Advanced Network Security

A. M. Sadeghzadeh, Ph.D.

Sharif University of Technology
Computer Engineering Department (CE)
Data and Network Security Lab (DNSL)

October 7, 2023

Most slides have been adapted from Steven Bellovin talk, Thinking Security, 2015.

Today’s Agenda

1 Course logistics

2 Security Thinking!

Course logistics

Course information

- Course Number: 40817-1
  - Time: Sun-Tue 15:00-16:30
  - Rooms: CE-204 and https://vc.sharif.edu/ch/amsadeghzadeh
- Instructor
  - Amir Mahdi Sadeghzadeh (amsadeghzadeh@gmail.com)
    - Office: CE-501
    - Office hours: by appointment and through email
- Course website: ans-sut.github.io
  - Syllabus, Lecture slides, Assignments, etc
- Quera: Quera page
  - Discussions and HWs
- TAs
  - Razieh Eskandari (Head TA)
  - Erfan Zarinkia
  - Fateme Babatabar
  - Mohammad Jangholi
  - Parham Chavoshian

References

- The main references for the course are many research papers in top-tier conferences and journals in computer security (SP, CCS, Usenix Security, EuroSP, TIFS, and TDSC) and the following textbooks:
  1. Thinking Security: Stopping Next Year’s Hackers, Steven M. Bellovin, Addison-Wesley, 2016.
  2. Cryptography and Network Security: Principles and Practice, William Stallings, Pearson, 2022.
  3. Network security essentials: applications and standards, William Stallings, Pearson, 2016.

References

- The main references for the course are many research papers in top-tier conferences and journals in computer security (SP, CCS, Usenix Security, EuroSP, TIFS, and TDSC) and the following textbooks:
  1. Thinking Security: Stopping Next Year's Hackers, Steven M. Bellovin, Addison-Wesley, 2016.
  2. Cryptography and Network Security: Principles and Practice, William Stallings, Pearson, 2022.
  3. Network security essentials: applications and standards, William Stallings, Pearson, 2016.

- Information security conferences
  1. IEEE Symposium on Security and Privacy (S&P)
  2. ACM Symposium on Computer and Communications Security (CCS)
  3. USENIX Security Symposium
  4. Network and Distributed System Security Symposium (NDSS)

- Information security journals
  1. IEEE Transactions on Information Forensics ans Security (TIFS)
  2. IEEE Transactions on Dependable and Secure Computing (TDSC)
  3. Computer and Security
  4. ACM Transactions on Privacy and Security (TOPS)

Course outline

- Review Data and Network Security
- Firewall
- Intrusion Detection systems (IDSs)
- Denial-of-Service (DOS)
- Worms
- Botnets
- Honeypot
- Spyware
- Phishing
- Traffic Analysis
- Anonymity
- Routing Security
- Wireless Security
- Network Forensics
- IoT Security
- ML Security
- Usability and People Issues
- Ethical Issues in Computer Security

Pre-requisite

- Data and Network Security 40-441

Homeworks

- There are 4 homeworks

Homeworks

- There are 4 homeworks

- Late policy
  - All students have 14 free late days for the assignments
    - You can distribute them as you want across your HWs
    - No more than 5 days for each homework
    - All subsequent late submissions will accrue a 20% penalty

Homeworks

- There are 4 homeworks
- Late policy
  - All students have 14 free late days for the assignments
    - You can distribute them as you want across your HWs
    - No more than 5 days for each homework
    - All subsequent late submissions will accrue a 20% penalty
- Ethics statement
  - Please read Sharif CE Department Ethics Statement
  - Every student must solve every homework by themselves
    - You may discuss the homeworks with your friends, but when you finally solve it, every line of your code (except libraries that have been okayed by course staff) must be written by you
    - **Your solution must be yours**

Grading Policy

- Homeworks (30%)
- Paper review and presentation (20%)
- Midterm (and Mini-Exam) (20%)
- Final (30%).

Presentations

- Each student has two presentations

Presentations

- Each student has two presentations
- Should cover at least one paper assigned for reading
- The list of candidate papers is determined by the instructor.

Presentations

- Each student has two presentations
- Should cover at least one paper assigned for reading
- The list of candidate papers is determined by the instructor.
- Ensure you explain the problem, proposed solution, and the evaluation clearly
  - May choose an appropriate format
  - Slides
  - Interactive demos
  - Code tutorials
  - Should involve class
  - Time the presentation to last 20 minutes

Presentations

- Each student has two presentations
- Should cover at least one paper assigned for reading
- The list of candidate papers is determined by the instructor.
- Ensure you explain the problem, proposed solution, and the evaluation clearly
    - May choose an appropriate format
    - Slides
    - Interactive demos
    - Code tutorials
    - Should involve class
    - Time the presentation to last 20 minutes
- Allocate enough time to make the presentation, it is not as easy as you think
- Will be evaluated by the instructor, TAs, and your classmates

Presentation rubric

- Technical
  - Depth of content
  - Accuracy of content
  - Paper criticism
  - Discussion lead

Presentation rubric

- Technical
  - Depth of content
  - Accuracy of content
  - Paper criticism
  - Discussion lead
- Soft presentation skills
  - Time management
  - Responsiveness to audience
  - Organization
  - Presentation aids

(Papernot, 2019)

Ethical Statement

- This course covers topics in personal and public privacy and security. As part of this investigation we will explore technologies whose abuse may infringe on the rights of others.
- As instructor, We rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels.
- Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.
- When in doubt, please contact the course professor for advice. **Do not** undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Dr. Sadeghzadeh.

(Papernot, 2019)

!

Enjoy the course :)

Security Thinking!

Security

Achieving some goal in the presence of an adversary.

Security

Achieving some goal in the presence of an adversary.

- **Policy**: the goal you want to achieve.
  - e.g. only Alice should read file F.
  - Common goals: Confidentiality, Integrity, Availability (CIA), and privacy.

Security

Achieving some goal in the presence of an adversary.

- **Policy**: the goal you want to achieve.
  - e.g. only Alice should read file F.
  - Common goals: Confidentiality, Integrity, Availability (CIA), and privacy.

- **Threat model**: assumptions about what the adversary could do.
  - e.g. can guess passwords, cannot physically grab file server.
  - The adversary might always surprise you in terms of what they might be able to do in practice.

Security

Achieving some goal in the presence of an adversary.

- **Policy**: the goal you want to achieve.
  - e.g. only Alice should read file F.
  - Common goals: Confidentiality, Integrity, Availability (CIA), and privacy.
- **Threat model**: assumptions about what the adversary could do.
  - e.g. can guess passwords, cannot physically grab file server.
  - The adversary might always surprise you in terms of what they might be able to do in practice.
- **Mechanism**: A security mechanism is a method, tool, or procedure that ensures our policy is followed as long as the adversary follows the threat model.
  - e.g. user accounts, passwords, file permissions, encryption.

Security

Achieving some goal in the presence of an adversary.

- **Policy**: the goal you want to achieve.
  - e.g. only Alice should read file F.
  - Common goals: Confidentiality, Integrity, Availability (CIA), and privacy.
- **Threat model**: assumptions about what the adversary could do.
  - e.g. can guess passwords, cannot physically grab file server.
  - The adversary might always surprise you in terms of what they might be able to do in practice.
- **Mechanism**: A security mechanism is a method, tool, or procedure that ensures our policy is followed as long as the adversary follows the threat model.
  - e.g. user accounts, passwords, file permissions, encryption.
- Result: no way for adversary within threat model to violate policy

(Zeldovich, 2014)

Why is security hard?

- It’s a negative goal.
  - It is easy to check whether a positive goal is upheld.
  - E.g., Alice can actually read file F.
- Harder to check that there’s no possible way Alice can read file F.
  - How would you even begin to enumerate all the possible ways Alice could go about reading the file?
  - Too many layers at which Alice could exploit bugs to gain access to file F.
- Difficult to think of all possible ways that attacker might break in.
- Realistic threat models are open-ended.
  - Iterative process: design, update policies, threat model, and Mechanisms as necessary.
  - The weakest link matters.

(Zeldovich, 2014)

Why is security hard?

- In this class, we’ll push the boundary of each system to see when it breaks.
- Each system will likely have some breaking point.
- Doesn’t necessarily mean the system is not useful. It depends on the context.
- Important to understand what a system can do, and what a system cannot.

(Zeldovich, 2014)

Goals

- Usual security trinity: confidentiality, integrity, availability
- Must insure these in two domains:
  - Over-the-wire
  - On the host (for network connected applications)
- Strategies are very different

(Bellovin, 2006)

Host

- The host is (or can be) well-controlled
- There are well-developed authentication and authorization models
- There is a strong notion of privileged state, as well as what program can use it
- Non of that is true for networks

(Bellovin, 2006)

Networks

- Any one can (and does) connect to the network
- Connectivity can only be controlled in very small, well-regulated environments, and maybe not even then
- Different operating systems have different notions of userIDs and privilages

A host can **trust nothing** that comes over the wire!

(Bellovin, 2006)

Unproductive Attitudes

- “Why would anyone ever do that?”
- “That attack is too complicated”
- “No one knows how this system works, so they can’t attack it”

(Bellovin, 2006)

Better Attitudes

- Assume that serial number 1 of any device is delivered to the enemy
- You hand your packets to the enemy to deliver; you receive all incoming packets from the enemy

(Bellovin, 2006)

The Art of War

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
- If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu, roughly 5th century BC

Cybersecurity

- What do you want to protect?
- Against whom?

These are the first two questions to ask in any security scenario

Change

- Businesses change
- Threats change
- Technology changes

How can we build secure systems, in a rapidly changing environment?

Assets

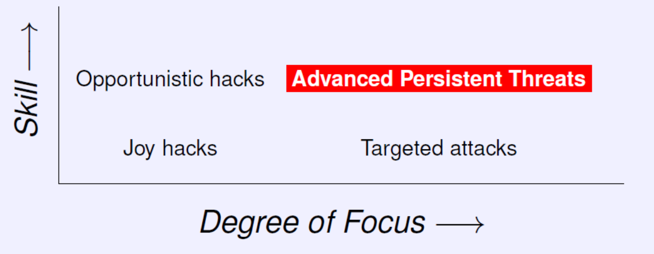
- Different assets require different levels of protection
- Contrast the value of military zone photos with this very ordinary picture
- Security measures have to be commensurate with the value of the assets

Assets and Hackers

- Different kinds of assets attract different kinds of hackers
- The NSA probably isn’t interested in celebrity selfies
  - But they may want such pictures if taken by one of their targets.
- They’re very interested in military and political information
- Most hackers, though, want money
  - They’ll go after anything they can monetize

Hackers

- Different kinds of hackers have different skill and different goals
- They also have different degrees of focus—do they really care what they get?



Skill ⟶

Opportunistic hacks

Advanced Persistent Threats

Joy hacks

Targeted attacks

Degree of Focus ⟶

Joy Hackers

- Little skill (mostly runs canned exploit scripts), not very good target selection
- Describes most novices
- Doesn’t really care about targets—anyone they can succeed against is whom they were aiming for
- They can do damage, but ordinary care is generally sufficient

Opportunistic Hackers

- Skilled, often very skilled, but they also don’t care much about targets
- Most viruses are written by this class of attacker
- Generally speaking, their goal is money: credit cards, bank account credentials, spambots, etc.
- Quite dangerous—but if you’re good enough, they’ll switch targets

Targetiers (An ancient word whose meaning I'm changing...)

- Attackers who target you specifically, but aren't that skilled
- Will do in-depth research on their targets, and tailor their attacks accordingly
- May even exploit physical proximity
- Sometimes a disgruntled insider or ex-insider
- Again, quite dangerous

Advanced Persistent Threats

- Very skilled attackers who focus on particular targets
- The best attackers in this class are national intelligence agencies—you know the countries on the list as well as I do. . .
- May discover and employ “0-days”—holes for which no patches exist, because the vendor doesn’t know of the problem
- May employ advanced cryptographic techniques
- Will employ non-computer means of attack as a complement “The Three Bs: burglary, bribery, and blackmail”
- No high-assurance defenses

Thinking About Insecurity

- In order to know how to defend systems, you have to know how to attack them
- What sorts of attacks are launched?
- Why do they sometimes succeed when you did get the threat model correct?

Thinking Sideways

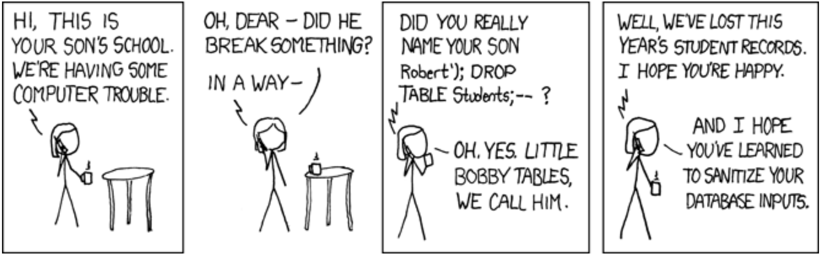
- Attacks frequently succeed when the attacker thinks of an input pattern that the programmer didn't anticipate
- If the choices for an exam question are (a), (b), or (c), enter (d)
- If you that doesn't work, can you sabotage the test?

"You don't go through strong security, you go around it"

Attackers Don’t Follow the Rules

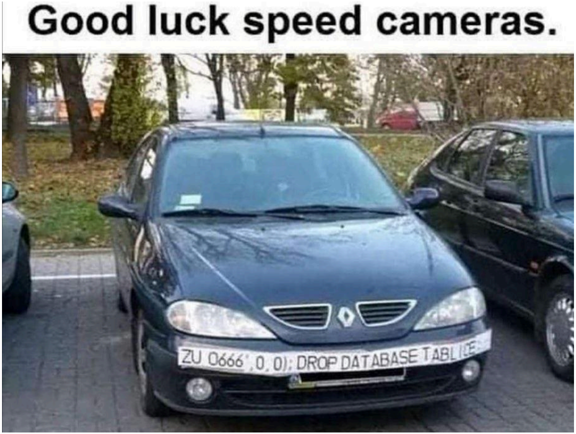
- Requirements document: “Program must accept input lines of 1024 characters”
- Programmer: “char buf[1025]; // leave room for NUL byte”
- Tester: “It accepted the 1024-byte test line; requirement fulfilled”
- Hacker: “What happens if I send 2000 bytes?”

Little Bobby Tables


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

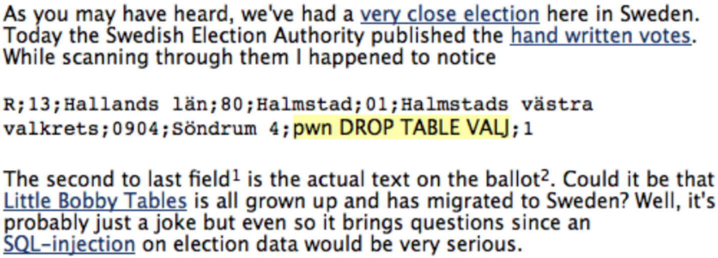
(https://xkcd.com/327/)

Little Bobby Tables



(redit)

Little Bobby Tables



As you may have heard, we've had a very close election here in Sweden. Today the Swedish Election Authority published the hand written votes. While scanning through them I happened to notice

```
R;13;Hallands län;80;Halmstad;01;Halmstads västra
valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
```

The second to last field[1] is the actual text on the ballot[2]. Could it be that Little Bobby Tables is all grown up and has migrated to Sweden? Well, it's probably just a joke but even so it brings questions since an SQL-injection on election data would be very serious.

((http://alicebobandmallory.com/articles/2010/09/23/))

Business and (In)Security

- The purpose of a business (or other organization, but for simplicity I'll speak of businesses) is not to stay secure
  - Rather, it's to achieve certain goals
- From that perspective, insecurity is simply a cost, not a state of sin
- So are security measures ...
- What is the right tradeoff?

Be very, very certain that you understand the assets at risk and who might go after them

Assessing Risk

- What assets do you have?
- What classes of attackers would be interested in them?
- How powerful are those attackers?
- How much security should you afford?

As computer people, we are not good at assessing the risks!

Target Selection

- The attackers have gotten quite sophisticated at target selection
  - They’ve gone after little-known sectors like credit card payment processors
  - Governments often want to build up their own industries, which means that industrial secrets of any sort are at risk from APTs
  - Passwords from otherwise-uninteresting sites may be valuable because people tend to reuse passwords elsewhere, including on financial sites
  - Don’t forget your company’s legacy systems

Target Selection

- The attackers have gotten quite sophisticated at target selection
  - They’ve gone after little-known sectors like credit card payment processors
  - Governments often want to build up their own industries, which means that industrial secrets of any sort are at risk from APTs
  - Passwords from otherwise-uninteresting sites may be valuable because people tend to reuse passwords elsewhere, including on financial sites
  - Don’t forget your company’s legacy systems

- We will review some case studies that illustrate misunderstandings of threats

Case Study: Manning and the Wikileaks Cables

- Much of the US government has come to believe that too much compartmentalization was bad, and loosened access controls on some information
- Their defenses against external attackers were pretty good
- They thought there were no insider risks
- Result: Manning downloaded ˜250,000 “cables” and leaked them

Case Study: Mobile Phone Cloning

- Early US mobile phones were easily cloned: an eavesdropper could pick up ESN/MIN pairs over the air, and burn one into another phone
- The designers had realized this, but overestimated the cost of the attack, the skill level required, and the distribution of such skills
- They assumed limited use of mobile phones (not many targets) and a motive of cost-avoidance
  - Electronics repair technicians simply bought off-the-shelf test gear
  - In fact, phones became widespread, and the motive was criminals wishing to avoid wiretaps
- The attack was easier and the attackers had stronger motives than had been anticipated

Case Study: Stuxnet

- The Iranians assumed that their uranium centrifuge plant was being targeted by serious adversaries—and of course they were right
- They thought that an air gap would defend the plant’s network
- The attackers were more powerful than they had assumed

Assumptions

- Why should technology changes affect our security reasoning?
- Speed? Applications? Bandwidth?
- Many of our security architectures are built around implicit assumptions—and since we don’t know what they are, we don’t react when they’re violated
- We have to identify those assumptions

Example: Passwords

- Assumption: attacker’s computational power is a very small number of computers
  - Today, they have botnets with GPUs
  - Result: guessing attacks are far more effective
- Assumption: users are primarily employees, who could be trained
  - Today, it’s mostly users who will shop or bank elsewhere if they don’t like a site’s rules
  - That’s why popular passwords include ”123456”, ”12345”, ”password”, ”iloveyou”, etc.

Example Assumptions: Smartphones

- Assumption: the IT department controls all devices
  - Smartphones are often employee-owned and operated devices, on your network
  - They’re also on home networks, hotel network, mobile phone networks, and more

We Won’t Identify All Implicit Assumptions

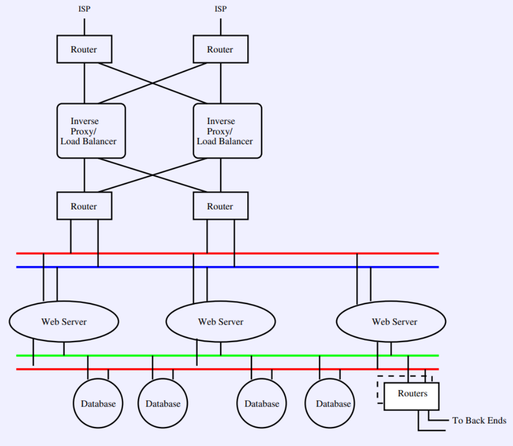
- We can’t—by definition, they’re implicit
- We can try asking, in different places, “why do you think this is secure?”
- In addition, deployed architectures should be reviewed every few years, to ensure that it is still sound and to exam unreviewed changes to the architecture

Security is a Systems Problem

- You don’t get security by sprinkling on crypto
- You don’t get security by requiring strong passwords
- You don’t get security by adding firewalls
- All of these help—but components interact, and it’s often the interactions that cause the problems

A Server Farm

- In a typical web server complex, the inverse proxies act as a firewall, allowing only ports 80 and 443 through
- You can’t get at the databases from the Internet unless you first hack the web servers
- But what about that link at the lower right to the rest of the company?



References

- Steven Bellovin, Thinking Security. Cyber Security Summer School, Estonia, July 2015.
- Nickolai Zeldovich, 6.858 MIT, 2014.
- Mehdi Kharrazi, CE 40-817, Sharif U. T., 2015.