitalWrite(contorl_1, LOW);
   digitalWrite(contorl_2, HIGH);
   }
 }
if ((result_1 == HIGH) AND (result_2 == LOW)) //RELAY RESULTS
 {
   if (databaseresult = LOW)
   {
   digitalWrite(contorl_1, LOW);
   digitalWrite(contorl_2, HIGH);
   }
 }
  if ((result_1 == HIGH) AND (result_2 == LOW))  //RELAY RESULTS
 {
   if (databaseresult = HIGH)
   {
   digitalWrite(contorl_1, HIGH);
   digitalWrite(contorl_2, LOW);
   }
 }

}
```

```
void updateTwitterStatus(String tsData)
{
  if (client.connect(thingSpeakAddress, 80))
  {
    // Create HTTP POST Data
    tsData = "api_key="+thingtweetAPIKey+"&status="+tsData;

    client.print("POST /apps/thingtweet/1/statuses/update HTTP/1.1\n");
    client.print("Host: api.thingspeak.com\n");
    client.print("Connection: close\n");
    client.print("Content-Type: application/x-www-form-urlencoded\n");
    client.print("Content-Length: ");
    client.print(tsData.length());
    client.print("\n\n");

    client.print(tsData);

    lastConnectionTime = millis();

    if (client.connected())
    {
      Serial.println("Connecting to ThingSpeak...");
      Serial.println();

      failedCounter = 0;
    }
    else
    {
      failedCounter++;

      Serial.println("Connection to ThingSpeak failed ("+String(failedCounter, DEC)+")");
      Serial.println();
    }

  }
  else
  {
    failedCounter++;

    Serial.println("Connection to ThingSpeak Failed ("+String(failedCounter, DEC)+")");
    Serial.println();

    lastConnectionTime = millis();
  }
```

Validation in Lab Experimentation

- Supervisor reports the situation to the enterprise system via a unidirectional network (Tweeting to the Twitter Account in this lab experiment)



X Factor
© 2013 Twitter About Help Terms Privacy
Blog Status Apps Resources Jobs
Advertisers Businesses Media Developers
Import your contacts from ravi.jaglal@gmail.com

Tweets

ArduinoHU @ArduinoHU 1m
Relay 2 down
Expand

ArduinoHU @ArduinoHU 2m
Relay 1 down
Expand

ArduinoHU @ArduinoHU 4m
Rishi
Expand

ArduinoHU @ArduinoHU 17 Apr
Rishi
Expand

ArduinoHU @ArduinoHU 14 Apr
Rishi
Expand

ArduinoHU @ArduinoHU 14 Apr
Rishi
Expand

ArduinoHU @ArduinoHU 11 Apr
Rishi
Expand

ArduinoHU @ArduinoHU 10 Apr
Rishi
Expand

ArduinoHU @ArduinoHU 10 Apr
Ravi
Expand

ArduinoHU @ArduinoHU 10 Apr
Danger
Expand

ArduinoHU @ArduinoHU 9 Apr
Danger
Expand

```
Tweets
ArduinoHU @ArdunioHuU            1m
Realy1 down
Expand
ArduinoHU @ArdunioHuU            17 Apr
Rishi
Expand
ArduinoHU @ArdunioHuU            10 Apr
Ravi
Expand
```

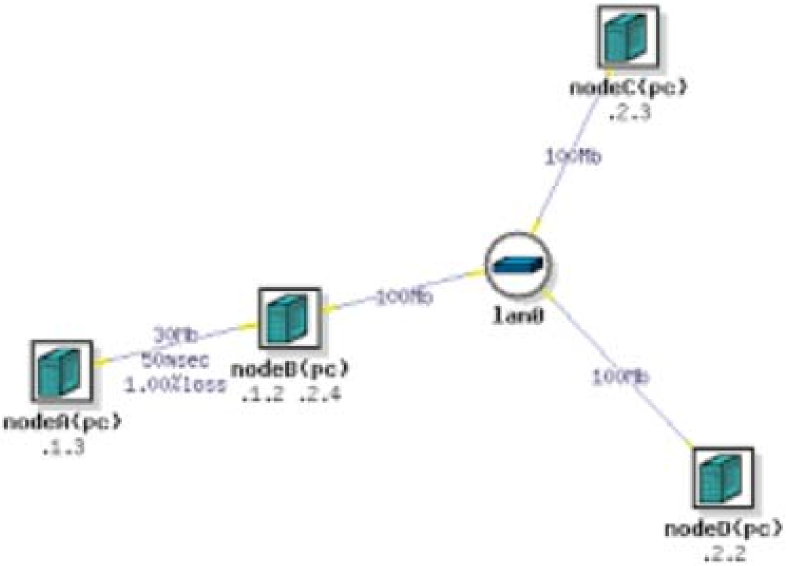
Validation in Cybersecurity Testbed

The DETER Project

deterlab
based on emulab

DETERlab (Cyber DEfense Technology Experimental Research Laboratory)

- 400 computer nodes
- 10 network interfaces/node
- >200 active projects
  - 6 power grid projects
  - 2 Control Systems
- USC, UC Berkeley, and DHS/NSF

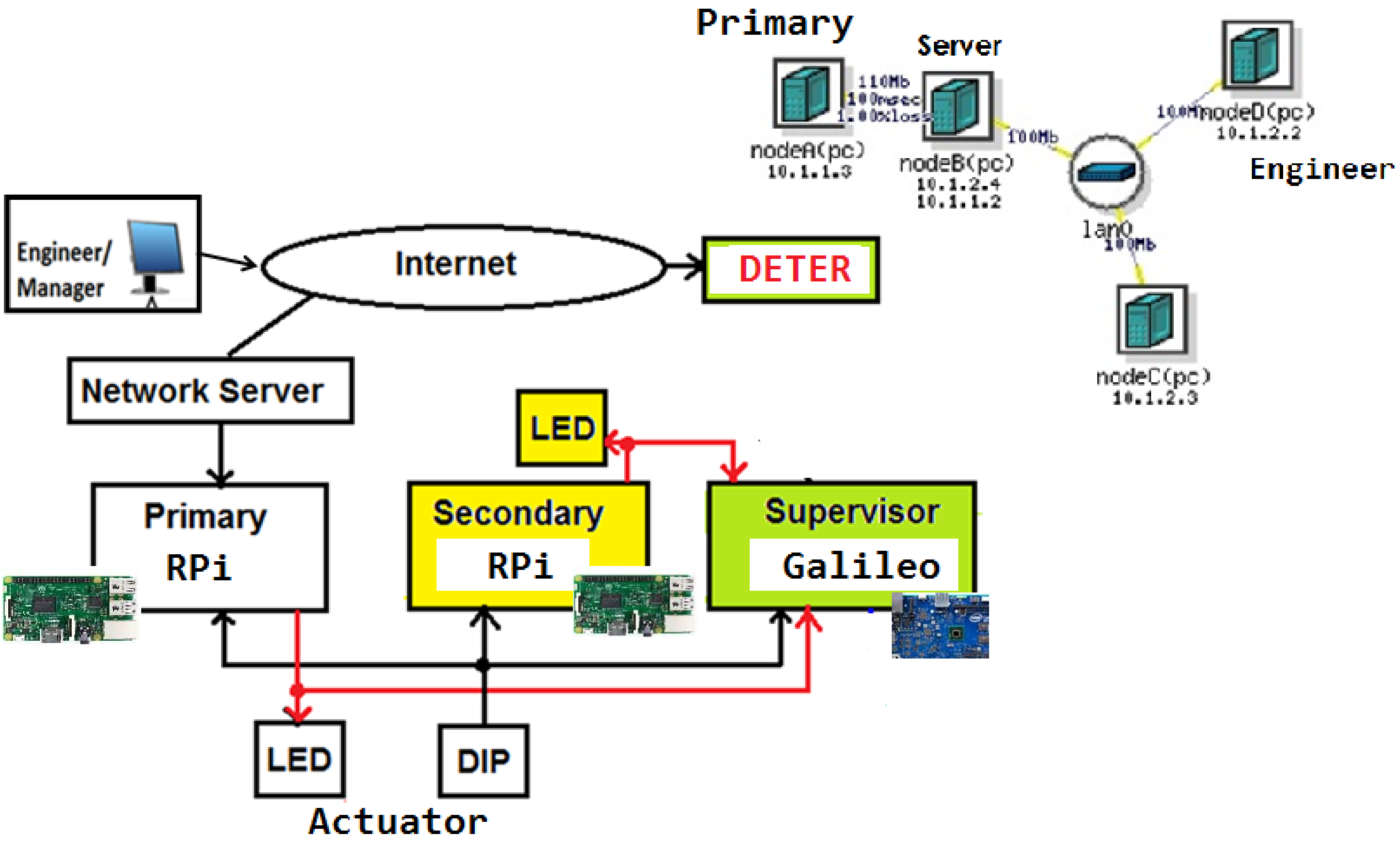


Experimentation in DeterLab

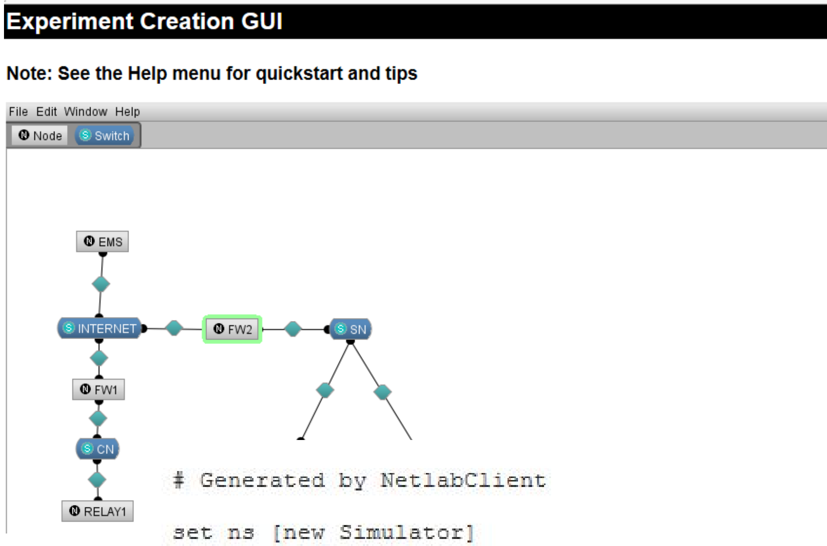
1. Inherent Problem: Isolated control devices such as secondary controllers and supervisors are not represented in DeterLab model
2. Approach
   - Develop a Network Model inside DETER
   - Physical System of the Diversified Redundant ICS at Howard University
   - Develop an interface between DETER and the real physical System: Primary Controller → a Node in DETER
   - In DETER, access/hack the designated Node (which actually controls the primary controller)
   - Test/Observe how the supervisor detects abnormal activity and transfer the control to the secondary controller

Physical System – DETER

- Physical components in the Diversified Redundant ICS are each represented by a DETER node
- A DETER node needs: OS (Linux), Network Connection



DeterLab Process: Experiment Creation



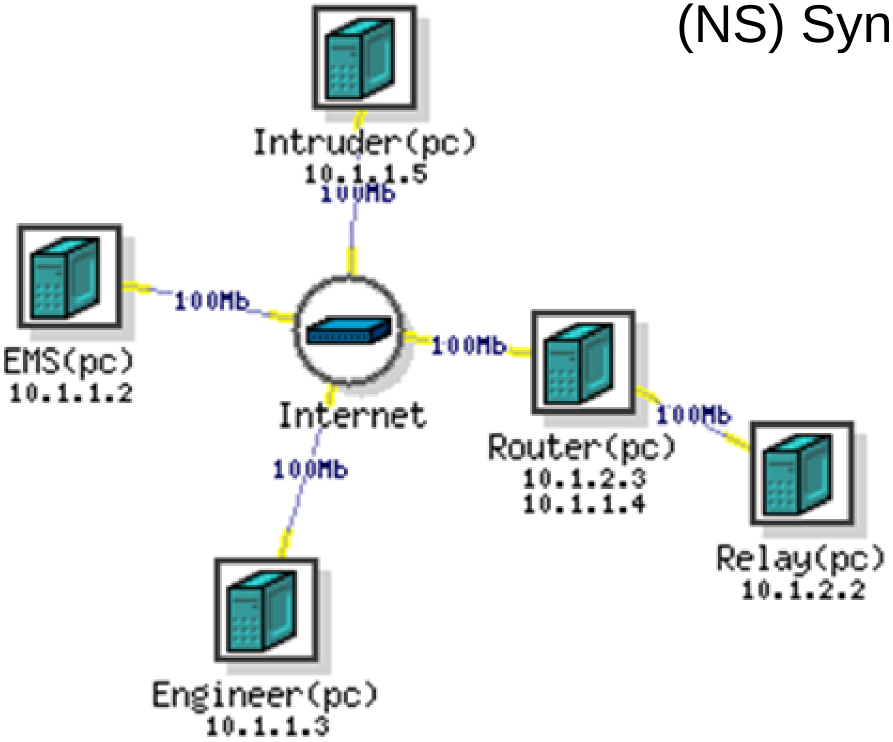
Experiment Creation GUI

'karwil' Logged in.
Sat Apr 05 10:51am PDT

Note: See the Help menu for quickstart and tips

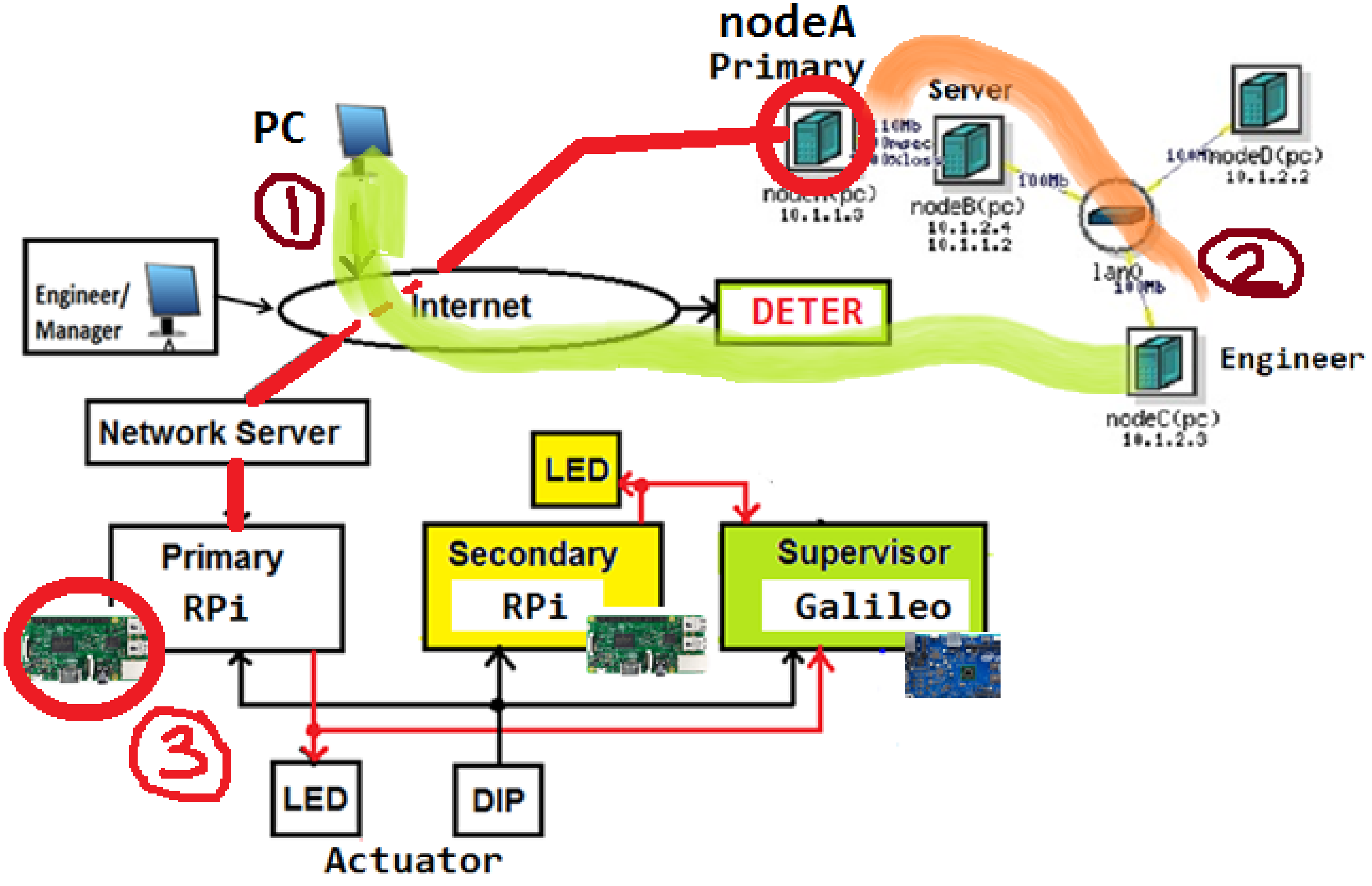
```
# Generated by NetlabClient

set ns [new Simulator]
source tb_compat.tcl

# Nodes
set DB [$ns node]
tb-set-node-os $DB WINXP-UPDATE
set EMS [$ns node]
tb-set-node-os $EMS WINXP-UPDATE
set FW1 [$ns node]
tb-set-node-os $FW1 WINXP-UPDATE
set FW2 [$ns node]
tb-set-node-os $FW2 WINXP-UPDATE
set REL [$ns node]
tb-set-node-os $REL WINXP-UPDATE
set SUP [$ns node]
tb-set-node-os $SUP WINXP-UPDATE

# Lans
set CN [$ns make-lan "$FW1 $REL" 100000.
set Internet [$ns make-lan "$EMS $FW1 $F
set SN [$ns make-lan "$DB $FW2 $SUP" 10(

$ns rtproto Static
$ns run

# NetlabClient generated file ends here.
# Finished at: 4/5/14 2:35 PM
```

- Network Simulation (NS) Syntax



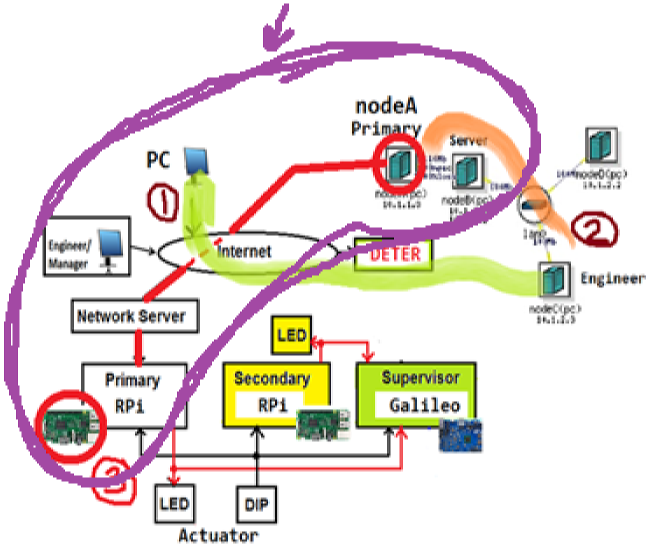
Interface Development

- Representation of a physical primary controller by a DETER node
- EFFECT: Hacking the DETER node (nodeA) inside the DeterLab is the same as hacking the physical primary controller

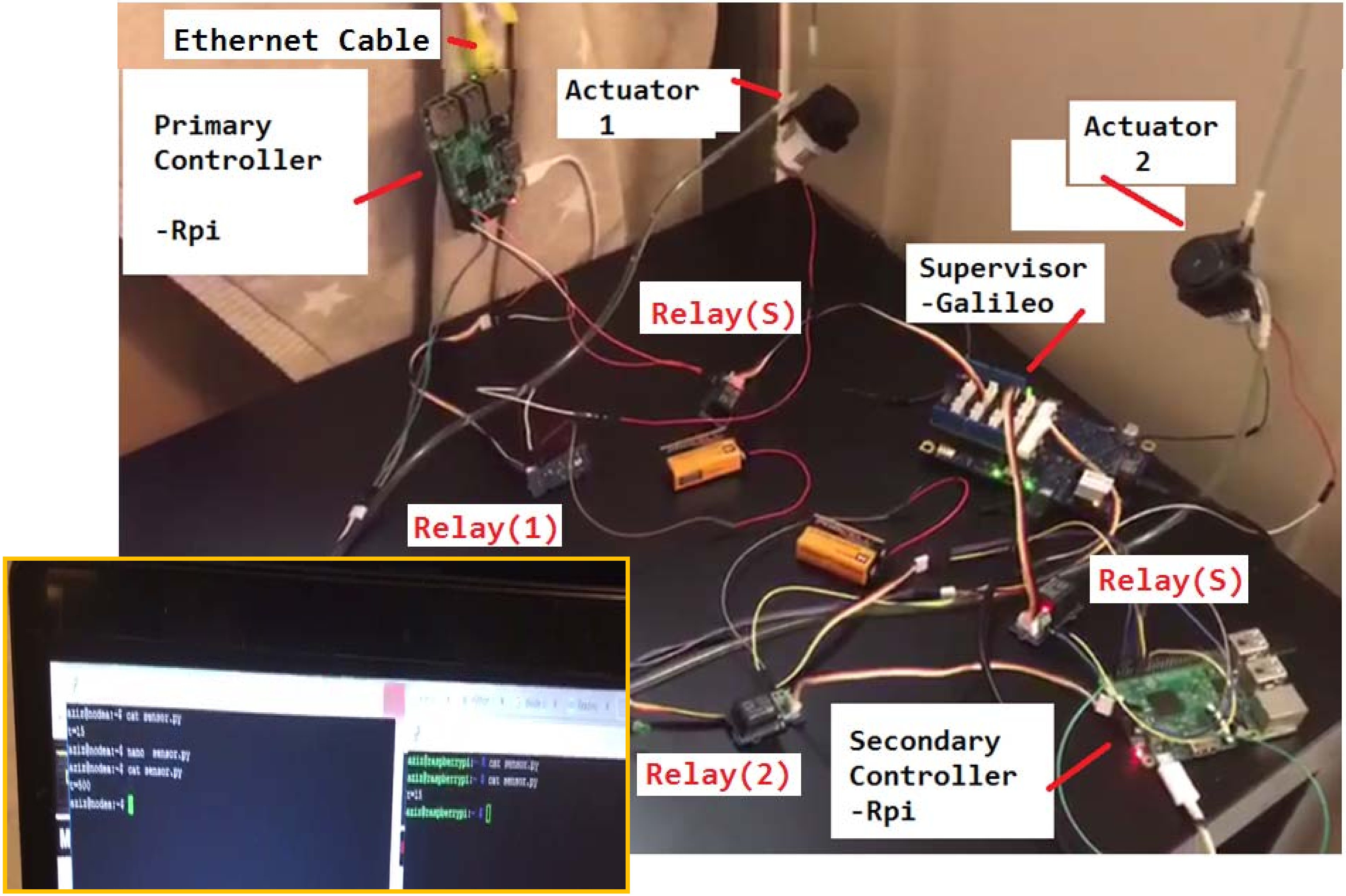


Interface Development

- Representation of a physical primary controller by nodeA
- **SSH tunneling**
  - We need to go through the portal.
  - Create a tunnel between Primary Controller & nodeA.
  - The tunnel will stay open as long as each machine is connected to each other.
  - Certain files updated automatically
  - The update will run every minute.



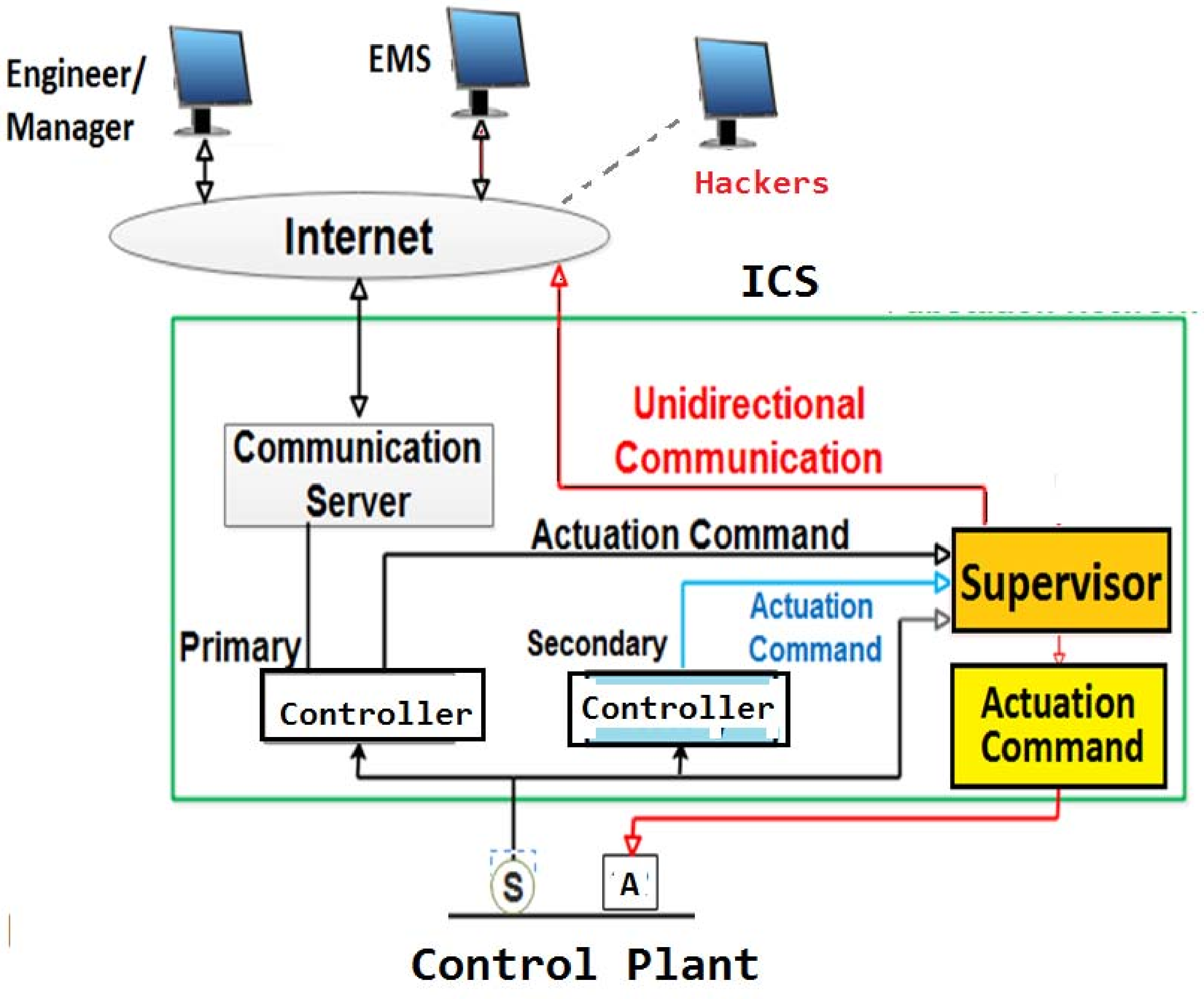
Testing the ICS – Hacked Flow Rate



```
aziz@nodea:~$ cat sensor.py
r=15
aziz@nodea:~$ nano sensor.py
aziz@nodea:~$ cat sensor.py
r=500
aziz@nodea:~$
```

```
aziz@raspberrypi:~ $ cat sensor.py
aziz@raspberrypi:~ $ cat sensor.py
r=15
aziz@raspberrypi:~ $
```

Diversified Redundant ICS - **summary**



- Primary Controller
  - Connected
  - Full functionality
- Redundant Controller
  - Isolated
  - Basic (safe-mode) functionality only
- Supervisor
  - Operation-based control transfer
  - Unidirectional connection - Notification sent to EMS
- Operation-Based Mitigation
  - maintains normal operation **under compromised situation**

Improvement to Diversified Redundant ICS Architecture by adding Intrusion Detection

The Diversified Redundant Architecture has vulnerabilities

- Only mitigates against operational anomalies
- Cannot confirm if a hacker is present (namely, pinging or reconnaissance)

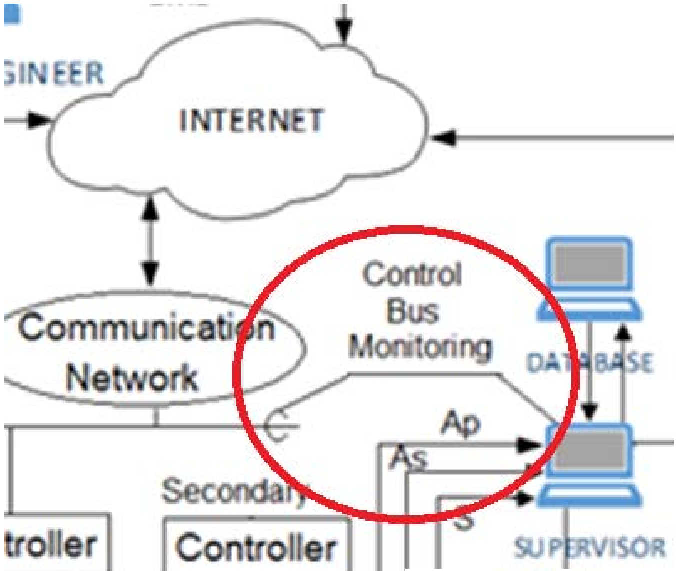
Improvement needed:

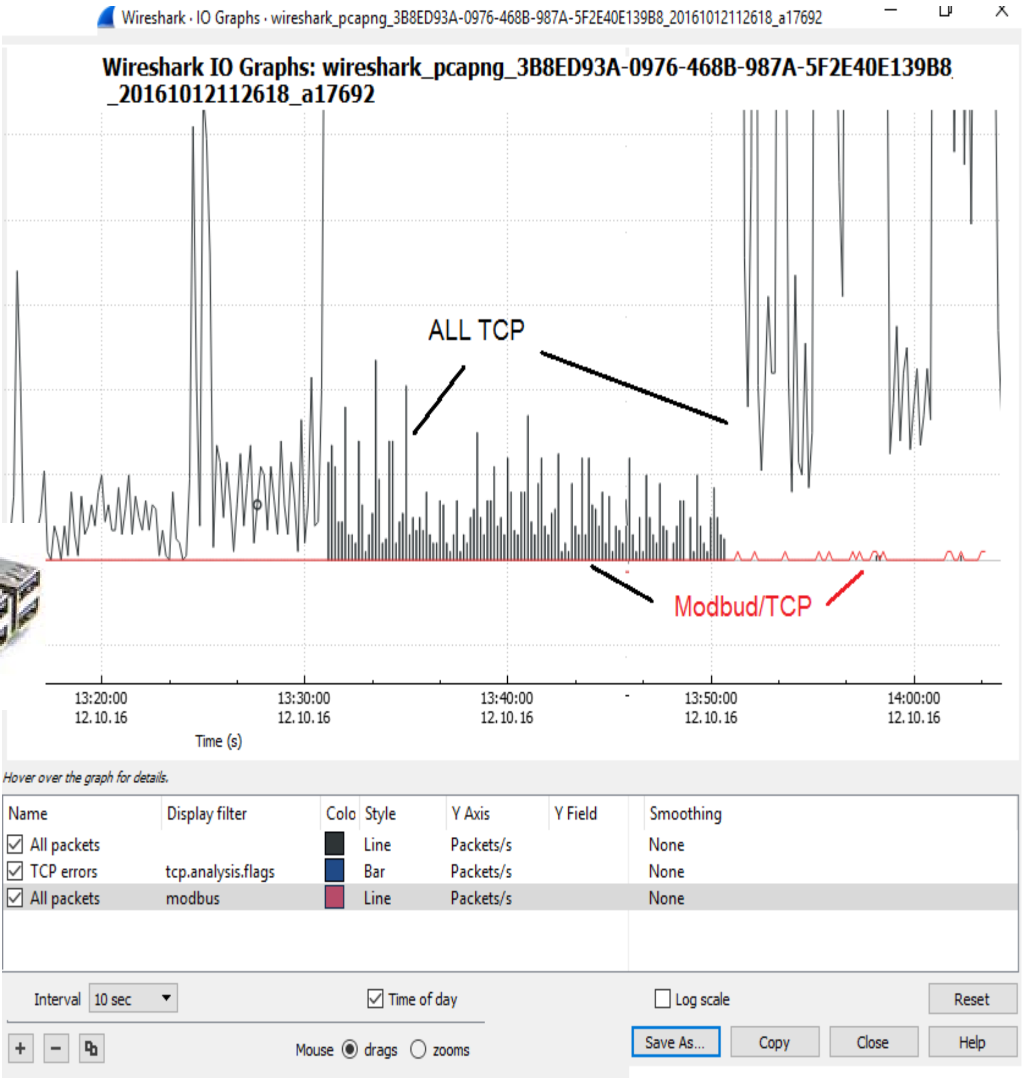
- Situational Awareness to detect and confirm the presence of hacking attempts

Approach: Control Data Bus (Modbus) monitoring and intrusion detection

- Detection of hacker presence on the control network
- Detection of known and unknown cyber attacks

Modbus Data Traffic - Example




Wireshark · IO Graphs · wireshark_pcapng_3B8ED93A-0976-468B-987A-5F2E40E139B8_20161012112618_a17692

Wireshark IO Graphs: wireshark_pcapng_3B8ED93A-0976-468B-987A-5F2E40E139B8_20161012112618_a17692

Hover over the graph for details.

Name	Display filter	Colo	Style	Y Axis	Y Field	Smoothing
☑ All packets		■	Line	Packets/s		None
☑ TCP errors	tcp.analysis.flags	■	Bar	Packets/s		None
☑ All packets	modbus	■	Line	Packets/s		None

Interval 10 sec ▾ ☑ Time of day □ Log scale

Mouse ● drags ○ zooms

mid Bit Technologies, LLC

ShartTrap

Intrusion Detection

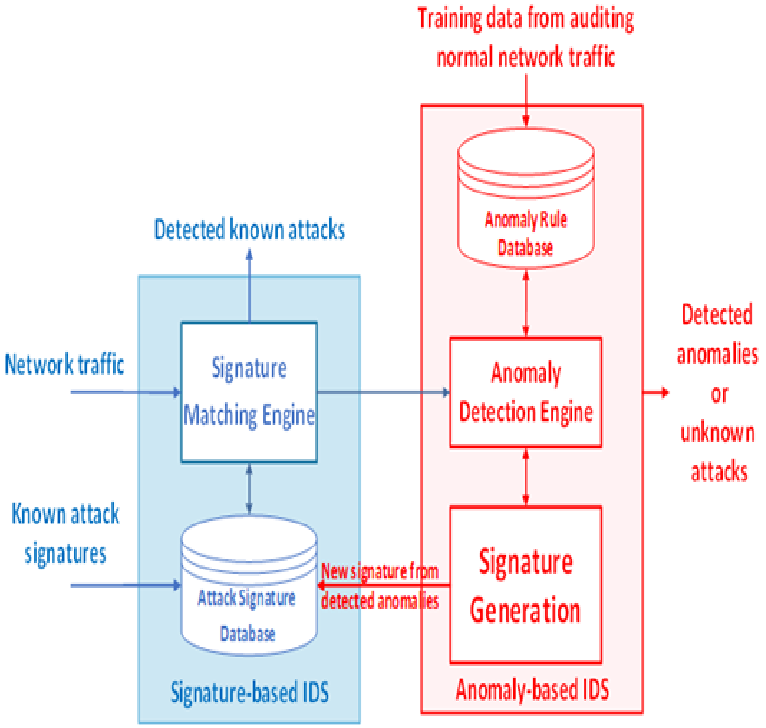
- An Intrusion Detection System (IDS):
  - a device or software that monitors a network or system for malicious activity.
  - used as both a reactive and proactive method to verify if a network has been compromised.

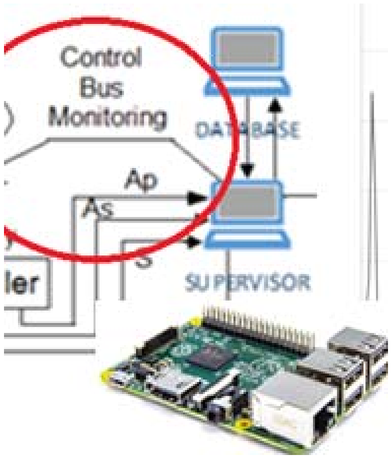
Intrusion Detection can be done in two types:

- Signature-based
- Anomaly-based

Implementation of Snort

- **Install Snort** – Location based on IDS strategy – “Supervisor” (our case)
- Create Snort directories
- Create Snort user and grant privileges
- **Configure Snort**
  - Design and configure **IDS signature rules**
  - Design and configure **IDS anomaly rules**
  - Setup and configure Snort Database
  - Configure and **execute Snort** as Daemon
- **Scan Snort log and generate email using Python**
- **Supervisor (now RPi) ←for Snort Installation**


Training data from auditing normal network traffic
Detected known attacks
Anomaly Rule Database
Network traffic
Signature Matching Engine
Anomaly Detection Engine
Detected anomalies or unknown attacks
Known attack signatures
Attack Signature Database
New signature from detected anomalies
Signature Generation
Signature-based IDS
Anomaly-based IDS



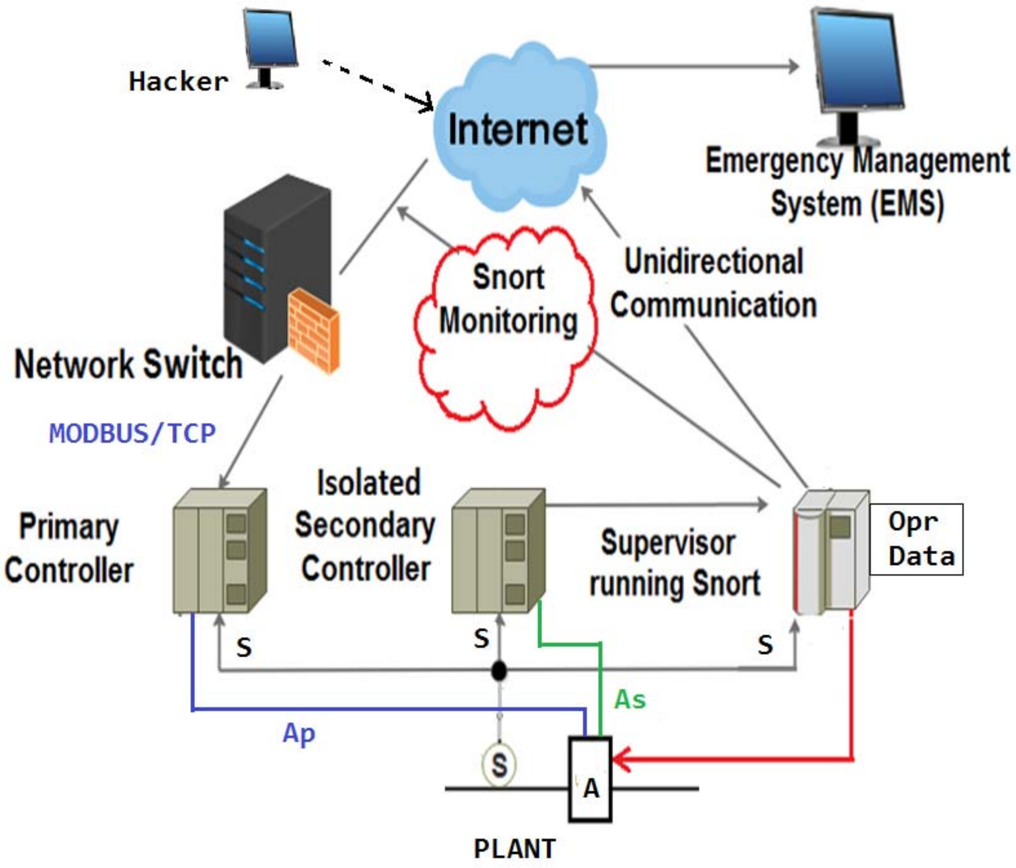
Designing and Writing Snort Rules

- **Example:**

```
alert tcp $EXTERNAL_NET any ->  $MODBUS_NET 502\
(content:!"|02|";offset:7;depth:1; flow:established,
to_server;\ msg:"MODBUS Function Not Allowed!!!”,
sid:1000001;rev:0;priority:5)
```

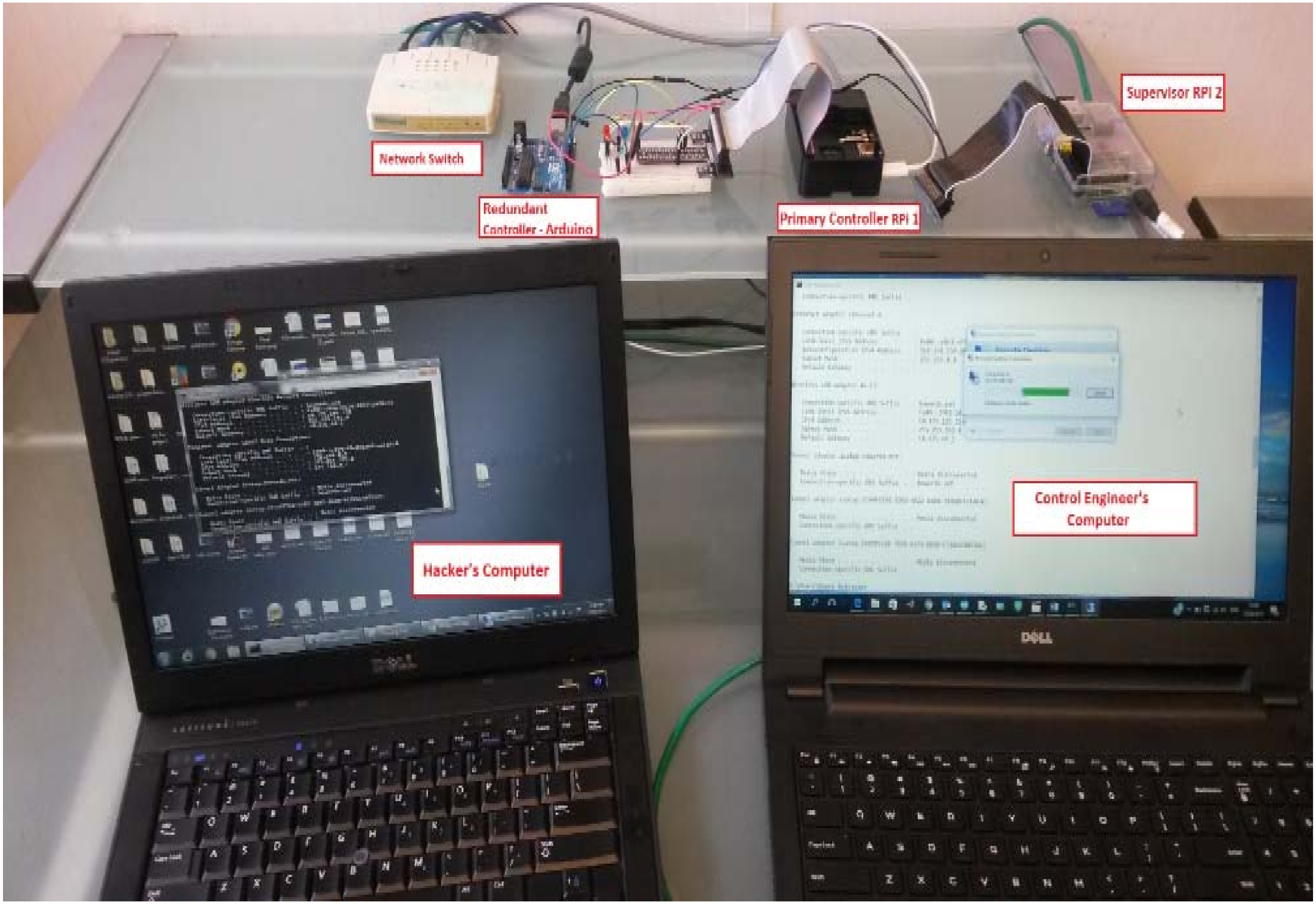
- The above rule allows discrete input operations only on a network for monitoring only functions
- The byte in the 8th position (offset 7) contains the Modbus function code.
- The rule will check the function code of Modbus TCP traffic going from the client network to server network for function code 2 which is “Read Discrete Input”.
- If the function code of the traffic is examined and is found to be other than 2, then an alert message will be generated.

ICS with Diversified Redundancy and Intrusion Detection



- Operation-based resiliency through safe-mode redundant and supervisor
- Added feature of Intrusion Detection in the supervisor
- Redundancy maintains the normal operation from external or insider attacks or sabotages
- Snort Rules Detects Abnormal Traffic in the Modbus
- Snort run in stealth mode and undetected by a potential attacker
- Alert message sent to the EMS

Experimental Testing Setup

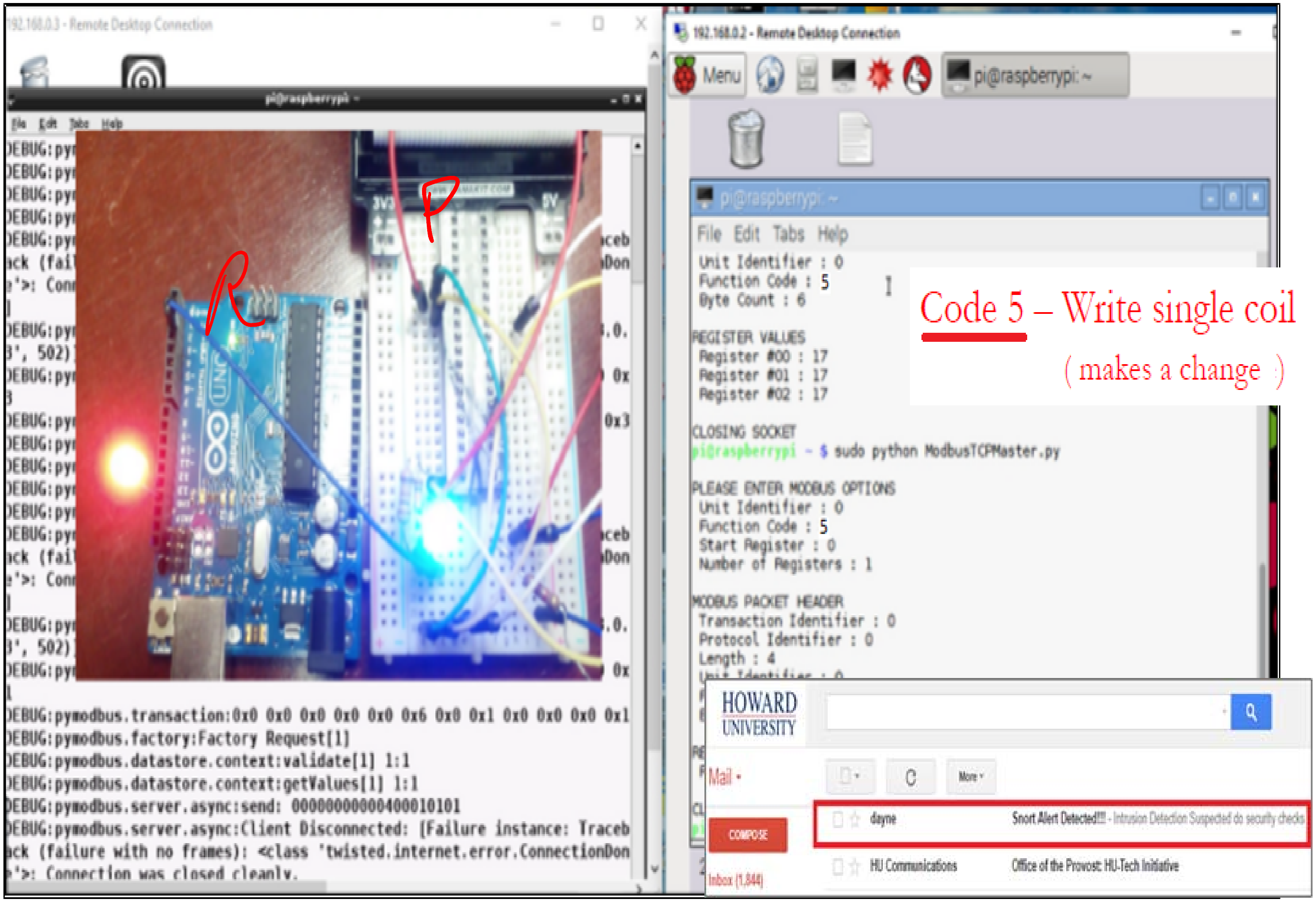


Experimental Validation – without IDS

Blue Light ON (Indication of an Event)

Control Transferred to Redundant Controller

Normal Operation maintained



```
DEBUG:py
DEBUG:py
DEBUG:py
DEBUG:py
DEBUG:py                                                     aceb
ack (fai                                                     nDon
e'>: Con
]
DEBUG:py                                                     .0.
3', 502)
DEBUG:py                                                      0x
3
DEBUG:py                                                      0x3
DEBUG:py
DEBUG:py
DEBUG:py
DEBUG:py
DEBUG:py                                                     aceb
ack (fai                                                     nDon
e'>: Con
]
DEBUG:py                                                     .0.
3', 502)
DEBUG:py                                                      0x
]
DEBUG:pymodbus.transaction:0x0 0x0 0x0 0x0 0x0 0x6 0x0 0x1 0x0 0x0 0x0 0x1
DEBUG:pymodbus.factory:Factory Request[1]
DEBUG:pymodbus.datastore.context:validate[1] 1:1
DEBUG:pymodbus.datastore.context:getValues[1] 1:1
DEBUG:pymodbus.server.async:send: 00000000000400010101
DEBUG:pymodbus.server.async:Client Disconnected: [Failure instance: Traceb
ack (failure with no frames): <class 'twisted.internet.error.ConnectionDon
e'>: Connection was closed cleanly.
```

```
 Unit Identifier : 0
 Function Code : 5
 Byte Count : 6

REGISTER VALUES
 Register #00 : 17
 Register #01 : 17
 Register #02 : 17

CLOSING SOCKET
pi@raspberrypi ~ $ sudo python ModbusTCPMaster.py

PLEASE ENTER MODBUS OPTIONS
 Unit Identifier : 0
 Function Code : 5
 Start Register : 0
 Number of Registers : 1

MODBUS PACKET HEADER
 Transaction Identifier : 0
 Protocol Identifier : 0
 Length : 4
 Unit Identifier : 0
```

Code 5 – Write single coil

(makes a change)

□ ☆	dayne	Snort Alert Detected!!! - Intrusion Detection Suspected do security checks
□ ☆	HU Communications	Office of the Provost: HU-Tech Initiative

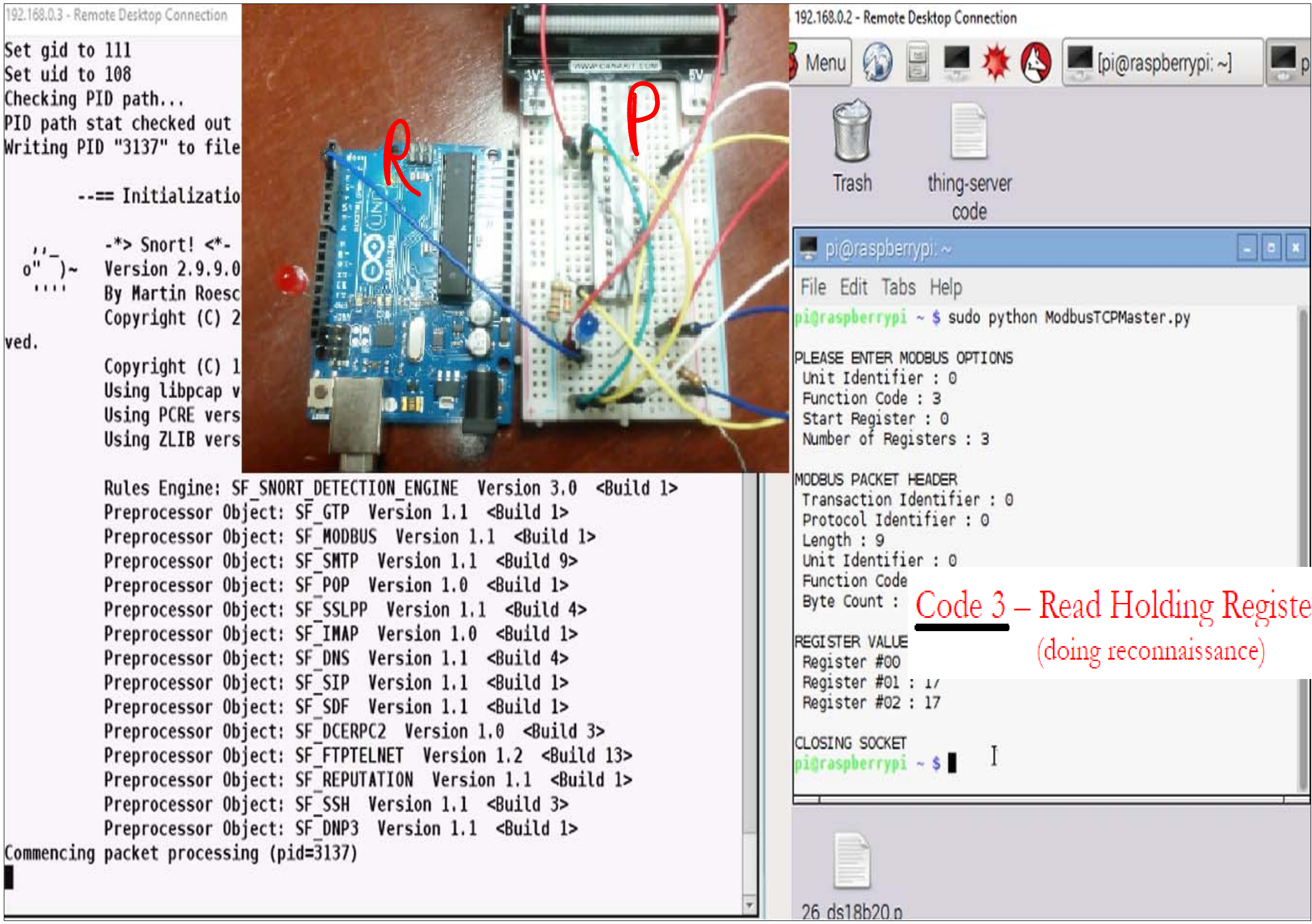
Threshold Change Detected – Hacker presence assumed – Notification Email sent

Experimental Validation – without IDS

Blue Light OFF (Indication of No-Event

Control Remained In the Primary Controller

Normal Operation maintained



```
Set gid to 111
Set uid to 108
Checking PID path...
PID path stat checked out
Writing PID "3137" to file

        --== Initializatio

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0
   ''''    By Martin Roesc
           Copyright (C) 2
ved.
           Copyright (C) 1
           Using libpcap v
           Using PCRE vers
           Using ZLIB vers

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=3137)
```

```
pi@raspberrypi ~ $ sudo python ModbusTCPMaster.py

PLEASE ENTER MODBUS OPTIONS
 Unit Identifier : 0
 Function Code : 3
 Start Register : 0
 Number of Registers : 3

MODBUS PACKET HEADER
 Transaction Identifier : 0
 Protocol Identifier : 0
 Length : 9
 Unit Identifier : 0
 Function Code
 Byte Count :

REGISTER VALUE
 Register #00
 Register #01 : 17
 Register #02 : 17

CLOSING SOCKET
pi@raspberrypi ~ $
```

Code 3 – Read Holding Registers

(doing reconnaissance)

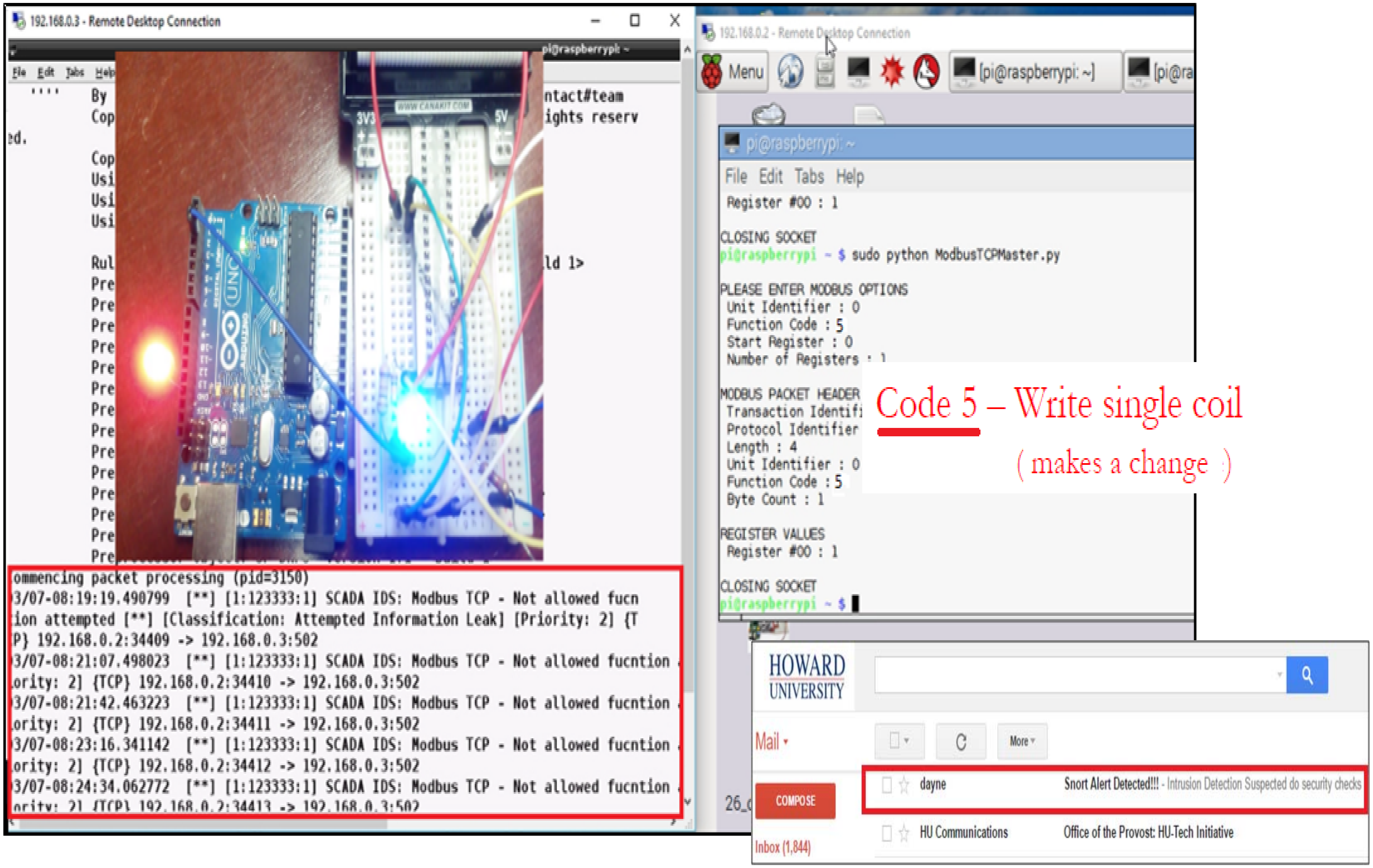
Reconnaissance Only - No Threshold Change – Hacker presence unknown

Experimental Validation – With IDS

Blue Light ON (Indication of an Event

Control Transferred to Redundant Controller

Normal Operation maintained



```
ommencing packet processing (pid=3150)
3/07-08:19:19.490799  [**] [1:123333:1] SCADA IDS: Modbus TCP - Not allowed fucn
ion attempted [**] [Classification: Attempted Information Leak] [Priority: 2] {T
P} 192.168.0.2:34409 -> 192.168.0.3:502
3/07-08:21:07.498023  [**] [1:123333:1] SCADA IDS: Modbus TCP - Not allowed fucntion
ority: 2] {TCP} 192.168.0.2:34410 -> 192.168.0.3:502
3/07-08:21:42.463223  [**] [1:123333:1] SCADA IDS: Modbus TCP - Not allowed fucntion
ority: 2] {TCP} 192.168.0.2:34411 -> 192.168.0.3:502
3/07-08:23:16.341142  [**] [1:123333:1] SCADA IDS: Modbus TCP - Not allowed fucntion
ority: 2] {TCP} 192.168.0.2:34412 -> 192.168.0.3:502
3/07-08:24:34.062772  [**] [1:123333:1] SCADA IDS: Modbus TCP - Not allowed fucntion
ority: 2] {TCP} 192.168.0.2:34413 -> 192.168.0.3:502
```

```
 Register #00 : 1

CLOSING SOCKET
pi@raspberrypi ~ $ sudo python ModbusTCPMaster.py

PLEASE ENTER MODBUS OPTIONS
 Unit Identifier : 0
 Function Code : 5
 Start Register : 0
 Number of Registers : 1

MODBUS PACKET HEADER
 Transaction Identifi
 Protocol Identifier
 Length : 4
 Unit Identifier : 0
 Function Code : 5
 Byte Count : 1

REGISTER VALUES
 Register #00 : 1

CLOSING SOCKET
pi@raspberrypi ~ $
```

Code 5 – Write single coil

(makes a change)

□ ☆	dayne	Snort Alert Detected!!! - Intrusion Detection Suspected do security checks
□ ☆	HU Communications	Office of the Provost: HU-Tech Initiative

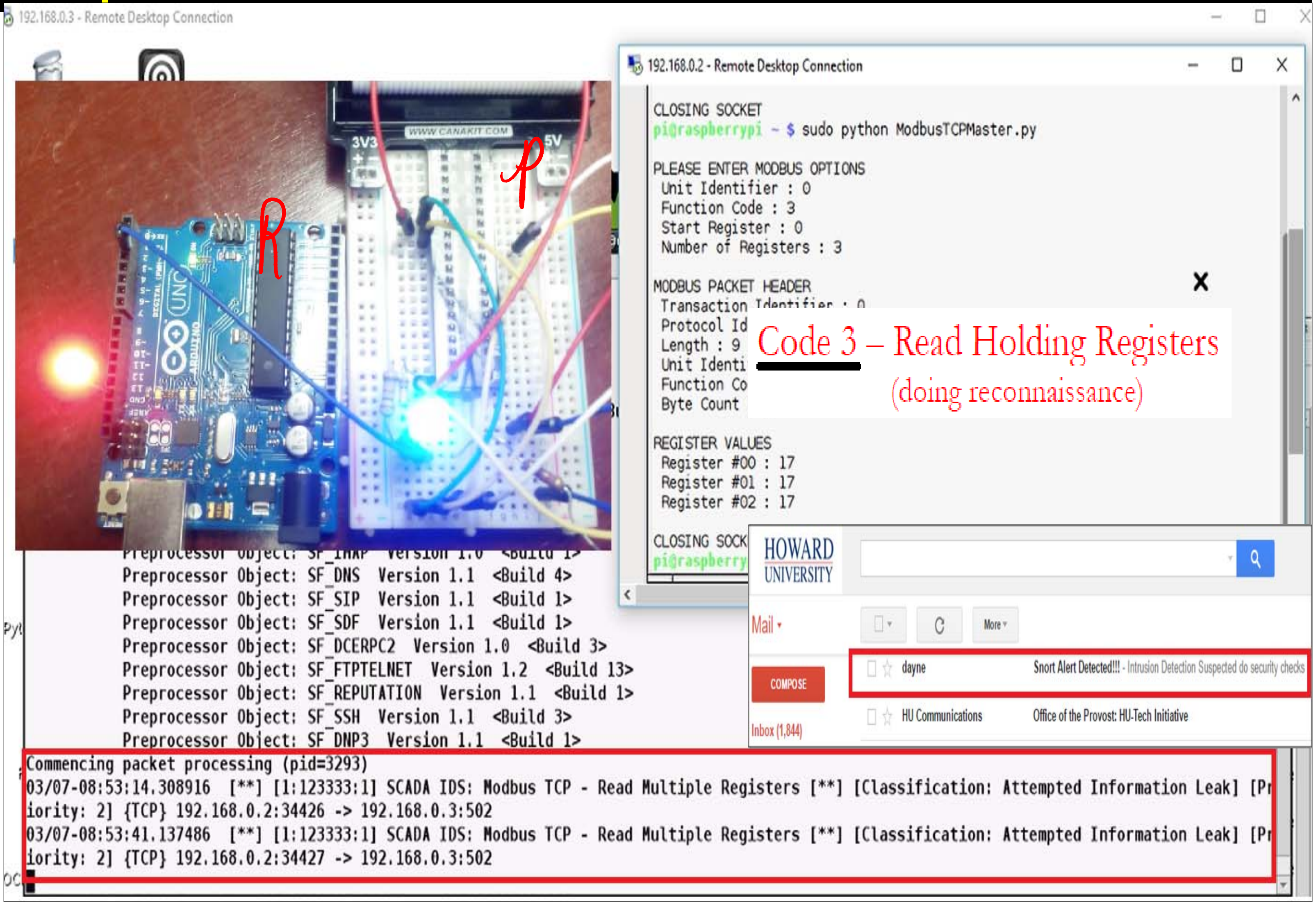
Threshold Change Detected – Snort verifies presence of Hacker and Notification Email sent

Experimental Validation – With IDS

Blue Light ON (Indication of an Event

Control Transferred to Redundant Controller

Normal Operation maintained


192.168.0.3 - Remote Desktop Connection
192.168.0.2 - Remote Desktop Connection
R
P
3V3
5V
WWW.CANAKIT.COM
UNO
ARDUINO
HOWARD UNIVERSITY
Mail
More
COMPOSE
Inbox (1,844)

```
CLOSING SOCKET
pi@raspberrypi ~ $ sudo python ModbusTCPMaster.py

PLEASE ENTER MODBUS OPTIONS
 Unit Identifier : 0
 Function Code : 3
 Start Register : 0
 Number of Registers : 3

MODBUS PACKET HEADER
 Transaction Identifier : 0
 Protocol Id
 Length : 9
 Unit Identi
 Function Co
 Byte Count

REGISTER VALUES
 Register #00 : 17
 Register #01 : 17
 Register #02 : 17

CLOSING SOCK
pi@raspberry
```

Code 3 – Read Holding Registers (doing reconnaissance)

□ ☆	dayne	Snort Alert Detected!!! - Intrusion Detection Suspected do security checks
□ ☆	HU Communications	Office of the Provost: HU-Tech Initiative

```
    Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
    Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
    Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
    Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
    Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
    Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
    Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
    Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
    Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=3293)
03/07-08:53:14.308916  [**] [1:123333:1] SCADA IDS: Modbus TCP - Read Multiple Registers [**] [Classification: Attempted Information Leak] [Pr
iority: 2] {TCP} 192.168.0.2:34426 -> 192.168.0.3:502
03/07-08:53:41.137486  [**] [1:123333:1] SCADA IDS: Modbus TCP - Read Multiple Registers [**] [Classification: Attempted Information Leak] [Pr
iority: 2] {TCP} 192.168.0.2:34427 -> 192.168.0.3:502
```

No Threshold Change, Reconnaissance Only - Detected – Snort verifies presence of Hacker and Notification Email sent

Conclusions

- ICS networking invites a new challenge of securing the control network against cyber vulnerabilities.
- Challenges of detecting ALL and NEW and Unknown viruses, worms, and Trojan horses
- Inherent Software Faults open door to errors, malicious viruses, and exploiters/hackers
- Cyber-Resilient Diversified Redundant ICS Architecture (Primary (connected), Redundant (isolated and "safe-mode"), and Supervisor (unidirectional): Strength and Weakness
- Intrusion Detection added with Snort: Diversified Redundant Architecture with Intrusion Detection ("DRAID") for resilient ICS
- Snort rules and python scripts integrated into the supervisor for Modbus Traffic Signature and Anomaly based Intrusion Detection
- Experimental Validation of the DRAID for hacker presence detection and control transfer to redundant controller
- DRAID can provide a resilient and secure ICS.

Related Works

- Dayne Robinson and Charles Kim, "A Cyber-Defensive Industrial Control System with Redundancy and Intrusion Detection," 2017 North American Power Symposium, Sept 17-19, 2017, Morgantown WV.
- Charles Kim and Dayne Robinson, "Modbus Monitoring for Networked Control Systems of Cyber-Defensive Architecture," 2017 IEEE SysCon, April 24-27, 2017.
- Charles Kim, "Cyber-Defensive Architecture for Networked Industrial Control Systems," International Journal of Engineering and Computer Science, Vol. 2, No. 1, pp. 1 - 9, Jan. 2017. doi:10.24032/IJEACS/0201/01.https://doi.org/10.24032/ijeacs/0201/01
- Charles Kim, "A Cyber-Resilient Industrial Control System with Diversified Architecture and Control Bus Monitoring," World Congress on Industrial Control System Security (WCISCSS 2016), December 12 - 14, 2016. London, UK.
- Charles Kim and Ravindranath Jaglal, "A cyber-robust connected-control system: Experimental validation," Proc. of the 29th International Conference on Computer Application in Industry and Engineering, pp. 133 - 138, Denver, CO. September 26-28, 2016.
- Charles Kim, Karen Green, and Andre Duarte Palhares, "Cybersecurity testbed experimentation of a resilient control system for power substations," Proc. of the 29th International Conference on Computer Application in Industry and Engineering, pp. 139 - 144, Denver, CO. September 26-28, 2016.
- Charles Kim, "Safety Challenges for Connected Cars", IEEE Transportation Electrification Community Newsletter June 2016.
- Charles Kim, "High-Tech Cars: Safety-Critical Computer Systems," Invited Talk in an IEEE Focused workshop for Exploring Cybersecurity Challenges in Electrified Transportation. Feb 24 & 25, 2016. Washington DC.