Institut für Informatik

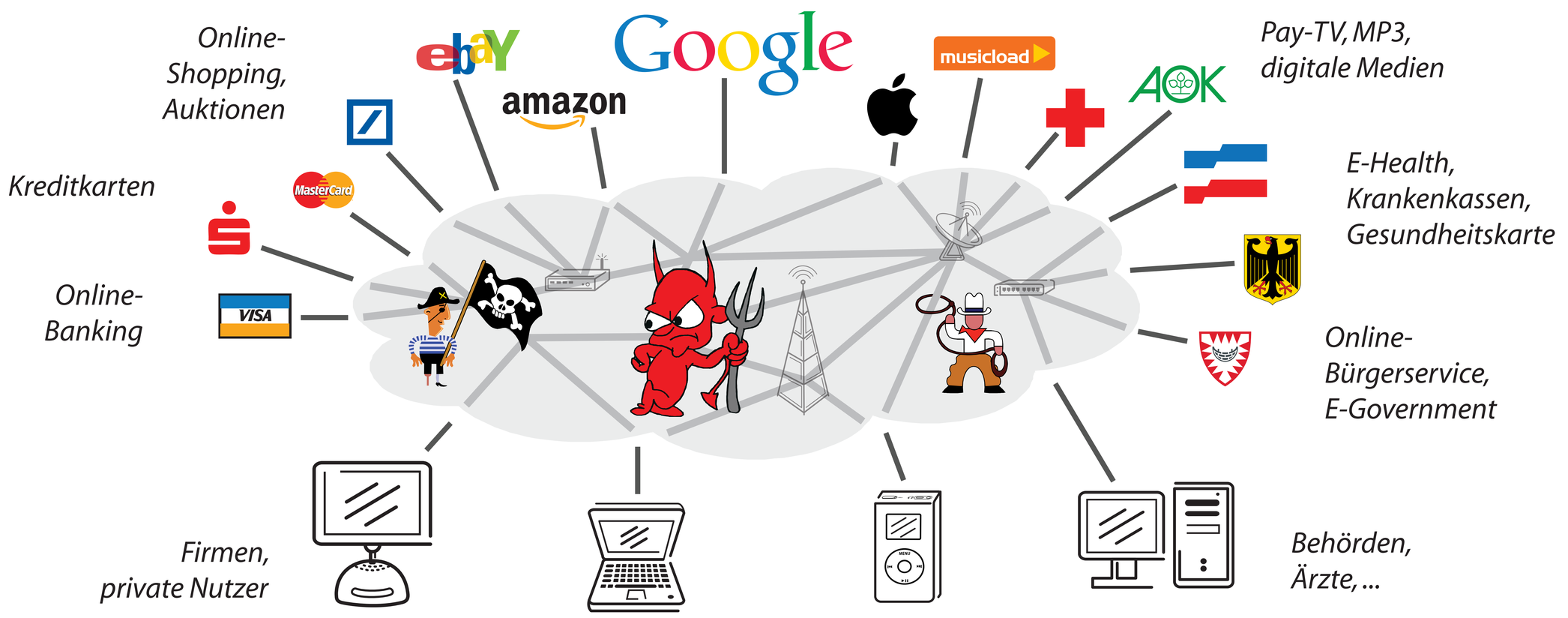
C | A | U

Christian-Albrechts-Universität zu Kiel

Technische Fakultät

Institut für Informatik

Arbeitsgruppe Theoretische Informatik



Wie schützt man digitale Kommunikation?

Sicherheitsbegriffe & -modelle

Entwicklung von mathematisch exakten Sicherheitsbegriffen und -modellen, beispielsweise für

– Vertragsabschlussprotokolle
– Web Services
– Authentifizierung

Analysemethoden & -werkzeuge

Entwicklung automatischer Verfahren für Sicherheitsanalysen von Protokollen, unter anderem basierend auf

– Termersetzungssystemen
– Model Checking
– endlichen Automaten

Designkriterien & -methodiken

Methoden

– zum modularen Entwurf sicherer kryptographischer Protokolle
– zur sicheren Komposition von kryptographischen Protokollen

Entwicklung einer grundlegenden Theorie der Sicherheit von Computersystemen und -netzwerken

Kryptographie | Komplexitätstheorie | Deduktion | ... | mathematische Logik | formale Methoden

Prof. Dr. Thomas Wilke
Arbeitsgruppe Theoretische Informatik
Christian-Albrechts-Universität zu Kiel
Olshausenstraße 40, 24098 Kiel
Tel.: +49 (0)431 880-7511
Fax: +49 (0)431 880-7614
wilke@ti.informatik.uni-kiel.de
http://www.ti.informatik.uni-kiel.de/

Priv.-Doz. Dr. Ralf Küsters
Arbeitsgruppe Theoretische Informatik
Christian-Albrechts-Universität zu Kiel
Olshausenstraße 40, 24098 Kiel
Tel.: +49 (0)431 880-7508
Fax: +49 (0)431 880-7614
kuesters@ti.informatik.uni-kiel.de
http://www.ti.informatik.uni-kiel.de/

INFORMATIK JAHR
Wissenschaftsjahr 2006

Gestaltung: Klaas Ole Kürtz