

物理学硕士，数学硕士

安诺夫·丹策 博士

SIEMENS

西门子股份公司
信息和移动通信
移动通信

通信地址：
Siemens AG, ICM N-MR TS SE 2
D-81359 Munich 联邦德国

办公地址：
Hofmannstr.51
D-81379 Munich

电话: +49 89 722 - 37212
传真: +49 89 722 - 54889
Arnulf.Deinzer@icn.siemens.de

物理学硕士，数学硕士

安诺夫·丹策 博士

系统工程 TD-SCDMA

Dr. Arnulf Deinzer

44a, married, 1 son (6a)

1980-86 Mathematics & Physics at University Würzburg

1998 PhD Computer Science at University of German Armed Forces



Dipl.-Phys., Dipl.-Math.

Dr. Arnulf Deinzer

Systems Engineering TD-SCDMA
Director Call Processing

Siemens AG
Information and
Communication Mobile

Postal Address:
Siemens AG, ICM N MR TS SE 2
D-81359 Munich

Office Address:
Hofmannstr. 51
D-81379 Munich

Tel. +49 89 722-37212

Fax +49 89 722-54889

arnulf.deinzer@icn.siemens.de

14.5a Siemens AG

- 8a SW Development (OS Switches)
- 1a Integrations test (Boca Raton FL, USA)
- 5a Systems Engineering for mobile Systems

University of Applied Sciences Kempten (Allgäu), Germany



Digital Right Management Systems - Agenda

Introduction

- IP has to be protected
- theft since ever
- copy (i.e. theft) much easier now
- definition **DRM**

Methods

- reuse of proven techniques
- cryptographics (symmetrical and asymmetrical)
 - authentication
 - watermarking
 - fingerprinting
 - code encryption
 - proprietary scrambling
- RML (Rights Management Languages)
- "dongling"

Future

- lightweight DRM
- worms

TLAs and XTLAs

AES	Advanced Encryption Standard		
BOBE	break-once, break everywhere		
CA	Certification Authority		
CPTWG	copy-protection technical working group	NGSCB	Next-Generation Secure Computing Base for Windows
CSS	Content Scrambling System		
DES	Data Encryption Standard	ODRL	Open Digital Rights Language
DMCA	Digital Millennium Copyright Act	RSA	Rivest, Shamir, Adleman
DPRL	Digital Property Rights Language	SDMI	secure digital music initiative
DRM	Digital Rights Management	TCG	Trusted Computing Group (ehemals TCPA)
EULA	End User Licence Agreement	TCPA	Trusted Computing Platform Alliance
EVA	Eingabe-Verarbeitung-Ausgabe	TLA	Three Letter Acronym
fhg	Fraunhofer-Gesellschaft	TPM	Trusted Platform Module
IIS	fhg-Institut für integrierte Schaltungen	TRIPS	Trade-Related Aspects of Intellectual Property Systems
IP	Intellectual Property		
IPSI	fhg-Institut für integrierte Publikations- und Informationssysteme	UCITA	Uniform Computer Information Transactions Act
LWDRM	Light Weight DRM	UrhG	Urheberrechts-Gesetzes
M4	Mince, Modify, Mix, Mend	WIPO	World Intellectual Property Organisation
		XrML	eXtensible rights Markup Language (ehemals DPRL)
		XTLA	Extended TLA

Theft of IP (Intellectual Property)...

...since early beginnings of human beings:

- stone tools (with metallic appearance)
- oracle columns
- money (notes)
- books
- "secret" holy mass, Habanera, Villoton songs,...
- ...

Theft of IP since ever (2nd century AC)

oracle columns:

1-1-1-6-4:

Aphrodite: Go wherever you want. Because you will happily come home.
Find you will and do what you have planned.

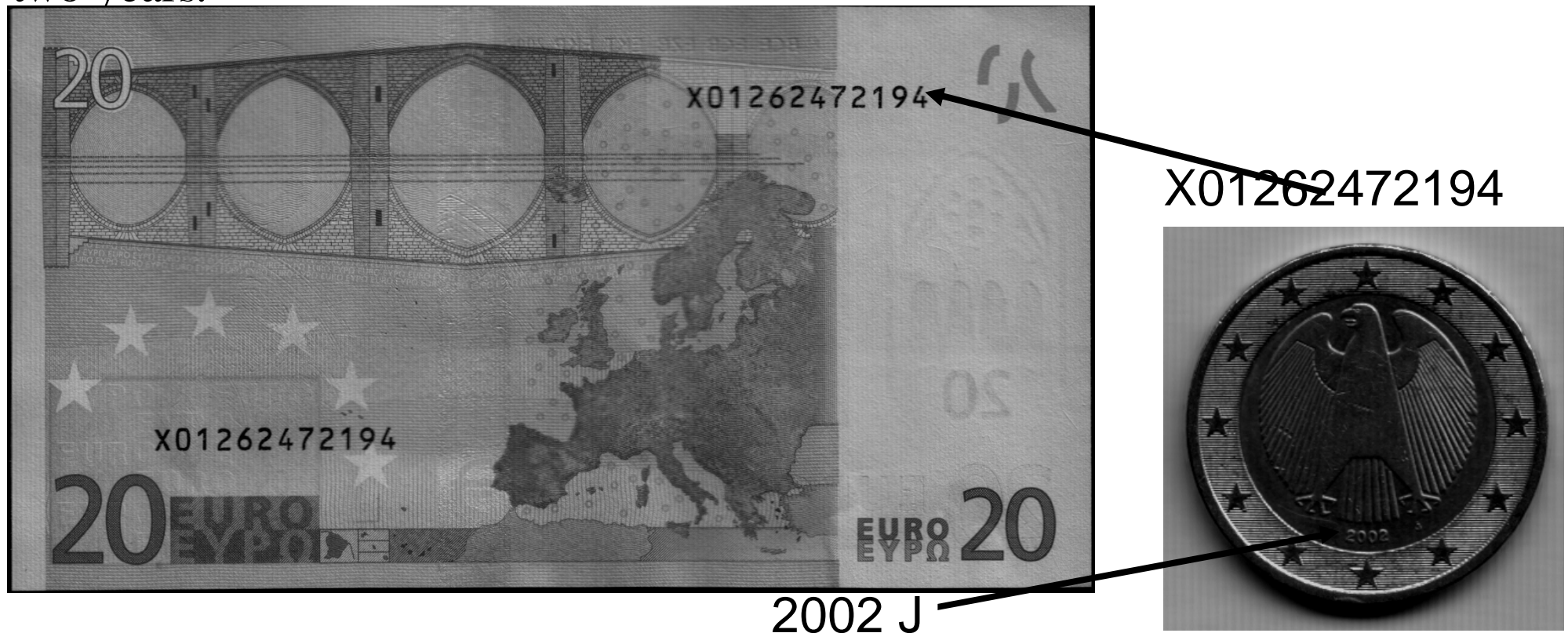
6-6-6-1-1:

Hephaistos: Nothing can be done: don't try in vane!

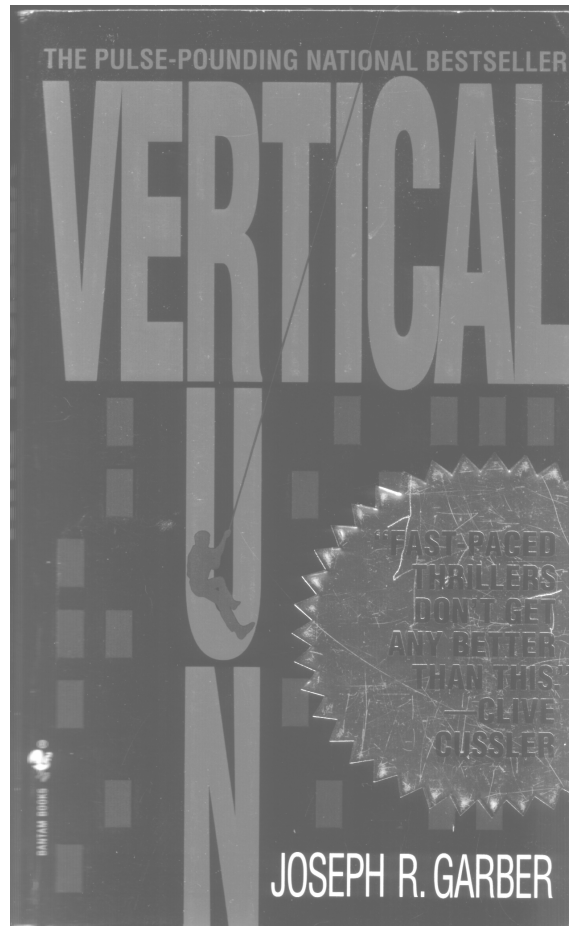
Stefan Schmitt, "Archäologie des Schicksals", ZEIT 27/2003

Money falsified since money exists

On old German money notes: "Wer Geldnoten nachmacht oder verfälscht oder nachgemachte oder verfälschte Geldnoten in Verkehr bringt, wird mit Gefängnis nicht unter zwei Jahren bestraft." "Who copies or falsifies money notes or introduces copied or falsified money notes will be punished by prison of at least two years."



Books - copied since ever



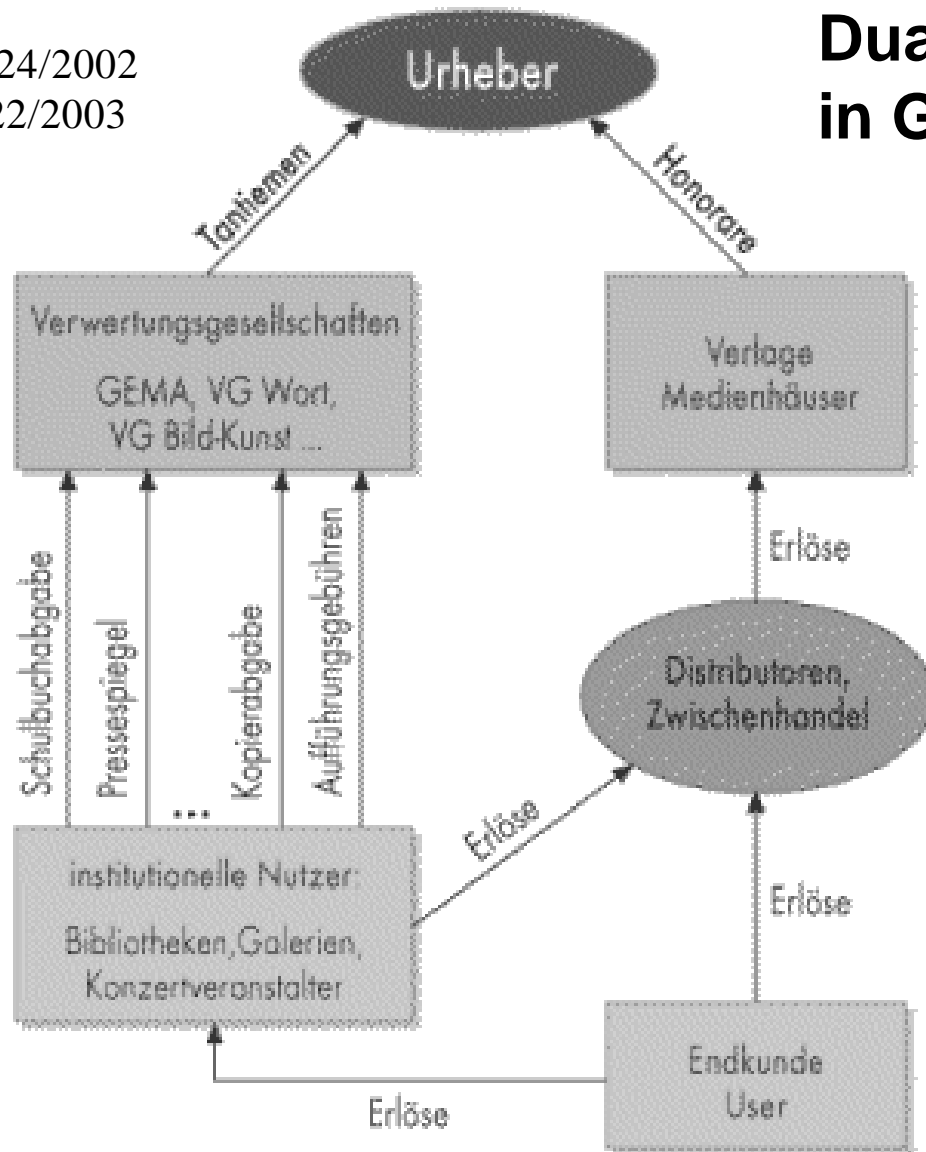
"If Hollywood would have had influence in the computer industry we now had 3.5" discs in the US and 9cm floppy discs in europe."
/Tanenbaum02/

If you purchased this book without a cover you should be aware that this is stolen property. It was reported as "unsold and destroyed" to the publisher and neither the author nor the publisher has received any payment for this "stripped book."

Theft much easier now

c't 24/2002
& 22/2003

Dual system of IP payment in Germany.



VCR: 9,21€/device

Cassette recorder: 1,28€/device

CD burning device: 6€/device

DVD burning device: 7,37€/device

Copy machine, Fax, Scanner:

8,18-306,78€/device

PC: 12€/device (*)

Printer, multi purpose devices (*)

empty cassette(audio): 0,0614€/h

empty cassette(VCR) : 0,087€/h (**)

(*) law suit pending

(**) also magnetic tape, DAT, MD, CD

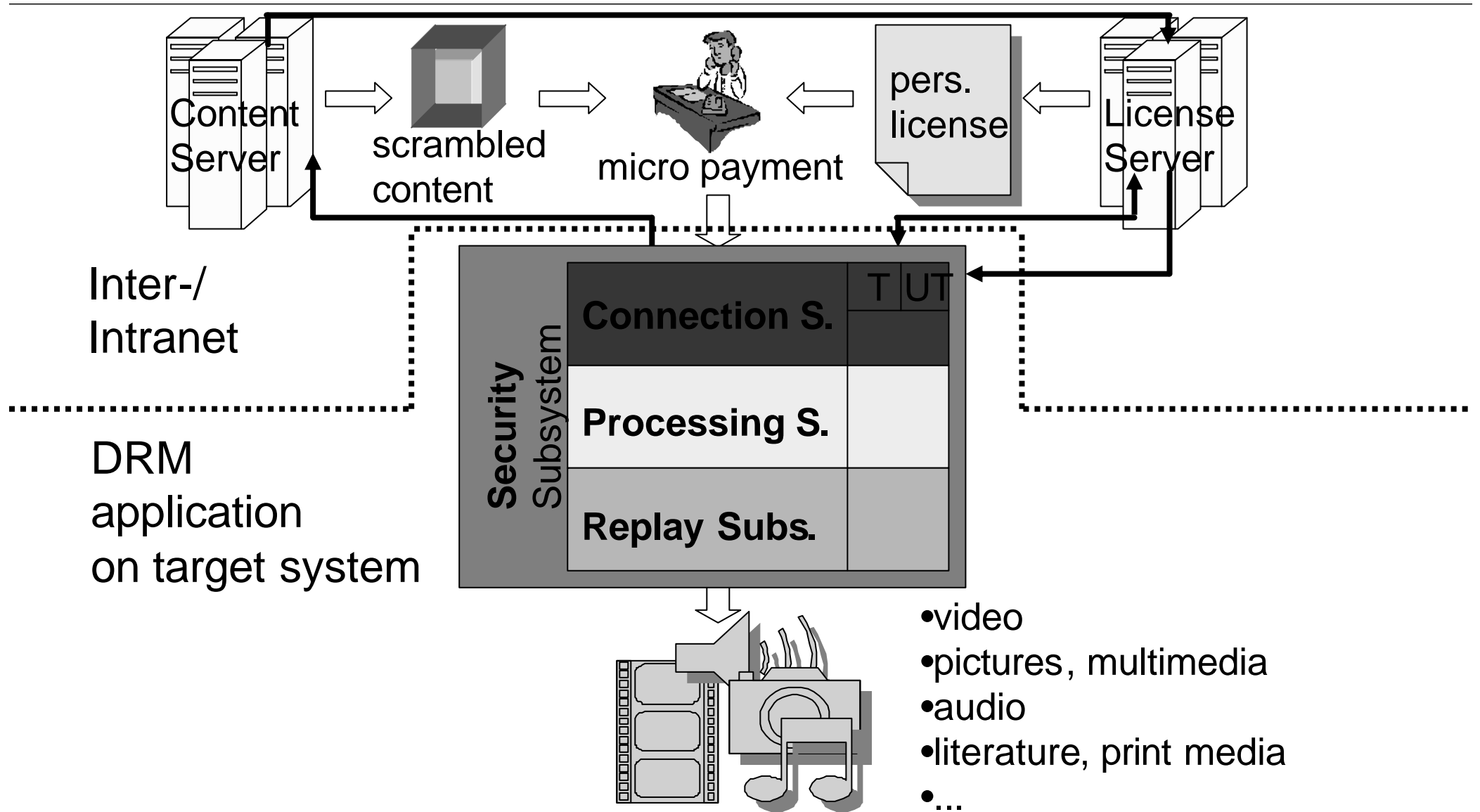
Definitionen Digital Right Management (DRM)

Digital rights management (DRM) can be viewed as an attempt to provide 'remote control' of digital content. The required level of protection goes beyond simply delivering the digital content - restrictions on the use of the content must be maintained after it has been delivered. In other words, DRM requires 'persistent protection', i.e., protection that stays with the content. Mark Stamp

Digital Rights Management (DRM) involves the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets - both in physical and digital form - including management of Rights Holders relationships. Renato Iannella

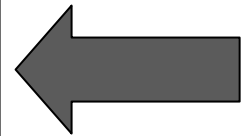
If you own a DVD or CD which you only can play at your birthday - that´s DRM! www.ccc.de

Methods in DRM systems - Divide et Impera



Methods of DRM systems - in **connection** subsystem

Security Subsystem <ul style="list-style-type: none"> •Code Encryption •Polymorphe Code •Code Obfuscation •SW Unification •Tamper Checking 	Connection Subsystem	Tethered M.	Untethered M.
		<ul style="list-style-type: none"> •Authentication •Rights Management Languages 	
	Processing Subsystem	<ul style="list-style-type: none"> •Cryptographics •Proprietary Scrambling 	
Replay Subsystem	<ul style="list-style-type: none"> •Watermarking •Fingerprinting •Dongling 		



Connection subsystem: authentication

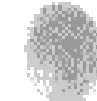
Methods of authentication.

Single factor and multi factor techniques.

Identification Based on Something the User Is:



Iris/Retina



Fingerprint



Face



Hand

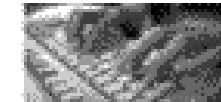
Identification Based on Something the User Does:



Signature



Voice



Keystroke

Identification Based on Something the User Has:



Token - USB Token



Token - Sync



Smart Card

Identification Based on Something a User Knows

USER ID/ PASSWORD/PIN

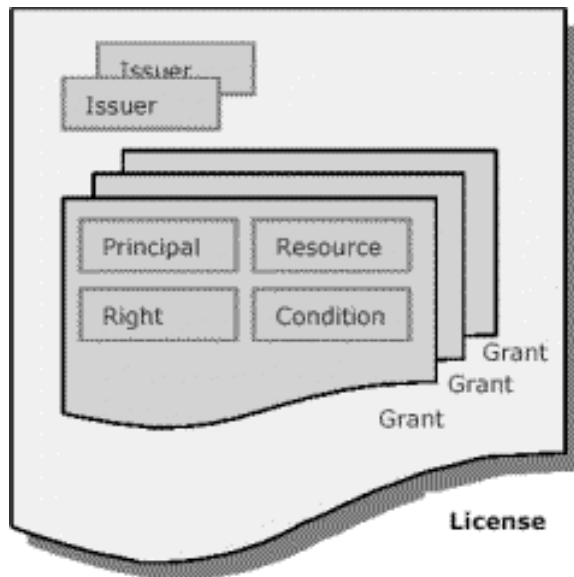
Authentication & Authorization: Complementary Solutions for Securing the Digital Enterprise,
BioNetrix Corporation, 29.04.2003, <http://www.bionetrix.com/pdf/Netegrity.pdf>

Connection subsystem: Rights Management Languages

Structure of a license in **XrML** (e**X**tensible rights

Markup Language).

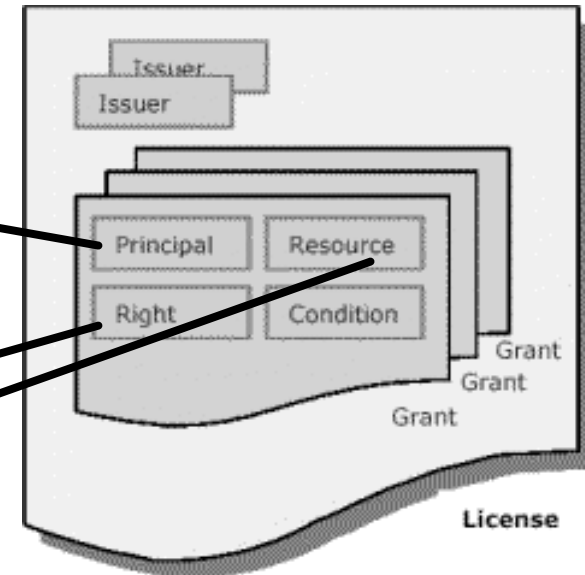
(was **ODRL** (**O**pen **D**igital **R**ights **L**ang.)
Xerox, Palo Alto Research Center)



XrML 2.0 Technical Overview,
Version 1.0 08.03.2002, 15.04.2003,
<http://www.xrml.org/reference>

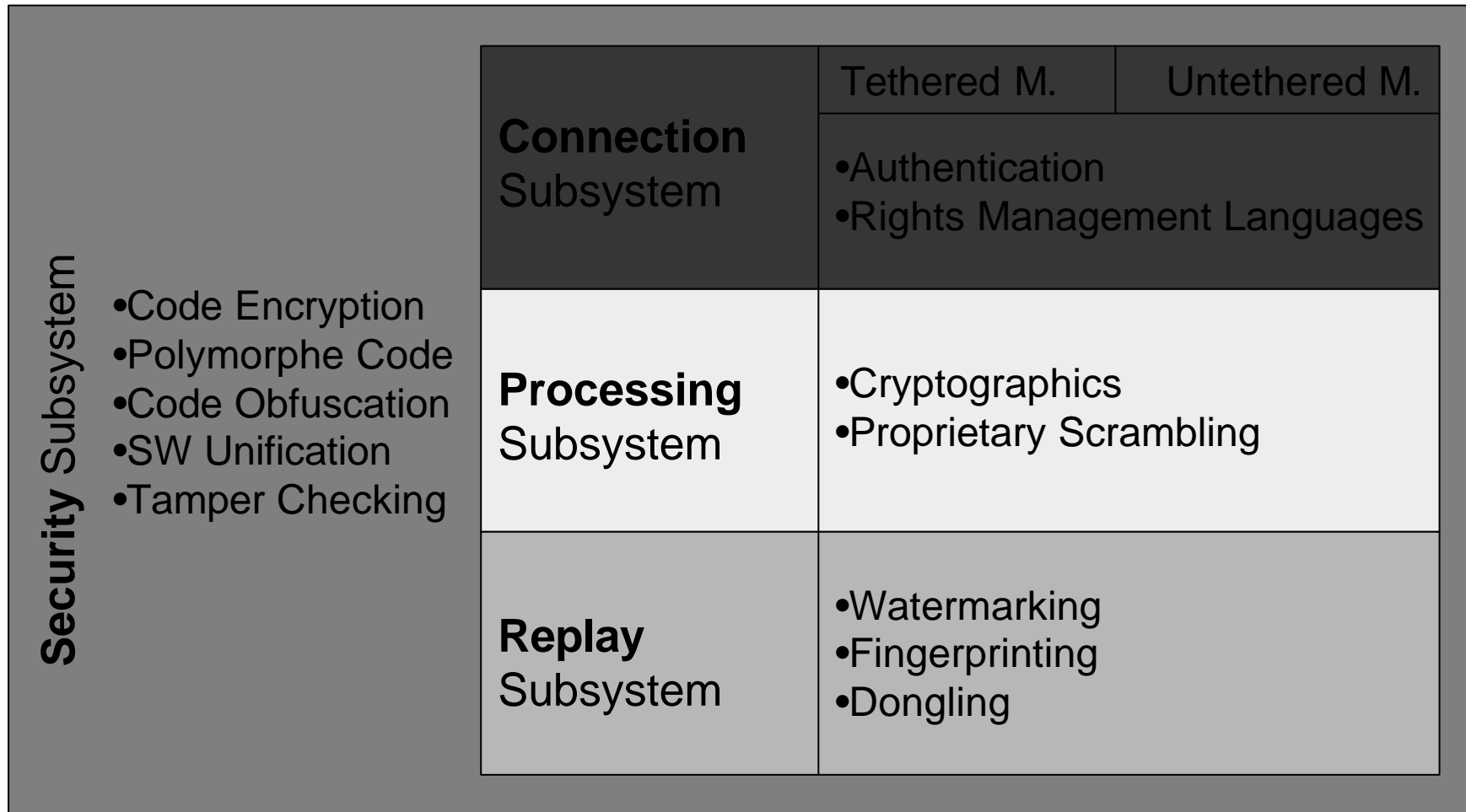
Conection subsystem: Rights Management Languages

```
<license>
  <grant>
    <keyHolder>
      <info>
        <dsig:KeyValue>
          <dsig:RSAKeyValue>
            <dsig:Modulus>Fa7wo6NYf...</dsig:Modulus>
            <dsig:Exponent>AQABAA==</dsig:Exponent>
          </dsig:RSAKeyValue>
        </dsig:KeyValue>
      </info>
    </keyHolder>
    <cx:print/>
    <cx:digitalWork>
      <cx:locator>
        <nonSecureIndirect
          URI="http://www.xrml.org/reference"/>
        </cx:locator>
      </cx:digitalWork>
    </grant>
  </license>
```

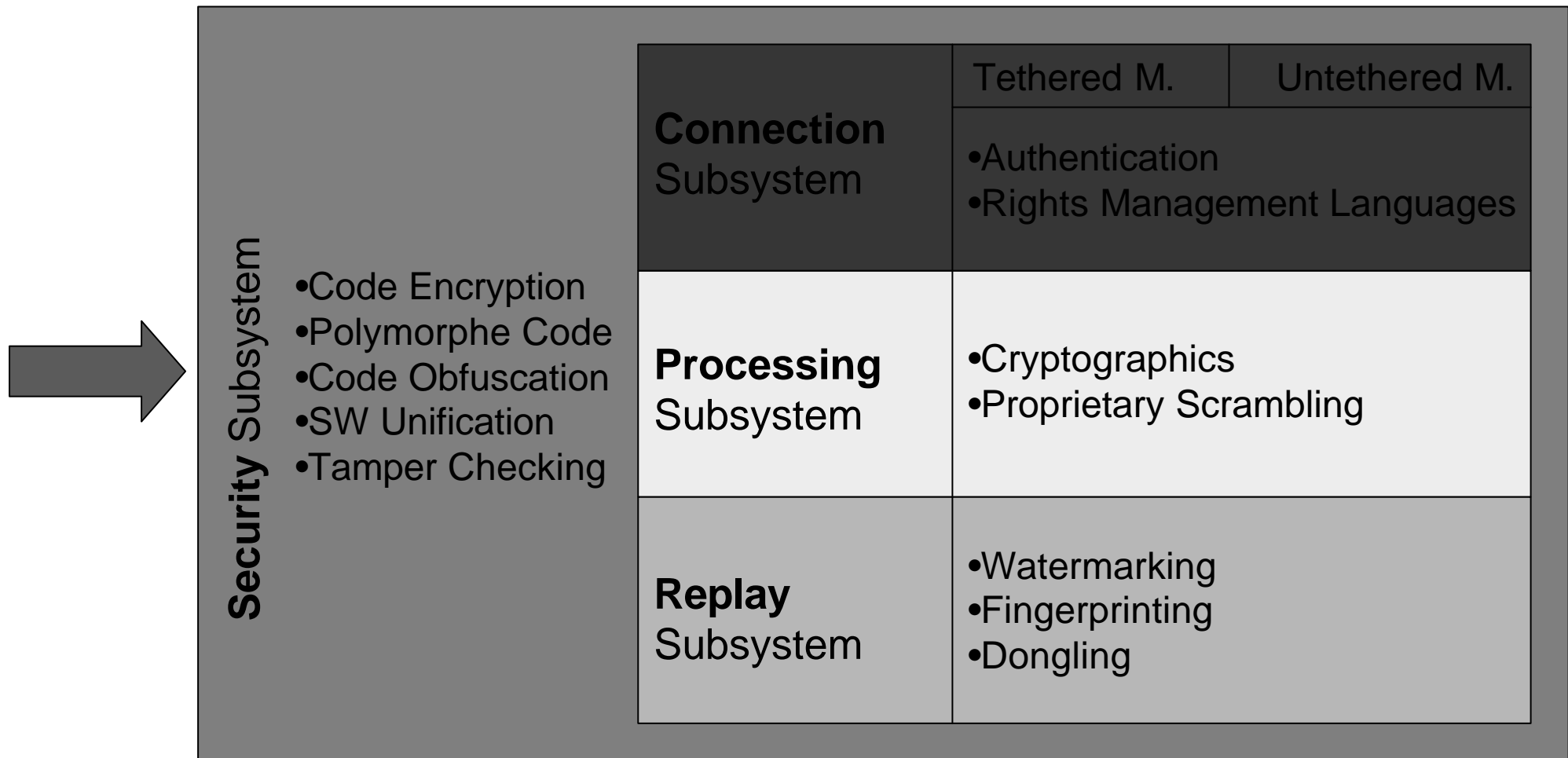


XrML 2.0 Specifications,
<http://xrml.org/>

Methods of DRM systems - in **processing** subsystem



Methods of DRM systems - in **security** subsystem



Security subsystem: try to be unvulnerable

Anti debugging measures:

- Code Encryption
- Polymorphe Code
- Software Unification
- Code Obfuscation
- Tamper Checking (Fragilization)



Nightmare Joker,

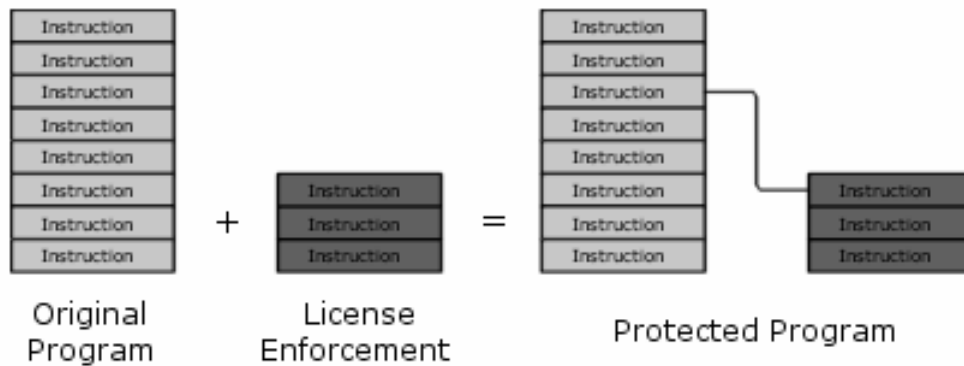
How to Encrypt Wordbasic and VBA Code,

<http://vx.netlux.org/texts/html/m6t.html>

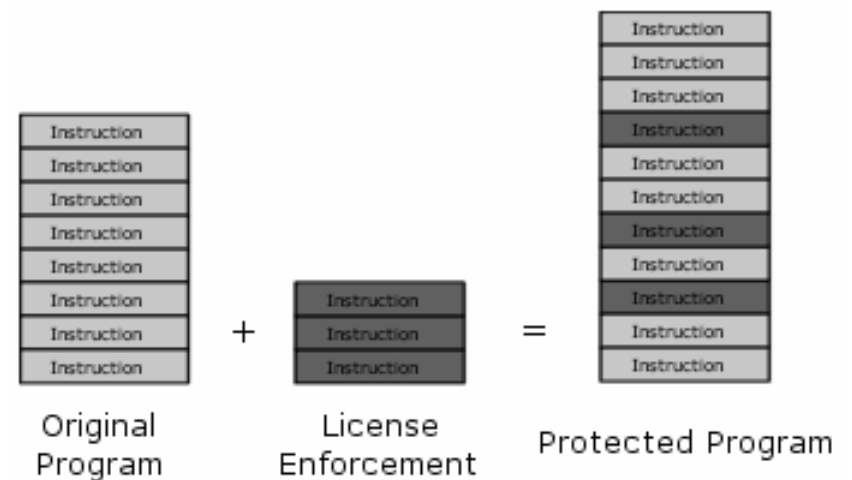
SnakeByte, *Polymorphe Viren,*

<http://www.snake-basket.de/d/poly.txt>

Security subsystem: Code Encryption



<http://www.licenturion.com> M4



More examples: Nightmare Joker,
How to Encrypt Wordbasic and VBA Code,
<http://vx.netlux.org/texts/html/m6t.html>

Security subsystem: Code Obfuscation

```
#!/usr/bin/perl
# Len - http://www.perlmonks.org/index.pl?node_id=176043
```

```
$_='
    $q = "\
    ile
    $z
    %c=
    0+
    6+
    s
    +1
    $
    t
    c
    /
    rl
    fo
    $ y
    ($/
    0")
    $/.
    s; ".
    's;\s;;g;eval

    $q = "\
    ile
    $z
    %c=
    0+
    6+
    s
    +1
    $
    t
    c
    /
    rl
    fo
    $ y
    ($/
    0")
    $/.
    s; ".
    's;\s;;g;eval

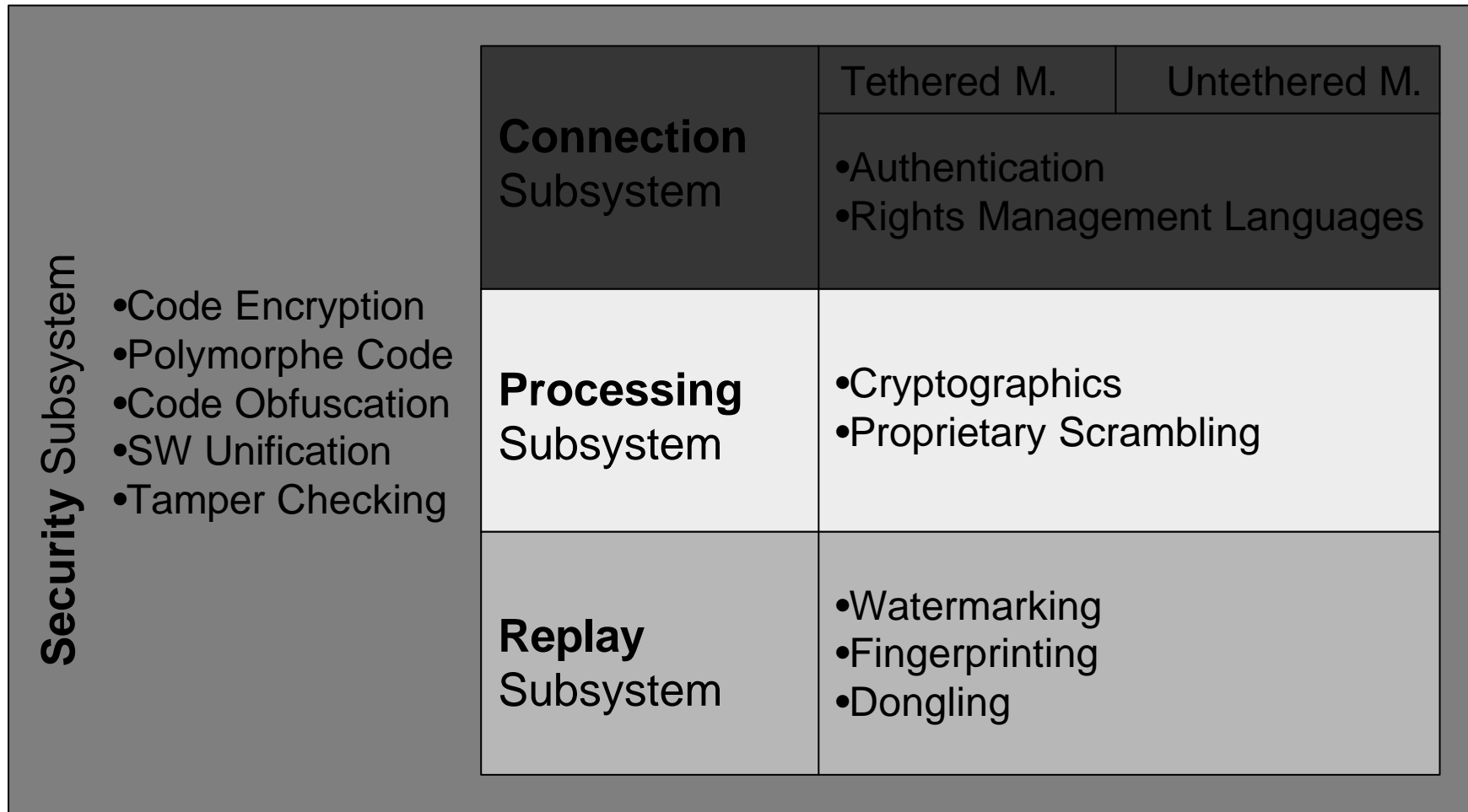
    $r=0;$ / ="";whi
    $z>($;+=.05)){ $c{int$
    r+= .0
    }{1
    =1for(0.
    ever se;$
    ar
    /bi
    $_=$q
    (1..20){ $c{$_}
    /.=chop$t
    .=""
    for(0.
    ="n"}pri
    chr(9 2)."s;;g; eval \n

    47"; wh
    ($ ;=
    .5 ){
    le(2
    _+ 2
    2) *
    -$_
    o s
    }$
    =`
    #!
    pe
    ;
    {
    :
    \4
    ;
    q;
    L};

    nt"$/$
    ;
```

Thomas Klausner, *Eine Einführung in Obfuscation mit Perl*,
 Linuxwochen 2002, 30.06.2002, 23.03.2003,
<http://domm.zsi.at/talks/obfu/linuxwochen/obfu/lw.html>

Methods of DRM systems - in **replay** subsystem

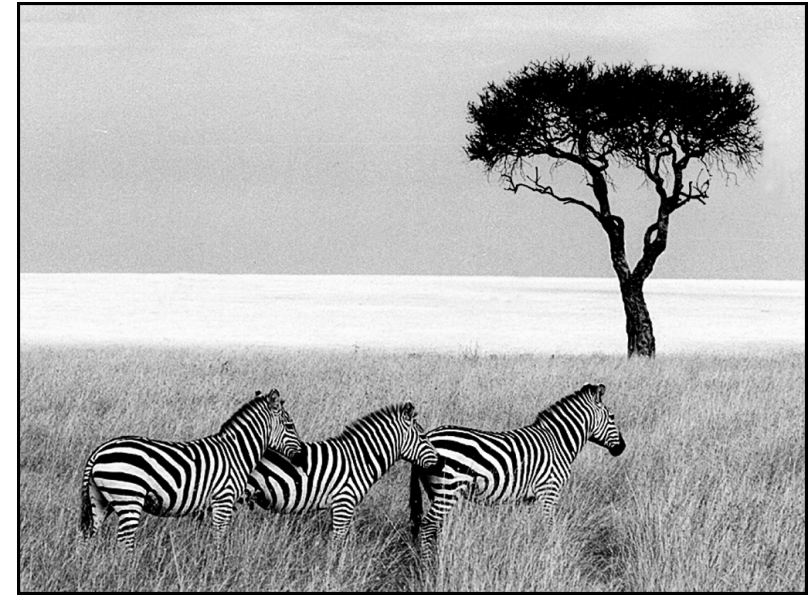


Steganographics: Base for Watermarking and Fingerprinting

/Tanenbaum02/



Three cebras and a tree



Three cebras a tree and
Hamlet, Macbeth, Julius Caesar
Merchant of Venice, King Lear

Future: Cooperation

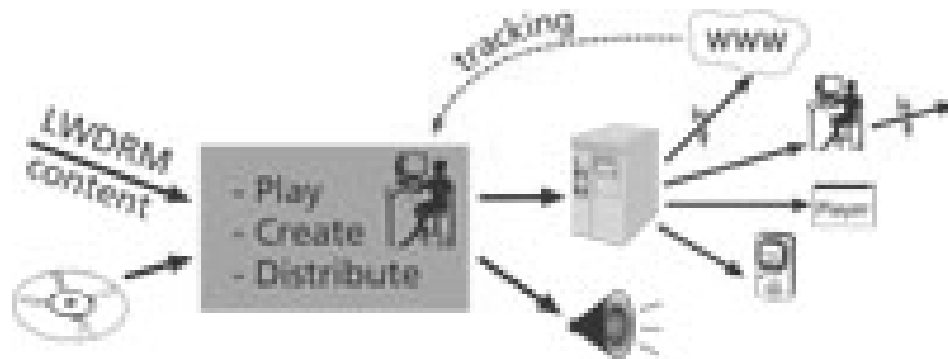
"*Das rechte Maß.* 15... 16 Sei nicht allzu gerecht und übertrieben weise!
17 Frevle nicht allzusehr und sei kein Tor! Warum sollst du sterben vor deiner
Zeit? 18 Gut ist es, wenn du an dem einen festhältst und auch vom anderen
deine Hand nicht abziehst. ..." Prediger 7

Ansatz LWDRM (Light Weight DRM)

Level 1: Play

Level 2: Play&Modify

Level 3: Play&Modify&Distribute



Fraunhofer Institut für Integrierte Schaltungen,
<http://www.iis.fraunhofer.de/amm/techinf/ipmp/>

Literature(1)

- [01] Gerald Himmelein,
"Ganz im Vertrauen: TCPA ist tot, es lebe die TCG",
c't Magazin für Computer Technik 9/2003: 52
- [02] Joerg Heidrich,
"Kopieren verboten?",
c't Magazin für Computer Technik 9/2003: 20
- [03] Richard Sietmann, Stefan Krempf,
"Zaghaft nach Digitalien: Das neue Urheberrecht auf Probe",
c't Magazin für Computer Technik 9/2003: 18-20
- [04] Dr. Ingolf Prinz,
"Musikkonserven mit Paragraphensauce: Kopiergeschützte Tonträger, Abspielhemmnisse und private Kopie",
c't Magazin für Computer Technik 7/2003: 150
- [05] Prof. Dr. Francesco P. Volpe, David Bär,
"Die Un-CDs: So arbeiten Abspielsperren für Audio-CD's",
c't Magazin für Computer Technik 7/2003: 144-149
- [06] Christian Wenz,
"Ohren auf den Schienen: Umgehungsmöglichkeiten für DRM-Schutzmechanismen",
c't Magazin für Computer Technik 6/2003: 238
- [07] Tobias Hauser,
"Finger weg: DRM-Systeme in der Praxis",
c't Magazin für Computer Technik 6/2003: 234-237
- [08] Sven Hansen, Dr. Volker Zota,
"Kaufrausch versus Tauschrausch",
c't Magazin für Computer Technik 6/2003: 144-145
- [09] Gerald Himmelein,
"Ganz im Vertrauen: Neues aus der Welt des Trusted Computing",
c't Magazin für Computer Technik 6/2003: 40
- [10] Richard Sietmann,
"Gegenpositionen aufbauen': Der Weltgipfel für die Informationsgesellschaft nimmt Konturen an",
c't Magazin für Computer Technik 5/2003: 54-55

Literature(2)

- [11] Holger Bruns,
"Wissensgesellschaft in der Diskussion",
c't Magazin für Computer Technik 5/2003: 34
- [12] Richard Sietmann,
"An der Klagemauer: Urheberrechts-Novelle: Klare Fronten, aber keine Alternativen",
c't Magazin für Computer Technik 4/2003: 20-21
- [13] Peter-Michael Ziegler,
"MS-E-Books schutzlos",
c't Magazin für Computer Technik 2/2003: 28
- [14] Brian Kahin,
"Auf dem Holzweg: was läuft schief in der Politik zum 'geistigen Eigentum'?",
c't Magazin für Computer Technik 1/2003: 74-79
- [15] Janko Röttgers,
"Wir brauchen offene Systeme!": Howard Rheingold über die soziale Revolution durch Mobiltechniken",
c't Magazin für Computer Technik 1/2003: 72-73
- [16] Michael Plura,
"Entmündigung des PC-Besitzers: Lucky Green, US-amerikanischer Kryptoexperte, über die von TCPA und Palladium ausgehenden Gefahren",
c't Magazin für Computer Technik 26/2002: 58-59
- [17] Michael Plura,
"Sicherheit und Vertrauen: Thomas Rosteck, Leiter des Product Marketing für Sicherheits-ICs bei Infineon, über die Technik und Vorzüge von TCP",
c't Magazin für Computer Technik 26/2002: 56-57
- [18] Michael Plura,
"Schlossgespenst: hat TCPA auch positive Seiten für den Anwender?",
c't Magazin für Computer Technik 26/2002: 54
- [19] Michael Plura,
"Der PC mit den zwei Gesichtern: TCPA und Palladium - Schreckgespenster oder Papiertiger?",
c't Magazin für Computer Technik 24/2002: 186-188
- [20] Richard Sietmann,
"Wissen ist Geld: Urheberrecht, 'Geistiges Eigentum' und die Rechteverwerter",
c't Magazin für Computer Technik 24/2002: 108-117

Literature(3)

- [21] Michael Plura,
"Der versiegelte PC: Was steckt hinter TCPA und Palladium?",
c't Magazin für Computer Technik 22/02: 204-207
- [22] Dirk Günnewig, Tobias Hauser,
"Musik im Hochsicherheitstrakt: Digital Rights Management - Stand der Dinge",
c't Magazin für Computer Technik 16/2002: 182-185
- [23] Mark Stamp,
Mark Stamp's CV,
24.03.2003,
<http://home.earthlink.net/~mstamp1/mss/ v.html>
- [24] Mark Stamp,
Digital Rights Management: The Technology Behind the Hype,
19.12.2002, Department of Computer Science, San Jose State University, 05.03.2003,
<http://home.earthlink.net/~mstamp1/papers/DRMpaper.pdf>
- [25] Renato Iannella,
Curriculum Vitae for Renato Iannella,
15.10.2002, 08.04.2003,
<http://renato.iannella.it/cv/index.html>
- [26] Renato Iannella,
"Digital Rights Management (DRM) Architectures",
D-Lib Magazine, Volume 7 Number 6, Juni 2001, 07.04.2003,
<http://www.dlib.org/dlib/june01/iannella/06iannella.html>
- [27] Margarita A. Kousseva,
Digital Rights Management: Literature Review,
06.12.2002, School of Computer and Information Sciences, Nova Southeastern University, 24.03.2003,
<http://www.nova.edu/~kousseva/literature/ review.html>
- [28] Ulrich Dieter Einbrodt,
Legale MP3-Downloads: Musik 2. Klasse oder geniale Anwendung neuer medialer Distributionsmärkte? Das Beispiel MP3.com,
1999, 27.02.2003,
<http://bibd.uni-giessen.de/ghm/1999/uni/p990010.htm>

Literature(4)

[29] Ulrich Dieter Einbrodt,

The Juxtaposition of Good and Bad or: Legal and Illegal Downloads. The MP3 Format and its Chances for Musicians and Fans,
2001, 27.02.2003,

<http://bibd.uni-giessen.de/ghtm/2001/uni/p010002.htm>

[30] *Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft*,
Drucksache 15/38 des Deutschen Bundestages (15. Wahlperiode) vom 06.11.2002, 23.04.2003,

<http://dip.bundestag.de/btd/15/000/1500038.pdf>

[31] Florian Weis, Christian Albrecht,

Digital Rights Management,

Semesterarbeit an der Technischen Fachhochschule Berlin, Dezember 2002, 27.02.2003,

<http://www.fth-berlin.de/~godberse/semesterarbeiten/%20ia2/drm.pdf>

[32] Judie Mulholland,

Digital Rights (mis)Management,

Position Paper for the W3C DRM Workshop, 23.01.2001, 27.02.2003,

<http://www.w3.org/2000/12/drm-ws/pp/fsu-mulholland.html>

[33] Austin Russ,

Digital Rights Management Overview,

The SANS Institute, 26.07.2001, 27.02.2003,

<http://www.sans.org/rr/securitybasics/rights.php>

[34] *Art & Commerce in the Digital Decade: Protecting intellectual property will take cooperation and innovation*,

03.06.2002, Microsoft Corporation, 01.04.2003,

<http://www.microsoft.com/issues/essays/2002/06-03digitalrights.asp>

[35] *Richard M. Stallman - List of Achievements and Awards*,

18.10.2002, Free Software Foundation, Inc., 01.04.2003,

<http://www.gnu.org/doc/Stallmanawards.html>

[36] Richard M. Stallman, Joshua Gay (Hrsgb.),

"Words to avoid",

Free Software, Free Society: Selected Essays of Richard M. Stallman, Philosophy of Software Freedom Series, GNU Press Oktober 2002,
01.04.2003 online unter

<http://www.gnu.org/philosophy/words-to-avoid.html>

Literature(5)

[37] 23 - *Nichts ist wie es scheint*,

Ein Film von Hans-Christian Schmid, beruhend auf den wahren Begebenheiten um den Tod des Hackers Karl Koch im Jahr 1989, Buena Vista International, 1998, siehe auch (17.05.2003)

<http://www.moviesite.de/kritik.cfm?id=31>

[38] Tim Gerber,
"Wunschkonzert",
Editorial zum

c't Magazin für Computer Technik 04/2003: 3

[39] Prof. Dr. W. Schmitt,

Scriptum zur Lehrveranstaltung *Datensicherheit* im Sommersemester 2002 an der FH Giessen-Friedberg, 10.03.2001

[40] Diana Kelley,

Authentication as the Foundation for eBusiness,

Security Technology for Safewww Inc., 15.11.2001, 29.04.2003,

<http://www.securityfocus.com/infocus/1513>

[41] Mark Vandenwauver, Rene Govaerts, Joos Vandewalle,

Overview of Authetication Protocols, 29.04.2003,

<https://www.cosic.esat.kuleuven.ac.be/sesame/papers/carnahan.pdf>

[42] *Authentication & Authorization: Complementary Solutions for Securing the Digital Enterprise*,

01.07.2001, BioNetrix Corporation, 29.04.2003,

<http://www.bionetrix.com/pdf/Netegrity.pdf>

[43] Microsoft .NET Passport, global Einheitlicher Authentikationsdienst (nicht nur) für DRM, 05.05.2003,

<http://www.passport.net/>

[44] Andrew Conry-Murray,

Emerging Technology: Microsoft's Passport to Controversy,

03.04.2002, 06.05.2003,

<http://www.networkmagazine.com/article/NMG20020304S0003>

[45] Renato Iannella,

Open Rights Language Requirements,

ISO/IEC JTC1/SC29/WG11 M6974, März 2001, 06.05.2003,

<http://www.iprsystems.com/MPEG/m6974.pdf>

Literature(6)

- [46] Renato Iannella,
Open Digital Rights Language (ODRL),
Version 1.1 08.08.2002, 06.05.2003,
<http://odrl.net/1.1/ODRL-11.pdf>
- [47] *Open Digital Rights Language: A Rights Expression Language for Digital Asset Management and E-Commerce*,
Informationsbroschüre der ODRL Initiative, 06.05.2003,
<http://odrl.org/>
- [48] *XrML 2.0 Technical Overview*,
Version 1.0 08.03.2002, 15.04.2003,
<http://www.xrml.org/reference>
- [49] *XrML 2.0 Specifications*,
Spezifikationen und Beispiele zum XrML-Standard 2.0, nach Registrierung per eMail anforderbar (15.04.2003) unter
<http://xrml.org/>
- [50] Prof. Dr Franck Leprevost, Prof. Dr Bertrand Warusfel,
Security Technologies for Digital Media,
Final Report to the European Parliament Directorate-General for Research, Directorate A, STOA Programme, Mai 2001, 29.04.2003,
<http://www.europarl.eu.int/stoa/publi/pdf/00-06-01/en.pdf>
- [51] Inbar Raz,
Anti Debugging Tricks,05.03.2003,
<http://www.geocities.com/angel-miguel/tutdown/antidebug.htm>
- [52] SnakeByte,
Polymorphe Viren, 24.03.2003,
<http://www.snake-basket.de/d/poly.txt>
- [53] Nightmare Joker,
How to Encrypt Wordbasic and VBA Code,23.03.2003,
<http://vx.netlux.org/texts/html/m6t.html>
- [54] Thomas Klausner,
Eine Einführung in Obfuscation mit Perl,
Linuxwochen2002, 30.06.2002, 23.03.2003,
<http://domm.zsi.at/talks/obfu/linuxwochen/obfu/lw.html>

Literature(7)

- [55] Gregory Wroblewski,
General Method of Program Code Obfuscation,
2002, 08.05.2003,
<http://www.mysz.org/papers/obfuscation.ps.gz>
- [56] Christian S. Collberg, Clark Thomborson,
"Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection",
IEEE Transactions on Software Engineering, Vol. 28, No. 8, August 2002, 25.03.2003,
<http://www.cs.auckland.ac.nz/~cthombor/Pubs/01027797a.pdf>
- [57] Jana Dittmann,
Digitale Wasserzeichen,
Springer-Verlag Berlin Heidelberg New-York 2000, ISBN 3-450-66661-3
- [58] Sven Hlawatsch,
Digital Watermarks,
Seminararbeit an der FH-Giessen, 12.05.2003,
<http://homepages.fh-giessen.de/~hg10013/>
- [59] "Digitale Wasserzeichen in Hörfunksendungen"
Heise Newsticker, 31.01.2003, 12.05.2003,
<http://heise.de/newsticker/data/anw-30.01.03-006/default.shtml>
- [60] *Hollywood wants to plug "analog hole," regulate A-D converters*,
Beitrag im Newsarchiv des Förderverein Informationstechnik und Gesellschaft e.V., 24.03.2002, 23.03.2003,
<http://www.fitug.de/news/horns/old/newsticker240502192617.html>
- [61] Hannes Federrath,
Scientific evaluation of DRM systems, 28.03.2003,
<http://page.inf.fu-berlin.de/~feder/drm/>
- [62] Sabrina Ehlers,
Proseminar: Sicherheitskonzepte im Internet,
Proseminararbeit an der Universität Tübingen, Lehrstuhl für Rechnerarchitektur, im Sommersemester 2002, 05.05.2003,
http://www-ra.informatik.uni-tuebingen.de/lehre/ss02/pro_sicherheit_ausarbeitung/proseminar_ehlers_ss02.pdf
- [63] *Die Bibell*
in der Übersetzung Martin Luthers, Buch des Predigers, Kapitel 7, Verse 16-18

Literature(8)

- [64] *LWDRM(r) - Light Weight Digital Rights Management*, Fraunhofer Institut für Integrierte Schaltungen, 05.03.2003, <http://www.iis.fraunhofer.de/amm/techinf/ipmp/>
- [65] <http://www.4friendsonly.org>
- [66] Heise Online News (16.11.1999): *PDF-Dateien werden käuflich* <http://www.heise.de/newsticker/data/jr-16.11.99-000/>
- [67] Rötzer, Florian: *Russischer Programmierer frei* <http://www.heise.de/tp/deutsch/inhalt/te/11340/1.html>
- [68] Fraunhofer IIS - *AudioID* <http://www.emt.iis.fhg.de/produkte/audioid/>
- [69] Balzert, Helmut: *Lehrbuch der Softwaretechnik*, Spektrum Akademischer Verlag 1996, ISBN 3-8274-0042-2
- [70] Berberich, Eric: *Hashfunktionen in der Kryptographie* <http://www-krypt.cs.unisb.de/lehre/veranstaltungen/ss2001/proseminar/vortraege/berberich/>
- [71] http://www.cdmediaworld.com/hardware/cdrom/cd_protections.shtml
- [72] *Audio-Kopierschutz* http://www.chip.de/praxis_wissen/praxis_wissen_8725919.html
- [73] *Audio-CD-Kopierschutz verärgert Kunden und Händler* CT 4/2000
- [74] Peeck, Klaus: *Musik hinter Gittern : Kopierschutz für Audio-CDs* CT 15/2001
- [75] Heise Online News (04.11.1999): *15-Jähriger knackte DVD-Video* <http://www.heise.de/newsticker/data/ghi-04.11.99-000/>
- [76] Heise Online News (01.11.1999): *Verschlüsselung von DVD-Video geknackt* <http://www.heise.de/newsticker/data/ghi-01.11.99-000/>
- [77] Heise Online News (11.01.2002): *Anklage gegen DVD-Hacker Johansen* <http://www.heise.de/newsticker/data/ghi-11.01.02-000/>
- [78] *Java Plug-in Developer Guide* http://java.sun.com/j2se/1.4/docs/guide/plugin/developer_guide/contents.html
- [79] Dittmann, Wohlmacher: *Aspekte der Sicherheit multimedialer Daten und Anwendungen mittels Kryptographie und digitaler Wasserzeichentechniken* <http://www.darmstadt.gmd.de/~dittmann/mgdbg/gi.doc>

Literature - Most important sources

- /Stadelmann03/ Thilo Stadelmann, FH Giessen
Digital Rights Management - Technik die begeistert?
- /Hasselbach02/ Jens Hasselbach, TU Ilmenau, Konzeption und Realisierung
der Client-Komponenten für ein P2P-File-Sharing-System
mit Umsatzbeteiligung für die Benutzer
- /EP1243998 01/ Thomas Lopatic, A technique for license management
and online software license enforcement
<http://www.epo.org>
- /CCC 04/ Digitaler Maulkorb?
<http://www.ccc.de/digital-rights/>
- /Biddle04/ Peter Biddle, Paul England, Marcus Peinado, Bryan Willman (MS!)
The Darknet and the Future of Content Distribution
- /Licenturion04/ Overview, M4 technology (mince, modify, mix, mend)
<http://www.licenturion.com>
- /Fraunhofer IIS 04/ LWDRM - Leight Weight Digital Rights Management
<http://www.iis.fraunhofer.de/amm/techinf/ipmp>

¿Preguntas?

¡Muchas Gracias!