CSE 509 Computer System Security

R. Sekar
Why care about computer security?
Egham, U.K., February 7, 2017

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 internet-connected computer systems

- 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
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

Most popular in US

Arizona Cardinals 15-49 Carolina Panthers: NFC championship game - as it happened

Aldi confirms up to 100% horsemeat in beef products

Netflix and thrill: TV industry braced for rollercoaster ride

The rise and fall of Sarah Palin: plucked away from Alaska, she lost her soul
An Unprecedented Look at Stuxnet, the World’s First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

Share 4.3k Tweet 1,485 +1 129 Share 693
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

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.
But the deeper aspects of your personality remain hard to detect.
"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 6:50p EST

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 access, and the second allows access to the internal configuration of a device. Both can be exploited through a remote attack.
The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE  DEC. 13, 2018
Ransomware attacks have been steadily increasing in the healthcare industry since the beginning of the year, and with the most recent attacks on New Jersey Spine Center, Marin Healthcare District and Urgent Care Clinic of Oxford, it doesn't look like the target placed on these providers will be shrinking anytime soon. Hospitals are recognizing the threat and are making cybersecurity a top priority. But as cybercriminals gain intelligence—and confidence—it may not be enough to make up for human error, outside vendors and other vulnerabilities.

Read the Analysis: Hollywood Presbyterian hack signals more ransomware attacks to come.
Data Leaks ...

Anthem 80,000,000
Experian / T-mobile
Hacking Team
IRS Invest Bank
Kromtech
Premera
Securus Technologies 70 million
MSpy
Mozilla

Home Depot 56,000,000
British Airways
Carefirst

AOL 2,400,000
Community Health Services
AOL dl; lister
Advocate Medical Group

Apple Drupal
Facebook

Evernote 50,000,000
Global Payments

Blizzard 14,000,000
Gamigo

Massive American business

Living Social 50,000,000
European Central Bank
Klosterman Cables

Nintendo

UBS

Target 70,000,000
Sanrio
Staples
T-Mobile

UBS

VTECH

Voter Database 191 million

Zappos 24,000,000
Washington State Court system

Office of the Texas Attorney General
South Carolina Government
Yahoo says data stolen from 1 billion accounts

by Seth Fiegelman  @sfiegelman

December 15, 2016  4:30 AM ET

Just when you think Yahoo’s security issues can’t get any worse, the company proves you wrong.

Yahoo (YHOO, Tech30) disclosed a new security breach on Wednesday that may have affected more than one billion accounts. The breach dates back to 2013 and is thought to be separate from a massive cybersecurity incident announced in September.

Yahoo now believes an “unauthorized third party” stole user data from more than one billion accounts in August 2013. That data may have included names, email addresses and passwords, but not financial information.
What is security?

- Wikipedia

  - Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.
What is computer security?

- Everyone has their own definition
  - No single one is perfect
- Computer security deals with protecting data, programs, and systems against intelligent adversaries.

Safety vs Security

- What’s the difference between the two?
- Do they interact?
CIA

- Security is about CIA

- **Confidentiality**: Keeping data and resources hidden or protected from unauthorized disclosure

- **Integrity**: Data and Programs are modified in specified and authorized ways. Data integrity and origin integrity.

- **Availability**: Systems and networks are available for use by legitimate users
Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows are the “vulnerability of the decade”
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.
Why is it hard?

- It is hard to get security right because:
  - Security is hard to test for
    - Testing correctness versus security
  - It requires a deep understanding of all technologies involved in the design and implementation of a system
    - Really hard in large real systems
  - Users are typically the weakest link
  - **Asymmetry** between attack and defense
● Course Focus

● Introduction to a wide range of topics in computer system and software security
  ● vulnerabilities, exploit and mitigation techniques
  ● malware trends and defenses against untrusted code
  ● binary analysis, reverse engineering and forensics
  ● software vulnerability scanning techniques and tools

● Cultivate the “security mindset”
  ● Understand the modus operandi of attackers: find vulnerabilities, subvert protections, bypass defenses, …

● Hands-on assignments in exploit development and mitigation

● Get a taste of security research through a project
Play Fair

Cannot teach defense without offense, but:

- Breaking into systems is illegal!
- Unauthorized data access is illegal!

Computer Fraud and Abuse Act (CFAA)

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 Logistics

- Lectures: Tue/Thu: 10:00AM to 11:20AM

- Grade breakdown (subject to minor tweaks):
  - 10% Homework quizzes (scaled up by 33%)
  - 18% Mid-term exam
  - 20% Programming assignments
  - 20% Project
  - 32% Final exam

- Blackboard will be used for assignments & grading
- Piazza for discussions

- Static information on the course web page: http://seclab.cs.stonybrook.edu/sekar/cse509
Code of Conduct

- The work that you present as your own, should be your own
  - Cite the resources that you used (other people’s code, documents, etc.)
  - Don’t allow your code/paper summaries to be copied
  - Don’t copy other people’s code or paper summaries
- Anything short of the above, will be grounds for immediate failing of the class and a stain in your record
Credits

- Some slides courtesy of Nick Nikiforakis and Michalis Polychronakis