RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F03V**

PKI Well Revised: Common Mistakes Which Lead to Huge Compromise of Identity

Mike Jankowski-Lorek, Ph.D.

CQURE Director of Consulting, Cybersecurity Expert
cqure.pl, cqureacademy.com
mike@cqure.us
@MJL_PL

RSAConference2020 APJ

A Virtual Learning Experience

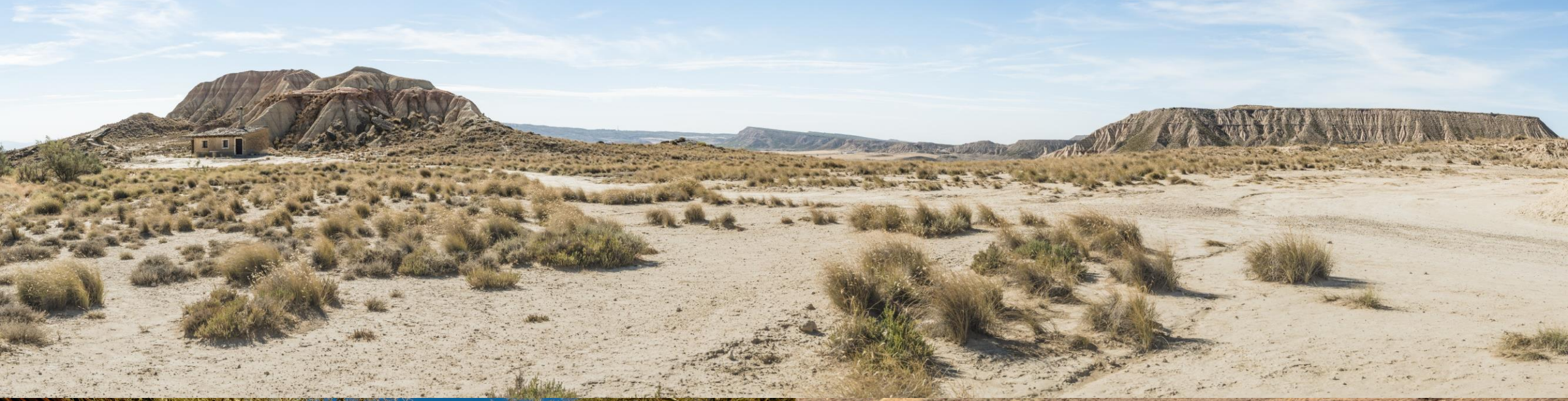
Agenda

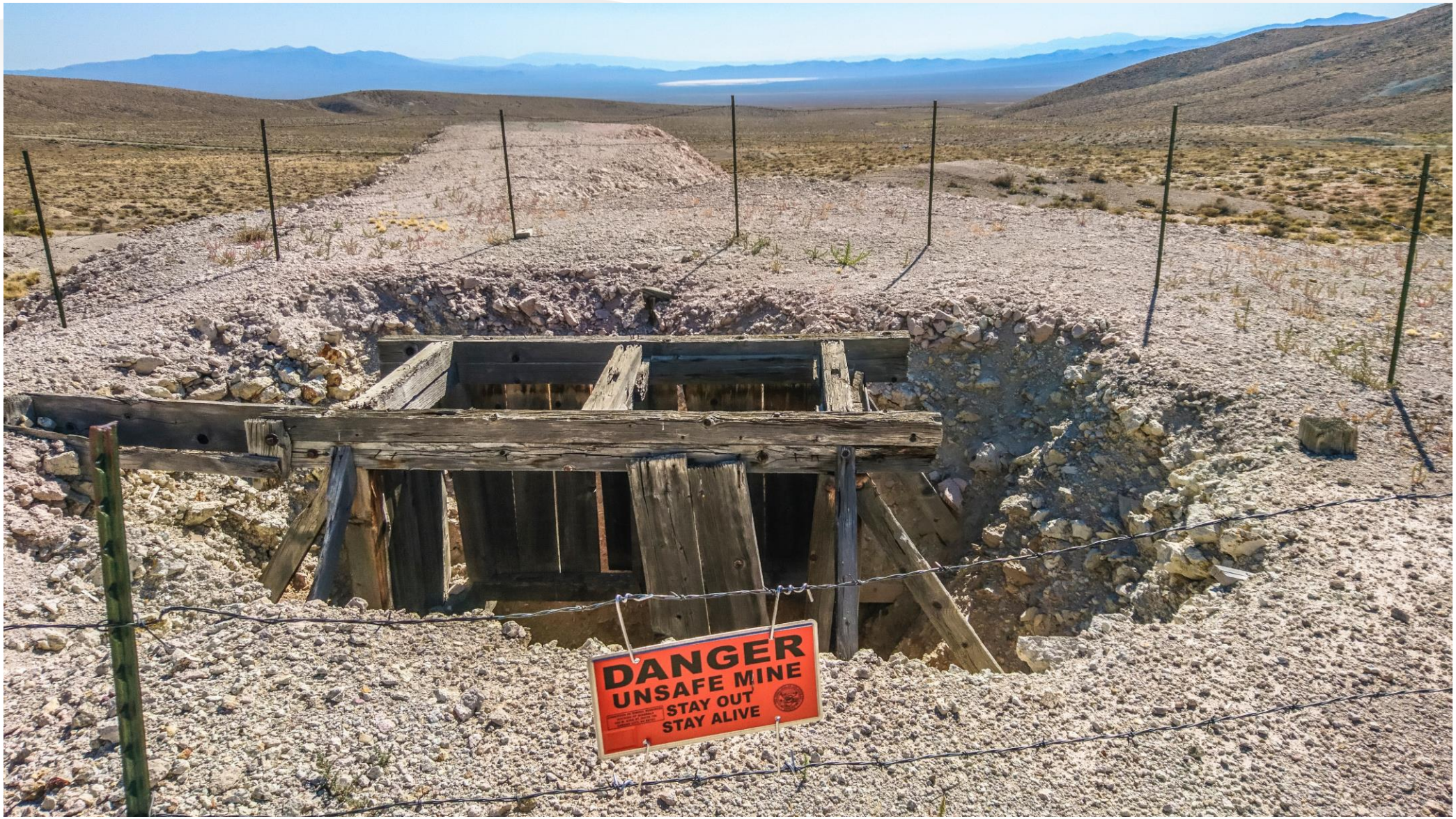
1 Cryptography 101

2 Real life scenarios

3 Common PKI pitfalls

4 Summary



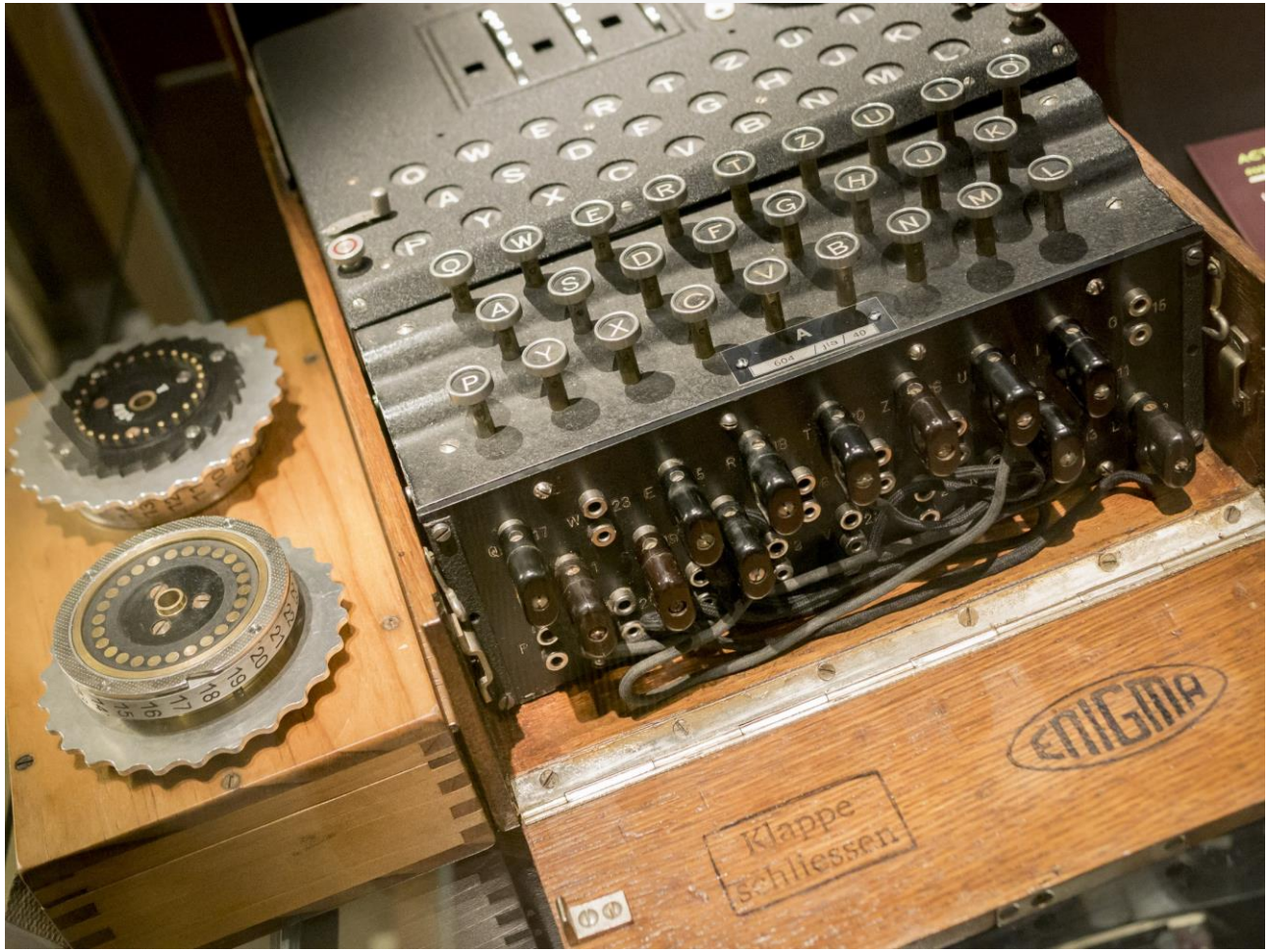


All that glitters is not gold

Cryptography 101

Basic concepts

- Encoding
- Encrypting
- Hashing
- Signing



Public Key Infrastructure 101

Basic concepts

- Certificate X.509
  - Private/Public Key
  - EKU/Application Policy
- Certificate Signing Request
- Certification Authority
  - Validation procedures/CPS
  - CRL/OCSP/CT
  - Certificate Trust

Multi organization trust

Cross certification

```
                 PKI 1 and 2 cross-certificates
                +-------------------------------+
                |                               |
                |                               v
                |                           +---------+
                |                     +----| Root CA |---+
                |                     |    +---------+   |
                |                     |       PKI 1      |
                |                     v                  v
                |                     +------+         +------+
                v PKI 2             +-|  CA  |-+       |  CA  |
               +------+             | +------+ |       +------+
      +------->|  CA  |<-----+      |     |    |         |   |
      |        +------+      |      |     |    |         |   |
      |         |    |       |      v     v    v         v   v
      |         v    v       |  +----+ +----+ +----+ +----+ +----+
      |      +----+ +----+   |  | EE | | EE | | EE | | EE | | EE |
      |      | EE | | EE |   |  +----+ +----+ +----+ +----+ +----+
      |      +----+ +----+   |
      v                      v
   +------+               +------+
   |  CA  |<------------->|  CA  |------+
   +------+               +------+      |
    |    |                 |    |       |
    |    |                 |    |       |
    v    v                 v    v       v
  +----+ +----+           +----+ +----+ +----+
  | EE | | EE |           | EE | | EE | | EE |
  +----+ +----+           +----+ +----+ +----+
```

Trust list

```
+-------------------------------------------------------+
|                      Trust List                       |
|                                                       |
|     +---------+     +---------+      +---------+      |
|  +--| Root CA |     | Root CA |      | Root CA |      |
|  |  +---------+     +---------+      +---------+      |
|  |      |                |                |          |
+--|------|----------------|----------------|----------+
   |      |                |                |
   |      |                |                |
   |      |                v                |
   |      |              +----+             |
   |      |         +----| CA |---+         |
   |      |         |    +----+   |         |
   |      |         |             |         |
   |      |         v             v         v
   |      |      +----+        +----+     +----+
   |      |      | CA |---+    | CA |-+   | CA |---+
   |      |      +----+   |    +----+ |   +----+   |
   |      |        |      |      |    |     |      |
   |      |        |      |      |    |     |      |
   v      v        v      v      v    v     v      v
+----+ +----+ +----+ +----+ +----+ +----+ +----+ +----+
| EE | | EE | | EE | | EE | | EE | | EE | | EE | | EE |
+----+ +----+ +----+ +----+ +----+ +----+ +----+ +----+
```

https://tools.ietf.org/html/rfc4158

PKI real life scenarios

Usage

- Server authentication
- Client authentication
- Smartcard logon
- Windows Hello for Business
- Secure E-Mail
- Other

RSA Conference2020 APJ
A Virtual Learning Experience

Demo: Live hacking

Common pitfalls of PKI

Common Mistakes

Points of interest

- Software key storage provider
- Multi purpose certificates
- CSR automatic approval
- Template permissions
- Unconstrained cross certification

RSAConference2020 APJ

A Virtual Learning Experience

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Username: student

Password: CQUREAcademy#123!

What does CQURE do?

1. Consulting Services:

- Extensive IT Security Audits and Penetration Tests of all kinds,
- Configuration Audit and Architecture,
- Design Social Engineering Tests,
- Advanced Troubleshooting and Debugging,
- Emergency Response Services.

2. R&D & CQLabs Tools & Hacks Publications

3. Trainings & Seminars:

- Offline worldwide,
- Online.

RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F03V**

PKI Well Revised: Common Mistakes Which Lead to Huge Compromise of Identity

Mike Jankowski-Lorek, Ph.D.

CQURE Director of Consulting, Cybersecurity Expert
cqure.pl, cqureacademy.com
mike@cqure.us
@MJL_PL