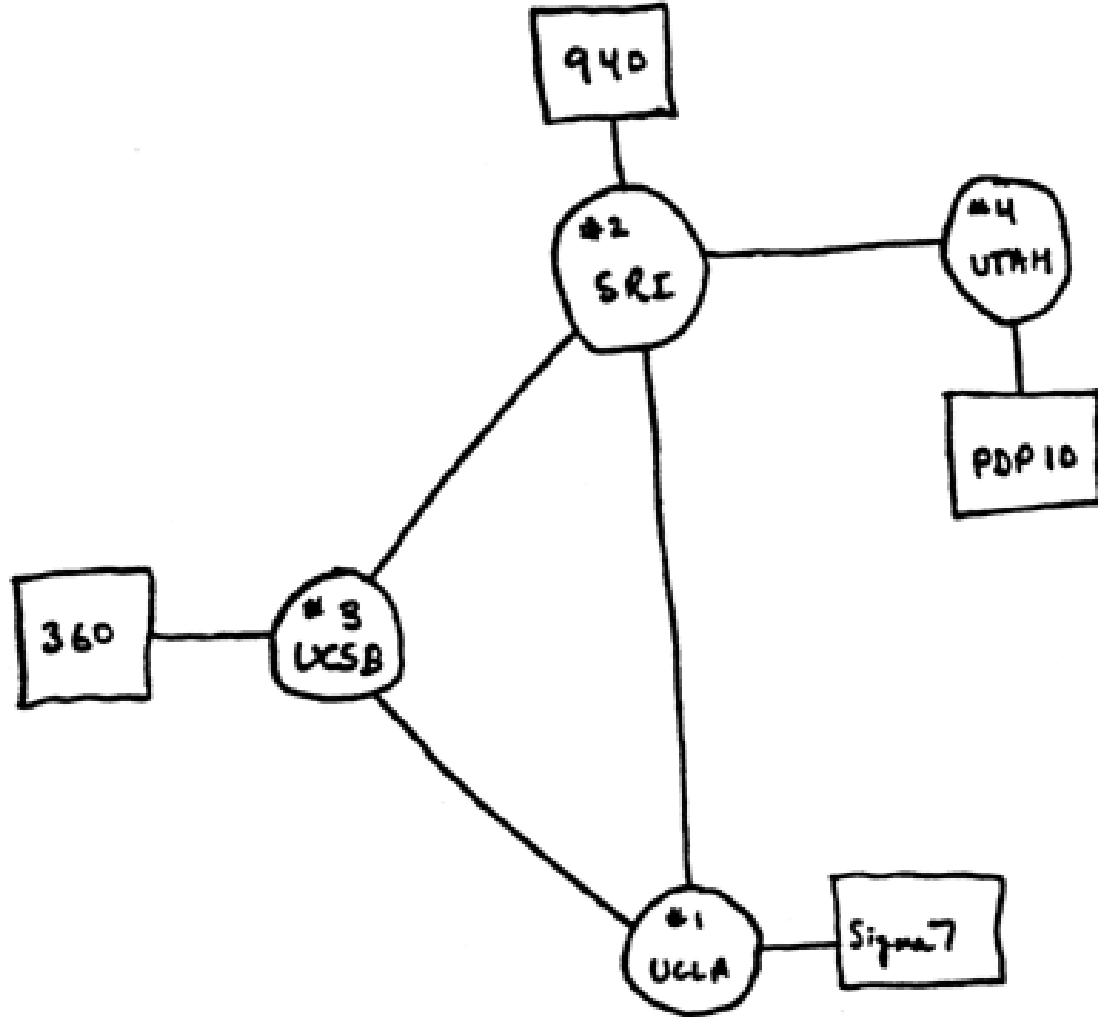CSE508   Network Security

8/29/2017   **Introduction and Basic Concepts**
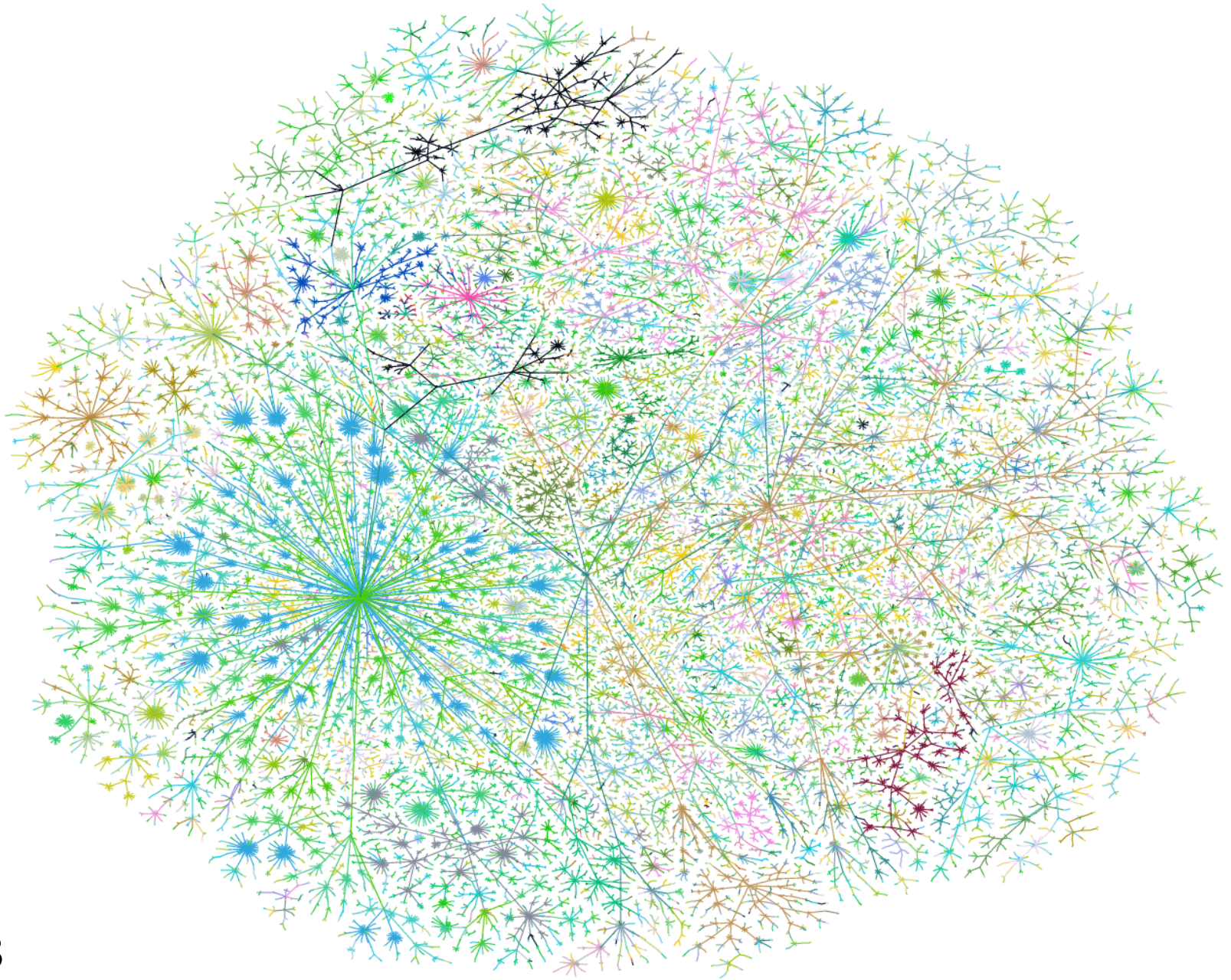
Michalis Polychronakis

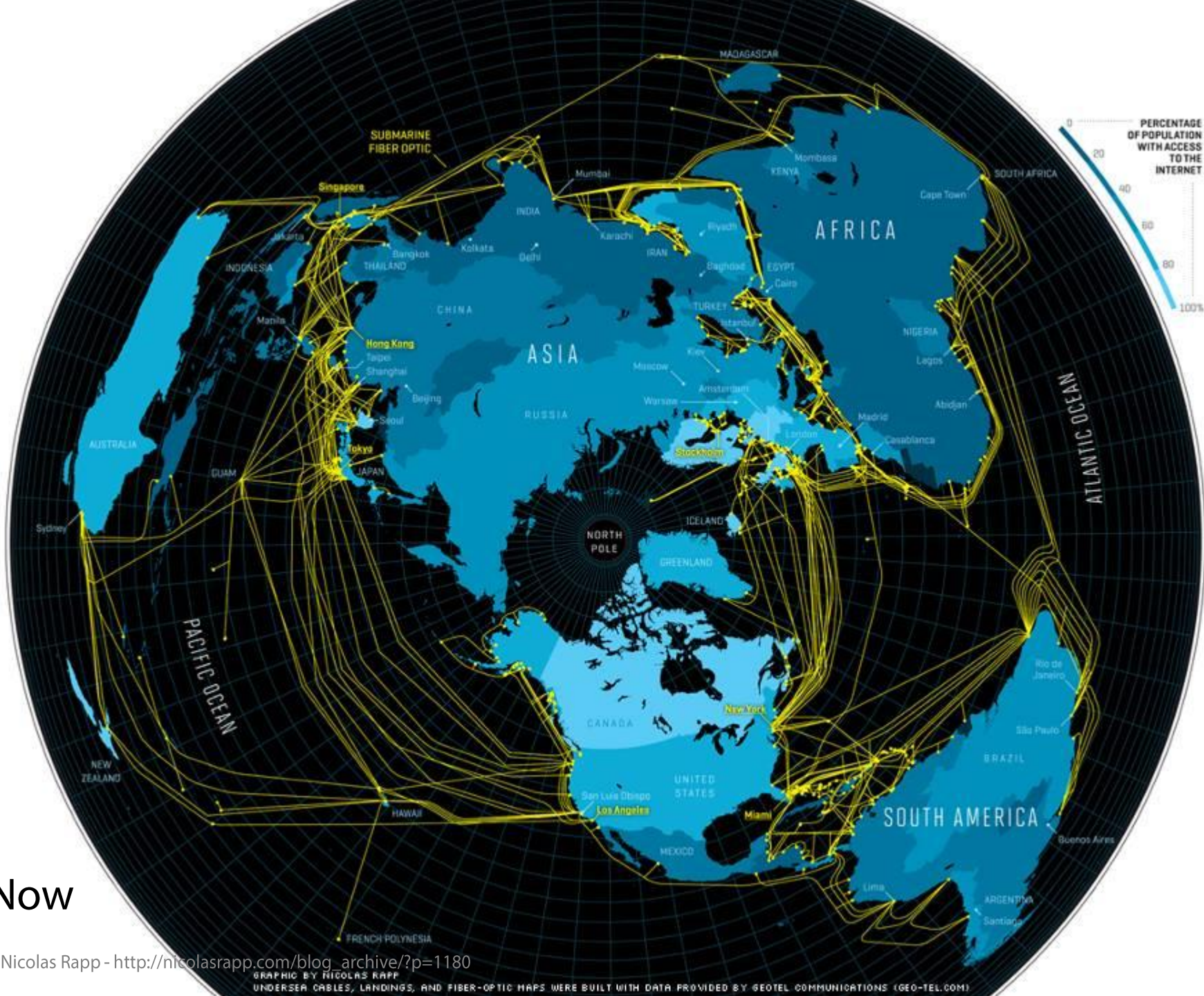*Stony Brook University*

Why care about network security?

1969

1998

PERCENTAGE OF POPULATION WITH ACCESS TO THE INTERNET

Now

Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016

Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017

Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

Regionally, Greater China, North America and Western Europe are driving the use of connected things and the three regions together will represent 67 percent of the overall Internet of Things (IoT) installed base in 2017.

Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017

The consumer segment is the largest user of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use (see Table 1). Businesses are on pace to employ 3.1 billion connected things in 2017. "Aside from automotive systems, the applications that will be most in use by consumers will be smart TVs and digital set-top boxes, while smart electric meters and commercial security cameras will be most in use

An increasing part of our business, social, and personal life involves the internet

> Web, email/IM, cloud, social networks, entertainment, …
>
> Mobile computing
>
> Cyber-physical systems
>
> Internet of things

Protecting the security and privacy of our digital interactions is critical

> Most of them involve *networked systems and applications*

SECTIONS   HOME   SEARCH

The New York Times

LOG IN

BUSINESS DAY

Millions of Anthem Customers Targeted in Cyberattack

By REED ABELSON and MATTHEW GOLDSTEIN   FEB. 5, 2015

Outside the Anthem facility in Indianapolis.   Anthem said it detected a data breach on Jan. 29, and that it was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images

Anthem, one of the nation's largest health insurers, said late

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS   JULY 9, 2015

Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than

www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 25th Apr 2017)

interesting story

| YEAR | | BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY | | ☑ SHOW FILTER |

latest

Brazzers Clinton campaign .ixSense

DaFont nterp: Lynda.cc Netflix Twitter account AQuest Diagnostic Cross Service Tesco Bank ree Wonta

Cellebrite

Dailymotion
85200000

Moss: Fonseca

Privatization Agency of the Republic of Serbia

Mutuelle Generale de la Police

ımato
by MGAR Ltd

Telegram **rahoo**
32000000

Bell

Verizon

Friend Finder Network
412, 000, 000

River City Media
1370000000

Weebly
43000000

World Check

Syrian government

2016

Banner Health

Linux Ubuntu forums

Wendy's

Fling
40000000

VK
100, 544, 934

uTorrent

Anthem
80, 000, 000

MySpace
164, 000, 000

Philippine Commiss on Elect

US Office of Personnel Management

Mail. ru

Code.org

2015

Adult Frie Find Australian Immigration Department

Carefirst

Minecraft

National Childbirth Trust

Secur Technolo

Turkish citizenshir databa

theguardian
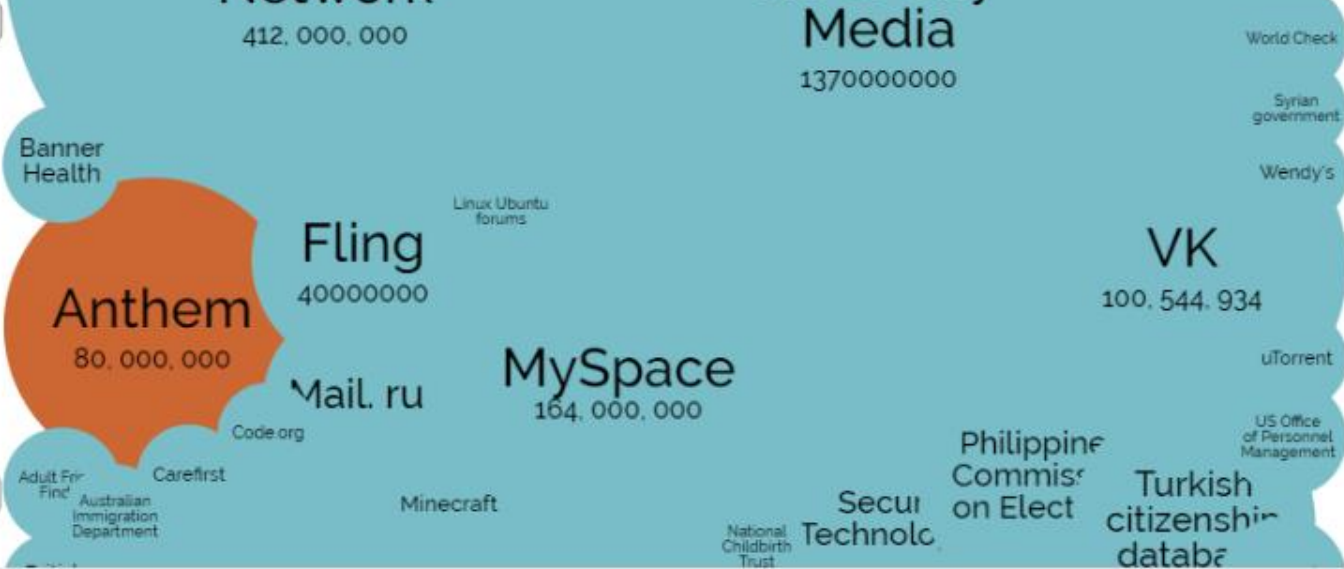
Hackers ground 1,400 passengers at Warsaw in attack on airline's computers

Polish state-owned airline LOT suffers hacking assault on ground systems that causes 10 national and international flights to be cancelled

📷 At no point was the safety of ongoing flights compromised, said a spokesman for LOT Polish airlines.
Photograph: East News/REX Shutterstock

Reuters

Sunday 21 June 2015 16.40 EDT

Save for later   ≪ Shares   💬 Comments

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE VIDEO INSIDER SUBSCRIBE

THREAT LEVEL ┤ cyberwar ─ cyberwarfare ─ stuxnet

FOLLOW WIRED

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

f Share ⟨4.3k⟩ 🐦 Tweet ⟨1,485⟩ g+1 ⟨129⟩ in Share ⟨693⟩ 📌 Pin it

theguardian

Cybercrime

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

Alex Hern

🐦 @alexhern

Thursday 7 January 2016
08.20 EST

Shares **150**   Comments **31**

🔖 Save for later

📷 Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

A power blackout in Ukraine over Christmas and a destructive cyberattack on a major Ukrainian media company were caused by the same malware from the same major hacking group, known as Sandworm, according to security researchers at Symantec.

ANDY GREENBERG SECURITY 06.20.17 06:00 AM

HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR

SHARE

f 33125

✉

The clocks read zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.

"The hackers don't want us to finish the movie," Yasinsky's wife joked. She was referring to an event that had occurred a

MOST POPULAR

Government Hackers Caught Using Unprecedented iPhone Spy Tool

WRITTEN BY LORENZO FRANCESCHI-BICCHIERAI

August 25, 2016 // 01:05 PM EST

On the morning of August 10, Ahmed Mansoor, a 46-year-old human rights activist from the United Arab Emirates, received a strange text message from a number he did not recognize on his iPhone.

"New secrets about torture of Emiratis in state prisons," read the tantalizing message, which came accompanied by a link.

Mansoor, who had already been the victim of government hackers using commercial spyware products from FinFisher and Hacking Team, was suspicious and didn't click on the link. Instead, he sent the message to Bill Marczak, a researcher at Citizen Lab, a digital rights watchdog at the University of Toronto's Munk School of Global Affairs.

Bits

SECURITY

Hackers Exploit 'Flash' Vulnerability in Yahoo Ads

By DINO GRANDONI   AUGUST 3, 2015 9:14 PM   💬 51 Comments

Email

Share

Tweet

Save

More

For seven days, hackers used Yahoo's ad network to send malicious bits of code to computers that visit Yahoo's collection of heavily trafficked websites, the company said on Monday.

The attack, which started on July 28, was the latest in a string that have exploited Internet advertising networks, which are designed to reach millions of people online. It also highlighted growing anxiety over a much-used graphics program called Adobe Flash, which has a history of security issues that have irked developers at Silicon Valley companies.

"Right now, the bad guys are really enjoying this," said Jérôme Segura, a security researcher at Malwarebytes, the security company that uncovered the attack. "Flash for them was a godsend."

The scheme, which Yahoo shut down on Monday, worked like this: A group of hackers bought ads across the Internet giant's sports, news and finance sites. When a computer — in this case, one running Windows — visited a Yahoo site, it downloaded malware code.

Visit the **Technology section** for complete coverage of the industry. »

MOST VIEWED

1. Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future

2. Uber's No-Holds-Barred Expansion Strategy Fizzles in Germany

3. Fans Demand Details After Death of a 13-Year-Old YouTube Star

4. At C.D.C., a Debate Behind Recommendations on Cellphone Risk

5. How Larry Page's Obsessions Became Google's Business

LATEST FROM BITS

Drone Lobbying Heats Up on Capitol Hill

Daily Report: Airbnb Urges Mayors to 'Please Tax Us'

theguardian
Winner of the Pulitzer prize

Computing

US police force pay bitcoin ransom in Cryptolocker malware scam

Unprepared officials blindsided by sophisticated virus call experience 'an education'

How A Coffee Machine Infected Factory Computers with Ransomware

By *Waqas* on July 28, 2017   ✉ *Email*   🐦 *@hackread*   🏷 **CYBER ATTACKS** **HACKING NEWS** **MALWARE** **SECURITY**

2817
SHARES

[f Share on Facebook] [🐦 Share on Twitter]

It's no surprise that the Internet of Things (IoT) devices are highly vulnerable to cyber attacks but who would know a time would come when these devices will become a security threat to institutions?

A few months ago researchers exposed life threatening vulnerabilities in IIoT (Industrial Internet of Things) devices specifically Industrial robots. In their findings, robots could be hacked, but in this case, we are about to discuss a smart coffee machine or an Internet connected coffee machine.

> **More: San Francisco Railway' Fare System Hacked for 100 Bitcoin Ransom**

The incident took place in June 2017 and was shared by a chemical engineer on Reddit who goes by the handle of "C10H15N1." He works as a PLC (Programmable Logic Controllers) expert in a company that has multiple petrochemical factories making chemicals in Europe.

bits.blogs.nytimes.com/2014/09/04/apple-says-it-will-add-new-security-measures-after-celebrity-hack/?_r=0

New Rules in China Upset Western Tech Companies

STATE OF THE ART
Uber's Business Model Could Change Your Work

ECONOMIC SCENE
Job Licenses in Spotlight as Uber Rises

DEALBOOK
After Alibaba Spinoff, Yahoo May Become a Takeover Target

Bits

Search Bits   SEARCH

SECURITY

Apple Says It Will Add New iCloud Security Measures After Celebrity Hack

By BRIAN X. CHEN   SEPTEMBER 4, 2014 11:32 PM   💬 21 Comments

THE BITS DAILY UPDATE

Every weekday, **get the latest technology news**, analysis and buzz from around the web — delivered to your inbox.

SIGN UP FOR OUR NEWSLETTER   See a Sample »

🤖 **SCUTTLEBOT** *News from the Web, annotated by our staff*

Netflix's Secret Special Algorithm Is a Human

NEW YORKER | His name, writes Tim Wu, is Ted Sarandos. -
Natasha Singer

Uber Releases Study on Drunk Driving and Transportation

UBER BLOG | A new study released by the ride-hailing company claims it is having a "measurable impact on driving down alcohol-related crashes." - *Mike Isaac*

MacBook Air

Armed With Facebook 'Lik ×

🗋 www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-a

The *Atlantic*

Get *The Atlantic* on Facebook

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

But the deeper aspects of your personality remain hard to detect.

VIDEO

How to Build a Tornado

A Canadian inventor believes his tornado machine could solve the world's energy crisis.

MORE IN TECHNOLOGY
▼

Introducing the Supertweet
IAN BOGOST

My Parents' Facebook Will
JAKE SWEARINGEN

≡ **SECTIONS**   **𝕿 HOME**   🔍 **SEARCH**

The New York Times

LOG IN ⚙

BUSINESS DAY

💬 410 COMMENTS

Attention, Shoppers: Store Is Tracking Your Cell

By STEPHANIE CLIFFORD and QUENTIN HARDY   JULY 14, 2013

✉ Email

f Share

🐦 Tweet

🗂 Save

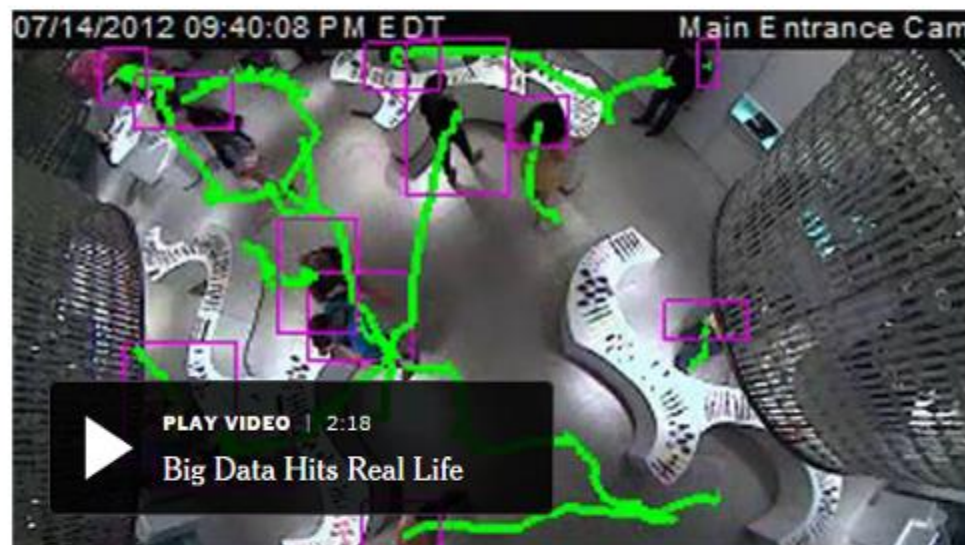➤ More

Like dozens of other brick-and-mortar retailers, Nordstrom wanted to learn more about its customers — how many came through the doors, how many were repeat visitors — the kind of information that e-commerce sites like Amazon have in spades. So last fall the company started testing new technology that allowed it to track customers' movements by following the Wi-Fi signals from their smartphones.

But when Nordstrom posted a sign telling customers it was tracking them, shoppers were unnerved.

"We did hear some complaints," said Tara Darrow, a spokeswoman for the store. Nordstrom ended the experiment in May, she said, in part because of the comments.

Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn

07/14/2012 09:40:08 PM EDT   Main Entrance Cam

PLAY VIDEO | 2:18

Big Data Hits Real Life

Brick-and-mortar stores are looking for a chance to catch up with their online competitors by using software that allows them to watch customers as they shop, and gather data about their behavior. Video by Erica Berenstein on July 14, 2013.

ars technica

🏠   MAIN MENU ⌄   MY STORIES: 25 ⌄   FORUMS   SUBSCRIBE   JOBS   ARS CONSORTIUM   🔍

MINISTRY OF INNOVATION / BUSINESS OF TECHNOLOGY

AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing

AT&T goes head to head against Google in KC on fiber and targeted ads.

by Jon Brodkin - Feb 16, 2015 12:38pm EST

f Share   🐦 Tweet   205

📷 AT&T

AT&T's gigabit fiber-to-the-home service has just arrived in Kansas City, and the price is the same as Google Fiber—if you let AT&T track your Web browsing history.

LATEST FEATURE STORY ◢

FEATURE STORY (2 PAGES)

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.

WATCH ARS VIDEO ◢

DONATE

PROPUBLICA
Journalism in the Public Interest

Receive our top stories daily

Email address   **SUBSCRIBE**

Home   Our Investigations   Data   MuckReads   Get Involved   About Us

Search ProPublica

Dragnets
Tracking Censorship and Surveillance

Verizon's Zombie Cookie Gets New Life

Verizon is merging its cellphone tracking supercookie with AOL's ad tracking network to match users' online habits with their offline details.

by *Julia Angwin* and *Jeff Larson*
ProPublica, Oct. 6, 2015, 1:15 p.m.

15 Comments | 🖶 Print

18

15

This is part of an ongoing investigation:

Dragnets
ProPublica investigates the threats to privacy in an era of cellphones, data mining and cyberwar.

Connect with Facebook to share articles you read on ProPublica. Learn more »

Enable Social Reading

Latest Stories in this Project

ars technica

RISK ASSESSMENT / SECURITY & HACKTIVISM

Dell does a Superfish, ships PCs with easily cloneable root certificates

Root certificate debacle that hit Lenovo now visits the House of Dell.

by Dan Goodin - Nov 23, 2015 12:40pm EST

f Share   🐦 Tweet   ✉ Email   222

LATEST FEATURE STORY ▴

FEATURE STORY (2 PAGES)

Reboots, remakes, and sequels need not apply— Ars' most anticipated games of 2016

Only original ideas allowed in this selection of upcoming titles.

WATCH ARS VIDEO ▴

ars

ars technica

MAIN MENU ⌄   **MY STORIES: 25** ⌄   **FORUMS**   **SUBSCRIBE**   **JOBS**

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Unauthorized code" in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

by Dan Goodin - Dec 17, 2015 6:50pm EST

f Share   **Tweet**   **Email**   133

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections," Juniper Chief Information officer Bob Worrall wrote. "Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS."

A separate advisory from Juniper says there are two separate vulnerabilities, but stops short of describing either as "unauthorized code." The first flaw allows unauthorized remote administrative
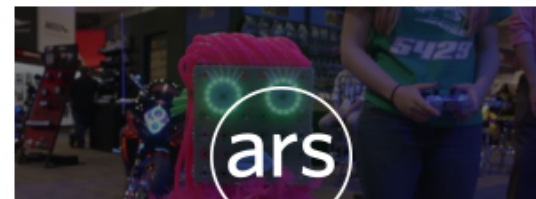
LATEST FEATURE STORY ▲

FEATURE STORY (2 PAGES)

Reboots, remakes, and sequels need not apply— Ars' most anticipated games of 2016

Only original ideas allowed in this selection of upcoming titles.

WATCH ARS VIDEO ▲

ars technica

🏠 **MAIN MENU** ▾   **MY STORIES: 24** ▾   **FORUMS**   **SUBSCRIBE**   **JOBS**   🔍

RISK ASSESSMENT / SECURITY & HACKTIVISM

Secret SSH backdoor in Fortinet hardware found in more products

Company warns customers to remove undocumented authentication feature ASAP.

by Dan Goodin - Jan 22, 2016 3:30pm EST

[f] Share   [🐦] Tweet   [✉] Email   50

A recently identified backdoor in hardware sold by security company Fortinet has been found in several new products, many that were running current software, the company warned this week.

The undocumented account with a hard-coded password came to light last week when attack code exploiting the backdoor was posted online. In response, Fortinet officials said it affected only older versions of Fortinet's FortiOS software. The company went on to say the undocumented method for logging into servers using the secure shell (SSH) protocol was a "remote management" feature that had been removed in July 2014.

In a blog post published this week, Fortinet revised the statement to say the backdoor was still active in several current company products, including some versions of its FortiSwitch, FortiAnalyzer, and FortiCache devices. The company said it made the discovery after conducting a review of its products. Company officials wrote:

FURTHER READING

ET TU, FORTINET? HARD-CODED PASSWORD RAISES NEW BACKDOOR EAVESDROPPING FEARS

Discovery comes a month after competitor Juniper disclosed unauthorized code.
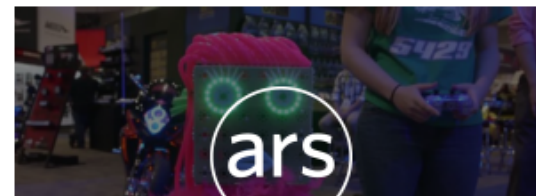
LATEST FEATURE STORY ◢

FEATURE STORY (2 PAGES)

Reboots, remakes, and sequels need not apply— Ars' most anticipated games of 2016

Only original ideas allowed in this selection of upcoming titles.

WATCH ARS VIDEO ◢

ars technica

RISK ASSESSMENT / SECURITY & HACKTIVISM

French agency caught minting SSL certificates impersonating Google

Unauthorized credentials for Google sites were accepted by many browsers.

by Dan Goodin - Dec 9 2013, 2:05pm EST

f Share   ⅴ Tweet   61

LATEST FEATURE STORY ◢

FEATURE STORY (2 PAGES)

Want high-end flight sim pedals? Put $500 in a Polish bank account and contact Slaw

Review: "Wait—$500 for *just* the Slaw Device BF 109?" Well, yes, but what pedals!

WATCH ARS VIDEO ◢

ars

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE VIDEO INSIDER SUBSCRIBE

THREAT LEVEL

FOLLOW WIRED

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

BY KEVIN POULSEN 09.13.13 | 4:17 PM | PERMALINK

f Share 222   Tweet 98   g+1 730   in Share 1   Pinit

Network vs. System vs. Computer vs. Information Security

Not always a clear distinction

    Infrastructure

    Protocols

    Applications

    Hosts/devices

Complex interactions

    Core internet protocols/services

    Distributed systems

    Web/cloud applications

There is more

    People

    Physical security

Threats span all these areas

Network Security Arsenal

Cryptography

Wide range of techniques for enabling secure communication

Access Control

Authentication and authorization, firewalls, …

Monitoring

Packet/flow monitoring, intrusion detection, …

Rigorous protocol and system design/implementation

Account for both benign failures and malicious actions

Data corruption, timeouts, dead hosts, routing problems, …
Eavesdropping, modification, injection, deletion, replay, …

Software bugs in network applications turn into **vulnerabilities**

Threats

Exposure of data

Tampering with data

Denial of service

Impersonation

Forbidden access

Exposure of information about individuals

Identification of unknown individuals

Threats

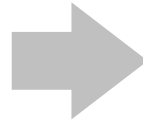Exposure of data

Tampering with data

Denial of service

Impersonation

Forbidden access

Exposure of information
about individuals

Identification of unknown
individuals

Goals

Confidentiality

Integrity

Availability

Authentication

Authorization

Privacy

Anonymity

Confidentiality

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [RFC2828]

Sensitive data must be protected

In transit: network packets, network connections, email messages, document files, …

At rest: main memory (buffers, message queues), storage, …

Cryptography is a tool to achieve confidentiality

Not the only one: access control, steganography, …

Content protection is often not enough

Data vs. metadata (e.g., phone call content vs. records)

Data Integrity

"The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." [RFC2828]

Cryptography is a tool to achieve data integrity

> Intentional or accidental data changes should be detectable

System integrity

"Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system." [CNSSI No. 4009]

> Fragile: weak authentication, vulnerable software, …

Availability

"The property of being accessible and useable upon demand by an authorized entity." [CNSSI No. 4009]

Denial of Service (DoS) attacks are the most common way of affecting the availability of networked systems

> Saturation of resources (bandwidth, CPU, memory, …)
>
> Disruption of configuration or state (routing, DNS, …)
>
> Jamming, physical damage, …

Malware can do more harm

> Ransomware: encrypt user files and then demand a ransom (Gpcode, cryptolocker, …)
>
> Just wipe out data/brick the system (Wiper, NotPetya, …)

Authentication

"The process of verifying an identity claimed by or for a system entity." [RFC2828]

Different approaches

- Something you know (password, pin, …)
- Something you have (phone, token, …)
- Something you are (fingerprint, retina, …)

Multi-factor authentication is a good thing!

Cryptography is a tool to achieve authentication

Password theft/leakage is a huge problem

Authorization

"Access privileges granted to a user, program, or process or the act of granting those privileges." [CNSSI No. 4009]

> Authorization verifies that a user has the proper privileges to access a resource (presumes successful authentication)

Related term: *access control*

> Access restriction based on various properties: identity, role, labels, date/time, IP address, domain, access frequency, …

One of the core goals of network security:
> **Keep unauthorized parties from gaining access to resources**

Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Beyond private data (messages/files):

Activities (browsing history, daily routine, voice commands, …)

Location (3/4G, GPS, WiFi, cameras, …)

Preferences ("likes," Amazon, Netflix, …)

Health (Fitbit, iWatch, …)

…

Anonymity

"The state of being not identifiable within a set of subjects, the anonymity set." [Pfitzmann and Köhntopp]

The larger the anonymity set, the stronger the anonymity

Very different from privacy:

An anonymous action may be public, but the actor's identity remains unknown (e.g., vote in free elections)

Anonymous communication

Sender anonymity

Receiver anonymity

Unlinkability of sender and receiver

Course Focus (you got the idea…)

Internet technologies, protocols, applications, attacks, and defenses, from a practical perspective

Indicative topics

> Core network protocols, eavesdropping, scanning, DoS attacks, firewalls, VPNs, proxies, intrusion detection, forensics, honeypots, encrypted communication, authentication, services and applications, botnets, targeted attacks, privacy, anonymity, …

Cultivate the "security mindset"

> Understand the modus operandi of attackers
>
> Find vulnerabilities, subvert protections, bypass all the things
>
> Think sideways
>
> How to secure a system – know what to defend against

Play Fair

Cannot teach defense without offense, but:

Breaking into systems is illegal!

Unauthorized data access is illegal!

Computer Fraud and Abuse Act (CFAA)

http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Practice on your own systems or controlled environment

Scanning/penetration testing/etc. of third-party systems may be allowed only after getting permission by their owner

Course Information

Mixed format

Lectures

Research paper discussions

Hands-on sessions

Requirements

Reading assignments of research papers for discussion (both in class and online)

4 programming assignments

Midterm and final exams

Grading

Assignments: 45%

Midterm: 20%

Final: 35%

Schedule (Tentative)

Threat Landscape

Lower Layers

Core Protocols

Denial of Service

Firewalls and Gateways

Encrypted Communication

Authentication

SSL/TLS

Crypto Failures

Schedule (Tentative)

Reconnaissance and Scanning

Intrusion Detection

Malware and Botnets

Honeypots, Deception, and Covert Channels

Email

Spam

Web/Cloud

Tracking/Privacy

Anonymity/Online Freedom

Course web page

http://www.cs.stonybrook.edu/~mikepo/CSE508/

Please sign up on Piazza!

All slides and other material will be posted there