Operation Black tulip: Certificate authorities loose authority

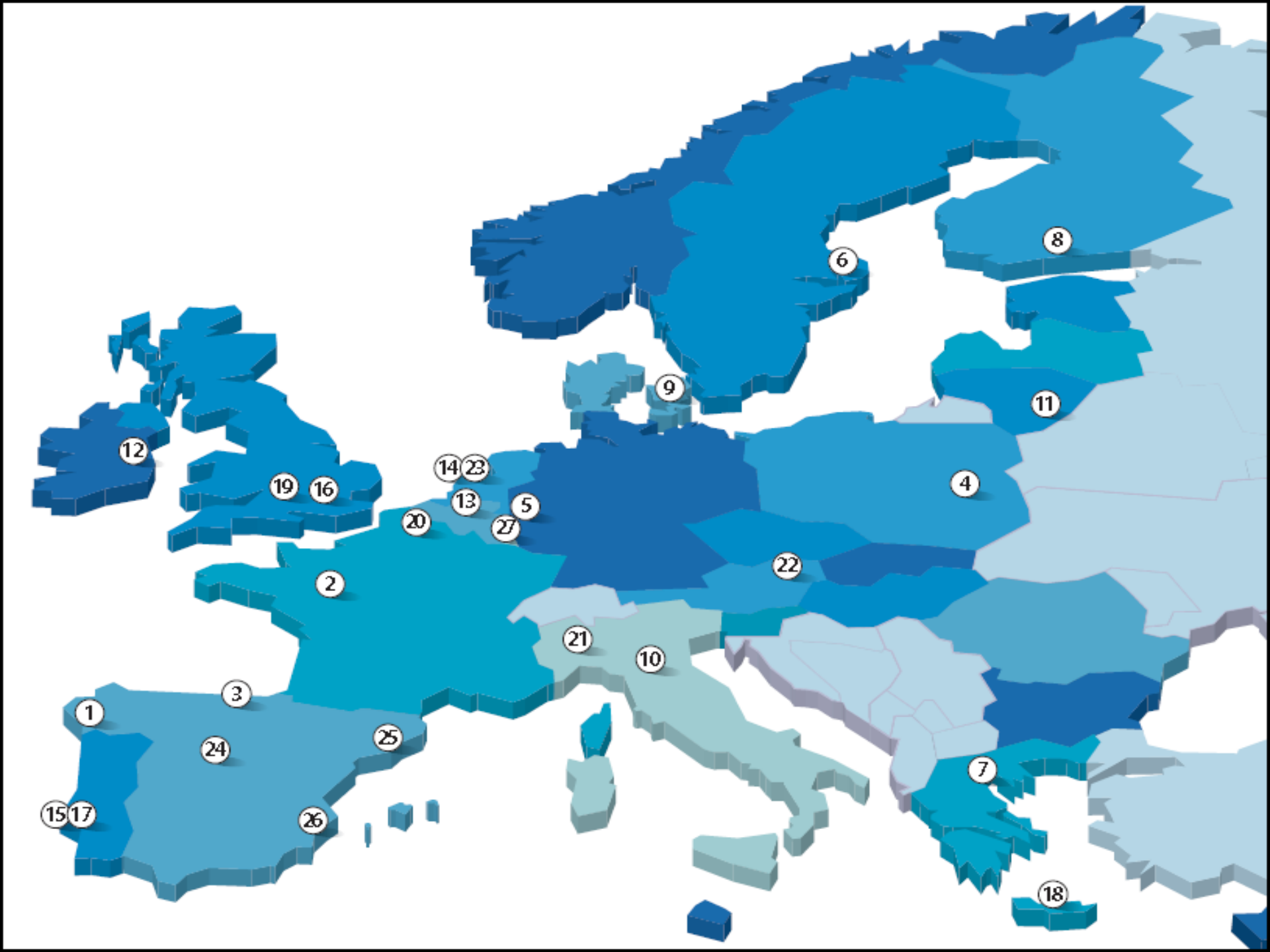
24th Annual FIRST Conference
19 June 2012, Malta

Dr. Marnix Dekker, CISA

Security expert
Information security officer
ENISA

About ENISA

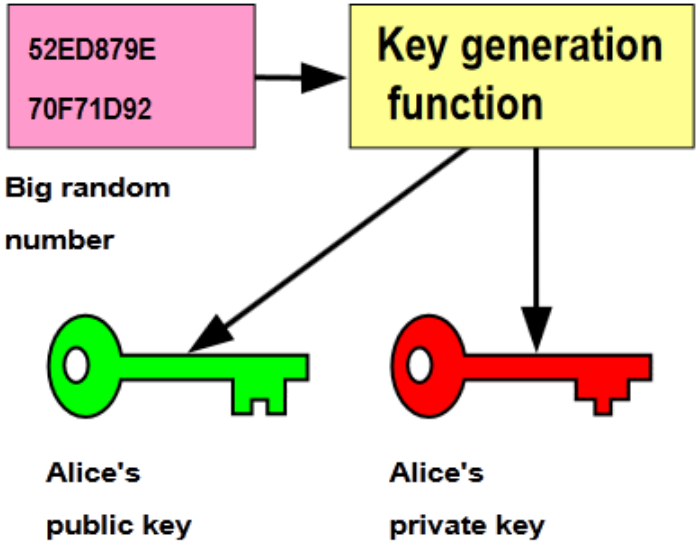
- The European Network and Information Security Agency
  - gives advice on information security issues
  - to national authorities, EU institutions, citizens, businesses
  - acts as a forum for sharing good NIS practices
  - facilitates information exchange and collaboration
- Set up in 2004 – EC proposed a new mandate for 2013.
- Around 30 security experts and 20 staff.
- ENISA has an advisory role (not operational) and the focus is on prevention and preparedness.


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27


Black tulips

Public key cryptography

- Public key crypto is great!
- Authenticate and encrypt
  - user to user (email)
  - machine to machine (WS)
  - user to server (login)
  - **server to user (https)**
- But who uses which key?
  - To prevent spoofing (MITM)



- One solution for this is called PKI
  - List of <name, key> pairs published by a trusted party (a CA)
  - Sometimes there is a hierarchy of CAs

Wide spread criticism of PKI

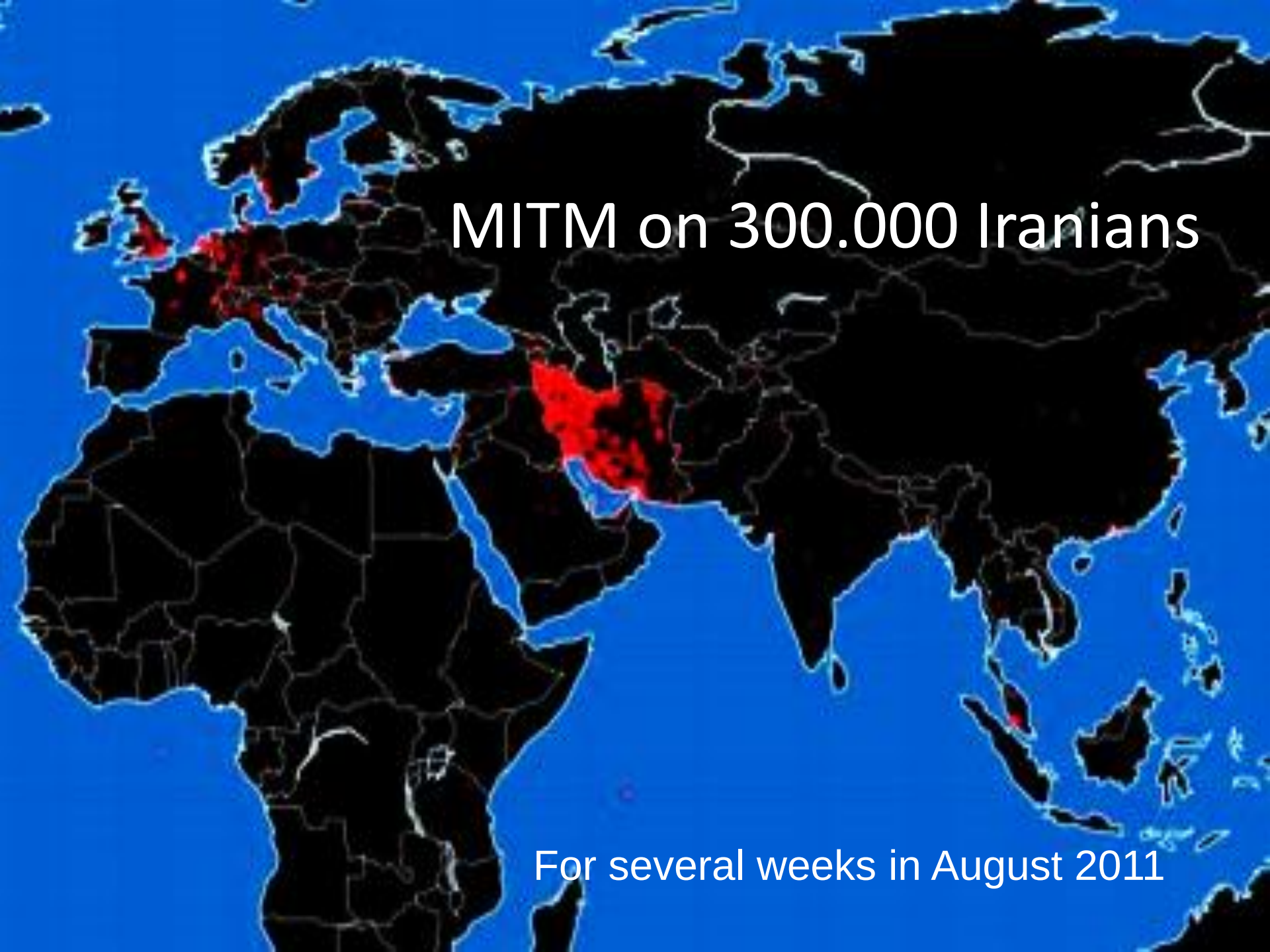
- PKI is cumbersome for authenticating or authorising users
  - No anonymous claims of attributes
  - No distributed trust (I am Bob's friend)
- Alternatives
  - SPKI (Carl Ellison)
  - SDSI (Ron Rivest, Butler Lampson) (like SXIP, Identity 2.0)
  - PGP (Phil Zimmermann)
- It is easy to see that PKI does not exploit the great possibilities of public key cryptography
- Even worse: the most common use of PKI, HTTPS (SSL + CA's in the browser + OCSP) is flawed.

… and this has been argued in many articles by well known experts.

Spy in the middle

- Matt Blaze http://www.crypto.com/blog/spycerts : "Products appear sophisticated, mature, and mass-produced… an active vendor community"
- On CA's: "a surprisingly large number of root authorities, from tiny, obscure businesses to various national governments"
- Moxie Marlinspike http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity : Repeated hacks of CAs, and you don't even need to hack.

And then…


MITM on 300.000 Iranians
For several weeks in August 2011

Dutch eGovernment offline

For several weeks in September 2011

Impact timeline

July 2011

Security breach at Diginotar

August 2011

Privacy breach in Iran

September 2011

Outage in the Netherlands

Let’s look at the impact, starting small first…

- Bankruptcy for Diginotar
- Vasco estimates losses at around 4 million euros
  - Vasco acquired Diginotar for 12 million euros

- eGov outage for millions of users for several weeks
- Dutch state claims 9 million euros in damages

Mikko Hyppönen: “It is plausible that people died.”

Critical information infrastructure: Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.

(So the CA's in your country are critical information infrastructure)

EU regulation for eID/eSig services

- New EU regulation contains:
  - Breach notification obligation
  - Appropriate security measures
  - Summary reporting of breaches to ENISA
- Some issues to keep in mind here
  - Detecting breaches is hard (see Verizon data breach report)
    - Most breaches are detected by 3rd parties (92%)
    - … and only weeks later (85%)
  - Security measures are difficult to enforce (the devil is in the details of the implementation)
  - Diginotar was well reputed, frequently audited and found compliant with security standards
  - We should go from certification to continuous monitoring

Is new regulation enough?

600 single points of failure…

(meaning: attacker needs to succeed at compromising 1 of 600 to allow attacks on any website!)

Job security

Aart Jochem (NCSC.nl) @ FIRSTCON 2012:

“The Diginotar crisis is over, but the PKI crisis is still ongoing.”

Key issues to address…

Weakest link?

- 600 CA's in the trusted list of browsers and operating systems
- 600 single points of failure
- Large CA's work with hundreds of resellers
- Do you even need to hack?

Revocation?

- Google: “Soft-fail revocation checks are like a seat-belt that snaps when you crash. “
- Hard-fail revocation checks require highly available OCSP responders at CA’s.
- Revocation checks add on average 1 second to page loading.
- Revocation checks allow CA’s to monitor who visited which websites.
- Google Chrome browser dropped OCSP
- Can we revoke trust in a CA? Is there a plan?

Usability?

- Educate the user?
- Extended validation certificates, blue bars, green bars, locks, warnings – do they help?

- Warnings when there is no attack (bad)
  - 1 in 300 users disconnected when a NZ banking website showed the wrong certificate for one hour.
- No warnings when there is an attack (worse)
- No choice for users about which CA's they trust
  - So sites have no incentive to use better CAs
  - So CA's have no incentive to get better

Who do we trust?

- Few trusted parties to establish trust between everyone else.
- Some very large businesses depend on very small ones, with a tough business model
- "Diginotar earned around 100.000 euros from its certificate business in the first half of 2011. "
- Can these small trusted parties withstand the attack pressure facing billion dollar companies?
  - Some CA's can not, TLD's can (DNSSEC)?
- Can we somehow leverage the large user base of the larger websites for conveying trust?

Some conclusions

- Prepare now for a CA failure!
  - E.g. have a spare certificate ready for critical sites
- Fix HTTPS
  - it is the foundation of online security
  - E.g. DNSSEC, DANE, Convergence, Tack
- eCommunications go beyond the last mile
  - Border gateway protocol, Internet exchange points
  - Routers, datacenters
  - CA's, TLD's, browsers, etc.
- EU Internet security strategy
  - Extending Article 13a beyond telecom sector
- Assess what is widely-used critical infrastructure

Contact

Dr. Marnix Dekker, CISA
CIIP and Resilience, ENISA

marnix.dekker@enisa.europa.eu

www.enisa.europa.eu

http://twitter.com/marnixdekker