EDU/SVS

CORONA
EMERGENCY
LECTURE

Security of Distributed Software

Prof. Dr.-Ing. Martin Gaedke
Chemnitz University of Technology
Department of Computer Science
Professorship of Distributed and Self-organizing Systems

http://vsr.informatik.tu-chemnitz.de

Chapter 1

INTRODUCTION

Introduction

- **Before**:
  - Public networks: closed, managed centrally
  - Internet: pure research network, not a worthwhile target, users trust each other
- **Now**:
  - Increasing decentralization of public networks by deregulation of telecommunications markets
  - Use of the open and decentralized Internet
  - Increasingly extensive use of the Web (Deep Web, Social Web, Web 2.0, Semantic Web)
- **Conclusion**:
  - Security mechanisms are becoming an indispensable part of modern communication systems
  - Security must be considered in a comprehensive and integrated way, taking new aspects into account: identity and privacy

What is Security?

- **Definition** – Ability to avoid being harmed by any risk, danger or threat
  (Cambridge Dictionary of English)
- In practice, an **unreachable goal**
- What does this mean for the IT infrastructure?
  - **YES – YOUR SOFTWARE IS NEVER(!!!!) Secure!**
- How to ensure security and how can it be managed?
- How secure must "secure" really be?
- What has to be done do?

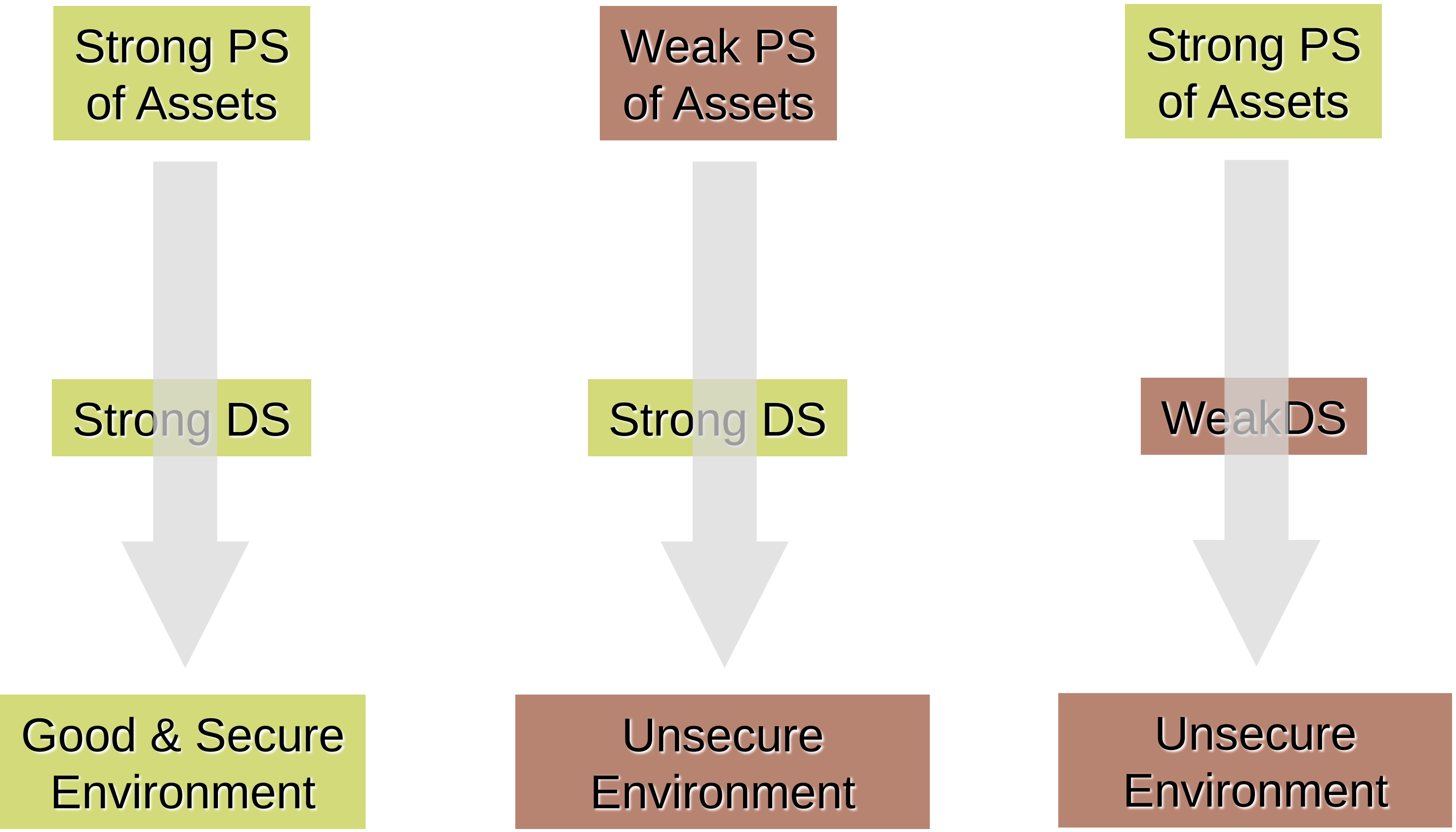
Security Goals (until now)

- Mnemonic for security goals: “**CIA**”
- **Confidentiality**
  - Data secrecy
- **Integrity**
  - Data intactness
- **Authenticity**
  - Secure data origin
- *Additional (soon-to-be-) major goals:*
  - **Liability (Non-Repudiability)**
    - Non-repudiation of data origin
    - Important for contracts or in the fight against SPAM
  - **Identity**
    - Verification of an individual entity
    - Nowadays, identity is of increasing significance!

Assets

- **Asset** – In this lecture, asset is a generic term denoting things worth protecting
  - Data
  - Services, e.g. business applications
- Our focus:
  - Actions to achieve security goals
  - Therefore, strong physical security is the foundation

Digital and Physical Security



Strong PS of Assets

Strong DS

Good & Secure Environment

Weak PS of Assets

Strong DS

Unsecure Environment

Strong PS of Assets

Weak DS

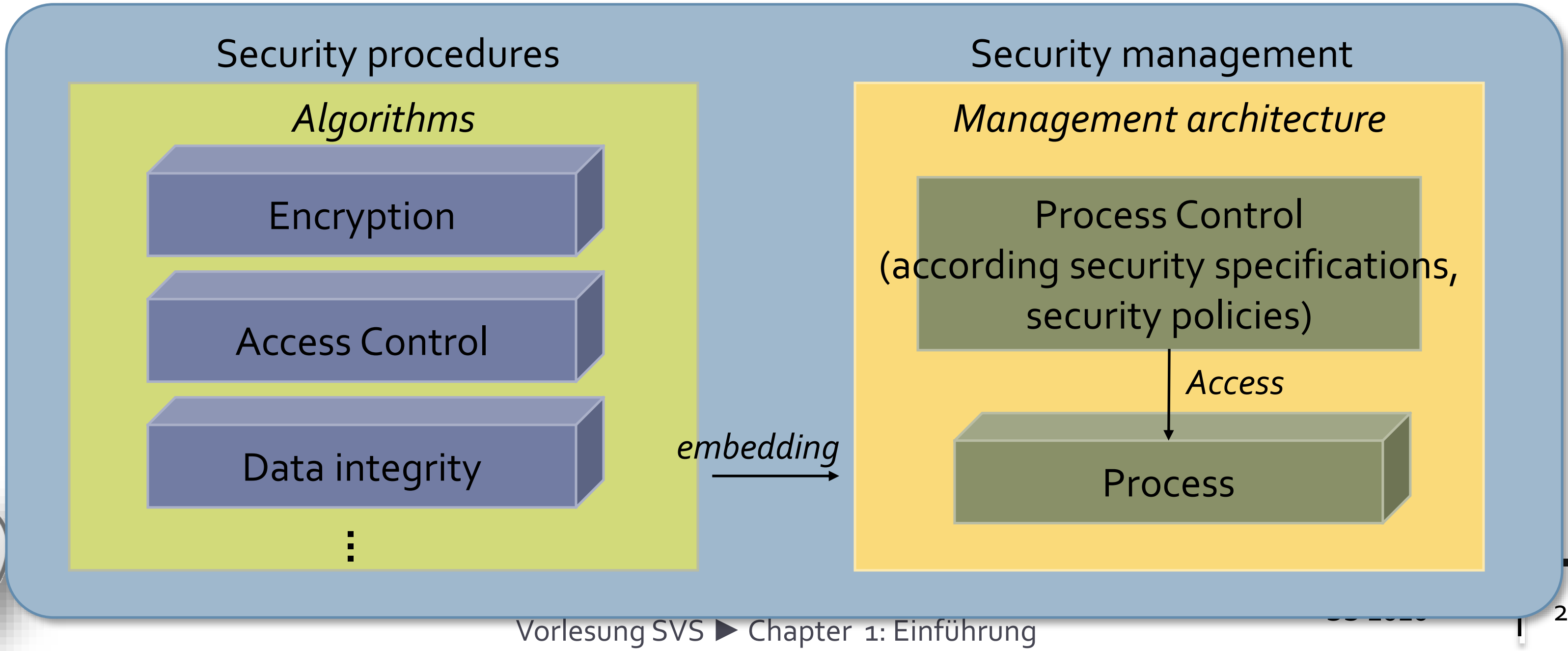
Unsecure Environment

PS – Physical Security
DS – Digital Security

Slide looks boring – but isn't – think about Virtualization!

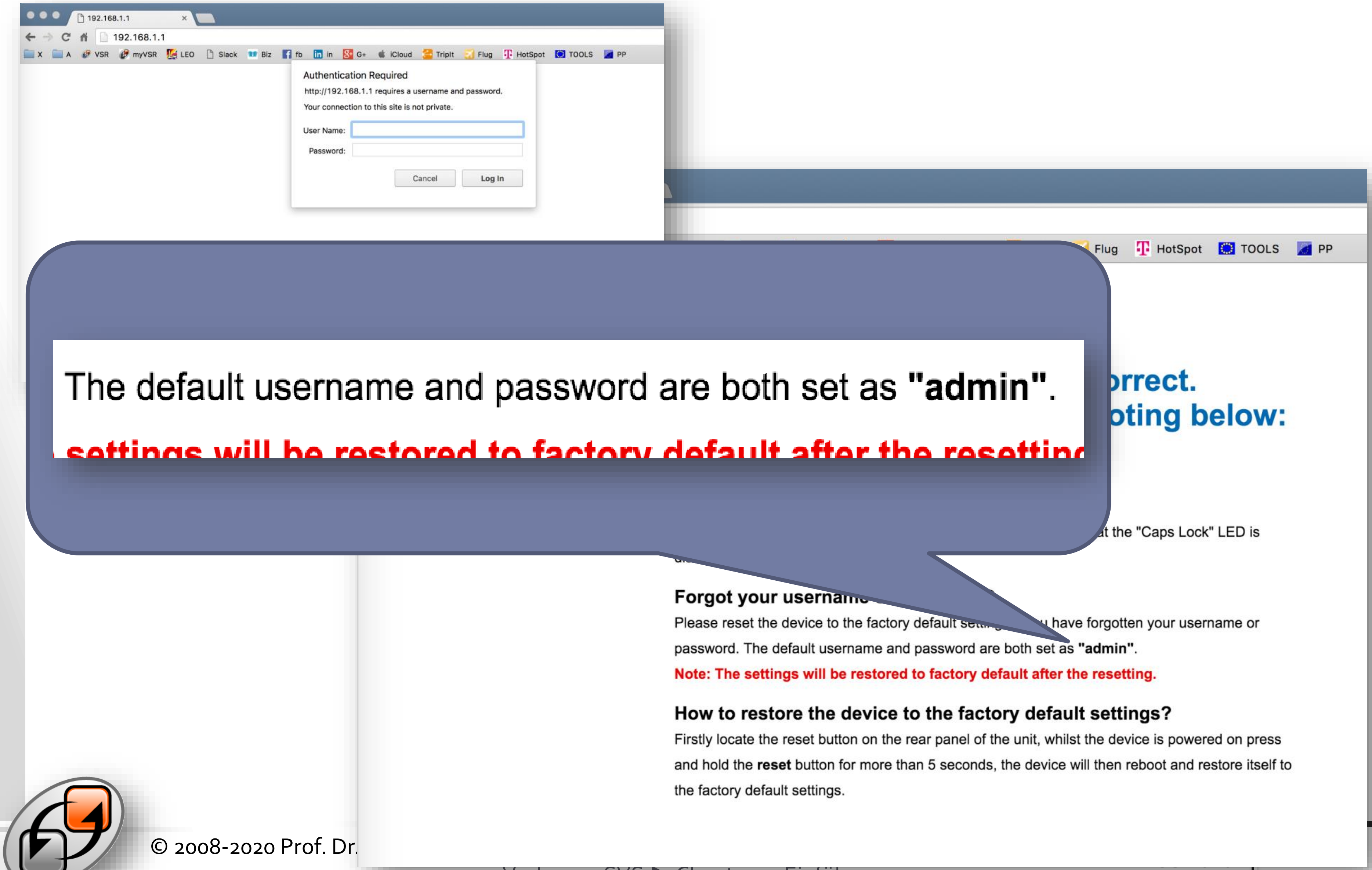
Numerous Challenges

- Achieving security goals by
  - Information encryption
  - Implementation of authentication
  - Establishment of security activities
  - Monitoring of the system or the network in terms of attacks
  - Continuous reduction of weak spots
  - Etc.



Enlarge your attack surface??... Or

How to improve TP-Link (TL-WR841N / TL-WR841ND)



Authentication Required

http://192.168.1.1 requires a username and password.

Your connection to this site is not private.

User Name:

Password:

The default username and password are both set as **"admin"**.

settings will be restored to factory default after the resetting

orrect.

oting below:

at the "Caps Lock" LED is

Forgot your username

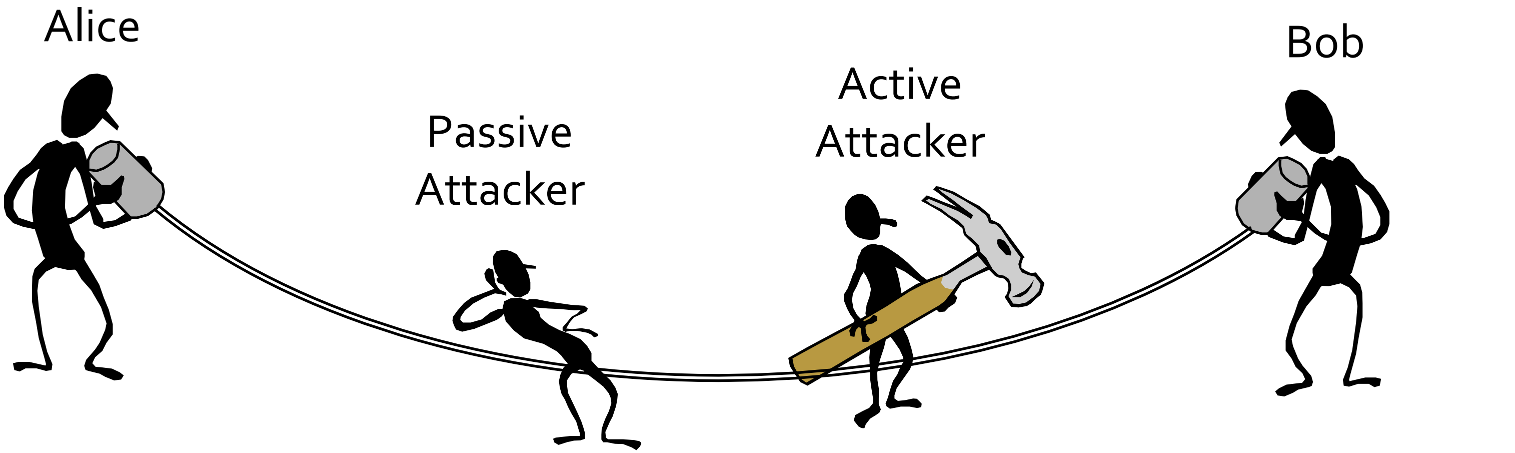
Please reset the device to the factory default setti u have forgotten your username or password. The default username and password are both set as **"admin"**.

Note: The settings will be restored to factory default after the resetting.

How to restore the device to the factory default settings?

Firstly locate the reset button on the rear panel of the unit, whilst the device is powered on press and hold the **reset** button for more than 5 seconds, the device will then reboot and restore itself to the factory default settings.

Data Transfer Model



- The classic scenario
  - **Passive Attacker:**
    - Can only listen, not manipulate
    - Confidentiality threat
  - **Active Attacker:**
    - Can listen, change, delete, duplicate
    - Threat for confidentiality, integrity and authenticity

Authenticity vs. Liability

- Difference between authenticity and liability:
  - Focus on internal and external relationships

- **Authenticity**:
  Bob is sure that the data comes from Alice
- **Liability**:
  Bob can prove it to third parties

Threats

- **Interception** of transmitted data
- **Modification** of transmitted data
  - Change
  - Delete
  - Insert
  - Reorder data blocks
- **Masquerade**
  - Faking a false identity
  - Sending messages with a false source address
- **Unauthorized access** to systems
  - Keyword „Hacking"
- **Sabotage** (Denial of Service)
  - Causing an overload situation (including hardware)
  - "Destroying" protocol instances by illegal packets

Some Attack Techniques

- **Tapping** cables or radio links
- **Interposing** (man-in-the-middle attack)
- **Replaying of intercepted messages** (replay attack)
  (e.g. replay of login messages for the purpose of unauthorized access)
- **Selective changing / swapping of bits or bit strings**
  (without being able to decrypt the message)
- **Break-in** by taking advantage of errors (buffer overflows)
- **Break-in** by means of active components (trojans, worms, backdoors)
- **Breaking cryptographic algorithms**
- **Social Engineering** (e.g. through direct contact and social web)
- **Countermeasures:**
  - **Don‘t use self-made algorithms,**
    use only proven algorithms that are considered safe!
  - Use safe methods and replace old algorithms
  - Behaviour (Pattern) analysis
  - Use Social Web the right way
  - **Know your enemy**

Integrated Security

- Security should be considered in an integrated way
  - Consideration of all assets
  - Based on risk assessment
  - Use adequate security approaches and services (often a mix of different techniques)
- Central question: Security vs. Identity
  - What is more important?
  - What is more effective?

Conclusion

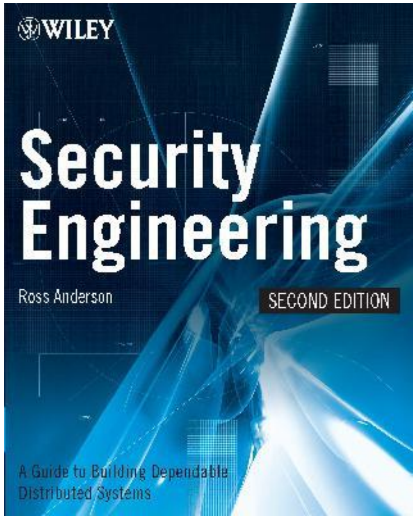
- It is almost impossible to achieve 100% security. Therefore, one has to clearly define what has to be protected and how high the according security requirements should be.
- Until now: A simple but effective approach:
  - Asset lists
  - Risk assessment for each asset

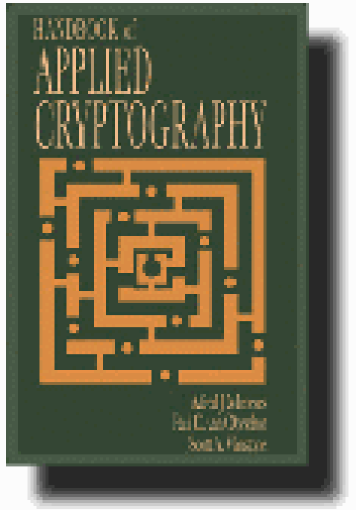
- **But: Is that still simple in the age of the Web?**
- **OUR approach:**
  - **Understand that someday an enemy will successfully attack your application (this might be tomorrow!!!)**
  - **Therefore: Limit the attack surface, limit identity properties, distribute attack surface, apply encryption everywhere**

Beware of Unexpected Risks!

Recommended Reading

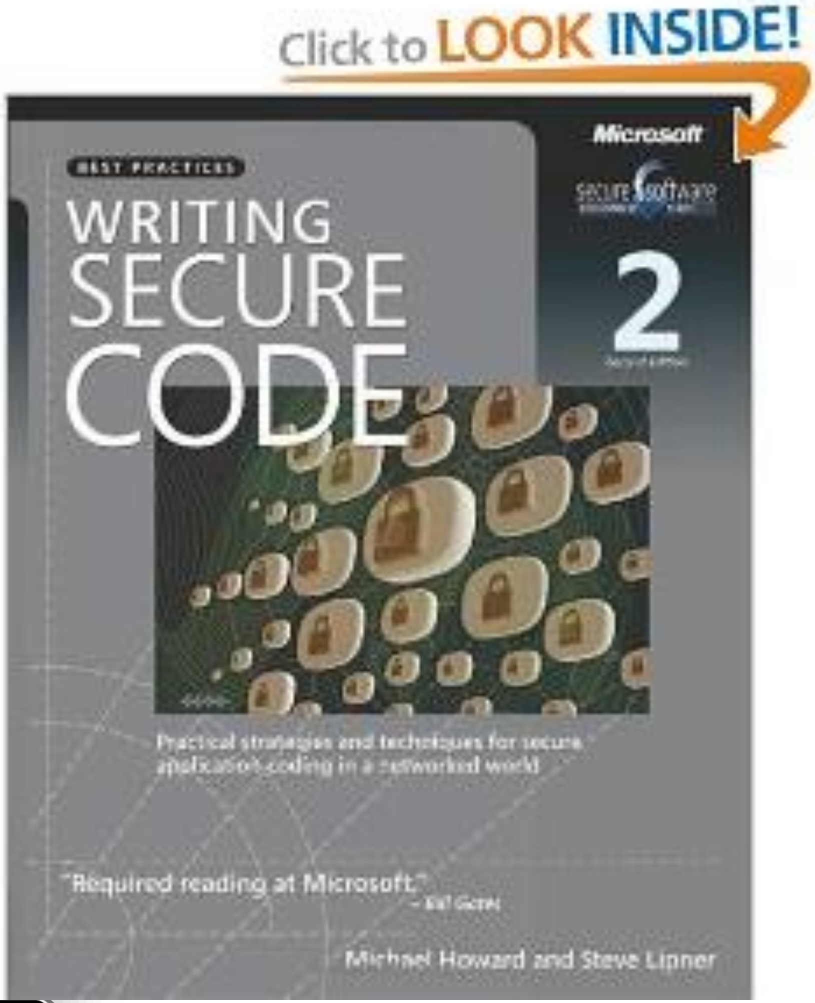
- Security Engineering
  - http://www.cl.cam.ac.uk/~rja14/book.html
- Applied Cryptography
  - http://cacr.uwaterloo.ca/hac/

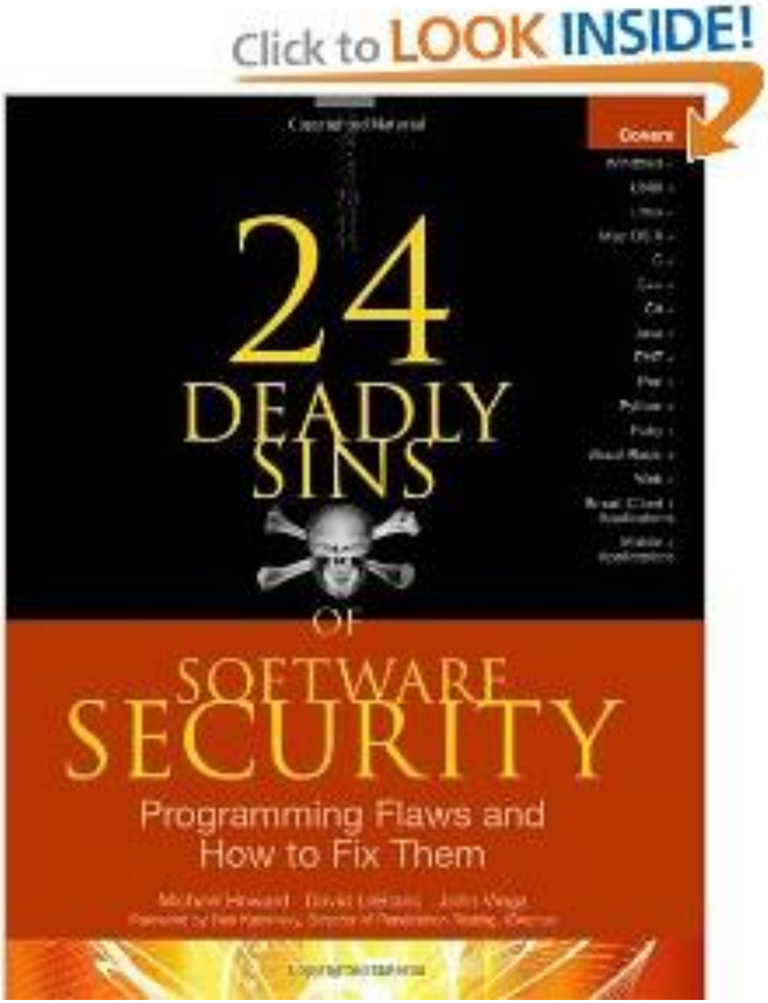




Further references will be given later… such as BlackHat, CCC, etc.

Also recommended


Click to LOOK INSIDE!
Microsoft
BEST PRACTICES
WRITING SECURE CODE
2
Practical strategies and techniques for secure application coding in a networked world
"Required reading at Microsoft."
– Bill Gates
Michael Howard and Steve Lipner


Click to LOOK INSIDE!
24 DEADLY SINS OF SOFTWARE SECURITY
Programming Flaws and How to Fix Them
Michael Howard · David LeBlanc · John Viega

Homework

- Start reading about GDPR:
  - https://www.eugdpr.org/the-regulation.html
  - https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

- Could you answer:
  - What is a data subject?
  - What are the data subject´s rights?
  - What is personal data and what not?
  - What is a data processor?
  - What is a data controler?