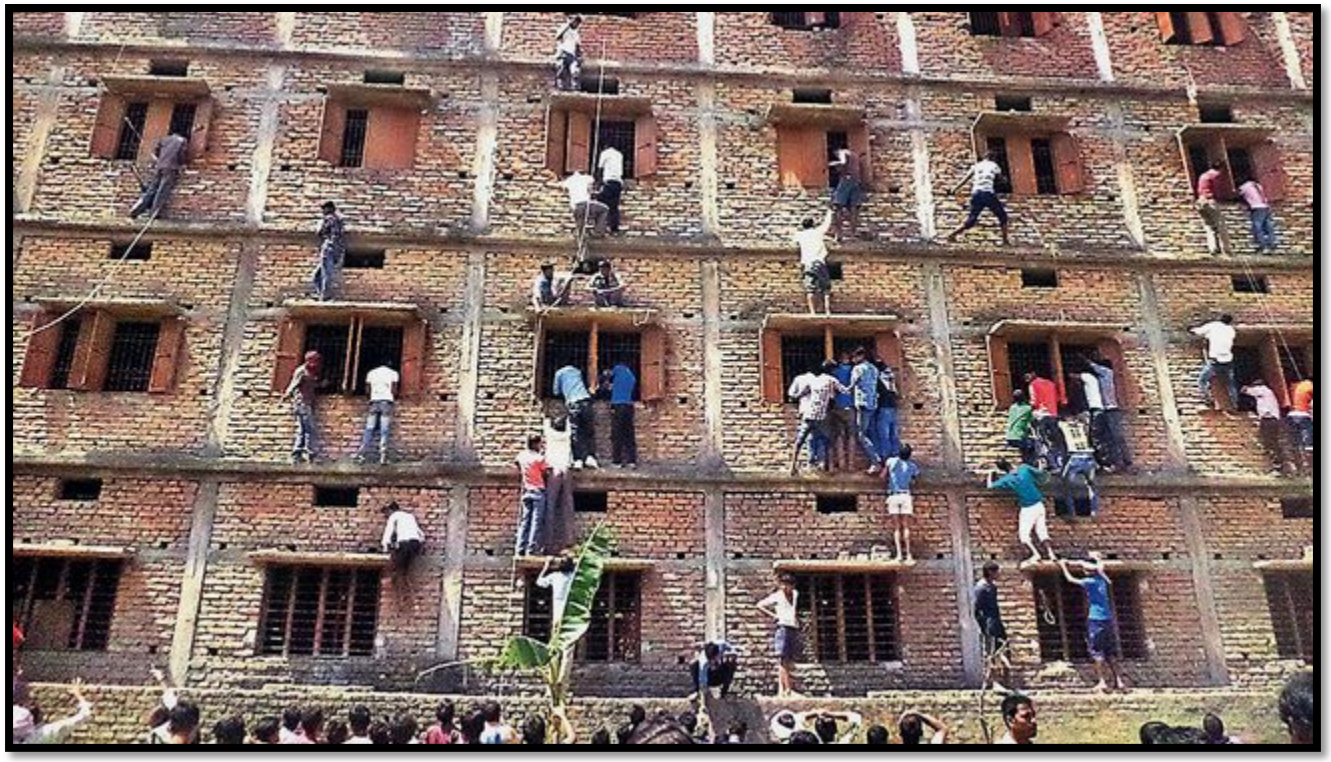
Tutorial zur Collaborated Security 8 Agenten in einem Pass Space

Wie kann die defensive Strategie der immer höheren Burgmauern und tieferen Gräben überwunden werden?

Ulf Ziske, CEO, KikuSema GmbH
Sophie Ziske, Schülerin, IT Gymnasiet Skövde/Schweden

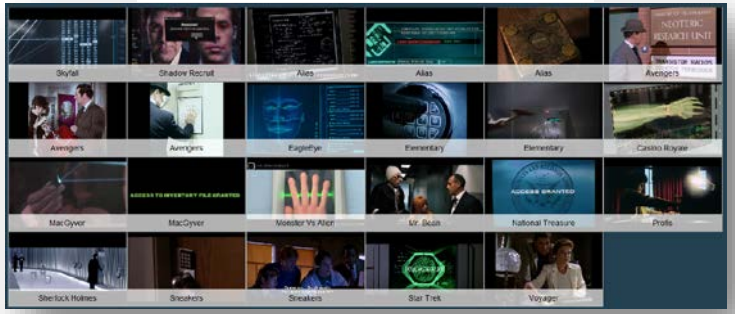
Start

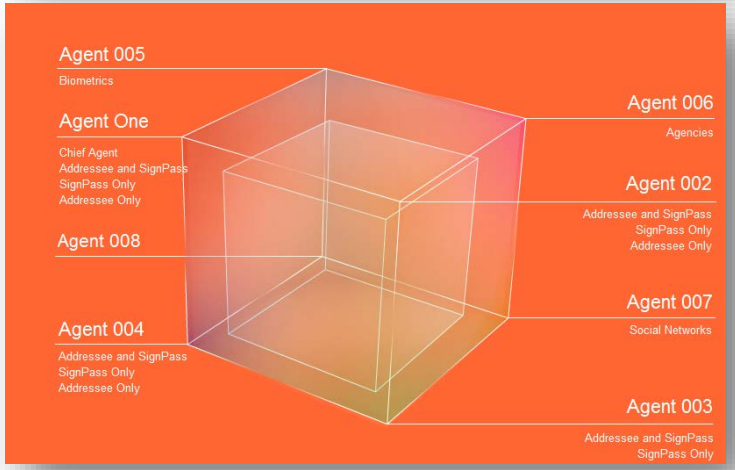


Quelle: 2015 - SVT.SE

Was passiert da?

Überblick





- Paradigma Wechsel – Sensibilisierung
- Security Technologie in Filmen

Urheberrecht: Die Filmausschnitte werden nur zu Ausbildungs- und wissenschaftlichen Zwecken verwendet - Die ausgewählten Teile beziehen sich ausschließlich auf IT Security und Authentifizierung - Es wird keine Beurteilung der Inhalte vorgenommen, vielmehr handelt es sich um einen Ausschnitt unserer Zeitgeschichte.

- Sicherheit durch Zusammenarbeit (Collaborated Security)
- Live Vorführung – Tutorial Scrambled Secret (ScramSec)

Paradigma Wechsel

- Collaborated Security – Sicherheit durch Zusammenarbeit
  vs. Keyhole Security
- Multi-Instanz- Authentifizierung (8 Agenten)
  vs. Multifaktor – Authentifizierung
- Entropie & PassSpace
- Grafisches Interface
- Fünf neue Protokolle
- Scrambled Secrets - Verschlüsselung durch Vermischung
  (vs. Security through Obscurity)

Security: Collaboration vs. Keyhole

Die meisten Authentifizierungsmethoden liefern als Ergebnis der Validierung nur ein **„Wahr“** oder **„Falsch“.**

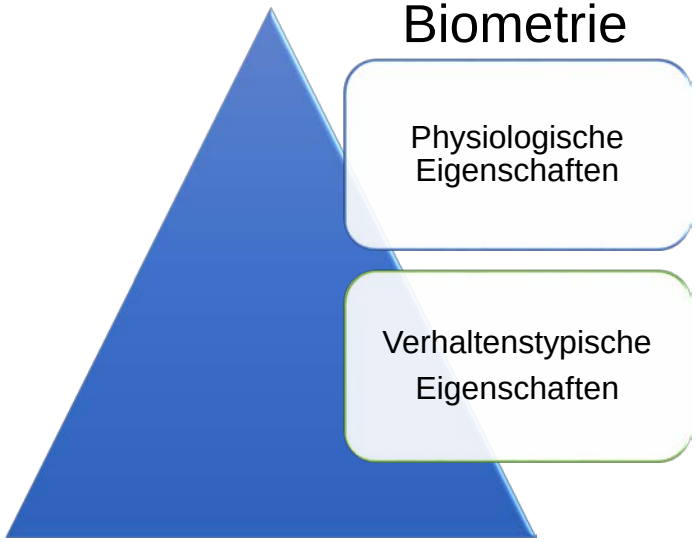
Das ist leicht zu hacken!

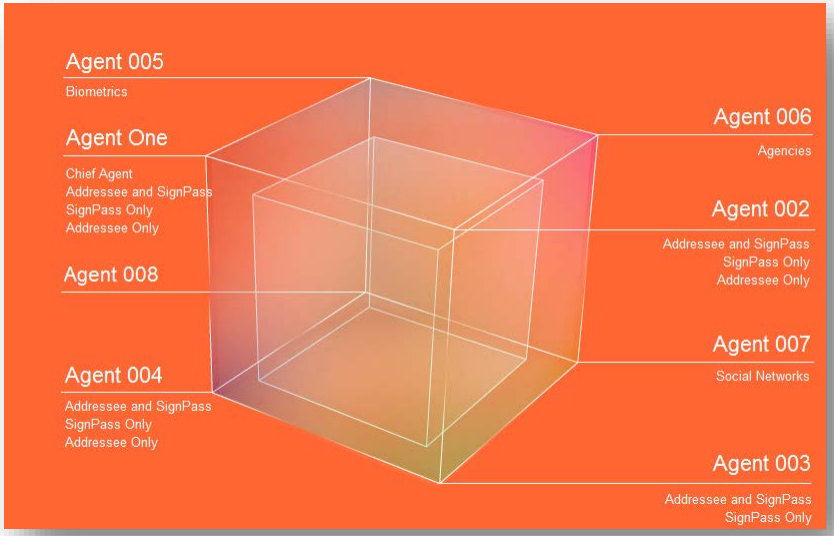
Es gibt nur einen Platz oder einen Zugang zu hacken.
Hat man erstmal den Zutritt, hat man Zugang zu allen „Geheimnissen“.

Das ist vergleichbar damit, eine **Burg** mit einer **Tür aus Pappe** zu schützen.

Quelle:RSAC2015 - 21.04.2015

Authentifizierung: Multi-Instanz vs. Multifaktor





Entropie & PassSpace (1)

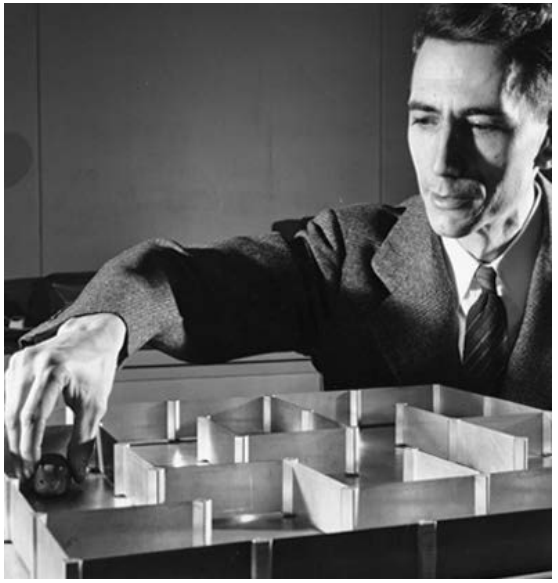
Kerckhoffs' Prinzip 1883 Quelle

Das Kerckhoffs'sche Prinzip ist der zweite der sechs Grundsätze zur Konstruktion eines sicheren Verschlüsselungsverfahrens, :

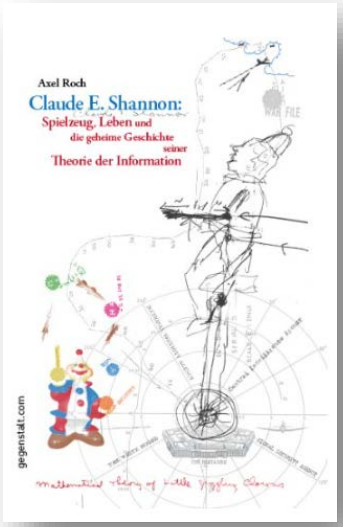
- Das System muss im Wesentlichen (…) unentzifferbar sein.
- Das System darf keine Geheimhaltung erfordern (…).
- Es muss leicht übermittelbar sein und **man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können** (…).
- Das System sollte mit telegraphischer Kommunikation kompatibel sein.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

Entropie & PassSpace (2)

Claude Elwood Shannon - Jongleur der Wissenschaft



$$\mathrm{H} = -\sum_i p_i \cdot \log_2 p_i \quad [\mathrm{Sh}]$$



Shannon (abgekürzt: **Sh**) ist die nach dem amerikanischen Mathematiker und Begründer der Informationstheorie Claude Elwood Shannon benannte Einheit für den Informationsgehalt einer Nachricht.

Entropy is as a mathematical criterion of the sufficient randomness

„You should call it entropy. Nobody knows what entropy really is, so in a debate you will always have the advantage."

J. VON NEUMANN

Entropie & PassSpace (3)

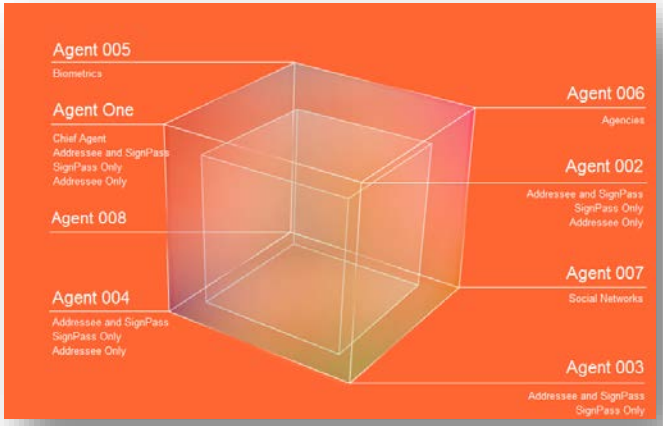
Entropie = 21.560

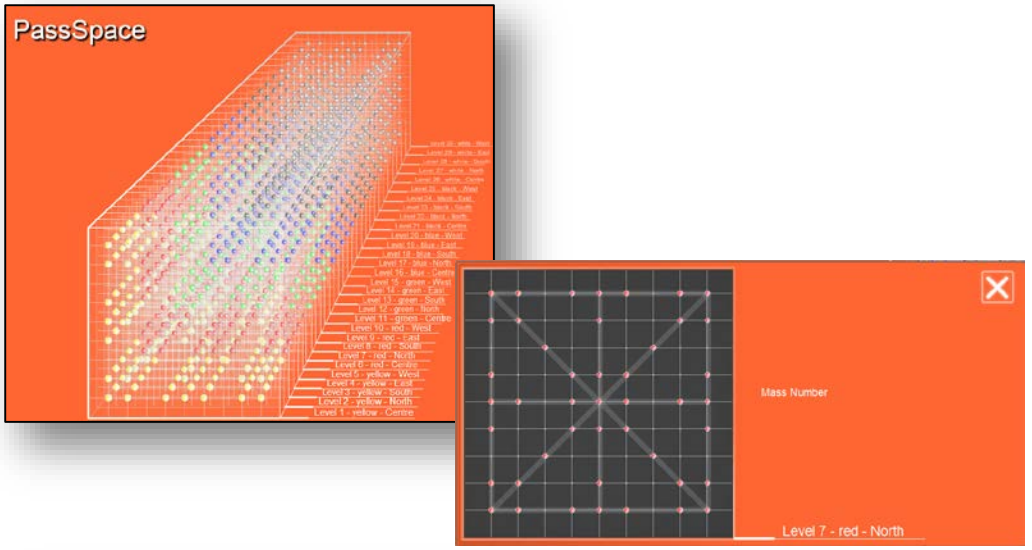
Theoretische Grenze
1350 Zeichen
aus dem UTF16 Zeichensatz
mit 65.535 Zeichen

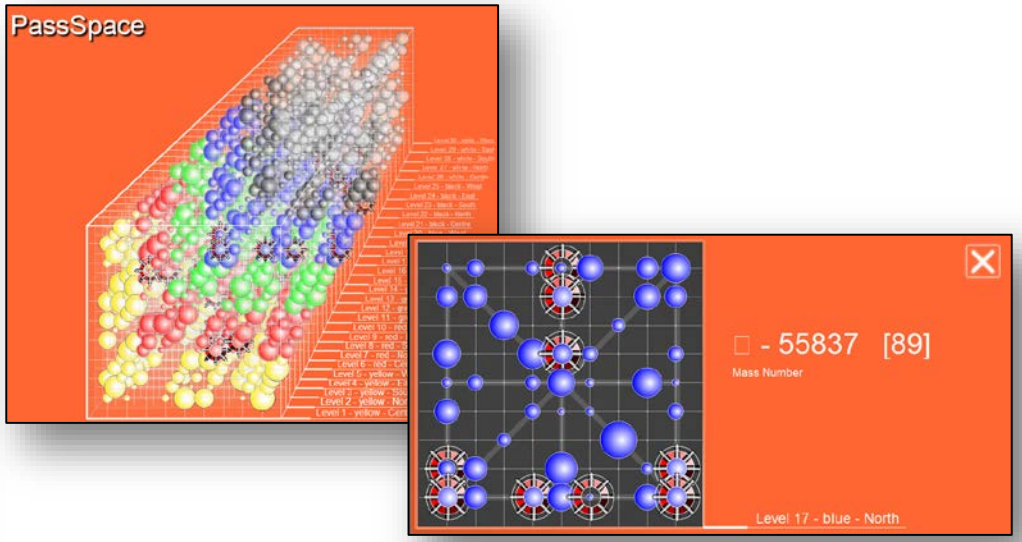
65.535 Zeichen ^{1350}

= 1,7 e+6502

(ZPR:6471)

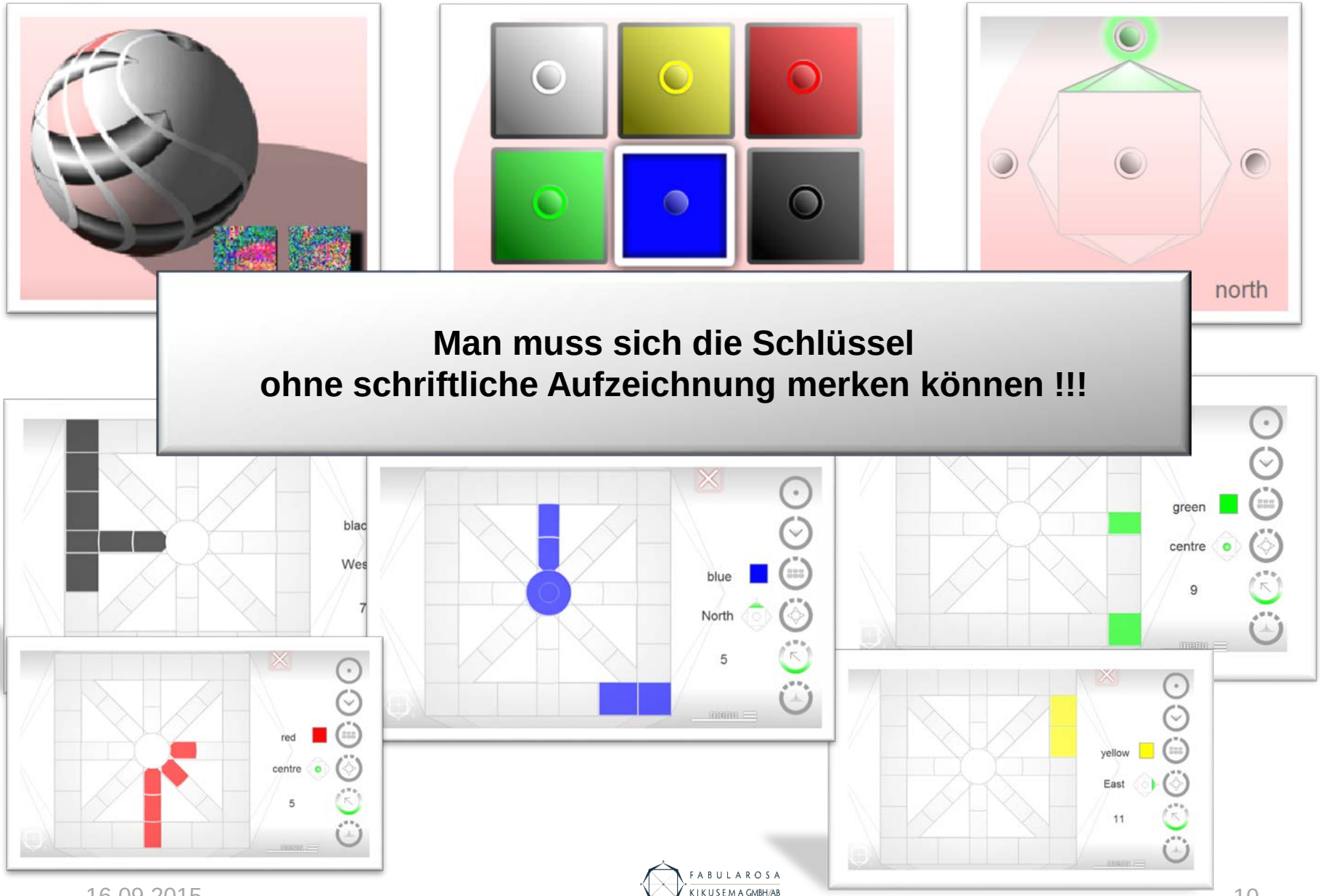






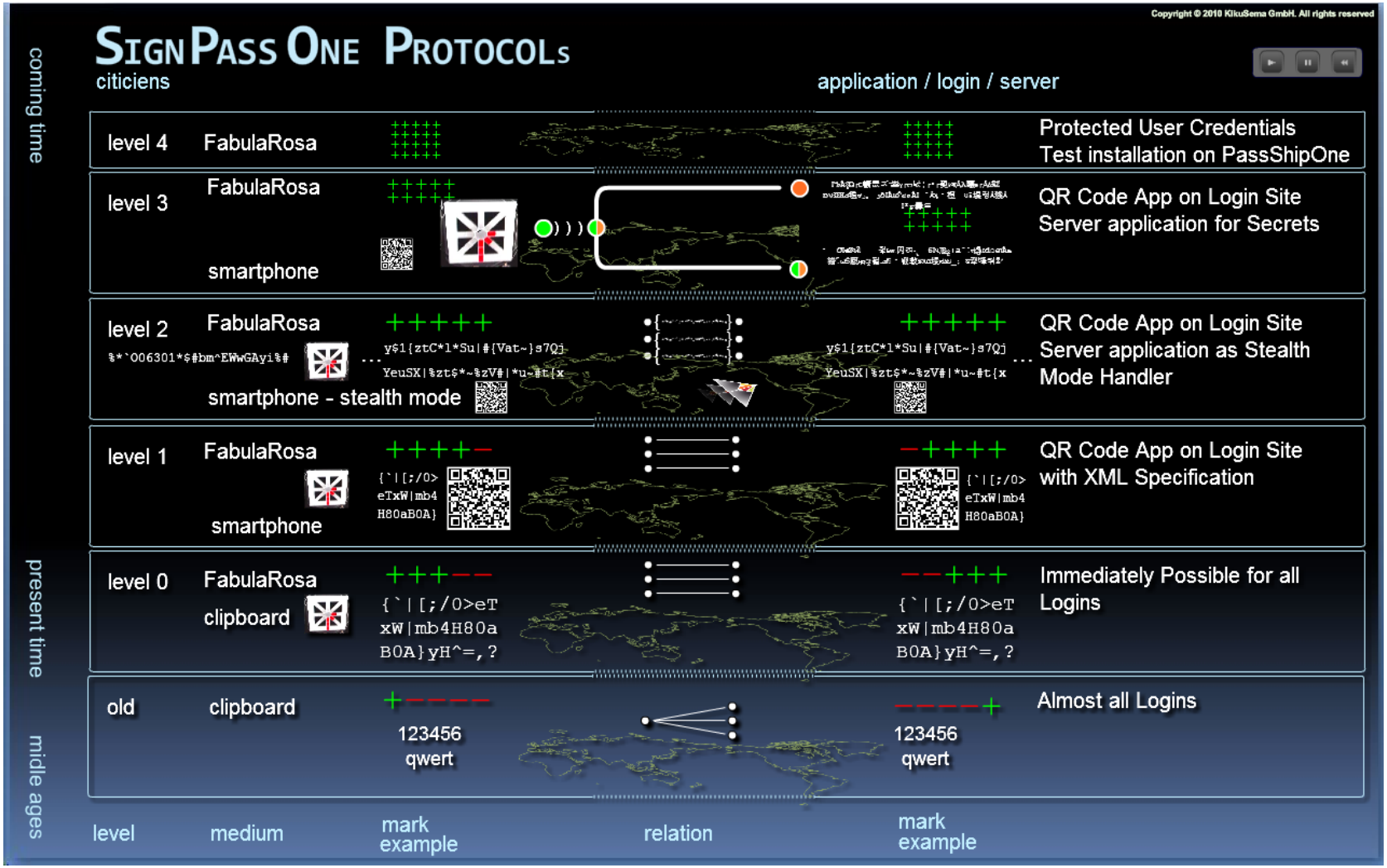
* ZPR = Z password range with a Standard Unit = 1.26821 e+31

Grafisches Interface



Man muss sich die Schlüssel
ohne schriftliche Aufzeichnung merken können !!!

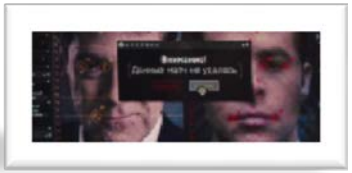
5 neue Protokolle



Level 5: Multi Instance Authentication/Scrambled Secrets

Scrambled Secrets

Verschlüsselung durch Vermischung vs. Security through Obscurity



Talking ’bout My Next Generation

Schützenswerte Güter eines Teenagers

Virtuelle Zukunft
Hatsune Miku

Tutorial - Live-Demo

Nicht wie man etwas hackt,
sondern wie mehrere Agenten bzw. Instanzen
gemeinsam
eine Authentifizierung durchführen
und wie man
den Zugang zu "schützenswerten Gütern"
sicherer machen kann.

Bruce Schneier – The Generation Gap

The **Internet** is the greatest generation gap since rock and roll,
and what we're seeing here is one particular skirmish across that gap.
The **younger generation**, used to spending a lot of its life in public,
clashes with an older generation in charge of a corporate culture
that presumes a greater degree of discretion and greater level of control.
There are two things that are always true about generation gaps.
The first is that the elder generation is always right about the problems
that will result from whatever new/different/bad thing
the younger generation is doing.
And the second is that the younger generation is always right that
whatever they're doing **will become the new normal**.
These things have to be true; the older generation understands the problems better,
but they're the ones who fade away and die.

Zusammenfassung

Wie kann die defensive Strategie der immer höheren Burgmauern und tieferen Gräben überwunden werden?

- Paradigma Wechsel
- Collaborated Security – Sicherheit durch Zusammenarbeit
- Multi-Instanz- Authentifizierung
- CYOP
- Scrambled Secrets - Verschlüsselung durch Vermischung

Welcomes the Paradigm Shift

Escaping Security's Dark Ages
Quelle: 21.04.2015

The Games has changed
Quelle: 22.07.2015

- "Building taller walls and digging deeper moats is not solving our problems"
- < 1% of successful advanced threats are spotted by SIEM Systems
- Identity and authentication matter more
- "… we run a path to change the paradigm under which the security industry has operated for decades. At RSA, we starting with ourselves."
- "We have sailed off the map…"
- "This is not a technology problem; this is a mindset problem"
- The game has changed – we must change too

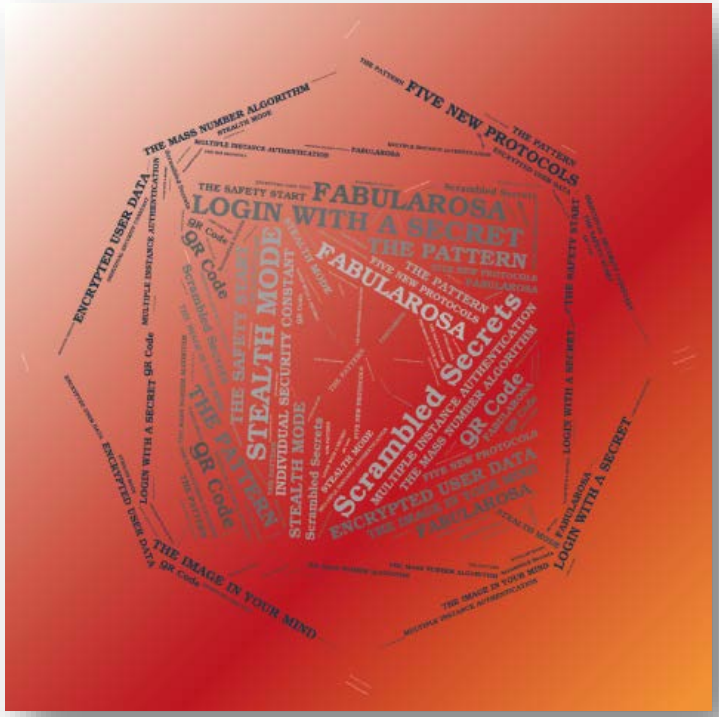
Welcomes the Paradigm Shift

…
Recently, the head of the National Security Agency provided a rare hint of what some U.S. officials think might be a technical solution. Why not, suggested Adm. Michael S. Rogers, require technology companies to create a digital key that could open any smartphone or other locked device to obtain text messages or photos, but divide the key into pieces so that no one person or agency alone could decide to use it?

"I don't want a back door," Rogers, the director of the nation's top electronic spy agency, said during a speech at Princeton University, using a tech industry term for covert measures to bypass device security. "I want a front door.
And I want the front door to have multiple locks. Big locks."

Quelle: 10.04.2015 The Washington Post

Welcomes the Paradigm Shift



A new kind of security a so called Multi-Instance-Mode is necessary

- Collaborate Security
  Mixture of trust, control and functioning when interests coincide
- Multi-Instance-Authentication vs. Multi-factor-Authentication
- Overcoming of the limitation caused by Keyhole-Security
- Claim your Own Privacy (CYOP) guaranteed by the government
- **Absolute part**: The impact of the intellectual power of human beings

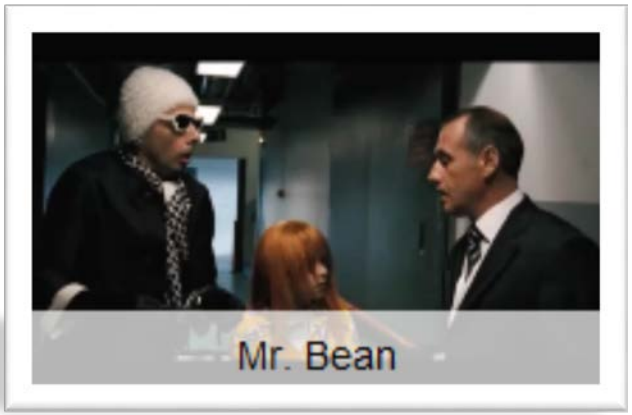
Quelle: 20.04.2015

Zum Schluss

Zwei vergnügliche Beispiele:

- MovieClip:
  Monsters vs. Aliens

- MovieClip:
  Mr. Bean macht Ferien



Zum Schluss - Dank

Vielen Dank für Ihre Aufmerksamkeit.

BOARDING PASS: J2M2216308717070

Zum Schluss – Die Zukunft beginnt jetzt

Difference between the knowing the path and walking the path

NASA'S JOURNEY TO MARS

Christine, Sophie, Ulf Ziske Your name will fly on INSIGHT Mission to Mars

BOARDING PASS: J2M2216308717070