Prof. Dr. Ralph Holz
Networks and Network Security Group
Computer Science Departement
University of Münster

Network and System Security
Assignment 1

Task 1 Security Goals

In this task, we will explore security goals.
Please research a so-called "cyber incident" – an incident in which attackers were able to successfully penetrate a system or network and profit from it. It may also be an incident of some notoriety – for example, names such as DigiNotar, Adobe (multiple times), Comodo (multiple times), Microsoft (multiple times), and many others can be mentioned. The names are, by the way, chosen at random, with no ill intent (especially Microsoft has exemplary security!). It should be easy to find something about a large company.
Find out what the attackers had to do to break into the system. Then identify 2-3 security goals that were broken.
Note: If you have trouble coming up with the required number of security goals, you may also describe several different attacks.
Submit a description of the attack and the broken security goals, including a justification ("Goal X was broken, because..."). You may be brief, but it must remain understandable.

Task 2 Framework

Now let us take a look at our framework consisting of policy, mechanism, incentive, and assurance. For each security goal from Task 1, please describe in one sentence:

- What policy may have been the basis?
- What mechanisms were there for defense? Alternatively: what mechanisms should there have been?
- What incentives did the attackers have?
- What assurance could one expect from a mechanism of your choice?

Note: You do not need to know or specify the exact technology of a mechanism; it is sufficient to describe what the mechanism must or should have been able to do.

Task 3 Privacy and the GDPR

In 2018, the General Data Protection Regulation (GDPR) of the EU came into effect. Around the same time, many websites began displaying "cookie warnings" – pop-ups that inform users that the website is setting a cookie. Figure 1 shows a pop-up displayed by `theguardian.com`.

- Argue, considering your knowledge of human decision-making, whether this is an effective way to obtain users' consent. Be brief.
- Discuss: Can this be exploited by attackers? 1–2 sentences are sufficient.

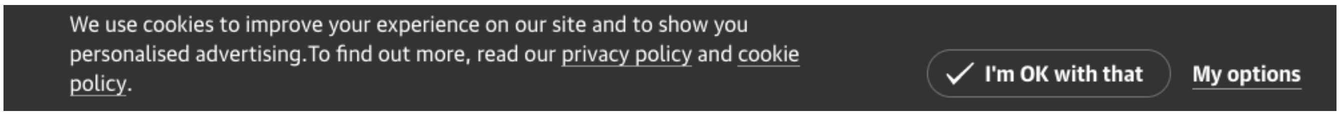
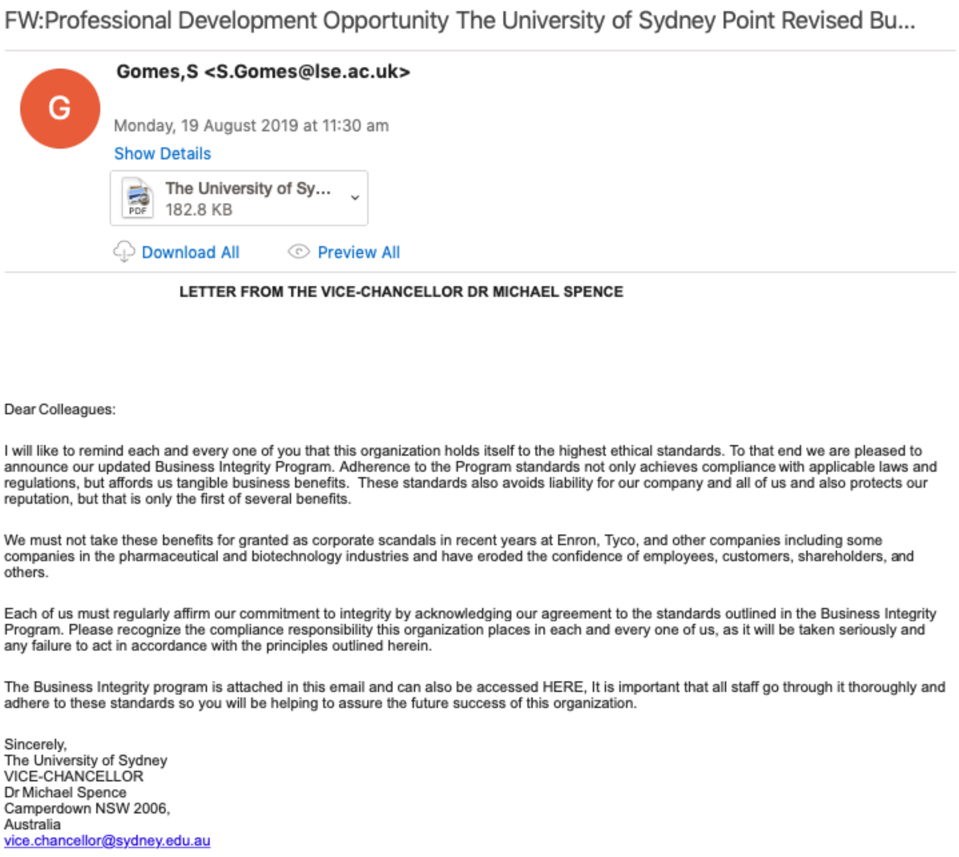

We use cookies to improve your experience on our site and to show you personalised advertising.To find out more, read our privacy policy and cookie policy.

Figure 1: Cookie warning on *theguardian.com*.


FW:Professional Development Opportunity The University of Sydney Point Revised Bu...

Gomes,S <S.Gomes@lse.ac.uk>

Monday, 19 August 2019 at 11:30 am

LETTER FROM THE VICE-CHANCELLOR DR MICHAEL SPENCE

Dear Colleagues:

I will like to remind each and every one of you that this organization holds itself to the highest ethical standards. To that end we are pleased to announce our updated Business Integrity Program. Adherence to the Program standards not only achieves compliance with applicable laws and regulations, but affords us tangible business benefits. These standards also avoids liability for our company and all of us and also protects our reputation, but that is only the first of several benefits.

We must not take these benefits for granted as corporate scandals in recent years at Enron, Tyco, and other companies including some companies in the pharmaceutical and biotechnology industries and have eroded the confidence of employees, customers, shareholders, and others.

Each of us must regularly affirm our commitment to integrity by acknowledging our agreement to the standards outlined in the Business Integrity Program. Please recognize the compliance responsibility this organization places in each and every one of us, as it will be taken seriously and any failure to act in accordance with the principles outlined herein.

The Business Integrity program is attached in this email and can also be accessed HERE, It is important that all staff go through it thoroughly and adhere to these standards so you will be helping to assure the future success of this organization.

Sincerely,
The University of Sydney
VICE-CHANCELLOR
Dr Michael Spence
Camperdown NSW 2006,
Australia
vice.chancellor@sydney.edu.au

Figure 2: Potential phishing email.

Task 4 Phish or Not?

Figure 2 shows a potential phishing email that landed in the inboxes of University of Sydney staff on 20.08.2019. It is a screenshot from the Outlook email program. Staff members were significantly confused as to whether the email was genuine or not.

- Name two weaknesses of the human psyche that the design of this email could target, and give one example from the email for each.
- The way the email is displayed by the email client tries to counteract certain weaknesses of the human mind. Name one way the email client tries to do this. Also name the weakness.

Task 5 Evaluation of a Bell-LaPadula-based Security Policy

Here we evaluate a security policy that attempts to implement a form of the Bell-LaPadula model.

Principals The principals are Arthur, Bertie, and Dylan. `beetle` is a game, `mspaint` is a generative AI for drawing, and `time` is used to run any other program and measure the CPU time required.

Rules There are definitions based on clearance levels, to be interpreted according to the rules of Bell-LaPadula. Each resource can be labeled with PROTECTED, SECRET, and TOP SECRET (in ascending order of clearance). Table 1 shows the clearance levels and the human principals holding a particular clearance. Table 2 shows which program or object requires which clearance level and who owns it. Table 3 shows an access matrix for objects, where each column defines an access control list (ACL). R stands for read, X for execute, A for append, W for write. This matrix can be changed by the owners of the respective objects.

Clearances	Accessible Resources	People
Baseline Vetting	$\leq$ PROTECTED	Arthur
Negative Vetting 1	$\leq$ SECRET	Bertie
Negative Vetting 2	$\leq$ TOP SECRET	Dylan

Table 1: Clearance levels and human principals.

Object	Required Clearance Level	Owner
`/tmp`	PROTECTED	Arthur
`transfers.csv`	SECRET	Bertie
`beetle.exe`	SECRET	Bertie
`time.exe`	SECRET	Bertie
`mspaint.exe`	TOP SECRET	Dylan

Table 2: Assignment of programs to clearance levels.

	`/tmp`	`transfers.csv`	`beetle.exe`	`time.exe`	`mspaint.exe`
Arthur	RW	RW	RX	RX	RX
Bertie	R	A	RX	RX	
Dylan	A	RW	R	RX	RWX

Table 3: Access control matrix.

a) To begin

- Which part of Bell-LaPadula (form of access control) is implemented by Table 3? Explain.
- And which part, then, is implemented by Tables 1 and 2? Explain.

b) Internal Consistency

- Which definitions in the ACL conflict with the definitions concerning the clearance levels? State the reason.

- If there are conflicts, which rules take precedence according to Bell-LaPadula?

c) Bad Actors

- Dylan is addicted to **beetle.exe**. Access has therefore been revoked. Can he reacquire it? *Hint: there are at least two ways.*
- Arthur wants to cheat on his travel expenses and claim a higher amount than he is entitled to. The travel expenses are stored in `transfers.csv` in an easily guessable format. Will he succeed?

d) Side Channels

Do you see a way to possibly extract secret information about what the secret generative AI has drawn? Explain.

e) Integrity

How would you design the rule for `transfers.csv` in the Biba model to ensure that Arthur cannot modify the travel expenses?

Task 6 Access Control and Operating Systems

A few questions about access control in operating systems:

a) General

- Can operating systems provide access control without relying on hardware? Why?
- How do operating systems prevent one application from overwriting the memory of another application?

b) Linux

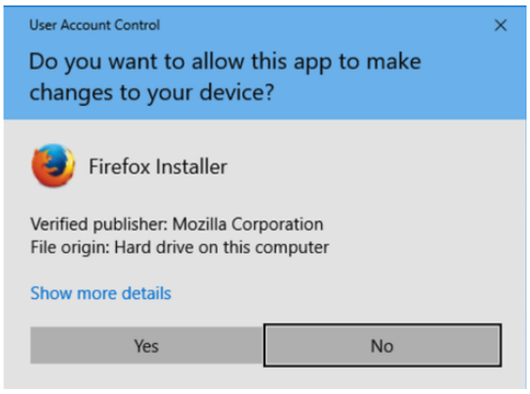
Consider the Linux operating system and how it handles file permissions.

- The `mount` command allows the Linux operating system to access additional block devices, e.g., USBs, additional hard drives, CD-ROMs, or even ISO images. What are the permissions for this command on a Linux system of your choice?
- Find a simple command to search the entire filesystem and return a list of all files that the current user has write access to.

c) Windows

Figure 3 shows a dialog box from Windows 10. This implements a variant of a security model.

- Which model is implemented here?
- Which rules of the model must have been violated for this dialog to appear?


User Account Control

Do you want to allow this app to make changes to your device?

Firefox Installer

Verified publisher: Mozilla Corporation
File origin: Hard drive on this computer

Figure 3: Dialogue from Windows 10.

Task 7 Software Dependencies

In the lecture, we discussed software dependencies. Use `https://deps.dev` and see if you can find a spectacular case where a program has many dependencies, or alternatively a program on which many dependencies rely. Also check if you can find the corresponding repository and whether, for example, the code is old, frequently updated, etc. You don't need to exhaust yourself here - the goal is to find an interesting case and then describe the problem in one paragraph.
In the tutorial, we will then vote on which case was the most spectacular. Please do not choose a case that was already presented in the lecture.

Task 8 This Time for Real

In the tutorial, you decrypted `enc.txt` (if not, please catch up now!). Now let's tackle the task properly.

- Write code to read the decrypted text file and encrypt it using AES-CBC. You may use any programming language.
- If you use Python:
  - The `pycrypto` library is a good choice: `https://pycryptodome.readthedocs.io/en/latest`.
  - You can get an IV with `Crypto.Random`.
- You will probably need to use padding. Why?
- We recommend a key length of 128 bits (unless you are being chased by the NSA, then you can use more).
- The console output should be a hex-encoded string.
- Also write the output as binary to `text.aes`.

Submit 1. the code you have written as well as a detailed explanation (as code comments) of how you implemented AES-CBC. 2. Text explanation of the importance of padding.

Task 9 The Problems of CTR Mode

In this task, we will take a closer look at CTR mode.

a) The Issue with the IV

Suppose someone wants to encrypt the messages m_1 and m_2 with CTR mode. For simplicity, let us only consider the first blocks $m_{1,1}$ and $m_{2,1}$ of each message.

- Show: $c_{1,1} \odot c_{2,1} = m_{1,1} \odot m_{2,1}$, where $\odot$ is the XOR operation.
- How could the above relation be exploited in practice? *Hint: think of protocols!*

b) Poor Man's CTR

Once again, one of your good friends comes by and presents you with their very own implementation of AES-CTR. You sigh, take a look at the code, immediately spot the problem, and quickly write some code to break the ciphertext encrypted with it.

Here are your tasks, along with some tips:

- We give you the source code. What principle does this follow?
- The previous subtask gives you the idea and important hints why the operation mode developed by your friend is not secure. Which is it?
- The easiest way is to outline and carry out the attack with pen and paper. How will it work?
- Now write source code to decrypt *encrypted.enc*. The file *main.py* contains the scaffold you need.
- From which book is the plain text taken? This question is optional, but we value education here.

Note: if you look carefully, you will find that the vulnerability you are exploiting here allows you to decrypt all the encrypted files if the number of lines is a multiple of 10. Otherwise you will only get half. Why?

Task 10 Euler's Totient Function

Leonhard Euler gave us the following formula to determine the number of integers that are co-prime to another integer:

$\phi(n) = n \prod_{i|n} (1 - \frac{1}{i})$, where $i|n$ indicates the number of (distinct) prime divisors of n.

Show: $\phi(n) = (p-1) \cdot (q-1)$ when p, q are prime. Hint: Even without this formula, the result is intuitive. Why?