



Mediensicherheit

Jana Dittmann

Andreas Lang, Claus Vielhauer

Otto-von-Guericke Universität Magdeburg

Arbeitsgruppe Multimedia and Security



Gliederung

- Sicherheitsaspekte
- Konzepte: Technikgestaltung zur Vertrauensbildung
 - Kryptographie, Steganographie und Wasserzeichen
 - Biometrische Benutzerauthentifizierung
- Zusammenfassung und Ausblick



Motivation

Bilder die lügen

Ein Alphabet der Lügen

- A wie Aktuelles:** Unter dem Titel „Ein Land wie im Krieg“ veröffentlicht der Schweizer „Blick“ ein Foto aus dem ägyptischen Theben, auf dem aus einer Wasserpflanze eine Blutlache wird.
- B wie Born, Michael:** Der freie Journalist verkauft mehreren Fernsehsendern gefälschte Bilder von angeblichen Mitglieder der PKK bei der Vorbereitung von Terroranschlägen
- C wie Comics:** Die deutschen Verlage betreiben teilweise Selbstzensur und lassen Granaten durch Steine ersetzen oder einen Gehängten durch Sprechblasen verdecken.
- D wie Damantio memoriae:** Auslöschung der Erinnerung durch Bildersturm.
- E wie Entnazifizierung:** Der badische Maler Adolf Riedlin beispielsweise übermalt drei Jahre nach dem Zweiten Weltkrieg sein Fresko von 1937, weil dort der Hitlergruß zu sehen ist.
- F wie Führermythos:** Sowohl Hitler, als auch Stalin und Mussolini ließen sich durch Fotomontagen verherrlichen, etwa auf Postkartenserien in staatsmännischer Darstellung.
- G wie Golfkrieg:** Das US-Verteidigungsministerium lässt nur ausgewählte Journalisten („Pool“) ins Sperrgebiet; sämtliche Bilder durchlaufen eine Vorzensur.
- H wie Hitler-Tagebücher:** Der „Stern“ veröffentlicht am 25. April 1983 die angeblichen Tagebücher Adolf Hitlers. Dass es sich um eine Fälschung handelt, stellt sich bald heraus.
- I wie Ikonen:** Was den Sowjets die rote Fahne auf dem brennenden Reichstag, war den Amerikanern die Siegesfahne auf Iwo Jima – beide Aufnahmen sind gestellt.
- J wie Jugendfrei:** „Eine Zensur findet nicht statt“ (Artikel 5 Grundgesetz). Stattdessen gibt es die „Freiwillige Selbstkontrolle“ (FSK), die sittenwahrende Zensur der Fünfzigerjahre.
- K wie Kalter Krieg:** Karl-Eduard von Schnitzler riss im DDR-Fernsehen zur Propaganda Zitate westdeutscher Politiker aus dem Zusammenhang und verdrehte dabei beliebig ihre Bedeutung.
- L wie Legendenbildung:** In der Broschüre „Jeder hat eine Chance“ versucht die Bundesregierung der Bevölkerung einzureden, wer unter Tische krieche, könne einen Atomangriff überleben.
- M wie Morphing:** eine Überblendungstechnik, mit der am Computer aus dem Bild Helmut Kohls das Gesicht Gerhard Schröders werden kann.
- N wie Nazikult und Nazierbe:** Für eine Titelstory druckte „Paris Match“ 1966 eine erfundene Reportage über deutsche Nazis. Die gezeigten SS-Uniformen kamen vom Kostümverleih!
- O wie Optische Täuschung:** Schon Protagoras erkannte, dass Wahrnehmung von den menschlichen Sinnen abhängig und deswegen relativ ist.
- P wie Paragraph:** Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet werden, ausgenommen Bilder aus dem Bereich der Zeitgeschichte, so das entsprechende Gesetz von 1907.
- Q wie Querschläger:** War es oder war es kein Tor, am 30. Juli 1966 im Wembley-Stadion im Spiel Deutschland–England? Für beide Thesen gibt es „beweisende“ Fotos.
- R wie Rufmord:** Dass Bilder sich auch im Kopf evozieren lassen, beweisen die Rufmordkampagnen gegen Heinrich Lübke als „KZ-Baumeister“ und gegen Willy Brandt als „Vaterlandsverräter“.
- S wie Satire:** Bildsatire hat eine lange Tradition: Gab es früher den „Kladderadatsch“ und den „Simplicissimus“, erscheinen heute Fotomontagen im „pardon“ und der „Titanic“.
- T wie Text und Bild:** In Zeitungen werden häufig Bilder durch die Textzeilen in einen anderen als den ursprünglichen Zusammenhang gestellt.
- U wie Ufos:** eines der beliebtesten Fälschungsobjekte.
- V wie Volksaufstand:** Bilder von Deutschen im Gespräch mit sowjetischen Soldaten sollten nach dem 17. Juni 1953 den Eindruck vom Einverständnis mit der Sowjetunion erwecken.
- W wie Werbung:** Fast jede Werbeanzeige ist eine Fotomontage; viele Bilder werden darüber hinaus elektronisch verändert.
- X wie Xenophobie:** Auch Wort- und Sprachbilder wie das vom Boot, das voll sei, sind geeignet, einen bestimmten Sinn zu transportieren.
- Y wie Yellow press:** „The Mirror“ veröffentlicht ein Foto von Lady Diana und Dodi al-Fayed, die sich zu küssen scheinen. Das klappte nur, nachdem Dodis Kopf elektronisch gedreht wurde.
- Z wie Zukunft:** Sichtbare und unsichtbare Wasserzeichen in Bildern sind eine Möglichkeit, um in der Zukunft einen gewissen Schutz vor Fälschungen zu bieten.

<http://home.t-online.de/home/binomi/bilder.htm>



Weitere Beispielszenarien...

Big mistake: Sierra Vista trio wrongly accused of Maryland murder; girls missed prom, band concert while in jail

Arizona Daily Star; Tucson, Ariz.; May 20, 2003; Ignacio Ibarra;

A grainy picture from an [ATM surveillance camera](#) aired by TV's "America's Most Wanted" connected three Sierra Vista residents to a June 2002 strangulation murder of a woman in Maryland. The [mom, daughter and friend](#), authorities had said, were believed to have been trying to [use the murder victim's bank card](#). The problem with that link, investigators now concede, is that the time recorded by the camera was three minutes off the time recorded by the ATM.

[The risks should be obvious](#); critical logs should be reliably synchronized either to each other or an independent source.

Nachtrag Risks-Digest : ATM time sync (RISKS-22.73)

The arrest of the wrong party based on defective "money machine" timestamps has also occurred in the District of Columbia.



Weitere Beispielszenarien...

Gesetzesänderung in Sachsen-Anhalt

Videoüberwachung erleichtert

Jens Kolze: „Schutz der Bevölkerung hat absolute Priorität.“

Dessau/Köthen (red). Am Donnerstag hat der Landtag von Sachsen-Anhalt die Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung (SOG) beschlossen.

Dazu erklärt der innenpolitische

Sprecher der CDU-Landtagsfraktion Jens Kolze: „Im Mittelpunkt steht die Sicherheit der Bevölkerung.

In Auswirkung des neuen Gesetzes darf die Polizei in Zukunft bestimmte Plätze per Videokamera nicht nur beobachten, sondern die Geschehnisse auch auf Band aufnehmen.“

Dies diene zum einen der Über-

führung von Straftätern und zum anderen werde damit auch das objektive Sicherheitsempfinden der Bürger erhöht.

Die SPD-Fraktion hat dagegen verfassungsrechtliche Bedenken angemeldet.

Mit dem neuen Gesetz werde laut Jens Kolze außerdem auf die erhöhten Anforderungen durch den immer besser organisierten

internationalen Terrorismus reagiert.

Die Anordnung der Rasterfahndung wird durch die Abschaffung des Richtervorbehalts vereinfacht.

In Zukunft soll für solche Maßnahmen eine schriftlich begründete Zustimmung des Innenministers oder seines Stellvertreters genügen.

„Super Sonntag“ 15. Juni 2003



Defining Aphorisms of Cyberspace

The New Yorker
5 July 1993





Anonymität/Vertraulichkeit im Web ...



The New Yorker
5 July 1993



Fragestellungen

Multimedia und Security

- Technikgestaltung und Security
 - Technikauswahl
 - Technikakzeptanz bei Nutzern
 - Rechtliche Rahmenbedingungen
 - erreichbares Sicherheitsniveau
 - Security-Evaluierungen, Restrisikoanalysen
 - Anpassungen an neue Technologien und Multimedia
 - ...
- Ganzheitliche Konzepte:
 - Authentizität
 - Integrität
 - Vertraulichkeit
 - Nachweisbarkeit
 - Verfügbarkeit



Fragestellungen

Gestaltung: Multimedia und Security



Service /
Erlebnis

- Inhalte
- Kommunikation
- Speicherung
- Identifikation
- Datenschutz
- Security
- ...

Funktion

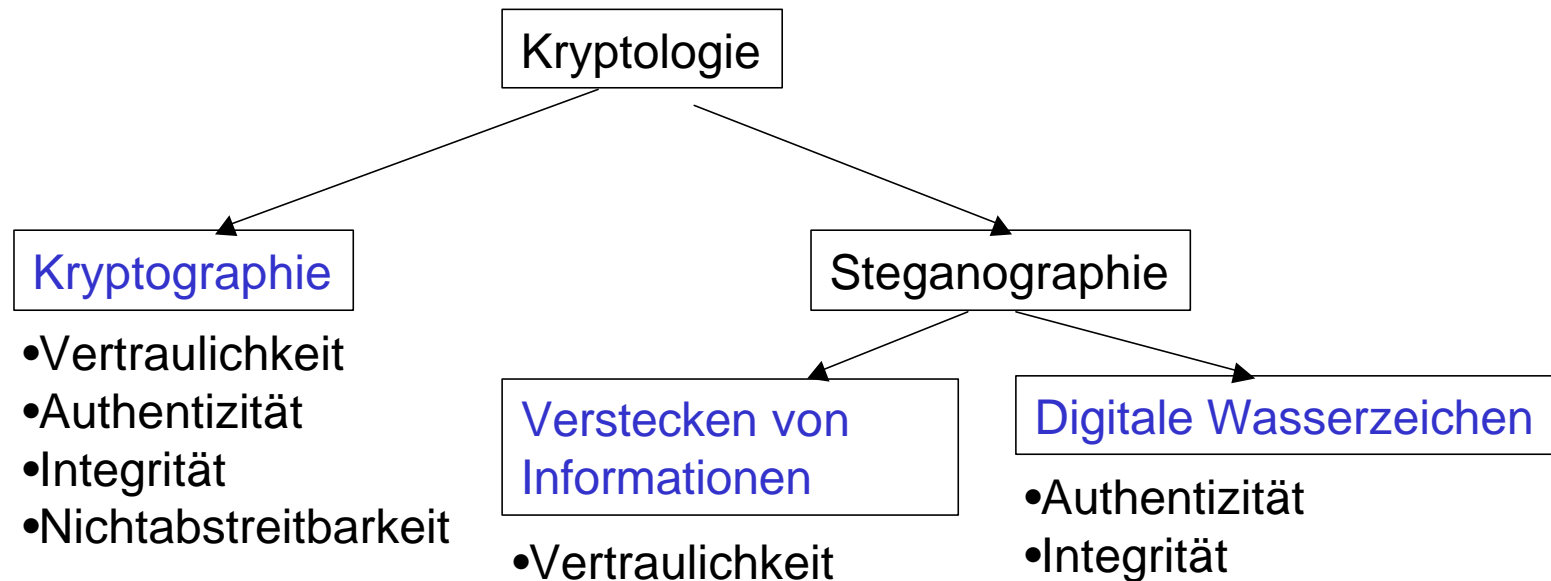
- Netzwerk
- Datenbanken
- Kryptographie
- Steganographie
- Wasserzeichen
- Biometrik
- ...

Technologie



Ganzheitliche Konzepte

Technikgestaltung zur Vertrauensbildung

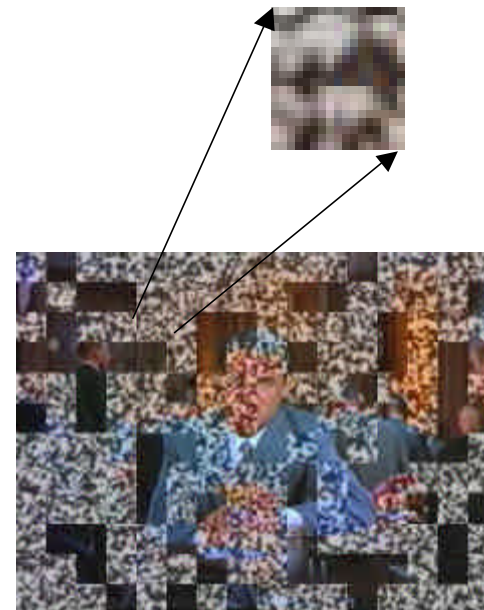




Digitale Wasserzeichen

Algorithmen und Anwendungsgebiete

- **Digitales Wasserzeichen:**
 - transparentes, nicht wahrnehmbares Muster (Signal)
 - Muster/Signal repräsentiert die eingebrachte Information, meist Zufalls-Rauschsignal (pseudo-noise signal)
 - Präsenzwasserzeichen oder Codierung von Informationsbits





Digitale Wasserzeichen

Algorithmen und Anwendungsgebiete

- Verfahren zur Urheberidentifizierung
 - Copyright Watermarks (robust)
- Verfahren zur Kundenidentifizierung
 - Fingerprint Watermarks (robust)
- Verfahren zur Durchsetzung des Kopierschutzes oder Übertragungskontrolle
 - Copy Control Watermarks (robust)
- Verfahren zum Nachweis der Unversehrtheit
 - Integrity Watermark (fragil)
- Verfahren zur Annotation des Datenmaterials
 - Caption Watermarks (robust \leftrightarrow fragil),
Illustrationswasserzeichen



Ganzheitliche Konzepte

Technikgestaltung zur Vertrauensbildung

Benutzerauthentifizierung

- durch physikalischen Besitz (Schlüssel, Chipkarte, ...)
- Durch Wissen (PIN, Passwort)
- Durch **Sein**: biometrische Merkmale (Gesicht, Fingerabdruck, Handschrift, ...)
- am besten durch eine Kombination davon



Ganzheitliche Konzepte

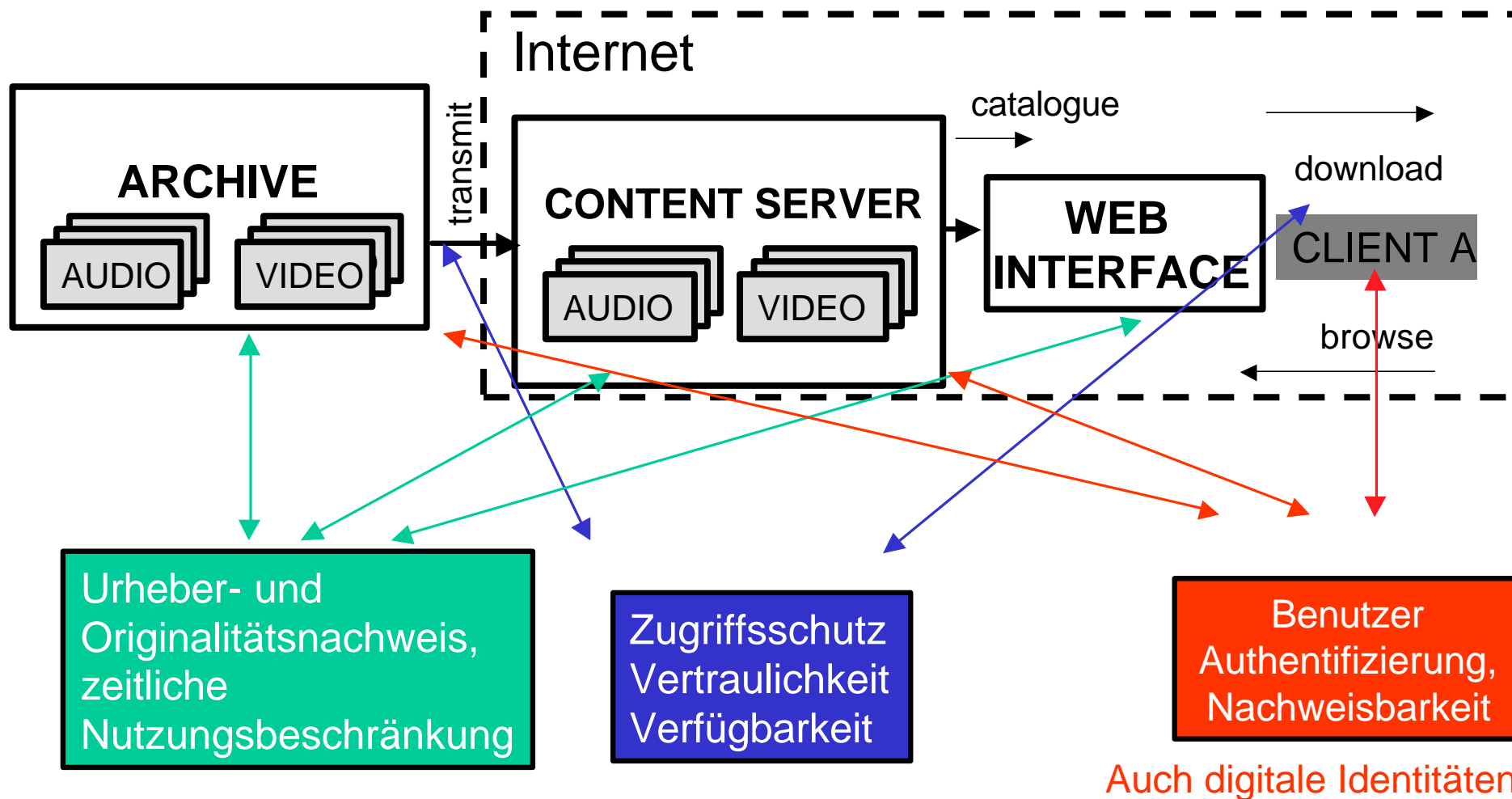
Biometrische Benutzerauthentifizierung

- Entwicklung neuer Algorithmen unter Einbezug der Forensik
- Multimodale Systeme und Bio-DB
- Kombination mit weiteren Security-Mechanismen – Authentizität und Integrität
- Datenschutz – Vertraulichkeit, Pseudonymisierung, Anonymisierung
- Anwendungen und Sicherheitsniveau
- Sicherheitsevaluierung – gezielte Angriffe und Langzeittests sowie Benutzerakzeptanz



Zusammenfassung

Beispielszenario: Archive





Zusammenfassung

Forschungsschwerpunkte und Beispiele

- **digitale Wasserzeichen:**
 - Klassifizierung (Applikationen, Parameter)
 - Algorithmen zum Nachweis der Urheberschaft und der Unversehrtheit
 - Entwurf neuer Geschäftsmodelle wie Illustrationswasserzeichen
- **steganographische Techniken und kryptographische Protokolle**
 - Kombination von Kryptographie, Wasserzeichen und Steganographie sowie Biometrie
 - Rechtliche Aspekte
 - Design von Vertrauen, Identität, Partizipation und Technologie
- **Benutzerauthentifizierung**
 - Biometrische Algorithmen
 - OpenSource Referenz
 - Biometrie in Anwendungen
- **Sicherheitsevaluierungen**
 - StirMark Benchmark: Mediensicherheit
 - Evaluation biometrischer Benutzerauthentifizierung
 - Securityscans: Netz- und Betriebssystemssicherheit



Zusammenfassung

Sicherheitsevaluierungen und Securityscans

- Beispiele:
 - Hackers-Contents
 - IT-Forensik
 - Angriffe auf Wasserzeichen
 - Erkennen verdeckter Kommunikation
 - Angriffe auf biometrische Verifikations- und Identifikationsmethoden
 - ...



Fragen