PA193 - Secure coding principles and practices

Security Code Review

Seminar

Łukasz Chmielewski *chmielewski@fi.muni.cz*
Centre for Research on Cryptography and Security, Masaryk University

CROCS
Centre for Research on Cryptography and Security

Outline

- Many simple exercises
  - looking at common mistakes in pairs.
- Topics:
  - Protecting Data, Preventing Cross-Site Scripting, Code Quality,
  - Memory Best Practices, Parameterized Statements,
  - Indirect Object References, and Input Validation…
- Explanation for the Assignment.
- That is all ☺

SIMPLE EXERCISES

Simple Exercises

- Form pairs (e.g., with your neighbour)
- Look and code together (before ready to answer the question)
- Two roles:
  - Educator – explains the answer to the given question to his/her pair
  - Sceptic – tries to find any flaw or weak point in Educator's reasoning
- Together try to find an answer on what is wrong in the code.
  - What can be a root of the issue?
  - Propose a correction.
- Switch roles after every question (from next slide)

Exercise (1): what is wrong with this class?

```
public class Account {
double principal,rate; int daysActive,accountType;
public static final int STANDARD=0, BUDGET=1, PREMIUM=2,
PREMIUM_PLUS=3;
}
...
public static double calculateFee(Account[] accounts)
{
double totalFee = 0.0;
Account account;
for (int i=0;i<accounts.length;i++) {
 account=accounts[i];
        if(account.accountType==Account.PREMIUM|| account.accountType
== Account.PREMIUM_PLUS )
        totalFee += .0125 * ( // 1.25% broker's fee
        account.principal*Math.pow
        (account.rate,(account.daysActive/365.25))
        - account.principal); // interest-principal
}
return totalFee;
}
```

Exercise (2): what is wrong and how to improve it?

```
String updateServer = request.getParameter("updateServer");
if(updateServer.indexOf(";")==-1 && updateServer.indexOf("&")==-1){
    String [] commandArgs = {
        Util.isWindows() ? "cmd" : "/bin/sh",
        "-c", "ping", updateServer
    }
    Process p = Runtime.getRuntime().exec(commandArgs);
}
```

Exercise (2): what is wrong and how to improve it?

```
String updateServer = request.getParameter("updateServer");
if(ValidationUtils.isAlphanumericOrAllowed(updateServer,'-','_','.')){
    String [] commandArgs = {
        Util.isWindows() ? "cmd" : "/bin/sh",
        "-c", "ping", updateServer
    }
    Process p = Runtime.getRuntime().exec(commandArgs);
}
```

Exercise (3): what is wrong and how to improve it?

```
String updateServer = request.getParameter("updateServer");
String cmdProcessor = Utils.isWindows() ? "cmd" : "/bin/sh";
String command = cmdProcessor + "-c ping " + updateServer;

Process p = Runtime.getRuntime().exec(command);
```

Exercise (3): what is wrong and how to improve it?

```
String updateServer = request.getParameter("updateServer");
List<String> commandArgs = new ArrayList<String>();
commandArgs.add("ping");
commandArgs.add(updateServer);
ProcessBuilder build = new ProcessBuilder(commandArgs);
```

Exercise (4): what is wrong and how to improve it?

```
String query = String.format("SELECT * FROM users WHERE usr='%s' AND pwd='%s'", usr, pwd);
Connection conn = db.getConn();
Statement stmt = conn.createStatement();


ResultSet rs = stmt.executeQuery(query);
```

Exercise (4): what is wrong and how to improve it?

```
String query = "SELECT * FROM users WHERE usr = ? AND pwd = ?";
Connection conn = db.getConn();
PreparedStatement stmt = conn.preparedStatement(query);
stmt.setString(1, usr);
stmt.setString(2, pwd);
ResultSet rs = stmt.executeQuery(query);
```

Exercise (5): what is wrong and how to improve it?

```
printf("Enter the master password:\n");
gets(userPass);

if(strncmp(userPass,MASTER_PASSWORD,9)==0){
    printf("PASSWORD VERIFIED\n");
}
```

Exercise (5): what is wrong and how to improve it?

```
printf("Enter the master password:\n");
fgets(userPass,9,stdin);

if(strncmp(userPass,MASTER_PASSWORD,9)==0){
    printf("PASSWORD VERIFIED\n");
}
```

Exercise (6): what is wrong and how to improve it?

```
char userPass[5];

printf("Enter the master password:\n");
fgets(userPass,9,stdin);

if(strncmp(userPass,MASTER_PASSWORD,BUFFER_SIZE)==0){
    printf("PASSWORD VERIFIED\n");
}
```

Exercise (6): what is wrong and how to improve it?

```
int BUFFER_SIZE = 9;
char userPass[BUFFER_SIZE];

printf("Enter the master password:\n");
fgets(userPass,BUFFER_SIZE,stdin);

if(strncmp(userPass,MASTER_PASSWORD,BUFFER_SIZE)==0){
    printf("PASSWORD VERIFIED\n");
}
```

Exercise (7): what is wrong and how to improve it?

```
int len = 0, total = 0;
while(1){
    fgets(buff1, MAX_SIZE, stdin);
    int len =  strnlen(buff1, MAX_SIZE);
    total += len;
    if(total <= MAX_SIZE) strncat(buff2, buff1, len);
    else break;
}
```

Exercise (7): what is wrong and how to improve it?

```
int len = 0, total = 0;
while(1){
    fgets(buff1, MAX_SIZE, stdin);
    int len =  strnlen(buff1, MAX_SIZE);
    total += len;
    if(total < MAX_SIZE) strncat(buff2, buff1, len);
    else break;
}
```

Exercise (8): what is wrong and how to improve it?

```
if(strncmp(userPass,MASTER_PASSWORD,BUFFER_SIZE)==0){
    printf("PASSWORD VERIFIED\n");
}
else{
    printf("Invalid password:");
    printf(userPass);
}
```

Exercise (8): what is wrong and how to improve it?

```
if(strncmp(userPass,MASTER_PASSWORD,BUFFER_SIZE)==0){
    printf("PASSWORD VERIFIED\n");
}
else{
    printf("Invalid credentials.");
}
```

Exercise (9): what is wrong and how to improve it?

```
String usr = request.getParameter("usr");
String pwd = request.getParameter("pwd");
User user = UserColl.find(usr);

if(user.getPassword().equals(pwd)){

    //password verified
```

Exercise (9): what is wrong and how to improve it?

```
String usr = request.getParameter("usr");
String pwd = request.getParameter("pwd");
User user = UserColl.find(usr);
String givenValue = Utils.PBKDF2(pwd, user.getSalt(), user.getIterations());
if(user.getPassHash().equals(givenValue)){

    //password verified
```

Exercise (10): what is wrong and how to improve it?

```
String url = "http://my-service.cloud.biz/Login?usr="+usr+"&pwd="+pwd;
URL obj = new URL(url);
HTTPURLConnection con = (HTTPURLConnection) obj.openConnection();
con.setRequestMethod("GET");
con.setRequestProperty("User-Agent", USER_AGENT);
```

Exercise (10): what is wrong and how to improve it?

```
String url = "https://my-service.cloud.biz/Login";
URL obj = new URL(url);
HTTPURLConnection con = (HTTPURLConnection) obj.openConnection();
con.setRequestMethod("POST");
con.setRequestProperty("User-Agent", USER_AGENT);
```

Exercise (11): what is wrong and how to improve it?

```
var transaction = {"custName":custName,"address":custAddress,"creditCardNumber":custCC.CCPAN};

s3.putObject({
    "Bucket": "ACME-customer-billing",
    "Key": "todayTransactions",
    "Body": JSON.stringify(transaction),
    "Content-Type": "application/json"
},
function(err,data){
});
```

Exercise (11): what is wrong and how to improve it?

```
var transaction = {"custName":custName,"address":custAddress,"creditCardNumber":dataCleaner.removeCCPAN(custCC)};
var encTransaction = cryptUtils.AES256GCM(transaction, secretsManager);
s3.putObject({
    "Bucket": "ACME-customer-billing",
    "Key": "todayTransactions",
    "Body": JSON.stringify(encTransaction),
    "Content-Type": "application/json"
},
function(err,data){
});
```

Exercise (12): usage of HTML encoding, what is wrong and how to improve it?

```
<div class="form-group">
    <label for="search">Search:</label>
    <input type="text" class="form-control" id="search" name="search">

    <input type="submit" id="submit" class="btn" value="Search">
    <div class="alert alert-danger <%=alertVisibility%>">
        Cannot find <%=request.getParameter("search")%>
    </div>
</div>
```

Exercise (12): usage of HTML encoding, what is wrong and how to improve it?

```
<div class="form-group">
    <label for="search">Search:</label>
    <input type="text" class="form-control" id="search" name="search">

    <input type="submit" id="submit" class="btn" value="Search">
    <div class="alert alert-danger <%=alertVisibility%>">
        Cannot find <%=StringEscapeUtils.escapeHtml4(request.getParameter("search"))%>
    </div>
</div>
```

Exercise (13): HTML Encoding, output context, what is wrong and how to improve it?

```
<script>
    <%
        String searchTxt = StringEscapeUtils.escapeHtml4(request.getParameter("search"));
    %>

    document.cookie = 'search=<%=searchTxt%>';
</script>
```

Exercise (13): HTML Encoding, output context, what is wrong and how to improve it?

```
<script>
    <%
        String searchTxt = StringEscapeUtils.escapeHtml4(request.getParameter("search")).replace("'","&#39;");
    %>

    document.cookie = 'search=<%=searchTxt%>';
</script>
```

Exercise (14): what is wrong and how to improve it?

- The application is implementing its own client side rendering of the input instead of taking advantage of a JS framework.

```
$get("/profile", function(data, status){
    if(data!=null){
        var dataArgs = data.split(",");
        if(dataArgs.length > 1){
            var displayName = dataArgs[0];
            var displayNameDiv = $("#displayNameDiv")[0];
            displayNameDiv.innerHTML = displayName;
            var avatarImg = $("#avatarImg")[0];
            avatarImg.src = dataArgs[1];
        }
    }
});
```

Exercise (14): what is wrong and how to improve it?

- The application is implementing its own client side rendering of the input instead of taking advantage of a JS framework.

```
$get("/profile", function(data, status){
    if(data!=null){
        var dataArgs = data.split(",");
        if(dataArgs.length > 1){
            var displayName = dataArgs[0];
            var displayNameDiv = $("#displayNameDiv")[0];
            displayNameDiv.innerText = displayNameDiv.textContent = displayName;
            var avatarImg = $("#avatarImg")[0];
            avatarImg.src = dataArgs[1];
        }
    }
});
```

Exercise (15): JavaScript parameterized statement, what is wrong and how to improve it?

```
$get("/profile", function(data, status){
    if(data!=null){
        var dataArgs = data.split(",");
        if(dataArgs.length > 1){
            var displayName = dataArgs[0];
            setTimeout(`showProfile('${displayName}')`, 1000);
        }
    }
});
```

Exercise (15): JavaScript parameterized statement, what is wrong and how to improve it?

```
$get("/profile", function(data, status){
    if(data!=null){
        var dataArgs = data.split(",");
        if(dataArgs.length > 1){
            var displayName = dataArgs[0];
            setTimeout(showProfile, 1000, displayName);
        }
    }
});
```

Exercise (16): what is wrong and how to improve it?

```
String file = request.getParameter("file");
file = "public/"+file;
InputStream input = null;
BufferedReader reader = null;
StringBuilder sb = new StringBuilder();
input = getServletContext().getResourceAsStream(file);
```

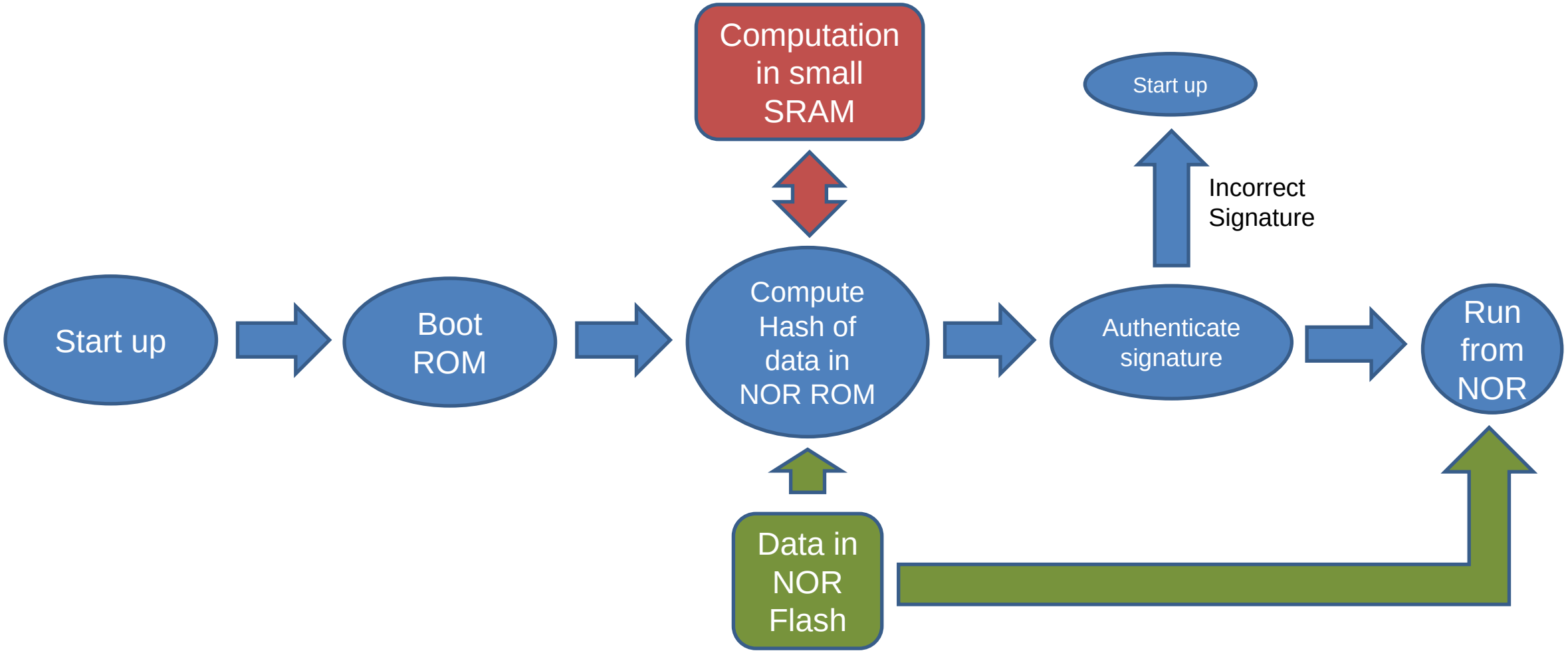
Exercise (16): what is wrong and how to improve it?

```
String fileId = request.getParameter("fileId");
file = "public/"+availableFiles[fileId];
InputStream input = null;
BufferedReader reader = null;
StringBuilder sb = new StringBuilder();
input = getServletContext().getResourceAsStream(file);
```

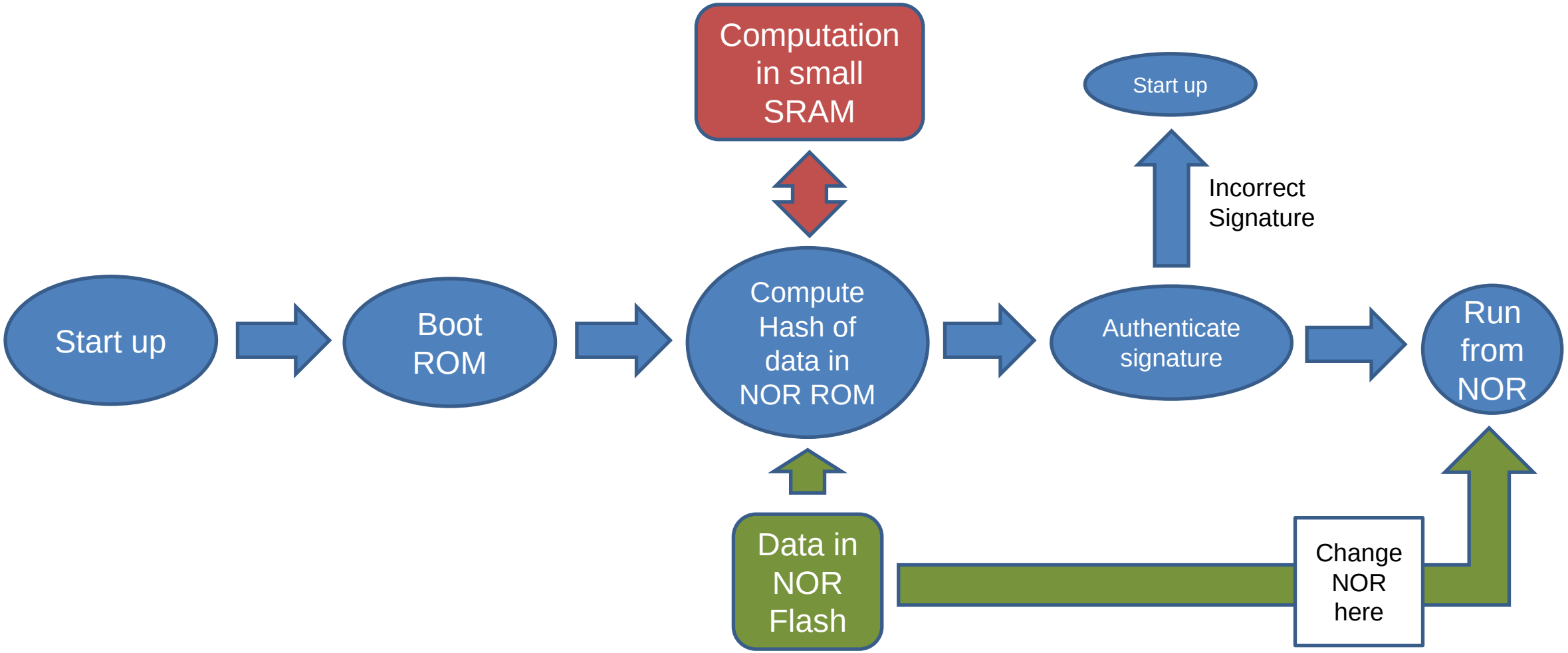
Intermission - CodeQL

- Installation process – not pleasant
  - https://codeql.github.com/docs/codeql-for-visual-studio-code/setting-up-codeql-in-visual-studio-code/
  - https://docs.github.com/en/code-security/codeql-cli/using-the-codeql-cli/creating-codeql-databases
- Tricky for C and C++
  - Heavy Computationally, I would recommend a strong machine (>16Gb RAM, etc.)
  - GitHub Actions do not work by default
- Still a very useful tool!
- DEMO

Exercise (17): what is wrong with the design and how to improve it?



Exercise (17): what is wrong with the design and how to improve it?



Future reading / Exercise (18): what is wrong and how to improve it?

- In load nitro firmware memory in:
- https://github.com/OP-TEE/optee_os/blob/3.14.0/core/pta/bcm/elog.c

Future reading / Exercise (18): what is wrong and how to improve it?

- Solution:
- https://github.com/OP-TEE/optee_os/security/advisories/GHSA-hhrc-h9xj-hppv
- Real issue that was found recently.
- What is the impact?

ASSIGNMENT – CODE REVIEW

Assignment 6: Source Code Review

- 2 sub-exercises
- `pin.c`
  - Incomplete 32-bit SIM smartcard application in C in the JavaCard style.
    - Exposed functions are being called directly from the APDU handler. That code sets all the lengths and offsets correctly.
    - The APDU handler and the main functions are skipped here since they are not relevant from the security point of view.
  - Find all the possible bugs. Scope: logical and side-channel issues
  - 5 points.
- `server_articles.c`, `server_setup.sh`
  - Find all the possible bugs. Scope: concentrate on logical issues
  - 5 points.
- For found issues: asses severity, risk, etc. like in the lecture; also give recommendations how to improve.
- There is no need to use automatic tooling but you can do it if you would like to.

Assignment 6 – what to submit

- Report found issues in the format presented in the lecture.
- Try to be compact but clear!
- Specify which editor or IDE you use. Also if any static analysis tools you used (for the second exercise).
- Submit **before 15.5. 23:59am** into IS HW vault
  - Soft deadline: -3 points for every started 24 hours
- Good luck!!!
- Consultation
  - Regular consultation on Friday 09.30 – 11.00 in my office: A406.
  - Email me to make an appointment: chmielewski@fi.muni.cz.

Conclusions

- A lot of different topics for source code review
- Just a shallow glance
- Many topics not touched, like boot loaders, crypto libraries, etc.
- Good luck with the exercise!

Questions ?