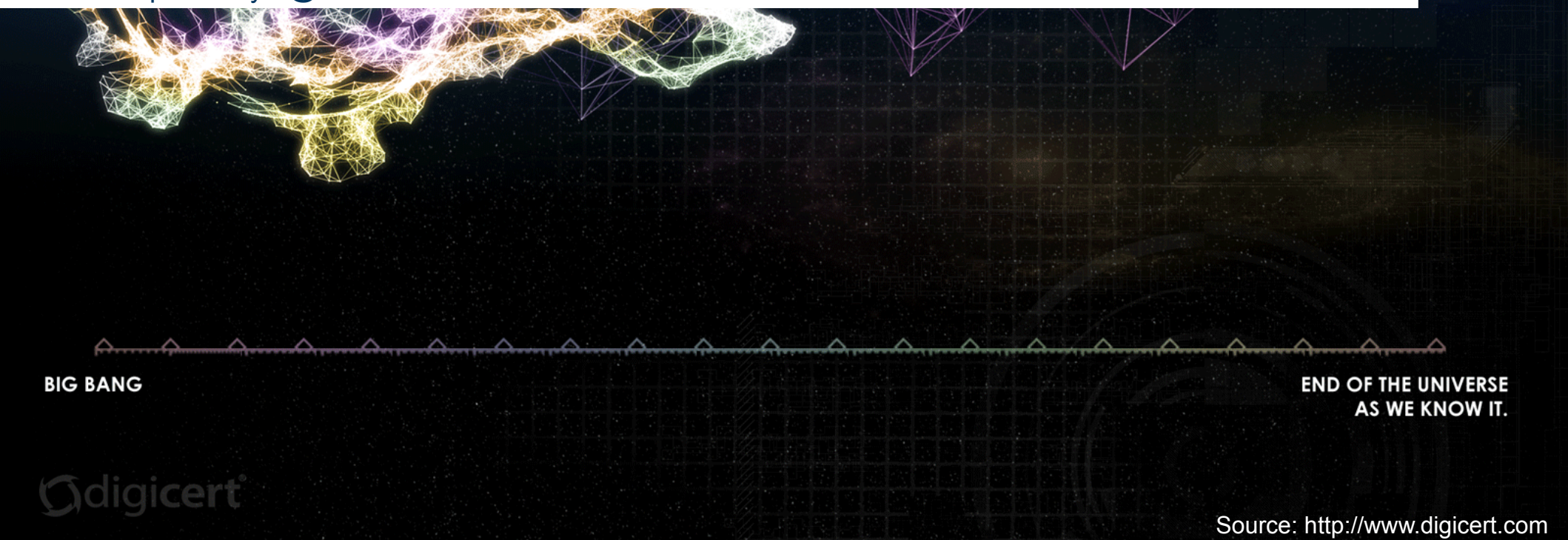
RUHR-UNIVERSITÄT BOCHUM

RUB

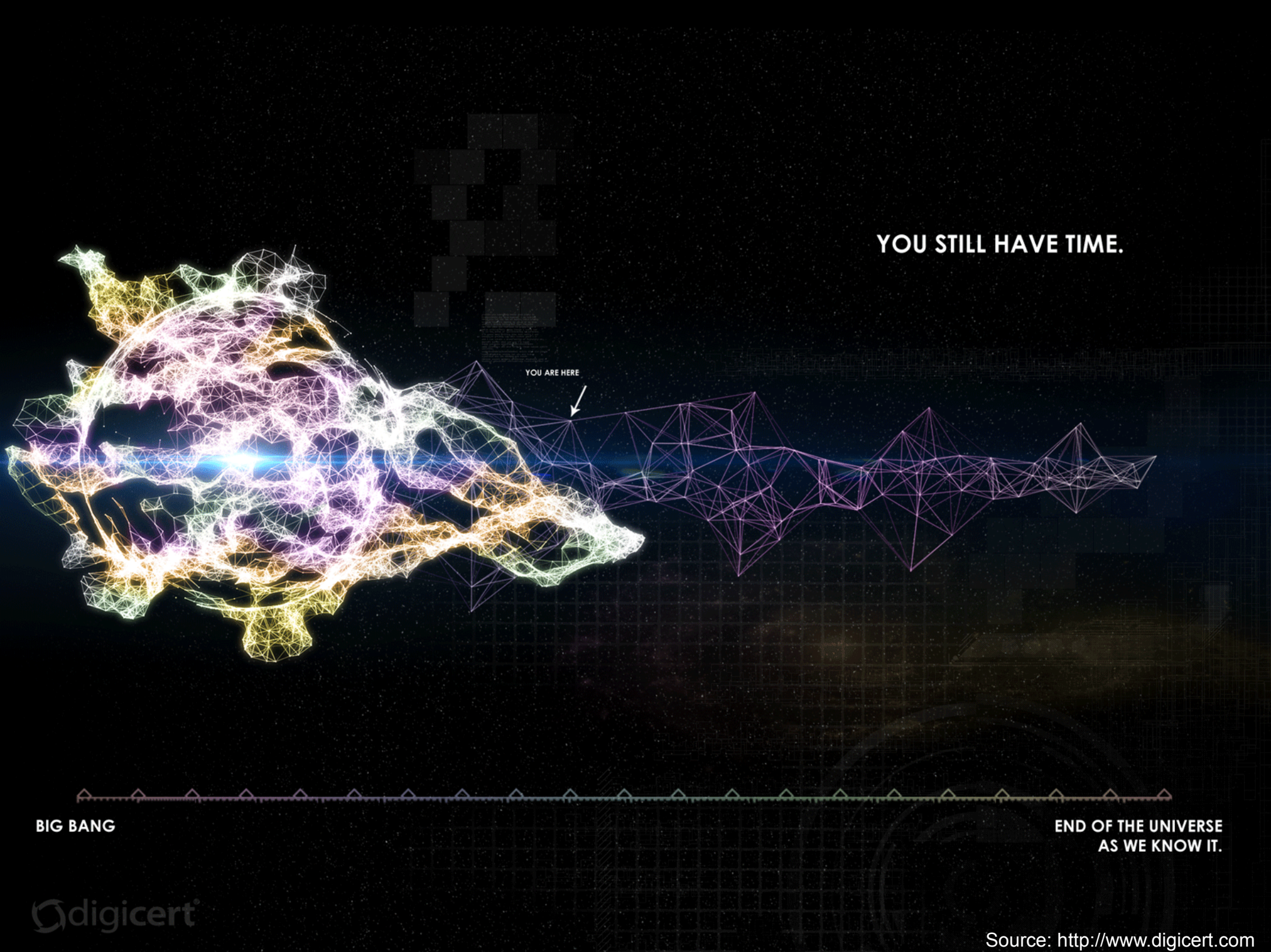
Systematization of Knowledge
Lessons Learned From SSL/TLS Attacks
20.08.2013

Horst Görtz Institute for IT-Security
Chair for Network and Data Security

christopher.meyer@rub.de



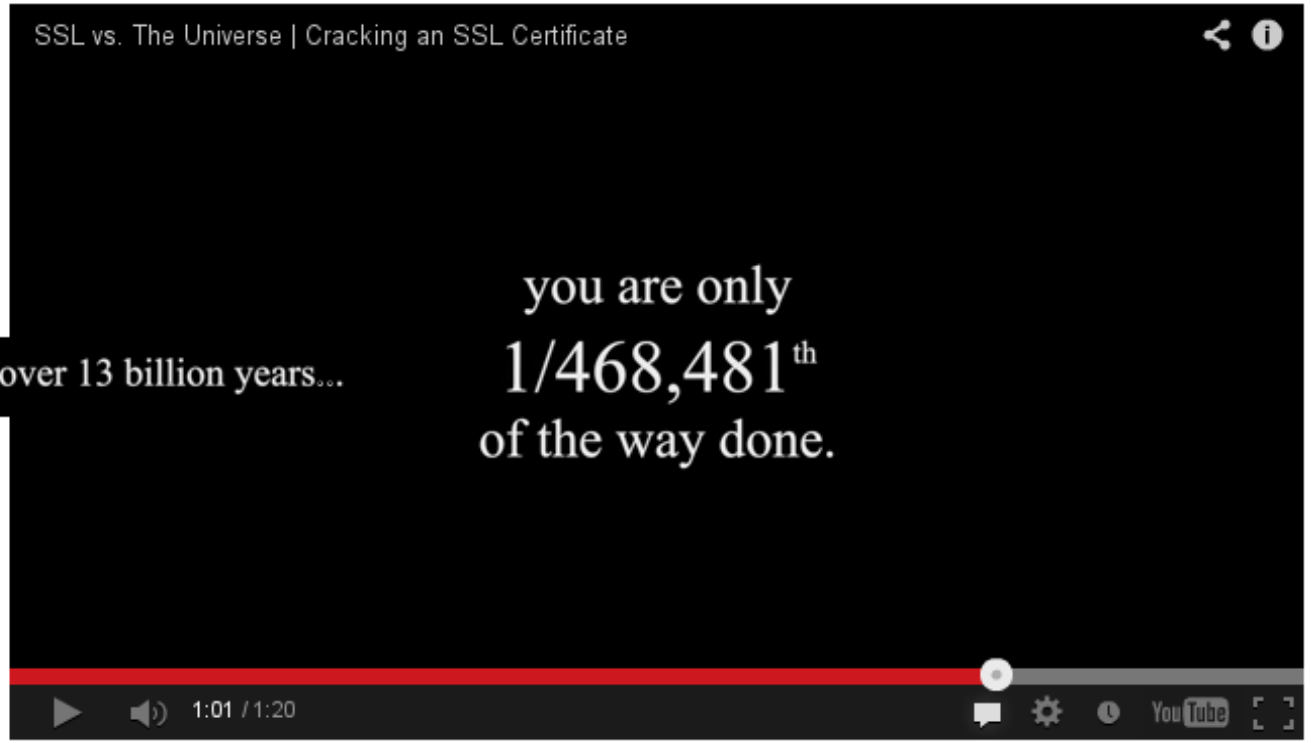
Source: http://www.digicert.com



Source: http://www.digicert.com

The Strength of an SSL Certificate

What Would it Take to Break a 2048 Bit SSL Certificate?



BIG BANG

END OF THE UNIVERSE
AS WE KNOW IT.

digicert

Source: http://www.digicert.com

What if we don't even need the private key?

Nearly 20 years of SSL/TLS

Nearly 20 years of SSL/TLS
Some key data

- **Invented in 1994**

Nearly 20 years of SSL/TLS

Some key data

- **Invented in 1994**
- **Evolutionary development**

Nearly 20 years of SSL/TLS

Some key data

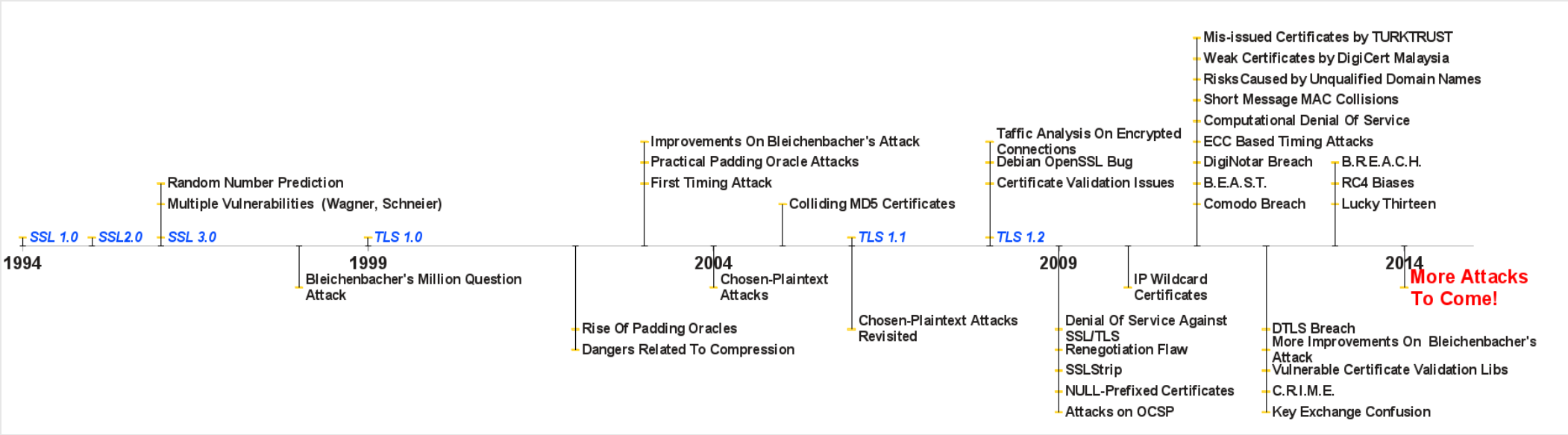
- **Invented in 1994**
- **Evolutionary development**
- **5 official and 1 unpublished revision**
  - **SSL 2.0, SSL 3.0**
  - **TLS 1.0, TLS 1.1, TLS 1.2**
  - **SSL 1.0**

Nearly 20 years of SSL/TLS

Some key data

- **Invented in 1994**
- **Evolutionary development**
- **5 official and 1 unpublished revision**
  - **SSL 2.0, SSL 3.0**
  - **TLS 1.0, TLS 1.1, TLS 1.2**
  - **SSL 1.0**
- **~ 39 theoretical and practical attacks so far**

Timeline


SSL 1.0
SSL2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
1994
1999
2004
2009
2014
Random Number Prediction
Multiple Vulnerabilities (Wagner, Schneier)
Bleichenbacher's Million Question Attack
Improvements On Bleichenbacher's Attack
Practical Padding Oracle Attacks
First Timing Attack
Rise Of Padding Oracles
Dangers Related To Compression
Colliding MD5 Certificates
Chosen-Plaintext Attacks
Chosen-Plaintext Attacks Revisited
Taffic Analysis On Encrypted Connections
Debian OpenSSL Bug
Certificate Validation Issues
Denial Of Service Against SSL/TLS
Renegotiation Flaw
SSLStrip
NULL-Prefixed Certificates
Attacks on OCSP
IP Wildcard Certificates
Mis-issued Certificates by TURKTRUST
Weak Certificates by DigiCert Malaysia
Risks Caused by Unqualified Domain Names
Short Message MAC Collisions
Computational Denial Of Service
ECC Based Timing Attacks
DigiNotar Breach
B.E.A.S.T.
Comodo Breach
DTLS Breach
More Improvements On Bleichenbacher's Attack
Vulnerable Certificate Validation Libs
C.R.I.M.E.
Key Exchange Confusion
B.R.E.A.C.H.
RC4 Biases
Lucky Thirteen
More Attacks To Come!

Contribution

Contribution

- **Collected attacks on SSL/TLS**

Contribution

- **Collected attacks on SSL/TLS**
- **Analyzed all attacks**

Contribution

- Collected attacks on SSL/TLS
- Analyzed all attacks
- Categorized each attack

Contribution

- Collected attacks on SSL/TLS
- Analyzed all attacks
- Categorized each attack
- Identified the root cause of the vulnerabilities for each attack

Contribution

- Collected attacks on SSL/TLS
- Analyzed all attacks
- Categorized each attack
- Identified the root cause of the vulnerabilities for each attack
- Concluded Lessons Learned for each attack

Contribution

- Collected attacks on SSL/TLS
- Analyzed all attacks
- Categorized each attack
- Identified the root cause of the vulnerabilities for each attack
- Concluded Lessons Learned for each attack
- Created a Guideline for Protocol Designers and Implementers

Attack Patterns

Abnormalities during the analysis of attacks

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**
- **Attacks can be grouped into 4 categories**

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**
- **Attacks can be grouped into 4 categories**
  1. **Attacks on the Handshake Protocol**

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**
- **Attacks can be grouped into 4 categories**
  1. **Attacks on the Handshake Protocol**
  2. **Attacks on the Record Layer**

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**
- **Attacks can be grouped into 4 categories**
  1. **Attacks on the Handshake Protocol**
  2. **Attacks on the Record Layer**
  3. **Attacks on the PKI**

Attack Patterns

Abnormalities during the analysis of attacks

- **Attacks focus on specific parts/layers of SSL/TLS**
- **Attacks can be grouped into 4 categories**
  1. **Attacks on the Handshake Protocol**
  2. **Attacks on the Record Layer**
  3. **Attacks on the PKI**
  4. **Various other Attacks**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **A**
  - **R**
  - **I**
  - **S**
  - **E**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **Alter messages or message parts**
  - **R**
  - **I**
  - **S**
  - **E**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **Alter messages or message parts**
  - **Replay communication or parts of it**
  - **I**
  - **S**
  - **E**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **Alter messages or message parts**
  - **Replay communication or parts of it**
  - **Interfere messages or message parts**
  - **S**
  - **E**

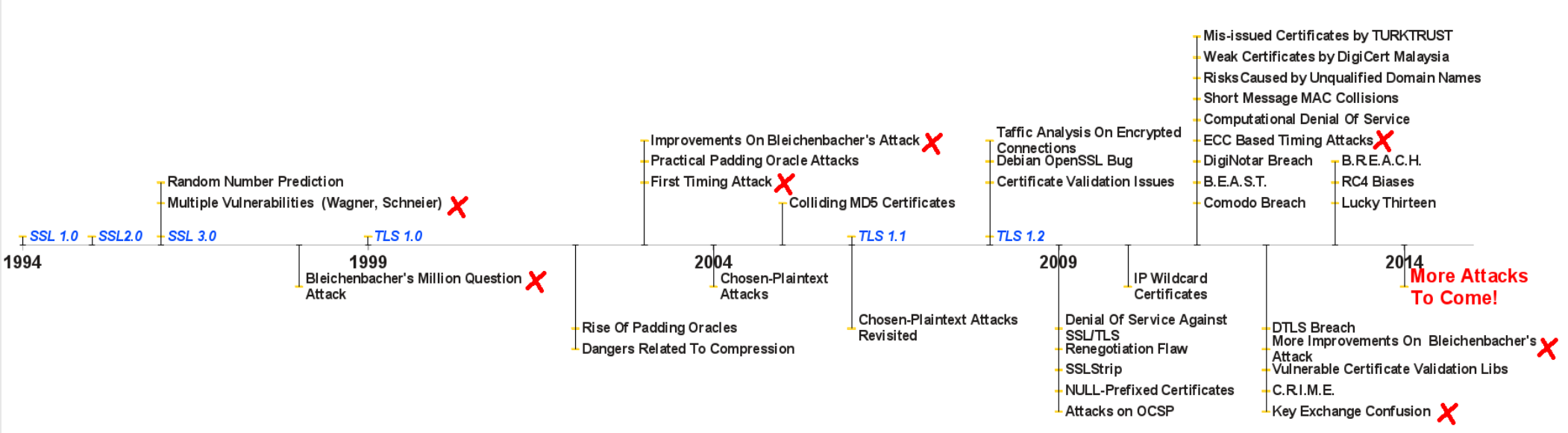
Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **Alter messages or message parts**
  - **Replay communication or parts of it**
  - **Interfere messages or message parts**
  - **Systematically analyze communication**
  - **E**

Attacks on the Handshake Protocol
Details

- **Main goal: Influence Handshake Phase**
  - **Alter messages or message parts**
  - **Replay communication or parts of it**
  - **Interfere messages or message parts**
  - **Systematically analyze communication**
  - **Establish own Cryptographic Primitives**

Attacks on the Handshake Protocol
Details



Attacks on the Record Layer
Details

- **Main goal: Violate Confidentiality or Integrity**

Attacks on the Record Layer
Details

- **Main goal: Violate Confidentiality or Integrity**
  - **B**
  - **A**
  - **T**

Attacks on the Record Layer
Details

- **Main goal: Violate Confidentiality or Integrity**
  - **Break Encryption**
  - **A**
  - **T**

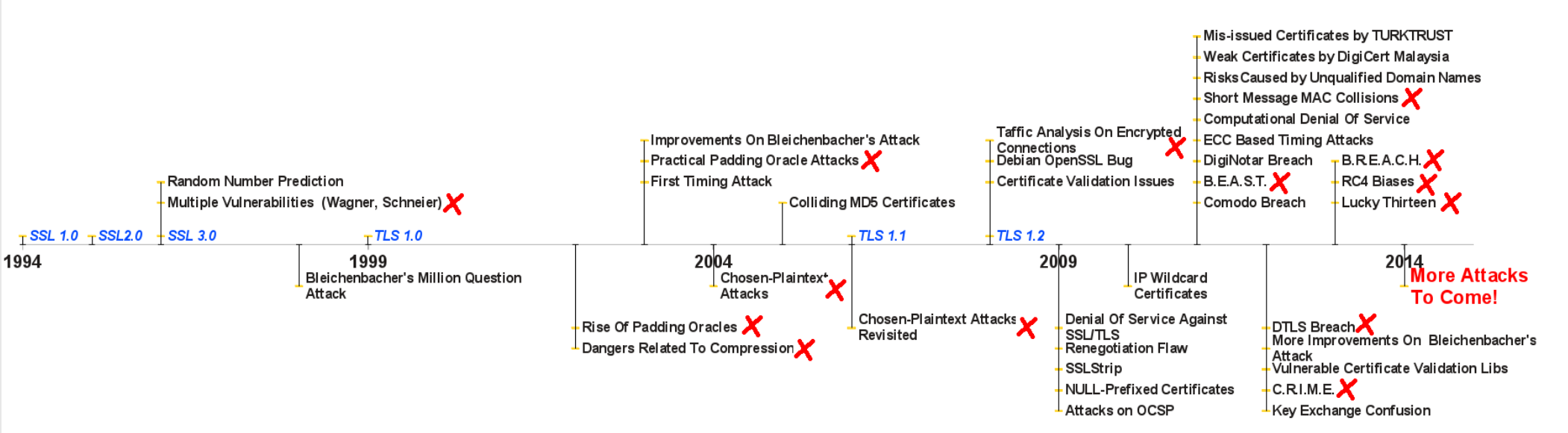
Attacks on the Record Layer
Details

- **Main goal: Violate Confidentiality or Integrity**
  - **Break Encryption**
  - **Analyze Encrypted Traffic**
  - **T**

Attacks on the Record Layer
Details

- **Main goal: Violate Confidentiality or Integrity**
  - **Break Encryption**
  - **Analyze Encrypted Traffic**
  - **Tamper with MAC**

Attacks on the Record Layer
Details



Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**

Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **R**
  - **I**
  - **T**
  - **C**
  - **H**

Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **Recover or Break Private Keys**
  - **I**
  - **T**
  - **C**
  - **H**

Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **Recover or Break Private Keys**
  - **Influence Certificate Revocation Systems**
  - **T**
  - **C**
  - **H**

Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **Recover or Break Private Keys**
  - **Influence Certificate Revocation Systems**
  - **Trick Certificate Validation**
  - **C**
  - **H**

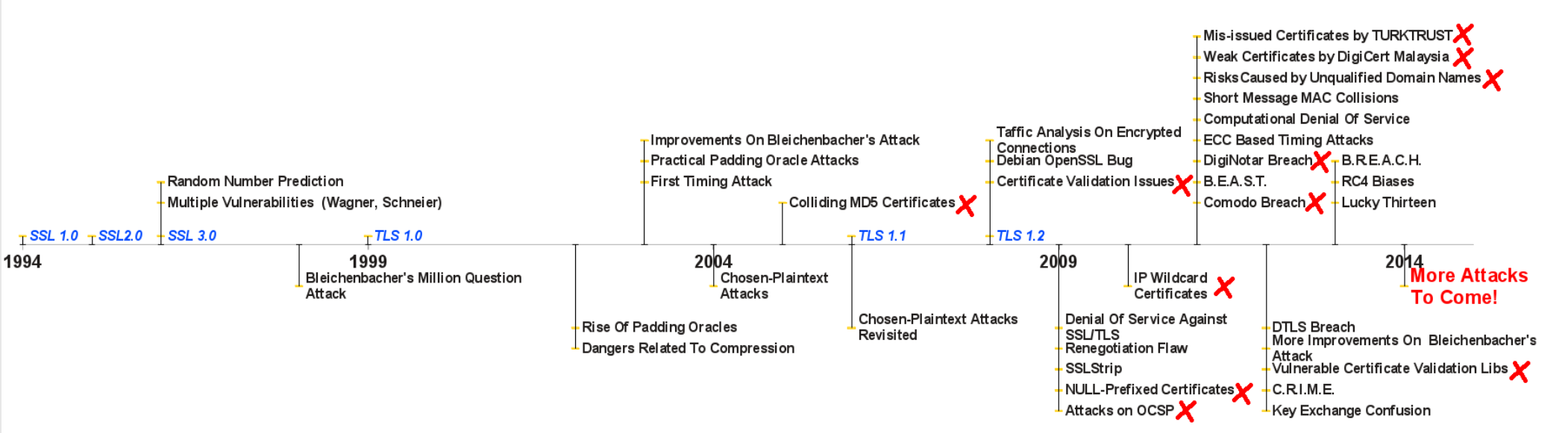
Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **Recover or Break Private Keys**
  - **Influence Certificate Revocation Systems**
  - **Trick Certificate Validation**
  - **Compute Colliding Certificates**
  - **H**

Attacks on the PKI
Details

- **Main goal: Influence, Compromise or Trick PKI**
  - **Recover or Break Private Keys**
  - **Influence Certificate Revocation Systems**
  - **Trick Certificate Validation**
  - **Compute Colliding Certificates**
  - **Hack or Trick Certification Authorities**

Attacks on the PKI
Details



Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**

Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**
  - **G**
  - **A**
  - **S**
  - **P**

Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**
  - **Guess Random Numbers**
  - **A**
  - **S**
  - **P**

Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**
  - **Guess Random Numbers**
  - **Affect Reliability**
  - **S**
  - **P**

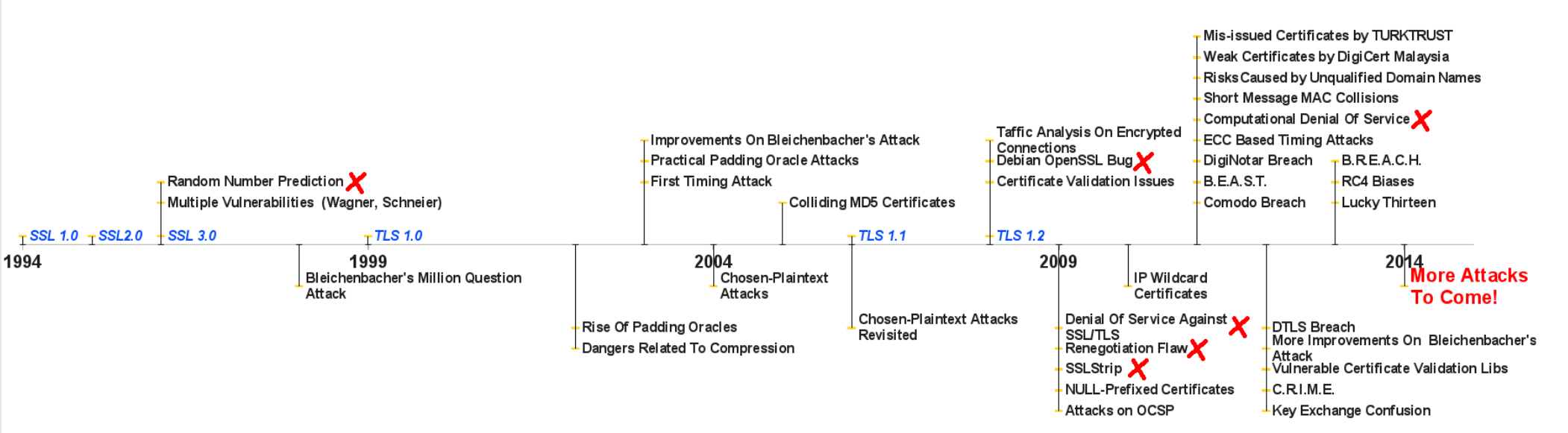
Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**
  - **Guess Random Numbers**
  - **Affect Reliability**
  - **Smuggle Data into Running Connections**
  - **P**

Various Other Attacks
Details

- **Main goal: Predict, Disturb, Inject, Disable**
  - **Guess Random Numbers**
  - **Affect Reliability**
  - **Smuggle Data into Running Connections**
  - **Prevent Traffic Encryption (disable SSL/TLS)**

Various Other Attacks
Details



Finally...

… I tried to put the keywords in a meaningful context

Finally...

… I tried to put the keywords in a meaningful context

unfortunately without success

Lessons Learned 1/2

… what can we conclude?

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**
2. **Side channels may appear at different layers in different situations**

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**
2. **Side channels may appear at different layers in different situations**
3. **Reliable cryptographic primitives are important**

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**
2. **Side channels may appear at different layers in different situations**
3. **Reliable cryptographic primitives are important**
4. **Processes must leak as little information as possible**

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**
2. **Side channels may appear at different layers in different situations**
3. **Reliable cryptographic primitives are important**
4. **Processes must leak as little information as possible**
5. **Specifications have to be implemented without own improvements**

Lessons Learned 1/2

… what can we conclude?

1. **Theoretical attacks can turn into practice**
2. **Side channels may appear at different layers in different situations**
3. **Reliable cryptographic primitives are important**
4. **Processes must leak as little information as possible**
5. **Specifications have to be implemented without own improvements**
6. **Critical parts in specifications and source code have to be highlighted**

Lessons Learned 2/2

… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**

Lessons Learned 2/2

… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**
8. **Details on requirements and preconditions are necessary**

Lessons Learned 2/2

… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**
8. **Details on requirements and preconditions are necessary**
9. **Data has to be protected**

Lessons Learned 2/2

… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**
8. **Details on requirements and preconditions are necessary**
9. **Data has to be protected**
10. **The interplay between different layers must be part of the security analysis**

Lessons Learned 2/2

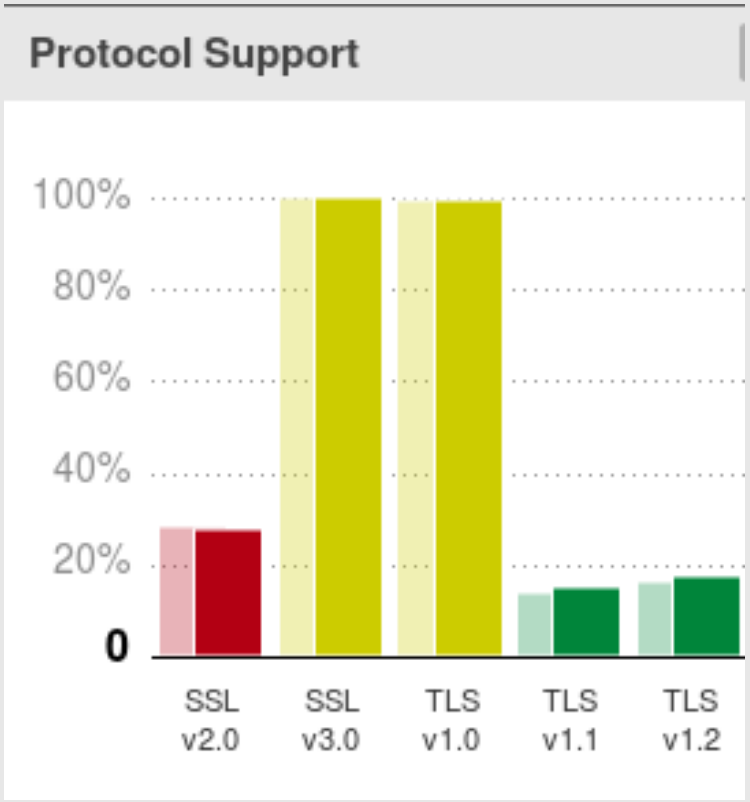
… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**
8. **Details on requirements and preconditions are necessary**
9. **Data has to be protected**
10. **The interplay between different layers must be part of the security analysis**
11. **Flexibility mostly means additional risks**

Lessons Learned 2/2

… what can we conclude?

7. **Specifications have to verbose, unambiguous and technically detailed**
8. **Details on requirements and preconditions are necessary**
9. **Data has to be protected**
10. **The interplay between different layers must be part of the security analysis**
11. **Flexibility mostly means additional risks**
12. **Always be careful and alarmed**



Source: https://www.trustworthyinternet.org/ssl-pulse/

hgi NDS **Chris Meyer**
christopher.meyer@rub.de

http://armoredbarista.blogspot.com
http://www.nds.rub.de/chair/people/cmeyer
@armoredbarista