NETWORK SECURITY

"Course introduction"

Corso di Laurea Magistrale in Ingegneria Informatica

Prof. Simon Pietro Romano

spromano@unina.it

WHAT IS THIS ALL ABOUT?

- Network Security...
- ...or, better yet, Security of Distributed Applications (in IP networks)*:
  - email, web applications, VoIP systems, information systems, mobile terminal applications
- Some topics related to network infrastructure security:
  - Remote Connectivity
  - Wireless Networks
  - Hardware Systems (overview...)

*See, e.g., ”Web & Real Time Communication Systems” class @ unina!

SECURITY: AN INFORMAL DEFINITION

"Preventing unauthorized entities from performing actions we do not want to be performed."

SECURITY: A FORMAL DEFINITION

- The “CIA” security triad:
  - Confidentiality
  - Integrity
  - Availability

CONFIDENTIALITY

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

* [excerpt from RFC 4949 – Internet Security Glossary]

CONFIDENTIALITY vs 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." [RFC 4949]

NB:

1. Privacy is one of the reasons that justify the need for "confidentiality"
2. Privacy is (also) closely linked to anonymity
3. Anonymity is (also) the main requirement for a 'hacker' to remain unpunished
4. Like many things in life, security properties often have multiple facets…

SPEAKING OF PRIVACY

> *"Arguing that you don't care about the right to privacy*
> *because you have nothing to hide is no different*
> *than saying you don't care about free speech*
> *because you have nothing to say"*

*Edward Snowden**

http://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for

*Someone who knows their way around privacy!

INTEGRITY [RFC 4949]

Data integrity:

“The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.”

System integrity:

“The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.”

AVAILABILITY [RFC 4949]

"The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them."

NB:

1. If my server is turned off, I certainly ensure confidentiality and integrity, but I completely fail in terms of availability!
2. "Denial of Service" (DoS) attacks specifically aim to undermine the availability of a service... and they are among the trickiest!

COURSE TOPICS

- IP Protocol Security
- Email Security
- Web Security
  - Including next-generation web architectures:
    - WebRTC (Web Real-Time Communication)
- Computer Network Intrusions
- Malware
- Firewalls
- Hacking Techniques:
  - Threats and Countermeasures

“HACKING” IN IP NETWORKS

- Preliminary stages of an attack:
  - Footprinting, Scanning, Enumeration
- Attack Techniques Targeting:
  - End-Systems & Servers;
  - Infrastructure:
    - VoIP (Voice over IP) Networks
    - Wireless Networks
    - Hardware Systems
    - Applications and Data:
      - Web
      - Mobile Devices
    - Databases

MENTAL APPROACH TO SECURITY

- Malicious actors do not follow the rules
- To understand how to make a system more secure, one must identify the attacks to which it may be susceptible...
- ...which, of course, does not imply the need to actually launch such attacks!
- A host cannot trust any data originating from the network

SECURITY "BY DESIGN"

- Any desired type of protection must be explicitly designed and implemented
- For example, secure protocol design:
  - Always leave room for encryption and authentication
  - Ensure that all sensitive fields are protectable
  - Envision mutual authentication
  - Envision authorization mechanisms
  - Envision defense mechanisms against malicious activities such as:
    - eavesdropping, selective modification, deletion, replay, and their combinations

SECURITY AND ‘BUGGY SOFTWARE’

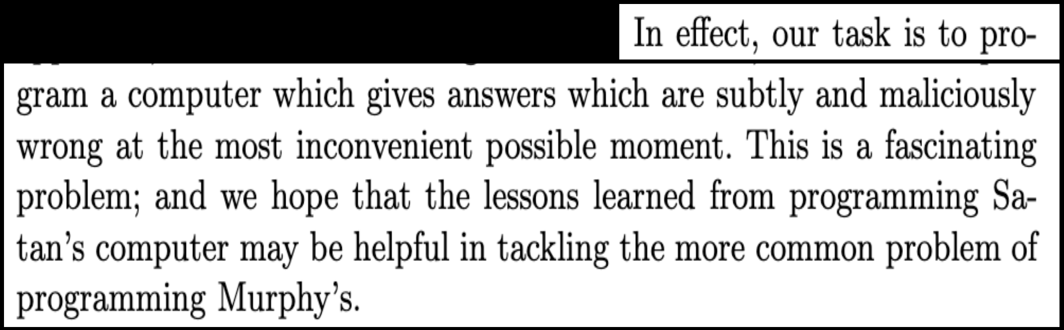
- Most security vulnerabilities are a result of 'faulty' code
- A flawed program that communicates over the network poses a serious security threat
- Software bug-fixing techniques are one of the primary prevention tools related to system security

COUNTERPRODUCTIVE ATTITUDES

- "Why would anyone want to do this?"
- "That attack is too complicated to have any chance of success!"
- "No one knows how this system works (because it's a 'closed' system), so no one can attack it!"

PRODUCTIVE ATTITUDES

- “Programming Satan’s computer” (Ross Anderson & Roger Needham)
  - http://www.cl.cam.ac.uk/~rja14/Papers/satan.pdf



In effect, our task is to program a computer which gives answers which are subtly and maliciously wrong at the most inconvenient possible moment. This is a fascinating problem; and we hope that the lessons learned from programming Satan’s computer may be helpful in tackling the more common problem of programming Murphy’s.

- “Assume that 'serial number 1' of any device is sold to the enemy"
- "All the packets you send are passed to the enemy"
- "All the packets you receive are delivered to you by the enemy"

NETWORK SECURITY TOOLS

- Cryptography
  - 'Out of Topic' for this course → See 'Systems Security' course
  - Network-based access control
    - ...including Firewalls
  - Network monitoring
  - Employment of so-called 'Paranoid Design' techniques
    - see previous slide on productive attitudes...

COURSE PROGRAM (1/2)

- Principles of Network Security
  - Functional Requirements for Security
  - Threats, Attacks, Countermeasures
- Wireless Network Security
- Network-Level Security
  - IPsec Protocol
- Transport-Level Security
  - Transport Layer Security (TLS)
- Application-Level Security:
  - Email
  - Web
    - HTTPS
    - WebRTC Security Architecture
- Cloud Computing and Security (overview)

COURSE PROGRAM (2/2)

- Malicious Software (i.e., malware)
  - Taxonomy
  - Advanced Persistent Threats (APTs)
  - Countermeasures
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks
- Intrusion Detection Systems (IDS)
  - Host-Based, Network-Based, and Hybrid Techniques
- Firewalls and Intrusion Prevention Systems (IPS)

PREREQUISITES

- This is an advanced course in computer networks, so:
  - Computer Networks
    - Prerequisite
- Web & Real Time Communication Systems
  - very useful for in-depth knowledge of Internet application protocols (Web, VoIP applications, real-time multimedia applications)
- There will be a significant focus on:
  - Software and programming techniques
  - Operating Systems
  - Computer Architecture
    - Believe it or not, understanding a 'buffer exploit' requires some knowledge of assembly language and subroutine calling techniques

METHODS OF ASSESSING PROFICIENCY

- 35% of the final grade will be based on the assessment of a practical project related to selected course topics agreed upon with the instructor
  - Option to work on group projects
    - Groups of up to 4 individuals
  - Project to be submitted to the instructor
    - at least 7 days before the oral exam
    - complete with documentation and source code
- 65% of the final grade will depend on the outcome of an oral exam, which will assess:
  - Mastery of course topics
  - Presentation and discussion of the project

REGARDING GROUP PROJECTS

- Cooperation vs. Dishonesty
  - A group can be defined as such when all its members contribute individually
- A project is valid if it contains original contributions
  - The purpose of projects is to deepen your understanding of certain topics and expose you to challenging problems that may not have immediate solutions
  - ...copying and pasting (from the Internet, a friend, ChatGPT, or any other source) is called plagiarism and is not ethically acceptable behavior
- Example of academic honesty policy:
  - http://www.cs.columbia.edu/education/honesty

LECTURES

- Presentation of course topics through slide projection
  - Please note:
    - slides are never exhaustive (if they were, they would be poor slides)
    - slides do not replace textbooks, articles, or any other materials recommended by the instructor
- To the extent possible (as this course does not involve explicit lab activities)
  - practical examples related to some crucial course topics are provided
    - useful for engineering-oriented explanations of the topics discussed
    - to be considered as starting points for defining practical projects

HOMEWORK

- A significant phase of learning will take place on one's own:
  - experimenting with the techniques and methodologies presented in class
  - delving deeper into topics of interest
  - preparing for the practical project in preparation for the exam
- Any issues you encounter at home can be discussed during office hours

PRACTICAL APPROACH

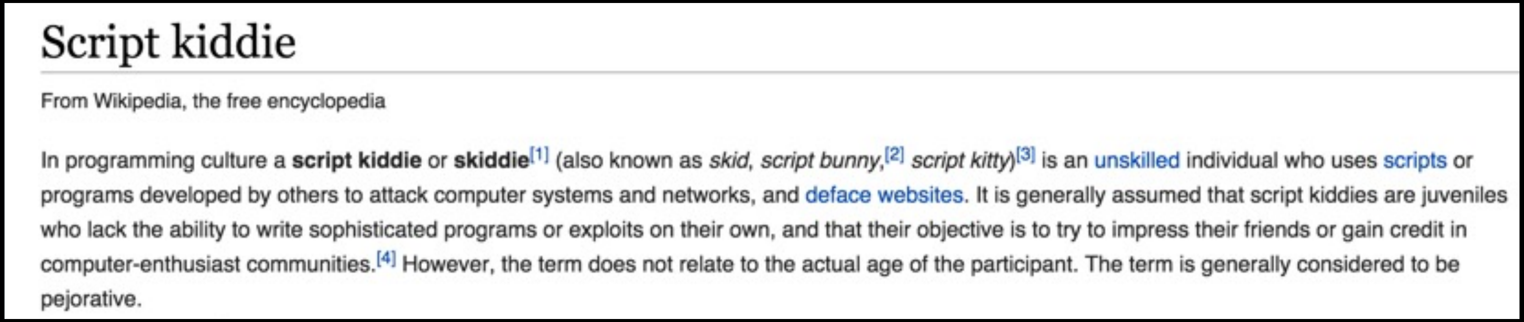
- As always, learning from examples is essential for an engineer
- It is impossible to achieve comprehensive expertise without 'getting your hands dirty'
- But:
  - Practice alone is not enough
  - It is the in-depth theoretical knowledge that distinguishes an engineer from a 'tinkerer'...
  - ...and you are almost engineers!
- The right approach is:
  1. Study
  2. Experiment
  3. Understand better what you have studied!

SECURITY ETHICS

- Taking a security course is not an excuse to behave like a malicious 'hacker'
- In its negative sense, the term 'hacking' refers to:
  - any form of unauthorized access to resources available on the network, including techniques that involve the abuse of authorized permissions
- The mere fact that a file or a computer is not properly protected does not justify unauthorized access
  - ...if (and only if) the legitimate owner of a resource 'invites' you to attack it, then you are authorized!
    - Ever heard of 'penetration testing'?
- In this course, we will not take serious matters lightly
  - we will not become infamous for inventing and spreading new 'Trojan Horses', new 'backdoors', or any other form of malicious code

ASSUMPTION OF RESPONSIBILITY

- You are all adults
- You are all responsible for your actions
- The purpose of this course is to create security experts...
- ...not *'skiddies'*



Script kiddie

From Wikipedia, the free encyclopedia

In programming culture a **script kiddie** or **skiddie**[1] (also known as *skid*, *script bunny*,[2] *script kitty*)[3] is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks, and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities.[4] However, the term does not relate to the actual age of the participant. The term is generally considered to be pejorative.

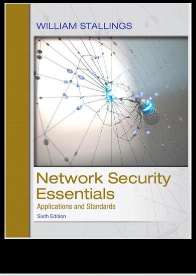
INSTRUCTOR'S REFERENCES

- Simon Pietro Romano
  - Dipartimento di Ingegneria Elettrica e delle Tecnologie dell’Informazione (DIETI)
  - Office:
    - Via Claudio 21, palazzina 3, quarto piano, stanza IV.08
    - ☎ +39 0817683823
    - ✉ spromano@unina.it
    - 🐦 @spromano

- Office hours:
  - Friday 3pm-5pm (also on Teams)

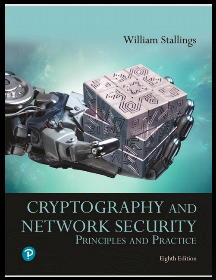
TEACHING MATERIALS (1/2)

- Books:
  - The primary academic ‘evangelist’ in the field of security:
    - William Stallings
  - Three famous books, all suitable for the purpose



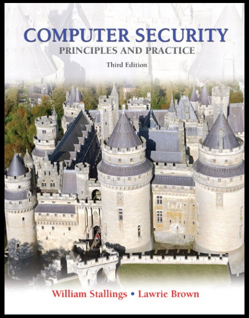
☺☺☺

“Network Security Essentials Applications and Standards”, 6/E
William Stallings
ISBN-13: 9780134528038 - (e-book: 9780134527598)
©2017 • Pearson



☺◖

“Cryptography and Network Security: Principles and Practice”, 8th Edition
William Stallings
ISBN-13: 9780135764039 (e-book: 9780135764268)
©2020 • Pearson

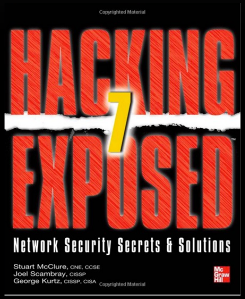


☺☺☺

“Computer Security: Principles and Practice”, 4/E
William Stallings Lawrie Brown
ISBN-13: 9780134794334 – (e-book: 9780134794181)
©2018 • Pearson

TEACHING MATERIALS (2/2)

- A bible for those who want to experiment:



"Hacking Exposed", 7th Edition
by Stuart McClure, Joel Scambray and George Kurtz
Mc Graw Hill
ISBN-10: 0071780289, ISBN-13: 978-0071780285

- Teaching materials available on-line
  - 'Formal' references:
    - e.g., Request For Comments (RFC)
      - www.ietf.org
  - 'Informal' references:
    - e.g.: Phrack Magazine
      - www.phrack.org

REGARDING EXPERIMENTATION

- *"The quiter you become, the more you are able to hear"*
- Kali Linux:
  - an open-source project created and managed by the 'Offensive Security' group, specialized in security training activities, with a focus on so-called 'penetration testing' services
  - a pre-packaged Linux distribution with an impressive arsenal of tools for security auditing

KALI LINUX TOOLS

- Information gathering
- Sniffing & spoofing
- Vulnerability analysis
- Exploitation
- Password attacks
- Wireless attacks
- Forensic analysis
- Hardware hacking
- Web applications attacks
- Reporting
- Stress testing
- Reverse engineering
- Social engineering
- …

QUESTIONS?