RUNNING A SYSSEC COURSE FOR FUN, NOT PROFIT

DIEGO F. ARANHA + STUDENTS @ AU CS/ENG

AARHUS
UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

DIEGO F. ARANHA
ASSOCIATE PROFESSOR

ABOUT ME

Previously, I was Assistant Professor for 7 years in Brazil.

Currently, Associate Professor at AU for (8 + ε) years.

My research interests are:

- **Cryptographic Engineering**
- Computer Security
- Privacy and social impacts of technology

Currently: member of Cryptography & Security research group.

ABOUT ME

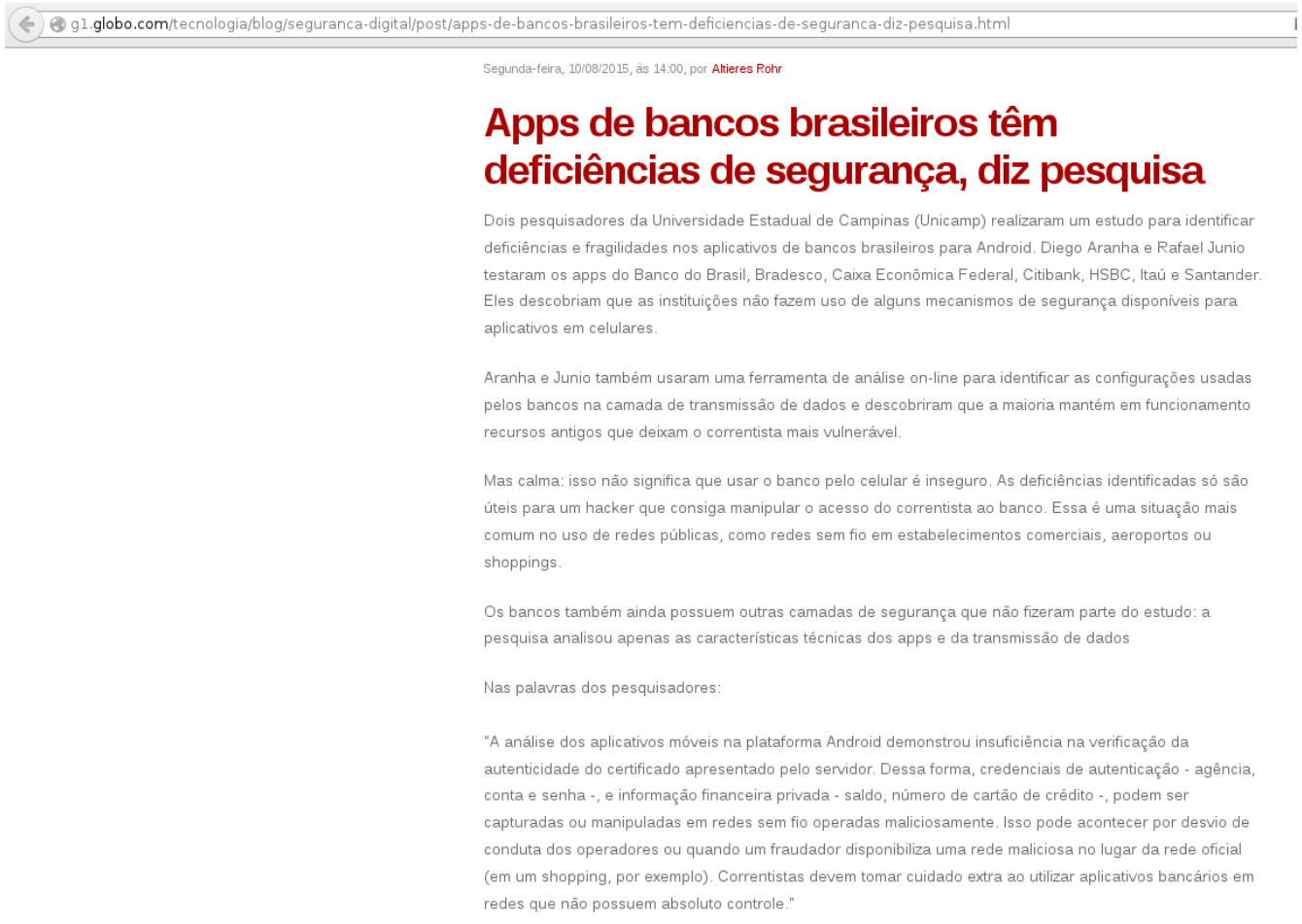
As part of my research, I have looked into:



e-Voting systems

Secure messaging apps

HOW IT STARTED



g1.globo.com/tecnologia/blog/seguranca-digital/post/apps-de-bancos-brasileiros-tem-deficiencias-de-seguranca-diz-pesquisa.html

Segunda-feira, 10/08/2015, às 14:00, por Altieres Rohr

Apps de bancos brasileiros têm deficiências de segurança, diz pesquisa

Dois pesquisadores da Universidade Estadual de Campinas (Unicamp) realizaram um estudo para identificar deficiências e fragilidades nos aplicativos de bancos brasileiros para Android. Diego Aranha e Rafael Junio testaram os apps do Banco do Brasil, Bradesco, Caixa Econômica Federal, Citibank, HSBC, Itaú e Santander. Eles descobriam que as instituições não fazem uso de alguns mecanismos de segurança disponíveis para aplicativos em celulares.

Aranha e Junio também usaram uma ferramenta de análise on-line para identificar as configurações usadas pelos bancos na camada de transmissão de dados e descobriram que a maioria mantém em funcionamento recursos antigos que deixam o correntista mais vulnerável.

Mas calma: isso não significa que usar o banco pelo celular é inseguro. As deficiências identificadas só são úteis para um hacker que consiga manipular o acesso do correntista ao banco. Essa é uma situação mais comum no uso de redes públicas, como redes sem fio em estabelecimentos comerciais, aeroportos ou shoppings.

Os bancos também ainda possuem outras camadas de segurança que não fizeram parte do estudo: a pesquisa analisou apenas as características técnicas dos apps e da transmissão de dados

Nas palavras dos pesquisadores:

"A análise dos aplicativos móveis na plataforma Android demonstrou insuficiência na verificação da autenticidade do certificado apresentado pelo servidor. Dessa forma, credenciais de autenticação - agência, conta e senha -, e informação financeira privada - saldo, número de cartão de crédito -, podem ser capturadas ou manipuladas em redes sem fio operadas maliciosamente. Isso pode acontecer por desvio de conduta dos operadores ou quando um fraudador disponibiliza uma rede maliciosa no lugar da rede oficial (em um shopping, por exemplo). Correntistas devem tomar cuidado extra ao utilizar aplicativos bancários em redes que não possuem absoluto controle."

HOW IT IS GOING

Students detect security breaches in popular apps

Millions of people use apps every day to communicate with friends, track their daily run, transfer money or check their covid-19 test result. As a result, security has become more critical than ever before, because many of these apps use and track personal data. But are they really secure? This was the focus in the final project for a class of Master's students attending the Network Security course taught by Associate Professor Diego F. Aranha. The students analysed an app of their own choice for potential threats and vulnerabilities. The 28 groups analysed 21 different apps, of which nine were found vulnerable enough for a follow-up vulnerability disclosure process. So far, students have been successfull in contacting half the companies to disclose their findings.

In 2015, Diego Aranha supervised a Bachelor's project in Brazil, in which the student was investigating security breaches in eight banking apps. The student found security vulnerabilities in seven of them. All the banks were contacted regarding the issues, but many were not interested in the findings or the suggested solutions. This made headlines in the Brazilian press. The episode is behind the idea for the Master's course **Network Security**, which Associate Professor Diego Aranha now teaches at Aarhus University.

"As a cryptographer, I know, that there are security breaches everywhere, but it was still alarming to see the number and seriousness of the errors in these banking apps," says Diego, and continues: "This gave me the idea for a course project, in which the students analyse apps from their everyday life to investigate how widespread the problem with security actually is. Moreover, they have to come up with solutions to the issues identified. Many people believe that 'hacking' is something negative, but in this course we are the good guys, and we hack apps to secure the users' personal data even better."

WHAT ABOUT THE DATA?

MSc. Students asked to perform a *preliminary* security analysis for apps collecting *sensitive* data in the following fields:

- **Financial**: banking and payments
- **Healthcare**: medical data and COVID contact tracing
- **Transport/travel**: train/bus tickets, booking hotels
- **Social Networks**: preferably a local one
- **e-Government**: there are plenty in Denmark!

I help to **review** results (*grading*), **disclose** to institutions, **uphold** ethical standards.

WHAT ABOUT THE DATA?

The *scope* of the analysis is:

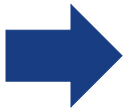
- **Software security**: decompilation/reverse eng, keywords
- **Network security**: client-side and server-side quality of TLS
- **Authentication**: factors and their assurance
- **Privacy**: nature of collected data, integration, policy

➡ We use *widely* accessible free/open-source tools.

THE PROTOCOL

The timeline is roughly the following:

- **April:** rules of engagement, spec, students commit to app
- **Late April:** instructor contacts parties
- **May:** actual work, urgent disclosures
- **Early June:** hand-in of reports
- **Late June:** exams, cross-validation, assessment
- **July-August:** coordinated disclosures



Probably the *fastest* security assessment in a course *worldwide*.

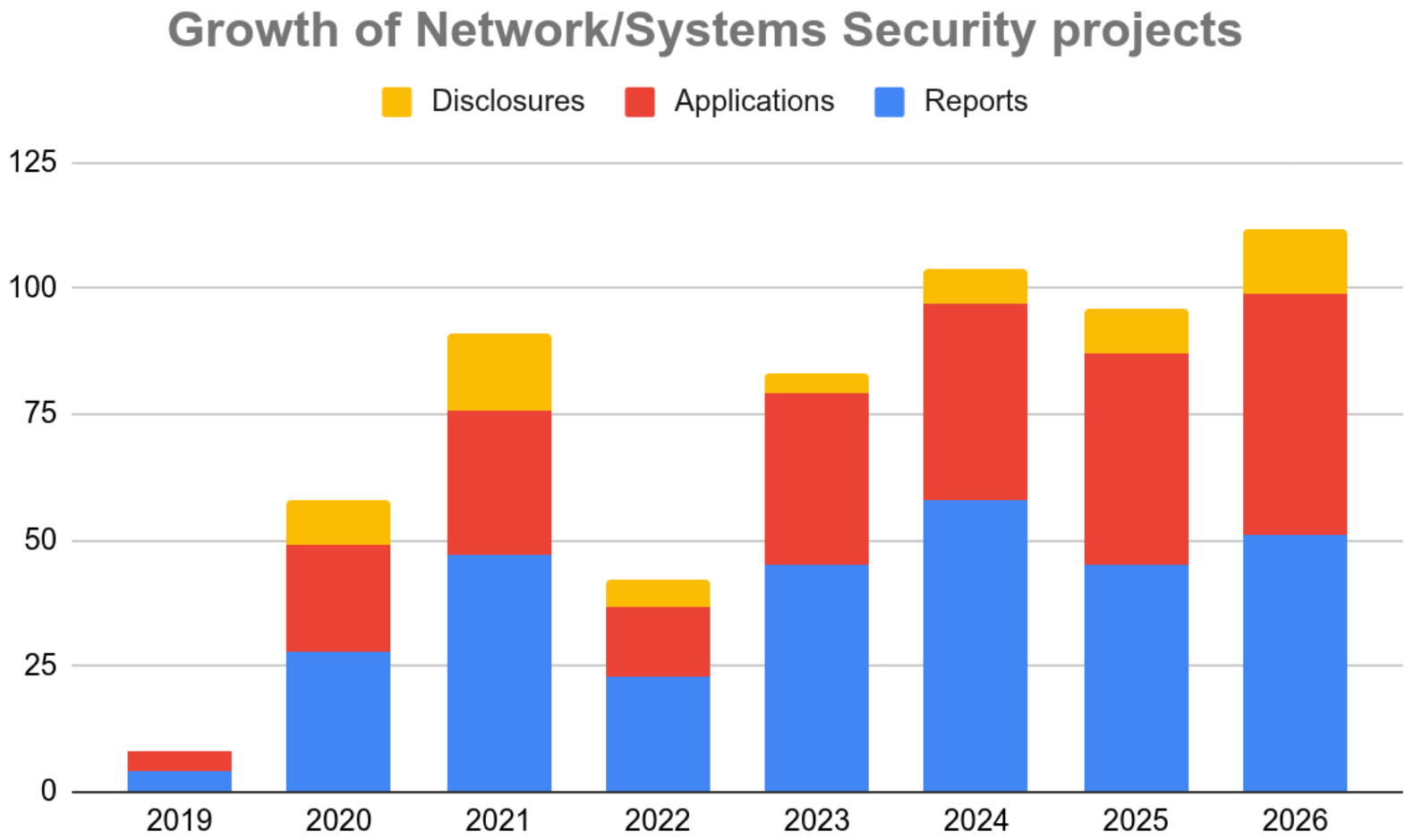
THE DATA

Running the course for 8 years shows some trends:

1. The **GOOD**: SSL/TLS deployments
2. The **BAD**: privacy policy + cryptography issues
3. The **UGLY**: session management + API design + authentication

DATA: ~180 different applications analyzed so far.

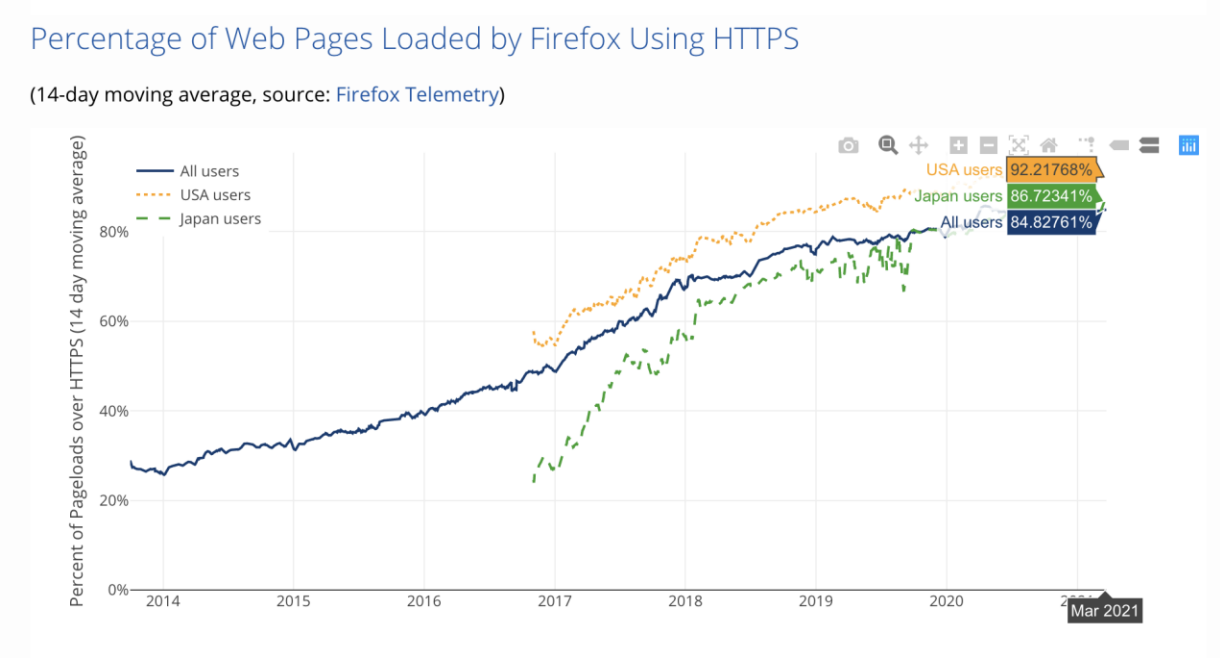
THE DATA


Growth of Network/Systems Security projects
Disclosures
Applications
Reports
125
100
75
50
25
0
2019
2020
2021
2022
2023
2024
2025
2026

THE GOOD

High-quality SSL/TLS connections:

1. Plaintext **nowhere** to be seen
2. TLS versions are **reasonably** up to date
3. MITM progressively **harder** (*certificate pinning*)



Partial credit to Android devs!

Please, do not override defaults to allow plaintext/user certs.

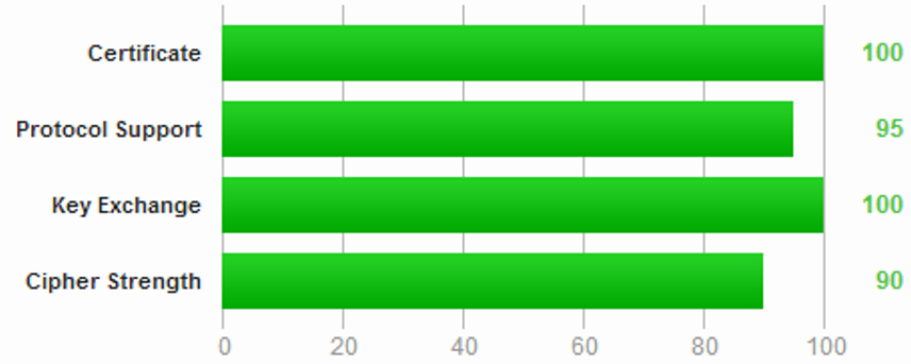
THE GOOD

Qualys. SSL Labs

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server is not vulnerable to the Heartbleed attack. (Experimental)

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

THE BAD

Some *recurrent* low-severity issues:

- **Homebrew** cryptography (CBC, no AEAD, weak algorithms, weird combos)
- **Logging** enabled in release builds
- Overly **permissive** shared activities
- *Incomplete* or **total lack** of privacy policy
- Permission **inflation** (*mitigated* in modern Android)
- Hardcoded API keys *absolutely* **everywhere**...

THE UGLY

The *nightmare*-inducing stuff:

- **Classical** password issues (short/predictable, brute-forceable)
- No client-side **hashing** of credentials (debatable)
- No **multi-factor** authentication (SMS *not* enough)
- **Improper** auth workflows (unverified e-mails, reset/delete)
- **Insecure** API allows UI manipulation, cross-user data access
- Session **management** (no expiration, TLS downgrade)
- Session keys without limits (**full** backend write in *one* case)

THE ABSOLUTE HORROR

The stuff which will *eat your children* at night:

- **Trusting the client device** for security
- **Publicly** available buckets
- **Leakage** of private data through APIs
- **Privilege escalation** flaws

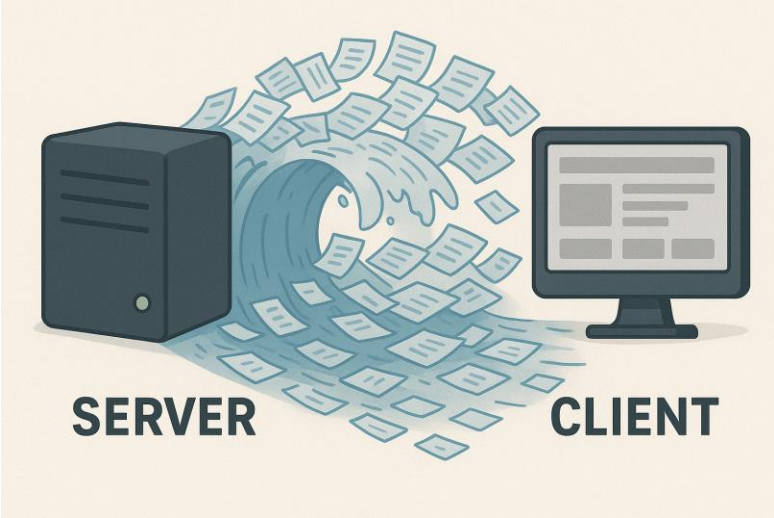
HORROR STORY 1 – LEAKING BUCKET


```
  "name": "allFirestoreDataBackup/all_namespaces/kind_companyUsers/output-5",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_configuration/all_namespaces_kind_configuration.export_metadata",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_configuration/output-6",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_configuration/output-7",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/all_namespaces_kind_employees.export_metadata",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-10",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-11",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-12",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-13",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-14",
  "bucket": "[redacted]"
},
{
  "name": "allFirestoreDataBackup/all_namespaces/kind_employees/output-8",
  "bucket": "[redacted]"
},
```




HORROR STORY 2 – DATA TSUNAMI

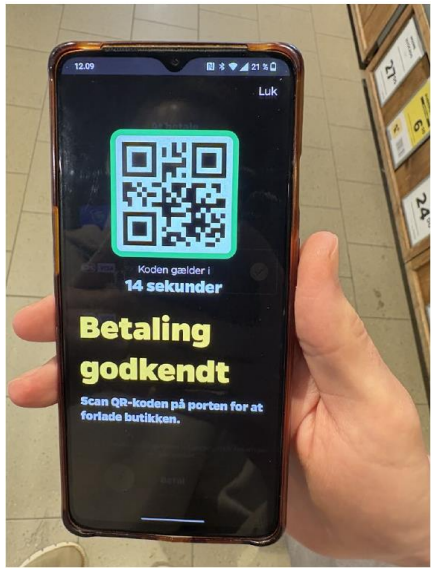
```
gRPC                                                    [m:auto]
2:
  1: 2e6b37e4-21e4-41ff-9d3e-60c3b4f46bf5
  2: momem74659@bamsrad.com
  3: Victor
  4: Jensen
  5: Victor Jensen
  9:
    1: Not a real City
    2: Danmark
    3: DK
    6: '1234'
    7: st1
  14:
    1: 1747305616  # !sint: 873652808
    2: 104970754  # !sint: 52485377
  15:
    1: 1747305718  # !sint: 873652859
    2: 562981813  # !sint: -281490907
  31: 7  # !sint: -4
  33: 2001  # !sint: -1001
  34: 2052  # !sint: 1026
```



HORROR STORY 3 – CLIENT-SIDE AUTH

```
{
    "status": "unpaid"
}
```

```
{
    "basketIsSelected": false
}
```




```
1 {
2     "pointBank": "Valgfri_kagemand",
3     "availablePoints": 5000
4 }
```



HORROR STORY 4 – IP CAM GEOGUESSR



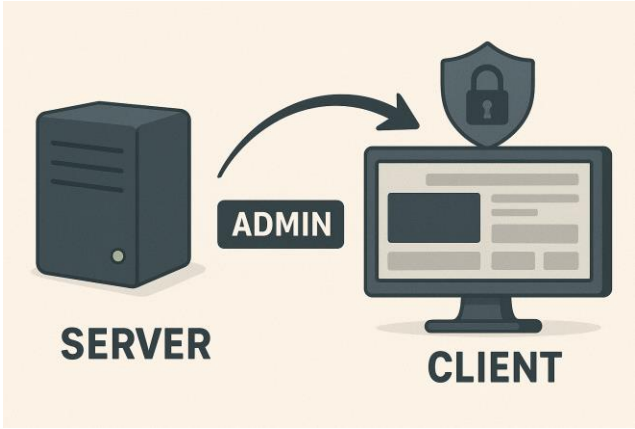
HORROR STORY 5 – PRIV ESCAL



HORROR STORY 5 – OPRAH ADMIN

```
179109      globalAdminPermissionGroup: {
179110        name: "Global Admin Permission Group",
179111        codeName: "globalAdminPermissionGroup",
179112        pagePermissions: ["*"],
179113        endpointPermissions: ["*"],
179114      },
```

```
{
  "admin": false,
  "color": "gold",
  "number": 123,
  "object": {
    "a": "b",
    "c": "d"
  }
}
```



JK, THIS IS THE ACTUAL HORROR

263(a) **A fine or imprisonment of up to 1 year and 6 months** shall be imposed on *anyone* who, *without authorization*,

1) commercially sells or widely distributes a means of access to a computer system or data,

2) attempts a large number of accesses to a computer system or data

3) acquires access to a computer system or data.

If the acts mentioned in subsection 1 are committed under particularly aggravating circumstances, the penalty may increase to imprisonment of up to 6 years. Particularly aggravating circumstances are considered to be cases where the disclosure, etc. occurs on a particularly large scale or involves a particular risk of significant damage or extensive misuse, or where both subsection 1, no. 1 and no. 3, letter c, have been violated.

LEGAL ASPECTS

The law imposes multiple obstacles:

- The writing is quite **evasive**, technical terms **undefined**
- It does not require evidence of **malicious** intent
- **Repercussions** for minor criminal offenses are broad in DK
- Case law shows several convictions, with sentences suspended or deferred

➡ Minister of Defense stays that anonymous disclosure to CSIRT is possible, so no changes to the law are needed. :)

CASE LAW

- **Attempted hacking is punishable:** Convictions are possible even without successfully accessing a system.
- **No damage or data theft required:** Unauthorized access itself can constitute a criminal offense.
- **Penalties vary significantly:** From conditional convictions without a fixed punishment to several years in prison (CSC case).
- **Authorization matters:** Technical ability to access a system does not necessarily imply legal permission.
- **Ethical hacking remains legally uncertain:** Case law provides little clarity on good-faith vulnerability research and disclosure.

COORDINATED DISCLOSURE

Usually, it is the most tense part of the process, performed after the exams to have no impact on grading (unless urgent).

We follow the general process below:

- Find security-relevant contact at the affected party (hardest)
- Send summary of the findings and ask for secure channel
- Disclosure of reports (with **feedback** incorporated)
- No need to agree on **timeline** for fixes (no public disclosure)
- Now we also help with vulnerabilities **not found** in the course

COORDINATED DISCLOSURE

Usually, it is the most tense part of the process, performed after the exams to have no impact on grading (unless urgent).

Some interesting notes about the process:

- Around 25% of parties will request a live meeting/call
- Contact national Data Protection Authority in case of data breach, tip about **incoming** disclosure
- As per the GDPR, parties have 72h to respond and mitigate

➡ **Loophole:** companies decide if there is risk to users :)

RECENT CHANGES

Some improvements this year:

- Partnership with Security Tech Space as middle-entity
- Partnership with Defend Denmark, a bug bounty platform
- Partnership with other universities on aligning the processes
- Tighter workflow to enforce ethical boundaries
- Hall of Fame to advertise the work

The better well-known the effort, the higher the resilience is.

RECENT CHANGES

Systems Security Hall of Fame

· Feb 12, 2026

The final project in my Systems Security course requires students to perform a non-invasive security analysis of a real-world system, usually an Android mobile application.

This Hall of Fame recognizes the projects that produced security analysis and successful vulnerability disclosures that led to meaningful improvements in real-world systems.

Successful Disclosures, 2026 edition

Students	Application / System	Findings
Mouhieddine Sabir Riccardo Bonavigo Diego Barbieri	Unnamed camera app	- Unauthorized access to video feeds - SQL injection in backend infra (under authorization)
Nikolaj Jehøj-Krogager Emil Viftrup Jepsen Jonas Iversen	Unnamed library app	- Broken DRM protection - API access allows enumeration of private user data - No 2FA, weak password policy
Adam Holmgård Nielsen Julian Brask Christensenc Gustav Helbo Kabel	Unnamed library app	- API access allows enumeration of private user data - No 2FA, weak password policy
Mads Overgaard Munk Kristopher B. E. Märcher Rasmus Christensen	Unnamed shopping app	- JavaScript injection - Insecure callback allows arbitrary redirect - Lack of certificate pinning - Leakage of financial data in some circumstances
Mads Pagh Marcus Mofjeld Marie Alkemade	Unnamed shopping app	- Publicly available cloud storage of user-provided data - Unlocked developer mode with access to privileged functionality - Bypass of basket check process - Bypass of transaction payment
Emil Klein Hansena Nicolai Binderup Hansen Louise Pedersen Møller	Unnamed shopping app	- Publicly available cloud storage of user-provided data - Bypass of basket check process - Bypass of transaction payment - Lack of e-mail verification during signup - No 2FA, weak password policy

TODOS

- The beginning is a bit bureaucratic, shorten it
- Focus less on coordinated disclosure
- Add something about incentives, law protects companies
- Something about no GDPR fines and compliance with NIS2 regulations

SECURE YOUR APPS

If you already received our contact, hi!

If not, we are just trying to help :)

dfaranha@cs.au.dk



AARHUS
UNIVERSITY