Impuls-Workshop vom 6.2.2018:

Fernmeldeüberwachung: Wohin geht die Reise?

Verschlüsselte Daten lesen: Möglichkeiten und Grenzen

www.cnlab.ch

Das Kerkhoff-Prinzip

Das Kerckhoffs'sche Prinzip ist der zweite der sechs Grundsätze zur Konstruktion eines sicheren Verschlüsselungsverfahrens, die Kerckhoffs 1883 in *La cryptographie militaire* einführt. ...

- Das System muss im Wesentlichen (…) unentzifferbar sein.
- Das System darf keine Geheimhaltung erfordern (…).
- Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (…).
- Das System sollte mit telegraphischer Kommunikation kompatibel sein.
- Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.
- Das System muss einfach anwendbar sein (…).

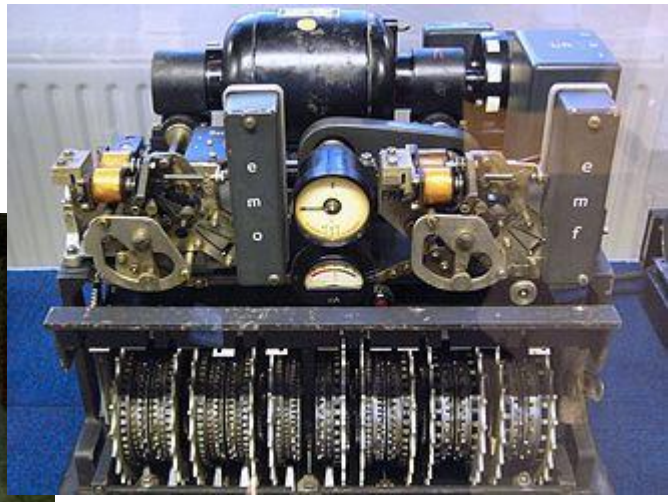
https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

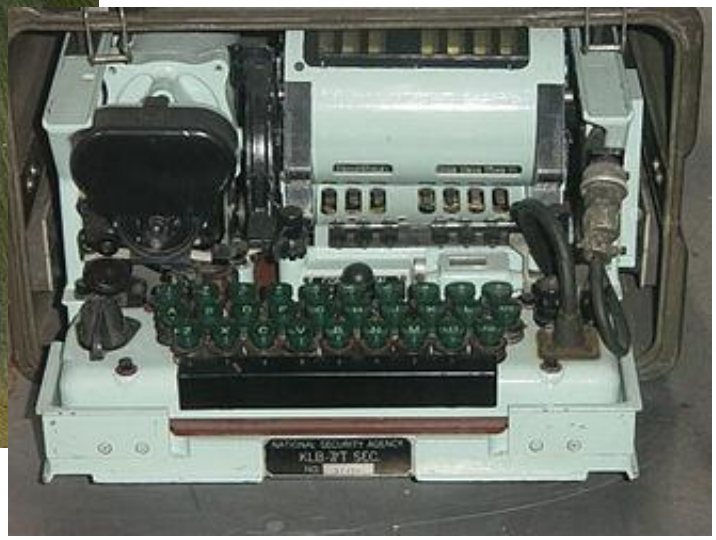
Chiffrierverfahren heute

Symmetrische Verfahren: Chiffrier- und Dechiffrierschlüssel sind gleich

Asymmetrische Verfahren:
(Public-Key-Verfahren) Chiffrier- und Dechiffrierschlüssel sind verschieden

Die traditionellen Verfahren (vor 1960)





Die aktuellen Verfahren: Standardis

Ohne Kenntnis des Schlüssels kann man moderne Verfahren nicht brechen

Jahr	Bezeichnung	Key	Bemerkung
1975	DES	56 Bit	IBM (NIST)
	3DES	112 bzw. 168 Bit	NIST
1990	IDEA	128 Bit	ETH/Ascom
2001	AES	128/256 Bit	NIST
1977	RSA	flexibel	Chiffrierung und Signaturen
1976	Diffie/Hellman	flexibel	Schlüssel-Austausch

Wie kommt man zum Schlüssel?

1. Auslesen des Schlüsselspeichers
2. Erraten des Schlüssels

- Windows
- Unix/Linux
- Alte Smartpones

2018: Spectre Meltdown

- Kurze Schlüssel
- Schnelle Prüfung

3. Schwachstellen in den Krypto-Protokollen
   a. Auslesen von Schlüssel-Teilen
   b. Einspeisen eigener (bekannter) Schlüssel

- SSL/TLS-Schwächen

2017: ROBOT Attack

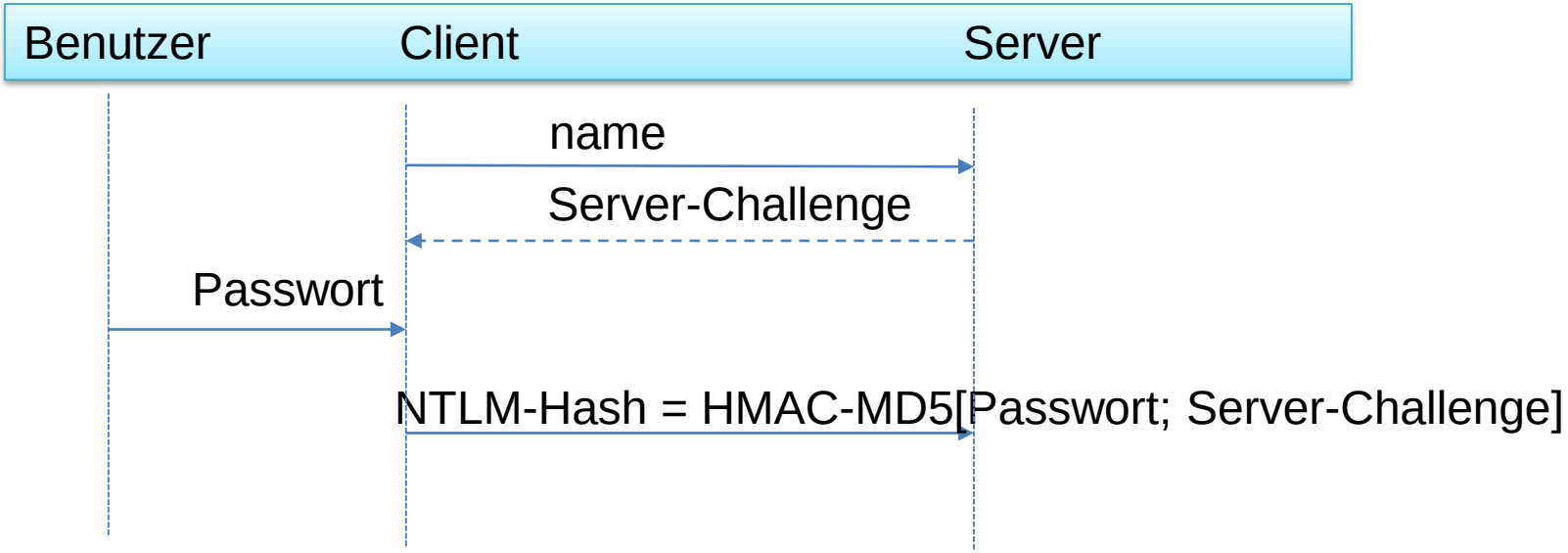
- PK-Systeme
- WhatsApp

Was ist eine «schnelle Prüfung»

Methode	Anwendung	#Prüfungen	Bemerkung
Passwort-Suche im Web	E-Banking	5 pro Stunde	Limiten im Server
PIN-Suche im Smart-Phone	Angriff	10 maximal	Limiten im Phone
PIN-Suche bei vorhandenem PIN-Hash	Analyse von alten Smart-Phones oder von Windows-Hashes	10^{11} pro Sekunde	Auf Spezial-PC mit Grafikkarten
Passwort-Suche mit vorberechneter Hash-Tabelle	Analyse von Windows-Hashes	n/a	Bruchteil von Sek, falls der PW-Hash in der Tabelle ist

PIN- oder Passwortsuche «mit Hash»

Beispiel: NTLM-Authentisierung



- Der Angreifer liest den NTLM-Hash und das Server-Challenge und möchte das Passwort kennen.
- Er rechnet den NTLM-Hash für alle möglichen Passwörter, bis er den richtigen gefunden hat.

Hashcat-Performance

sagitta>

sales@sagittahpc.com

Home | Hardware | Software | Engineering | Support | Why Sagitta? | Company

Brutalis

Brutalis is an eight-GPU monster, clawing its way through hashes at unprecedented speeds. Providing up to eight Nvidia GTX GPUs, two Intel Xeon E5-2600 v4 CPUs, up to 3TB ECC memory, and up to 18TB of SSD storage, the Brutalis is the fastest, meanest, most hardcore password cracker money can buy. Ships with a 3-year warranty and full commercial support.

Base configuration price: 21,169.00 USD

8x Nvidia GTX 1080 Hashcat Benchmarks

Product: Sagitta Brutalis 1080 (PN S3480-GTX-1080-2697-128)

Software: Hashcat v3.00-beta-145-g069634a, Nvidia driver 367.18

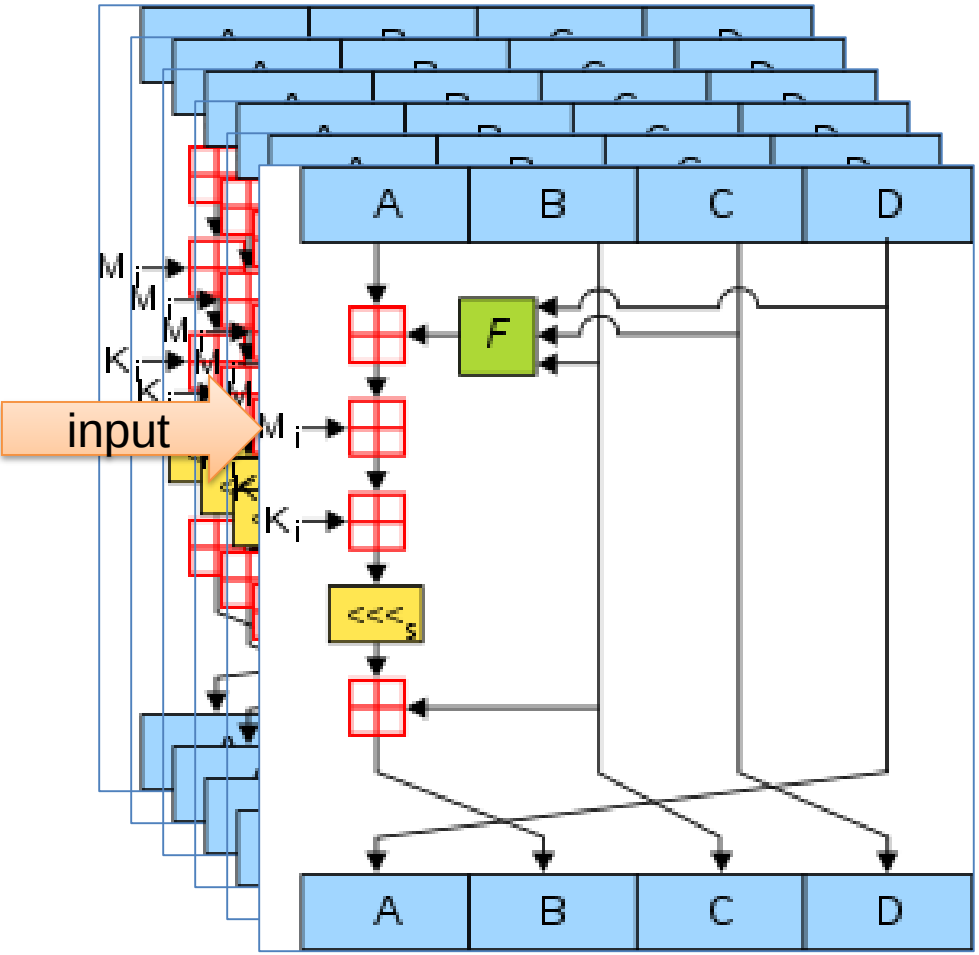
Accelerator: 8x Nvidia GTX 1080 Founders Edition

Highlights

1. World's fastest 8-GPU system -- 14% faster than 8x GTX Titan X OC!
2. First system to break 330 GH/s on NTLM -- will easily break 350 GH/s with OC!
3. First system to break 200 GH/s on MD5!

1 GH/s = 10^9 H/s

Beispiel: MD5-Hash



MD5 besteht aus 64 Operationen dieses Typs, gruppiert in 4 Durchläufen mit jeweils 16 Operationen.

F ist eine nichtlineare Funktion.

M_i ist ein 32-Bit-Block des Eingabestroms und K_i eine Konstante (pro Operation).

«<<<$_s$» bezeichnet die bitweise Linksrotation um s Stellen, wobei s für jede Operation variiert.

«+» bezeichnet die Addition modulo 2^{32}.

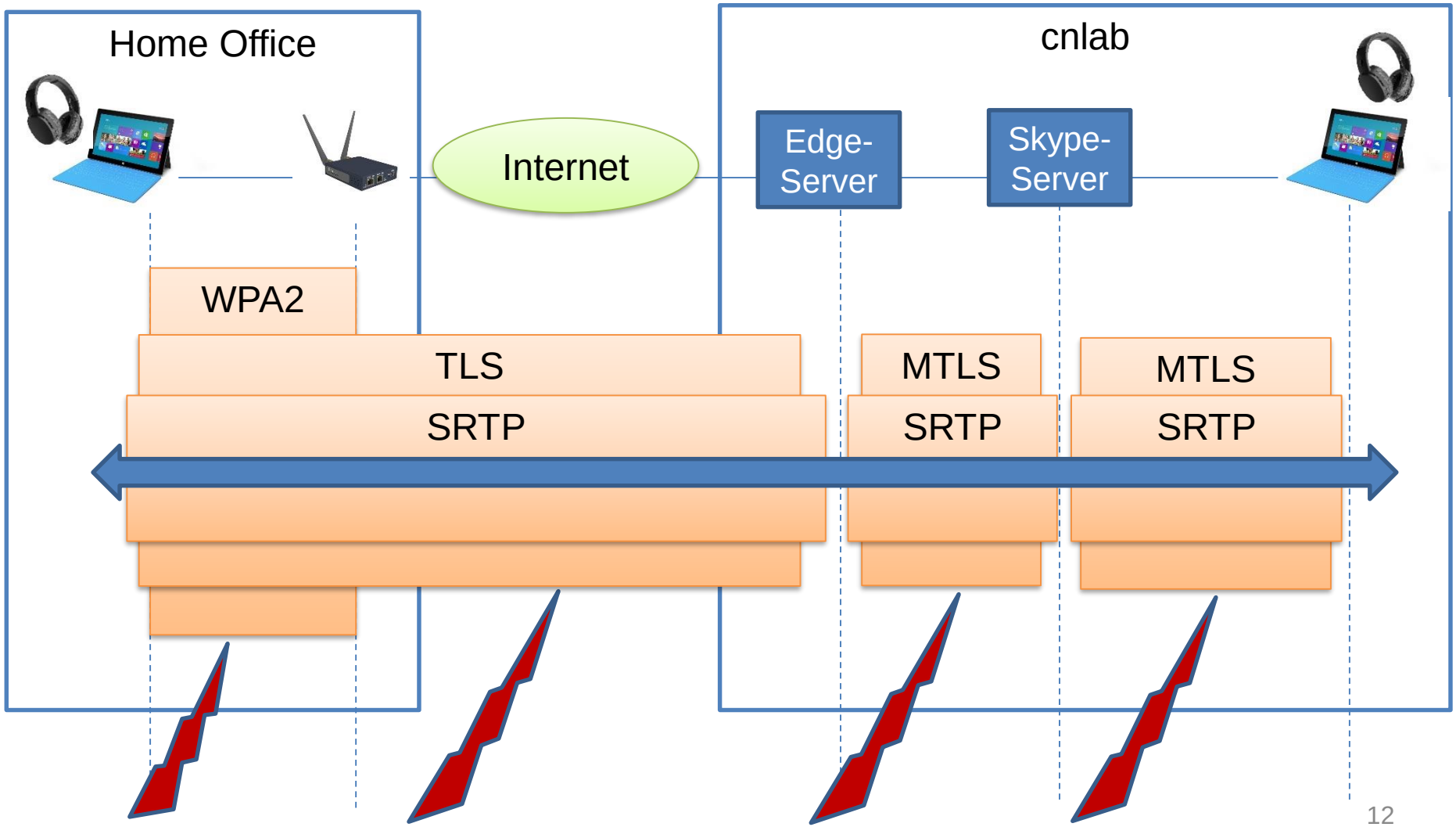
Quelle: https://de.wikipedia.org/wiki/Message-Digest_Algorithm_5

Was findet man mit einer schnellen Prüfung?

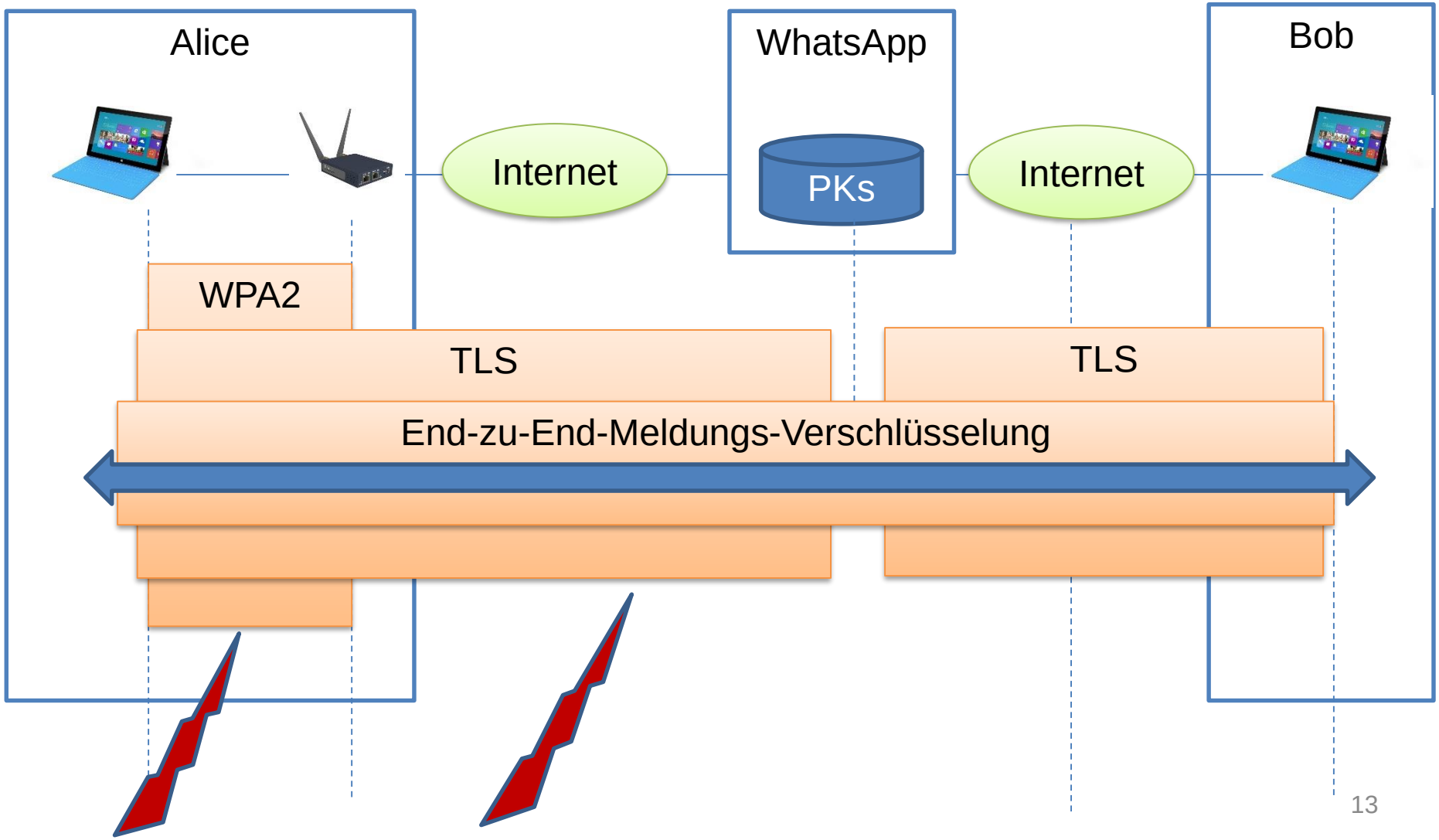
- Eine 6-stellige PIN hat 1 Million Möglichkeiten. Die Suche dauert einige Mikrosekunden.
- Ein 6-stelliges Passwort hat 10^{11} Möglichkeiten. Die Suche dauert eine Sekunde.

- Ein 56-Bit-Schlüssel hat 10^{17} Möglichkeiten. Die Suche dauert 10^{6} Sekunden oder 8 Tage.
- Ein 128-Bit-Schlüssel hat 10^{38} Möglichkeiten. Die Suche dauert 10^{27} Sekunden oder 10^{20} Jahre oder 10^{10} mal so lang wie das Universum alt ist.

Mehrstufige Verschlüsselung: Beispiel Skype for Business



Mehrstufige Verschlüsselung: Beispiel WhatsApp



Fazit

- Moderne Krypto kann man nicht brechen.
- In modernen Systemen haben Telecom-Provider keinen Zugriff auf Klartext.

- PIN oder Passwort-Suchen führen zum Ziel, wenn man Hashes hat.
- Schlüssel-Suchen dauern zu lang.

- Krypto-Protokolle haben immer wieder Schwächen, welche **Zugriff auf die Schlüssel** ermöglichen.

Danke

Paul Schöbi
paul.schoebi@cnlab.ch
+41 55 214 33 33