CSE 509: System Security

Fall 2024

R. Sekar

Why do we want to study Security?

1. It is important
2. There is never a dull day!
3. It is fun!

1. Security is Important

- An increasing part of our business, social, and personal life involves internet-connected computer systems
  - Web, email, social networks, entertainment, . . .
  - Internet of things
  - Cyber-physical systems
- Protecting the security and privacy of our digital interactions is critical
  - Most of them involve networked systems and applications

2. There is never a dull day!

- Every day, we hear news of yet another high-profile hack, data theft, etc.
- New vulnerabilities surface all the time, and we have to find new solutions
- High-stakes game where attackers and defenders innovate constantly in order to stay ahead of each other

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

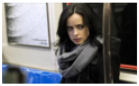
Polish state-owned airline LOT suffers hacking assault on ground systems that causes 10 national and international flights to be cancelled

At no point was the safety of ongoing flights compromised, said a spokesman for LOT Polish airlines.

Most popular in US


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

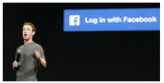
Aldi confirms up to 100% horsemeat in beef products


Netflix and thrill: TV industry braced for rollercoaster ride

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

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

MOST RECENT WIRED POSTS



Facebook Just Had Another Record Quarter, and It Has Apple to Thank

Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable

A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online

Amazon Challenges Google and Microsoft With Its Own Email Service

These Are the

How A Coffee Machine Infected Factory Computers with Ransomware

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

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

"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

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

3. It is fun!

- System security brings together all of the fun CS topics we have learned through other courses
  - Architecture
  - Operating Systems
  - Networks
  - Compilers and Programming Languages
  - Algorithms
  - AI
- System security helps us make connections between these topics, helping us to understand them and remember them better.

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?

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.

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

Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems tend to be complex
  - Complexity is the #1 culprit behind most security failures

Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems tend to be complex
  - Complexity is the #1 culprit behind most security failures
- Implementations are buggy
  - Buffer overflows have been the “vulnerability of the decade” for multiple decades!
  - Cross-site scripting and other Web attacks

Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems tend to be complex
  - Complexity is the #1 culprit behind most security failures
- Implementations are buggy
  - Buffer overflows have been the “vulnerability of the decade” for multiple decades!
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks

Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems tend to be complex
  - Complexity is the #1 culprit behind most security failures
- Implementations are buggy
  - Buffer overflows have been the “vulnerability of the decade” for multiple decades!
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks exploit the weakest link in the chain: Humans!
  - Phishing, social engineering, etc.

Why is it hard?

- 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
- *Asymmetry* between attack and defense

Course Focus

- Introduction to a wide range of topics in computer system and software security
  - software vulnerabilities and advances in exploit techniques
  - vulnerability analysis and mitigation techniques
  - binary analysis and instrumentation; reverse engineering
  - OS security, isolation and sandboxing
  - advanced attack campaign detection and forensics
- Cultivate the "security mindset"
  - Think like an attacker: find vulnerabilities, subvert protections, bypass defenses, ...
- Hands-on assignments in exploit development and mitigation techniques
  - These will be relatively short assignments
- Get a taste of security research through a project

Ethics and Legal Considerations

- 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

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 "F" grade and further disciplinary action

Credits

- Some slide contents in this lecture and future ones are courtesy of Nick Nikiforakis and Michalis Polychronakis