mobile business

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Lecture Q&A

Information & Communication Security (SS 2022)

Exam Prep and Wrap Up

Prof. Dr. Kai Rannenberg,

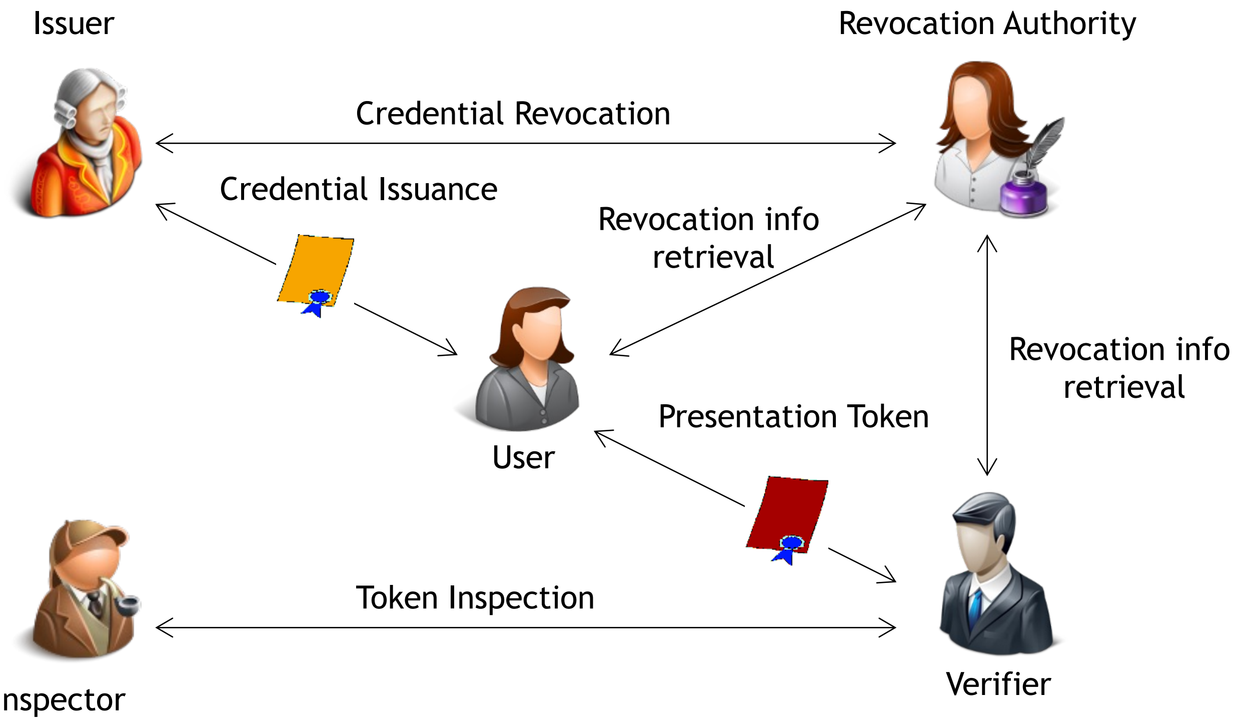
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

Question 1

- Lecture 2 - Authentication: could you please explain slide 48 and 49 again?

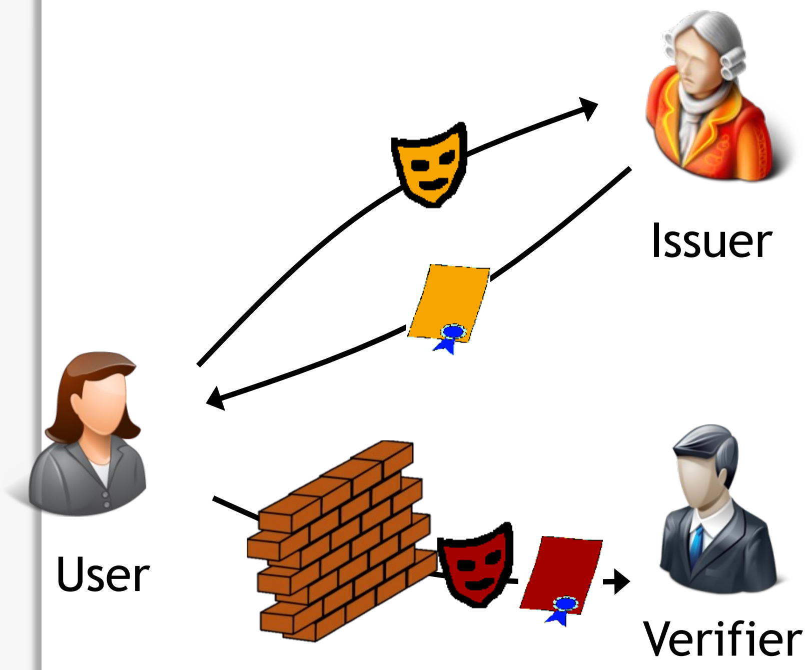
ABC4Trust architecture

Interactions and Entities



Existing Privacy-ABC Technologies

Zero-Knowledge Proofs

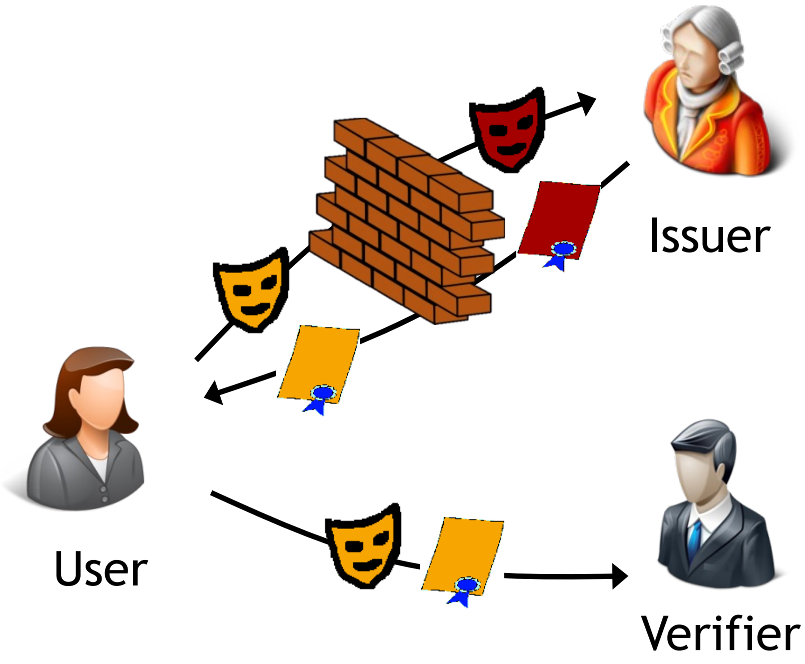


Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya

Strong RSA, pairings (LMRS, q-SDH)

Blind Signatures



U-Prove

Chaum, Brands et al.

Discrete Logs, RSA,…

Question 2

- **Q2:** Assignment - Access Control, Exercise 1: If a person has the right to "write" does he/she automatically has the right to "append"?

- **A2:** “Write” includes “read” and “append”.

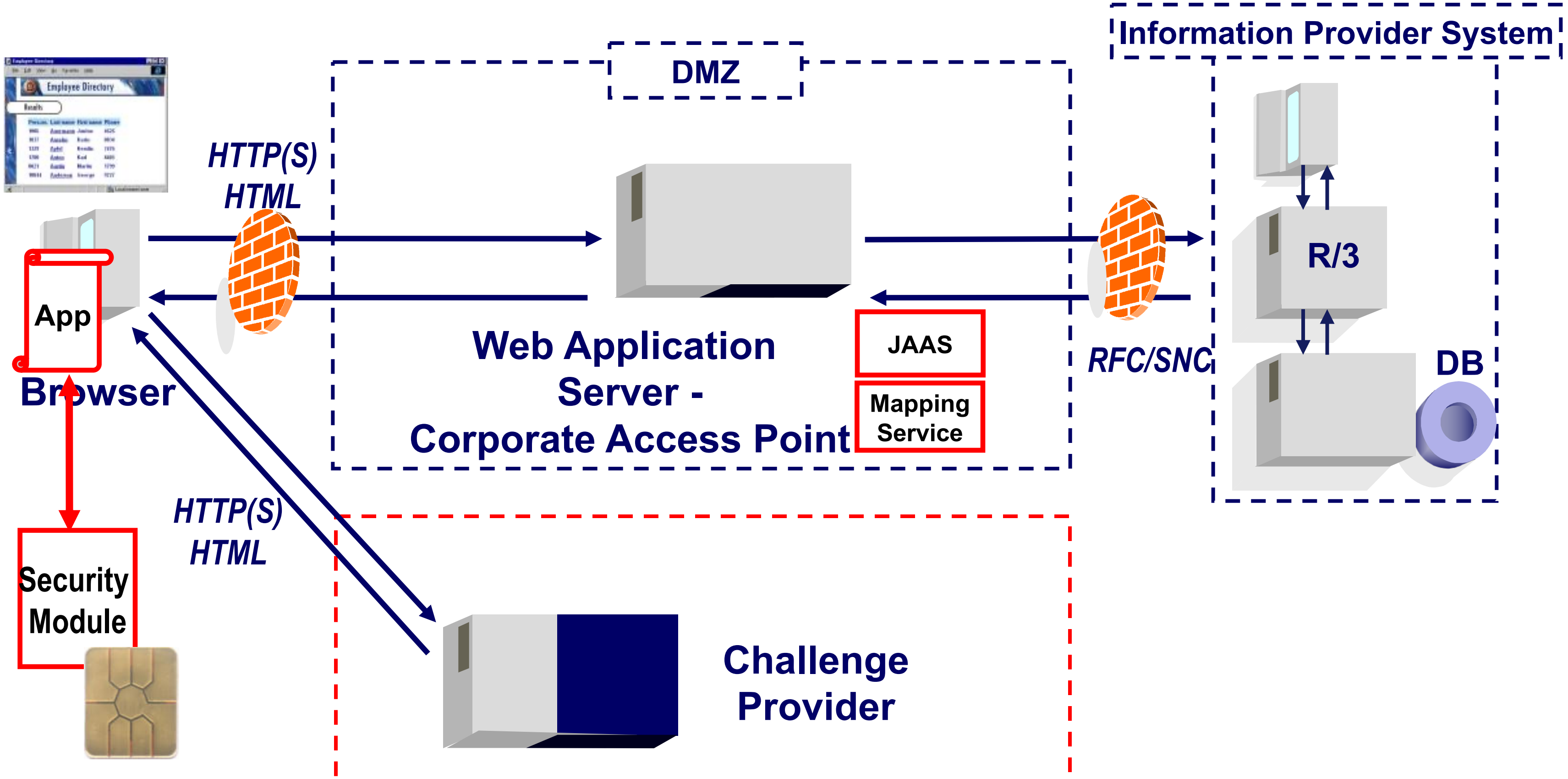
Question 3

- What about the slides 42 until the end of lecture Computer System Security? I think we didn't talk about it.

Question 4

- Lecture 11 - Network Security I: Could you please explain slides 24
and 41-44 again?

Example: WiTness Security Module for Login Authorisation – System view (S24)



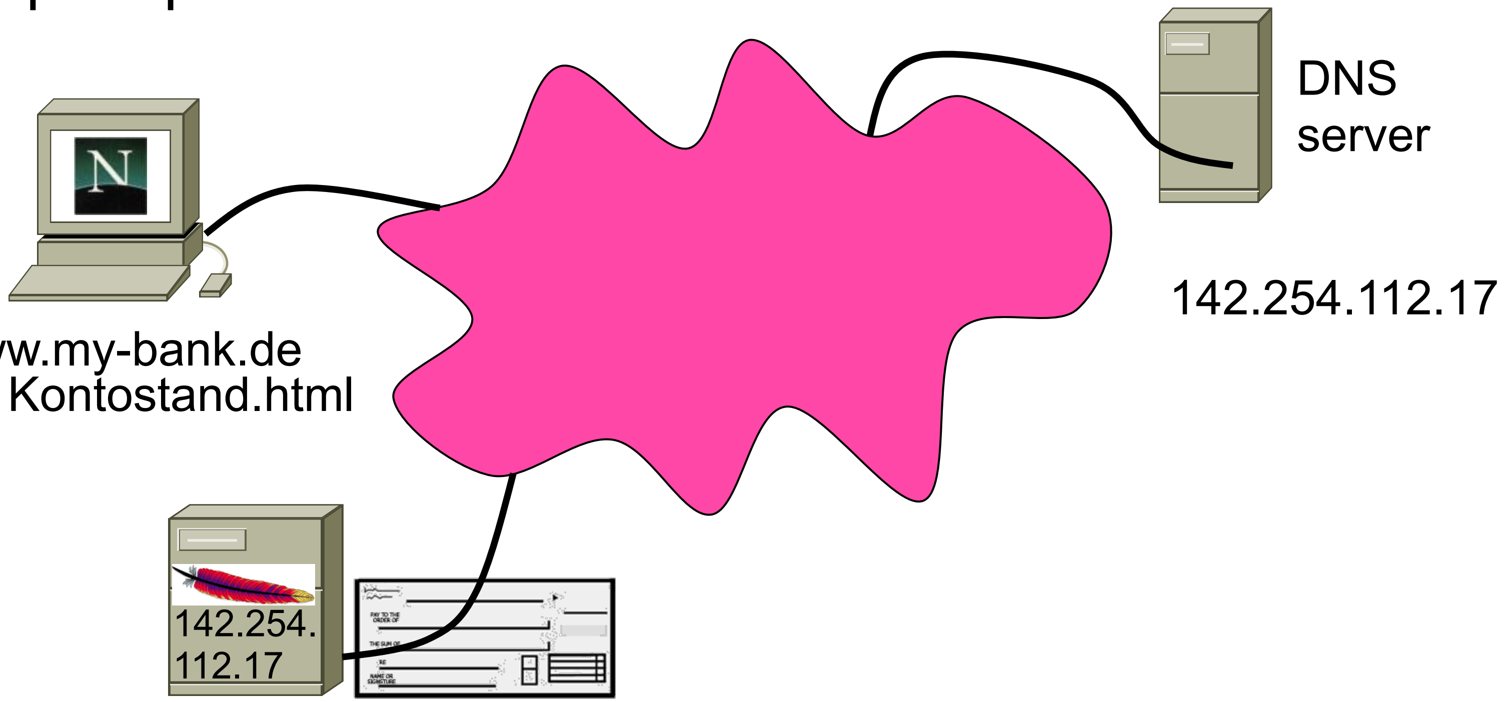
JAAS = Java Authentication and Authorization Service

Example: Online-Banking (S41)

www.my-bank.de/Kontostand.html

Actions of the browser:

1. DNS-Request
2. http-Request



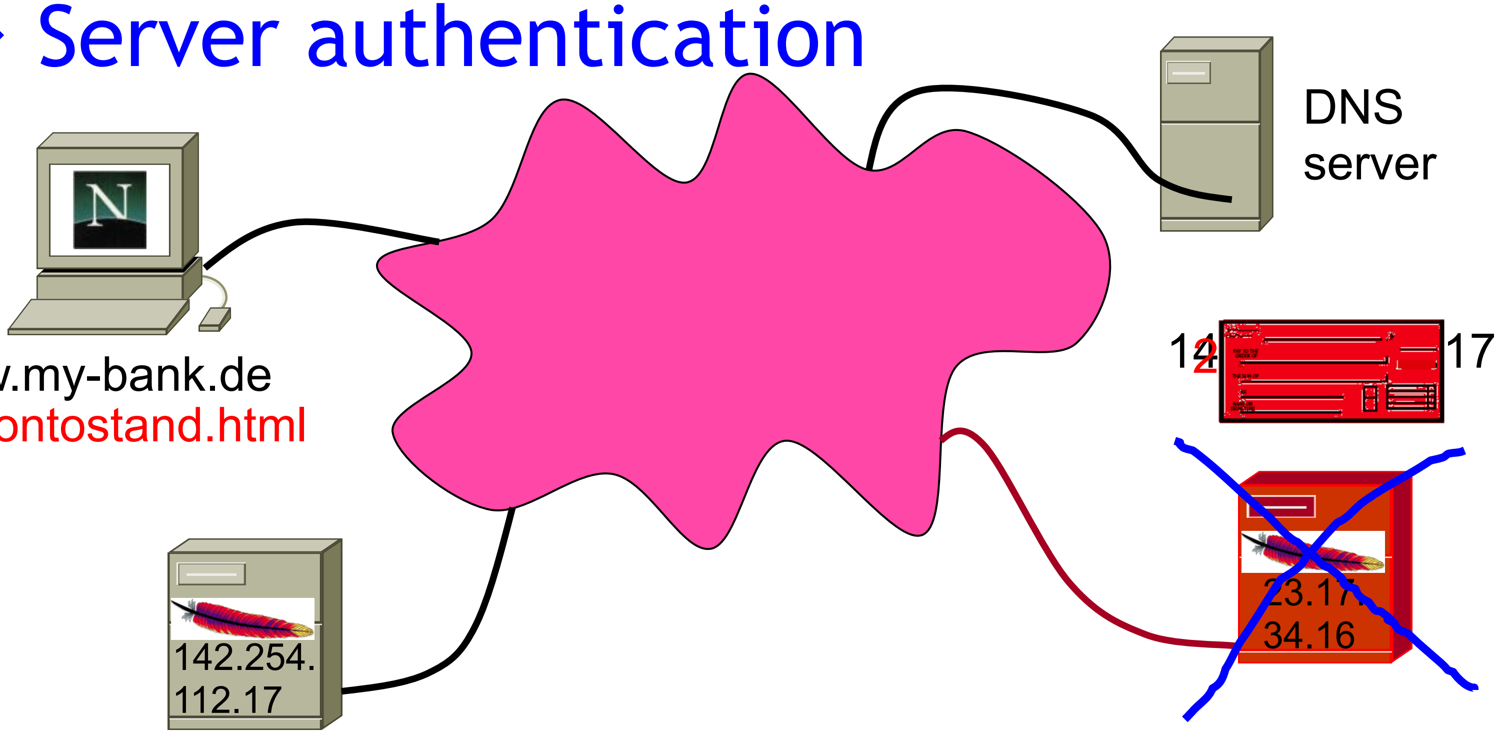
[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

DNS spoofing

Possible attacks:

1. Compromise of DNS (DNS spoofing)

   → Server authentication



www.my-bank.de

get Kontostand.html

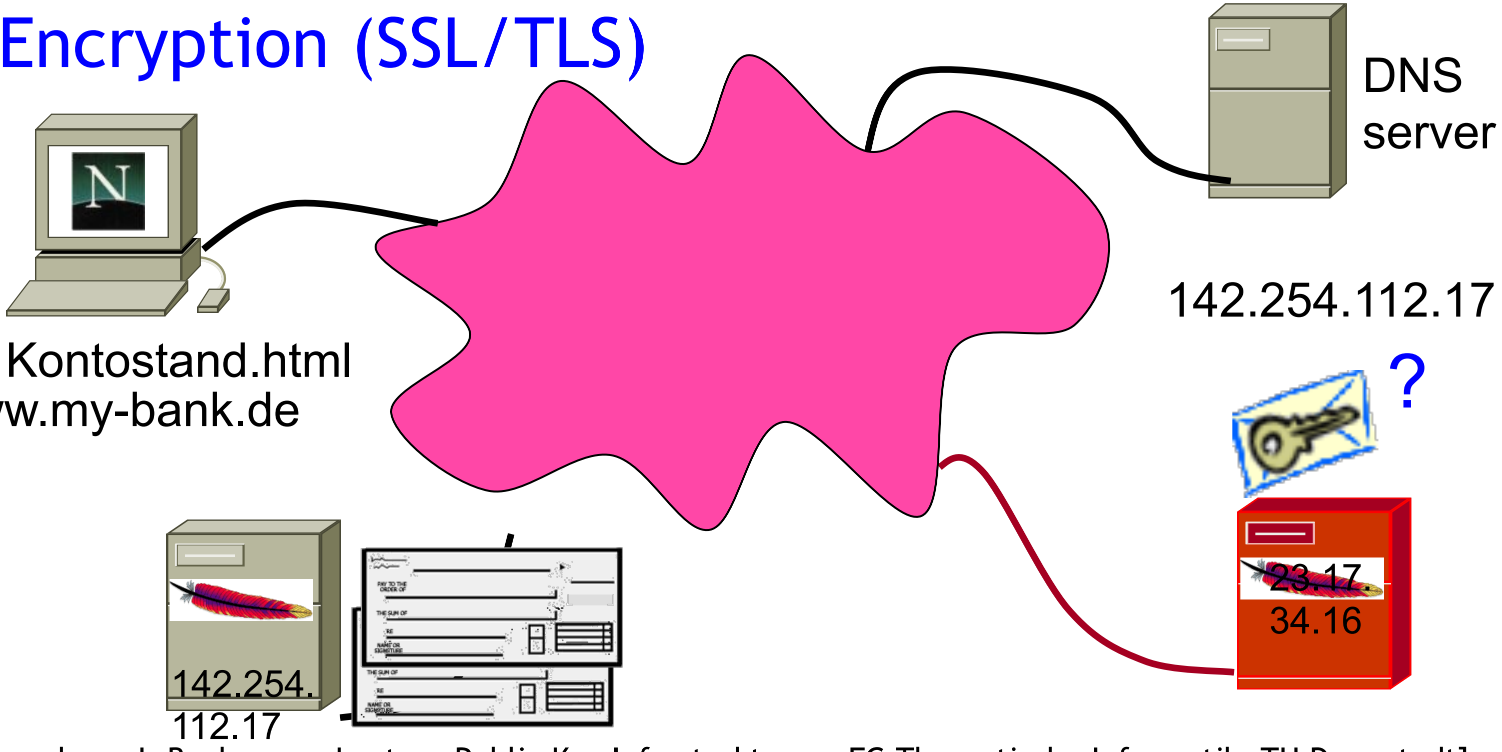
[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

HTTP sniffing

Possible attacks:

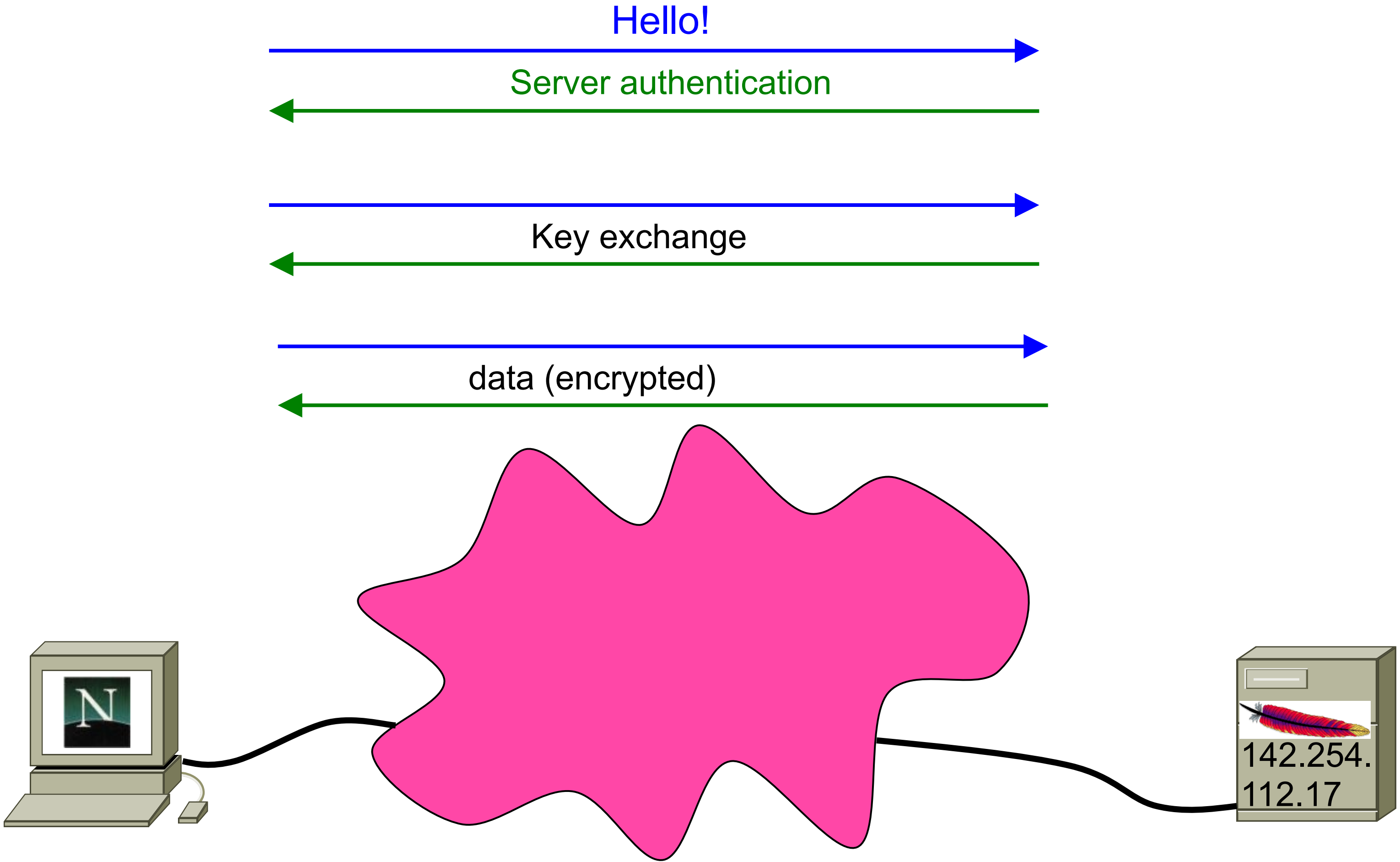
1. Compromise of DNS
2. Eavesdropping

   → Encryption (SSL/TLS)



[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

SSL/TLS (simplified):



[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Question 5

- Cryptography: Shannons concept of confusion and diffusion: What is this dependancy between chiphertext and plaintext, key?

Cryptography – Important Concepts

- Shannon’s perfect secrecy
  - All plaintexts have the same probability for a given ciphertext.
- One-Time Pad – Shannon / Vernam
  - Theoretically completely unbreakable, but highly impractical
- Shannon’s concepts: Confusion and Diffusion
  - Relation between M, C, and K should be as complex as possible (M = message, C = cipher, K = key)
  - Every ciphertext character should depend on as many plaintext characters and as many characters of the encryption key as possible.
  - “Avalanche effect” (small modification, big impact)
- Trapdoor function (one-way function)
  - Fast in one direction, not in the opposite direction (without secret information)
  - Knowing the secret allows the function to work in the opposite direction (access to the trapdoor).

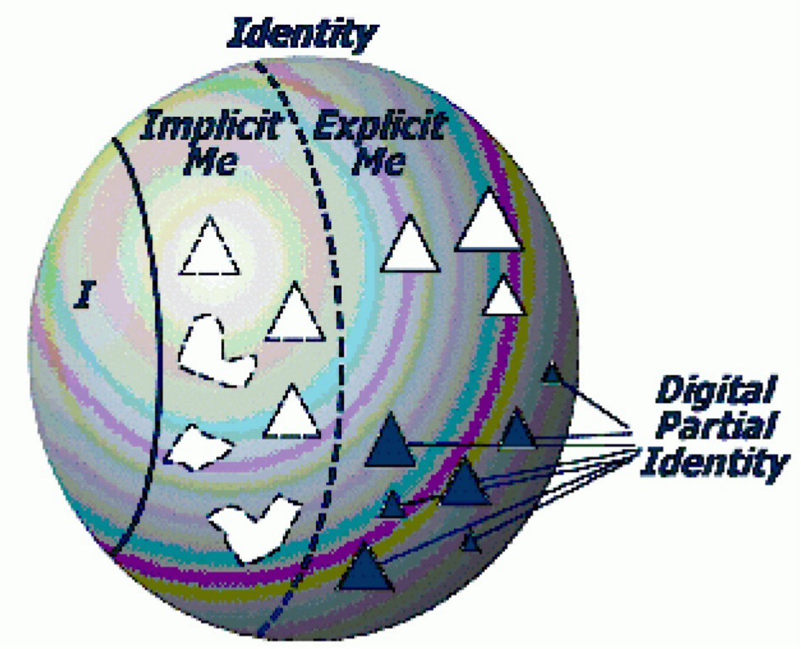
Question 6

- Identity management: Why is account management tier 2 (assigned identity) and not tier 1, when I can choose my user name?

Identity Concepts
Implicit vs. Explicit View

The procedural identity (Me) can be further differentiated

- The I
  the indeterminate first person perspective
- Implicit Me
  how a person perceives her-/himself
- Explicit Me
  how this person is perceived and represented



Identity Concepts
View of Identity (Control)

- ***Tier 1 (T1):*** True ('My') identity
- ***Tier 2 (T2):*** Assigned ('Our') identity
- ***Tier 3 (T3):*** Abstracted ('Their') identity
- The different tiers can be distinguished by the factor 'control': ***Who controls the identity?***

[Durand2003]

Identity Concepts
Tier 1: True Identity

- *A Tier 1 (true - ‘My’) identity is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit.*
- *T1 identities are both timeless & unconditional.*

[Durand2003]

Identity Concepts
Tier 2: Assigned Identity

- A Tier 2 (assigned – ‘Our’) identity refers to our digital identities that are assigned to us by corporations (e.g. our ‘customer accounts’).
  - *Our* job title (assigned to us by our employer)
  - *Our* cell phone number (assigned to us by our mobile phone operator)
  - *Our* United Mileage Plus number (assigned to us by United Airlines)
  - *Our* social security number (assigned to us by the Government)
  - *Our* credit card number (assigned to us by our credit card companies)

[Durand2003]

Identity Concepts
Tier 3: Abstracted Identity

- A Tier 3 (abstracted – 'Their') identity is an abstracted identity in that it identifies us through our demographics and other reputation like attributes, but does not need to do so in a 1:1 manner.
    - T3 identities speak to the way in which companies aggregate us into different marketing buckets for the purposes of advertising or communicating with us.
    - E.g., we're either a 'frequent buyer' or a 'one time customer' etc.
    - T3's are typically based upon our behaviour in our interactions with business.
    - The entire CRM market caters to T3 identities.

[Durand2003]

Quesiton 7

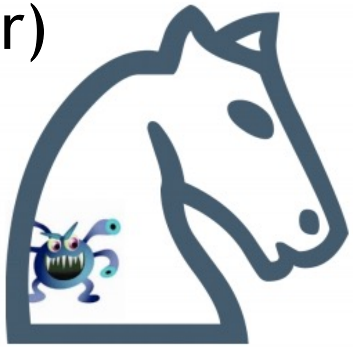
- **Q7:** - Computer System Security: different types of malware, viruses and worms: what should I take away from here, do I have to know the different types and compare them or is it enough to be able to describe the threats on a superficial level.

- **A7:** Know that they exist and be able to explain how they work.

Types of malware

- Trojan Horses
  - Programs with a covert purpose, non-spreading
- Viruses
  - Self-spreading program – it replicate relying on user activity
- Worms
  - Propagate autonomously from system to system
- Logic Bombs
  - Hidden code, triggered by external event

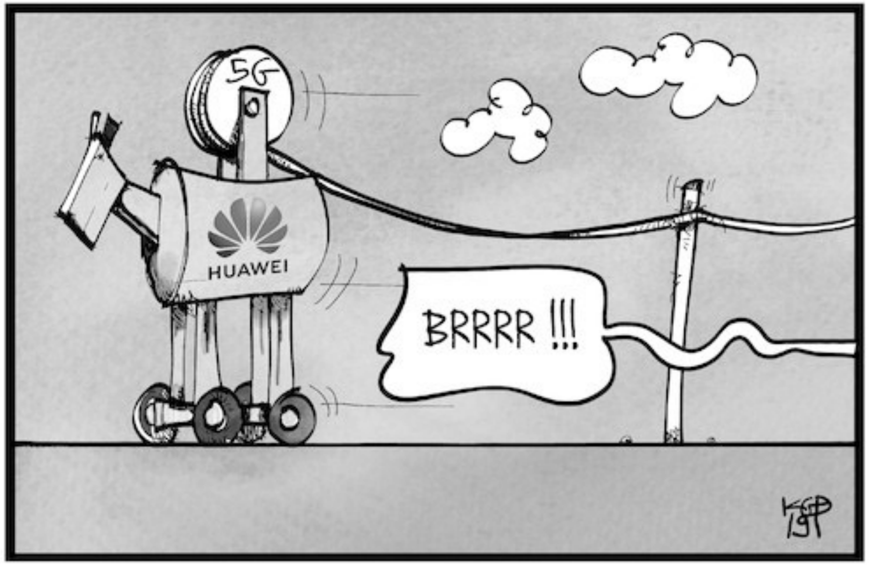
Trojan Horses (I)



- Program with an *overt* purpose (known to user) and a *covert* purpose (unknown to user)
  - Often called a Trojan
  - Named by Dan Edwards in Anderson Report *[Anderson72]*
- Example 1: NetBus
  - Designed originally as remote maintenance tool for early Windows systems
  - Victim downloads and installs it:
    - Usually disguised as a game program, or integrated within one
  - Acts as a server, accepting and executing commands for remote administrator
    - This includes intercepting keystrokes and mouse motions and sending them to attacker.
    - Also allows attacker to upload, download files

Trojan Horses (I)

- Example 2: Huawei 5G switches
  - Public discussion about possible security risks due to Huawei 5G network components
  - Huawei's 5G networks were named a "trojan horse" by US officials in 2019 who also warned the NATO about the companies technology (CNBC 2019)
  - See Lecture 12 for more information

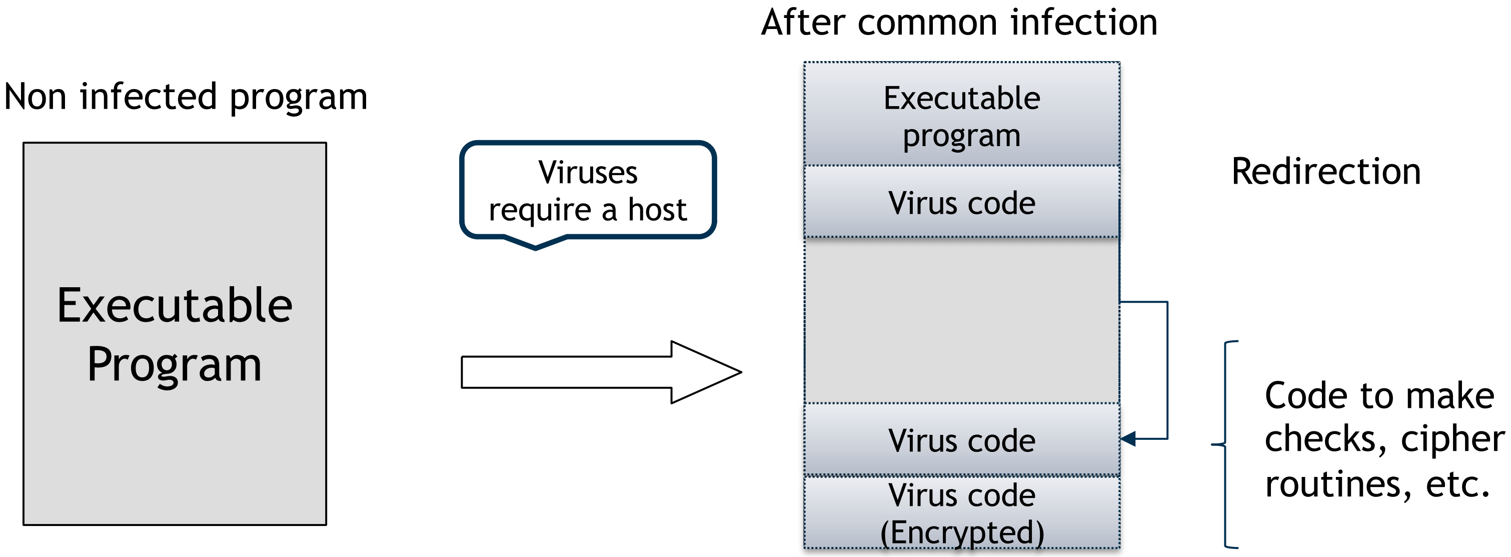


https://de.toonpool.com/cartoons/5G-Ausbau%20mit%20Huawei_328821#

Viruses

Program that replicates itself, e.g. by inserting itself into one or more files, and that may perform some other action, too:

- *Insertion phase*: Virus is inserting itself into a file.
- *Execution phase*: Virus is performing some (possibly null) action.



Types of Viruses (1)

- Boot Sector Infector
  - Inserts itself into the boot sector of a disk
- Executable Infector
  - Infects executable programs, e.g. .EXE or .COM programs
  - May prepend itself (as shown) or put itself anywhere, fixing up binary so it is executed at some point
- Multipartite Virus
  - Can infect multiple platforms (e.g. either boot sectors or executables)
- TSR Virus (Terminate and Stay Resident)
  - Stays active in memory after the application is completed
- Stealth Virus
  - Conceals its presence on a system

Types of Viruses (2)

- Encrypted Virus
  - Is enciphered except for a small deciphering routine
- Polymorphic Virus
  - Changes its form each time it inserts itself into another program
- Macro Virus
  - Composed of a sequence of instructions that are interpreted rather than executed directly
  - Can infect either executables (Duff’s shell virus) or data files (Highland’s Lotus 1-2-3 spreadsheet virus)
  - Independent of machine architecture
- Retro Virus
  - Attacks anti-virus software present on the system

Worms

- A program that copies itself from one computer to another
- Origins: distributed computations
  - Animations, broadcast messages
- Segment
  - part of program copied onto workstation
  - processes data, communicates with worm's controller
  - Any activity on workstation causes segment to shut down.

Logic Bombs

- A program that performs an action that violates the site security policy when some event occurs
- Example: program that deletes company's payroll records when one particular record is deleted
  - The "particular record" is usually that of the person writing the logic bomb.
  - If/when the person is fired and the payroll record deleted, the company loses *all* those records.

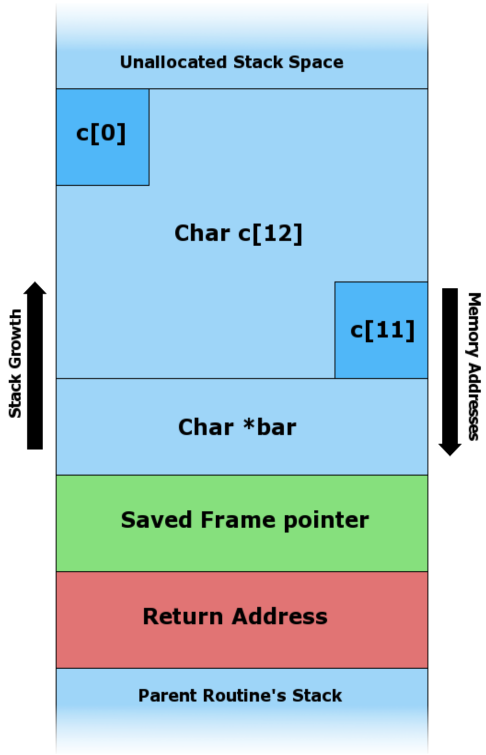
Question 8

- Computer System Security: can you explain again, how the buffer overflow works and what it does?

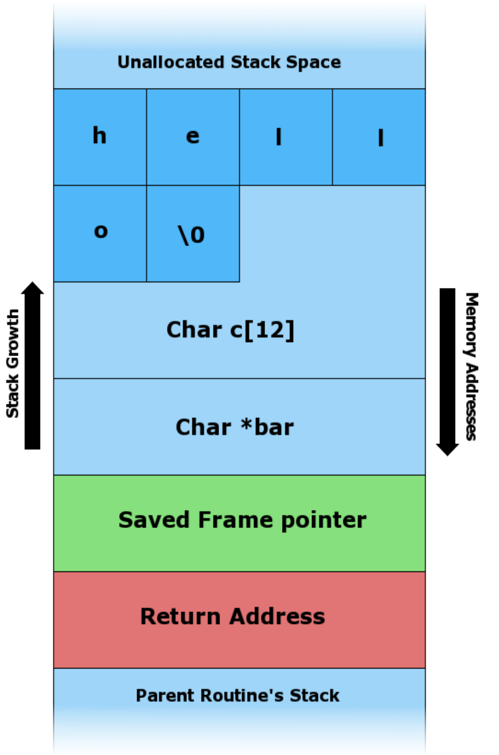
Buffer Overflow (1)

- Caused by failure to check input
  - Occurs when more data is put into a fixed-length buffer than the buffer can handle.
- Offers attackers the ability to write arbitrary data to memory.
  - The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space.
- Persisted for decades
  - Users do not bother to install patches supplied (free) by software vendors.
- Example of vulnerability that permits remote injection of hostile code, recruiting bot nets for later DDoS attacks

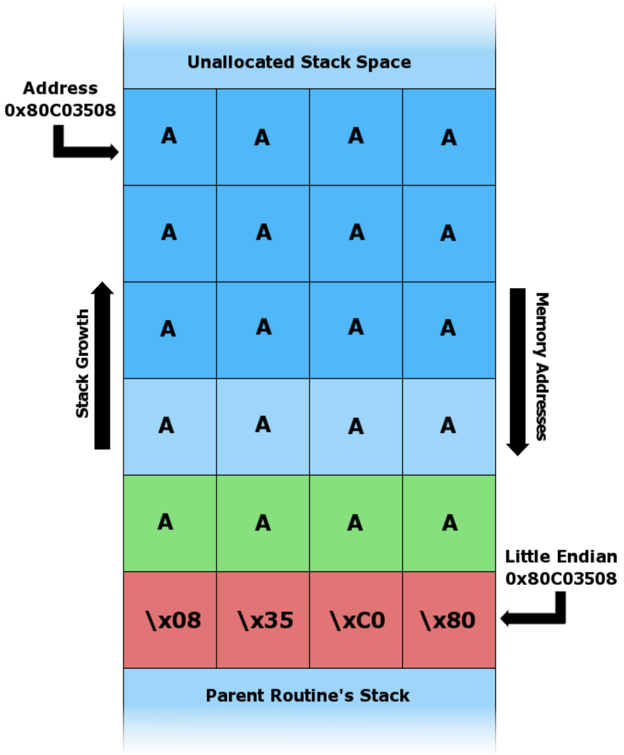
Buffer Overflow (2)



Before data is copied.



"hello" is copied.



"AAAAAAAAAAAAAAAAAAAA\x08\x35\xC0\x80" is copied.

[Wikipedia]

Buffer Overflow (Network Security I)

- A buffer is an area of memory designated to receive input (size set by the programmer).
- A buffer overflow is an attack against poor programming techniques and a lack of quality control. An attacker injects more data into a buffer than it can hold.

[Based on Ba10]

XSS (Cross-site Scripting)

- Similar to SQL injection, but attacks visitors to a website rather than grant access to the back-end database
- XSS Attack submits (attacking) script code to a benign or trusted website.
- User browser trusts web server and executes (attacking) script.
- How does script arrive on web server?
  - Persistent: Attacker modifies website, e.g. via misusing the comment function on e.g. a blog.
  - Non-persistent: Attacker makes user call the website with a special link including attacking code, e.g. via sending email with that link to the user.
- Fundamental problems
  - Websites don't check input properly.
  - Browsers trust websites too blindly.
- Work around
  - Users to check links before they click on them.

[Based on Ba10, Wikipedia]

Distributed Denial of Service (DDoS)

- Distributed denial of service (DDoS) attacks advance DoS attacks through massive distributed processing and sourcing.
- Bots (zombies): malicious code implanted on victim systems across the Internet with the Command and Control server controlling the bots
- Target systems: attacked by DDoS attacks

Question 9

- What is the finding from the privacy protection part that we should
look at, and should we just be aware of the regulation and laws or
should we also know the different types of regulation what they aim
for and development over time.

Answer 9

- Regulation needs support by standards. The GDPR is an example for that.

Question 10

- In exercise 2 on slide 36 I don’t understand why Alice can’t write to file Z even though she has direct writing access to it and doesn’t violate the don’t write down rule. In this context: does write contain automatically read?

Exercise 3

Exercise 3: Bell-LaPadula Model

Given the access rights defined in exercise 1, the subject's security levels are

L_{Alice} = Confidential and
L_{Bob} = Secret,

the object's security levels are

$L_{file\ X}$ = Unclassified,
$L_{file\ Y}$ = Secret,
$L_{file\ Z}$ = Top Secret.

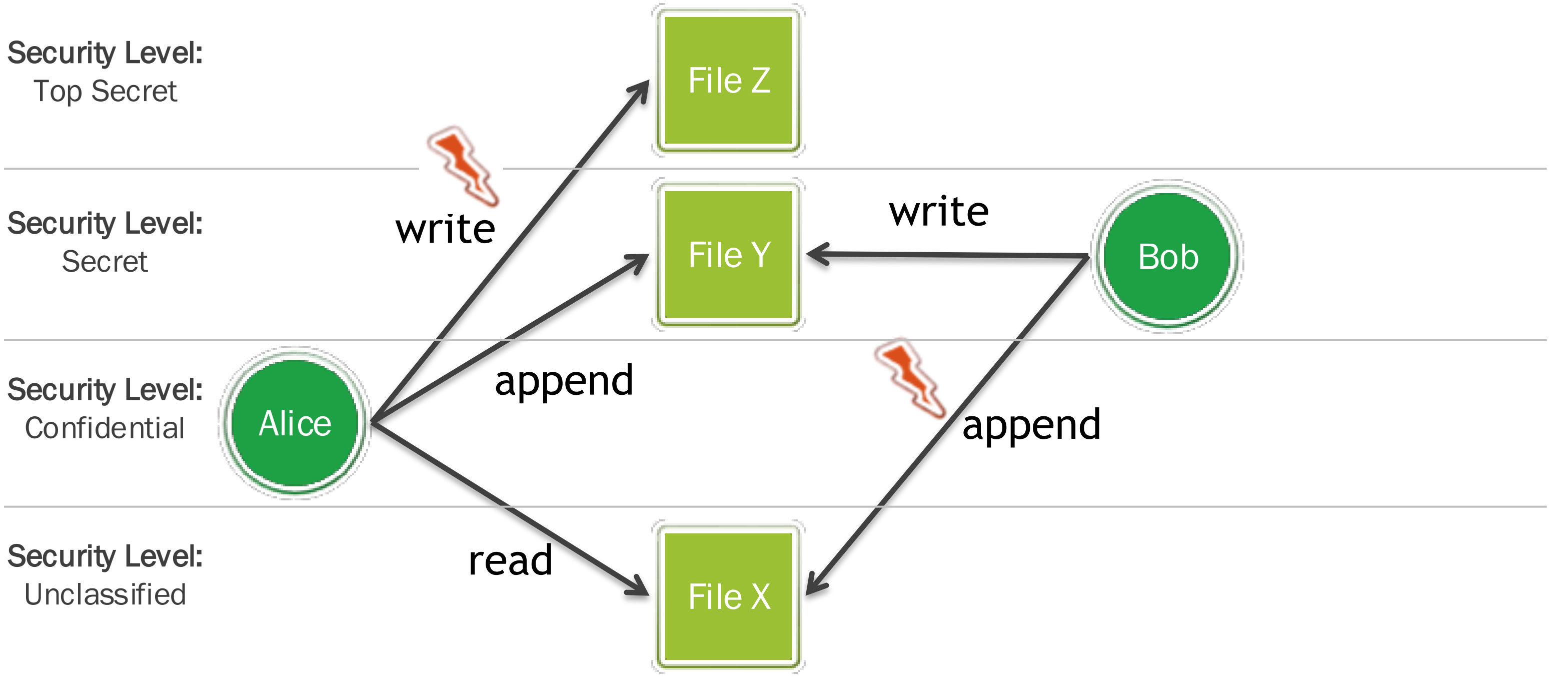
(Top Secret > Secret > Confidential > Unclassified)

Exercise 3

	file X	file Y	file Z
Alice	{read}	{append}	{write}
Bob	{append}	{write}	{ }

Subjects' Level: L_{Alice} = Confidential, L_{Bob} = Secret
Objects ' Level : $L_{file\ X}$ = Unclassified, $L_{file\ Y}$ = Secret, $L_{file\ Z}$ = Top Secret

3 a) Draw a Bell-LaPadula model which visualizes the access rights defined in access control matrix M.



Question 11

- **Q11:** - Guest lectures exam relevant or rather included?

- **A11:** All guest lectures are exam relevant, especially the guest exercise/assignment.

Question 12

- **Q12:** - Do you know the proportion of theoretical questions and exercises in the exam?
- **A12:** Practically any exam question could happen in an exam. Be aware that exercise questions are not simply repeated.

Exam Information

- 90 Points
- Non programmable calculator allowed