

Special Master Track IST Information Security Technology

Sandro Etalle & Berry Schoenmakers

▼ **This has nothing to do with IST, it is a general rule**

- / Homologatievakken moeten gehaald zijn voordat aan het afstudeerproject kan worden begonnen. Regel: maximaal 10 ECTS open bij beginnen aan het afstudeerproject, maar dat geldt alleen voor reguliere vakken.
- / Met ingang van dit jaar werken we met *verplichte* inschrijving voor vakken via OASE. Studenten moeten zich aanmelden voor het vak begint
- / Inschrijving voor een vak betekent geen automatische inschrijving voor een eventueel tentamen, dat moeten studenten via de reguliere manier nog steeds doen.

Special Master Program IST

▼ **4 semesters (2 years)**

- ▮ 30%: obligatory courses
- ▮ 15% (at least): optional courses (security)
- ▮ 30%: more choice in the courses (local)
- ▮ 25%: master thesis

▼ **Cooperation with Nijmegen (RU) and Twente (UT)**

- ▮ Some traveling and some telelecturing involved.
- ▮ Most Kerckhoff's courses offered on Monday and Friday.

What You Should Do (1st year students)

- ▼ **Mail info@kerckhoffs-institute.org to register**
 - / otherwise lecturers at the other universities may not know you
 - / see second slide
- ▼ **Register officially with TU/e, RUN & UT**
 - / otherwise your marks cannot be transferred
- ▼ **Regularly check www.kerckhoffs-institute.org/**
 - / otherwise you may not be up to date on the schedules
- ▼ **Consider Algebra as homology**
 - / otherwise you may not be able to pass Cryptography I
- ▼ **Join the Kerckhoffs student association Auguste**
 - / otherwise you will not be able to share your problems with your peers in an effective manner
- ▼ **Join the mailing list**
 - / <https://listserv.surfnet.nl/archives/kerckhoff.html>
 - / otherwise we will not be able to reach you.

- ▼ **Mail info@kerckhoffs-institute.org, providing**
 - / first name (full)
 - / initials
 - / last name (full)
 - / email address (the one you read)
 - / date of birth
 - / “home University” (RU, UT, TU/e)
 - / student number at each of the three universities
 - *if you don't have it yet, leave this blank.*
 - *if you don't have it you might have forgotten to register*
 - / previous education (one line)

What You Should Do (2nd year students)

▼ **You have to decide the topic of your master thesis**

- / and look for a lecturer/professor
- / and a company if you want to do this externally (we can help)
- / abroad is also possible (but you have to organize it yourself, and get it approved)

▼ **Go to the student administration HG 6.33**

- / tell them you are going to graduate
- / there are a number of things you have to do, they will give you the right info
- / in particular, you'll have to get your list of courses “approved” by the “examencommissie” (not a problem if you have followed the rules, but it has to be done).

Year 1

A green BACKGROUND indicates a telelecture.
Telelectures can be followed at the TU/e in Auditorium 14

Year 1, Fall, Semester 1

day	mon	tue	wed	thu	fri
site	UT (<i>route + maps</i>)	UT, RU, TU/e	UT, RU, TU/e	UT, RU, TU/e	TU/e (<i>route + maps</i>)
time slot					
3-4	(local courses)	Network Security for Kerckhoffs students	(local courses)	(local courses)	Cryptography 1
5-6	<i>Introduction to Biometrics</i>	(local courses)	(local courses)	(local courses)	<i>Hacker's Hut</i>
7-8	<i>Cyber Crime Science</i>	(local courses)	(local courses)	(local courses)	(local courses)

Year 1, Spring, Semester 2

day	mon	tue	wed/thu	fri
site	TU/e (<i>route + maps</i>)	UT, RU, TU/e	UT, RU, TU/e	RU (<i>route + maps</i>)
time slot				
3-4	Verification of Security Protocols	(local courses)	(local courses)	Software Security
5-6	<i>Cryptography 2</i>	(local courses)	(local courses)	<i>(Privacy) Seminar</i>
7-8	<i>Seminar Information Security Technology</i>	(local courses)	(local courses)	(local courses)

Year 2

A green BACKGROUND indicates a telelecture.
Telelectures can be followed at the TU/e in Auditorium 14

Year 2, Fall, Semester 3

day	mon	tue	wed/thu	fri
site	RU (<i>route + maps</i>)	UT, RU, TU/e	UT, RU, TU/e	UT (<i>route + maps</i>)
time slot				
3-4	Security in Organisations	(local courses)	(local courses)	Secure Data Management
5-6	Law in Cyberspace			Security and Privacy in Mobile Systems
7-8	Hardware and Operating Systems Security			(local courses)

Year 2, Spring, Semester 4

day	mon	tue	wed/thu	fri
site	UT (<i>route + maps</i>)	UT, RU, TU/e	UT, RU, TU/e	TU/e (<i>route + maps</i>)
time slot				
3-4		Master thesis		
5-6				
7-8				

- ▼ **Distributed Trust Management**
- ▼ **Physical Aspects of Computer Security**

Now, the theory

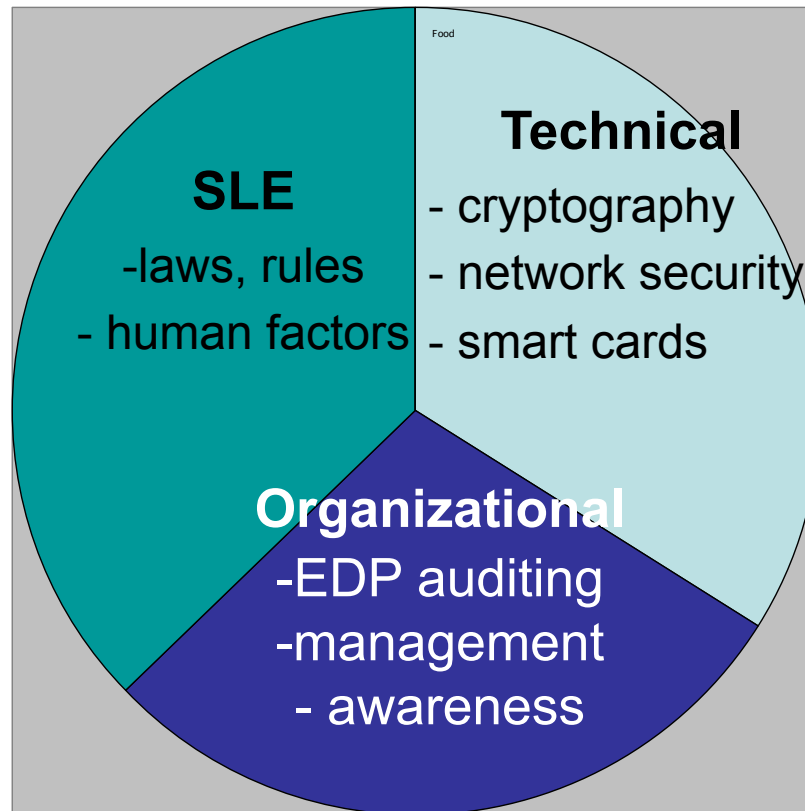
- ▼ Intro: Information Security & Cryptography
 - / security is ubiquitous
 - / cryptography is a fundamental tool
- ▼ IST master program
 - / master thesis projects
 - / employers

“Security is everywhere”

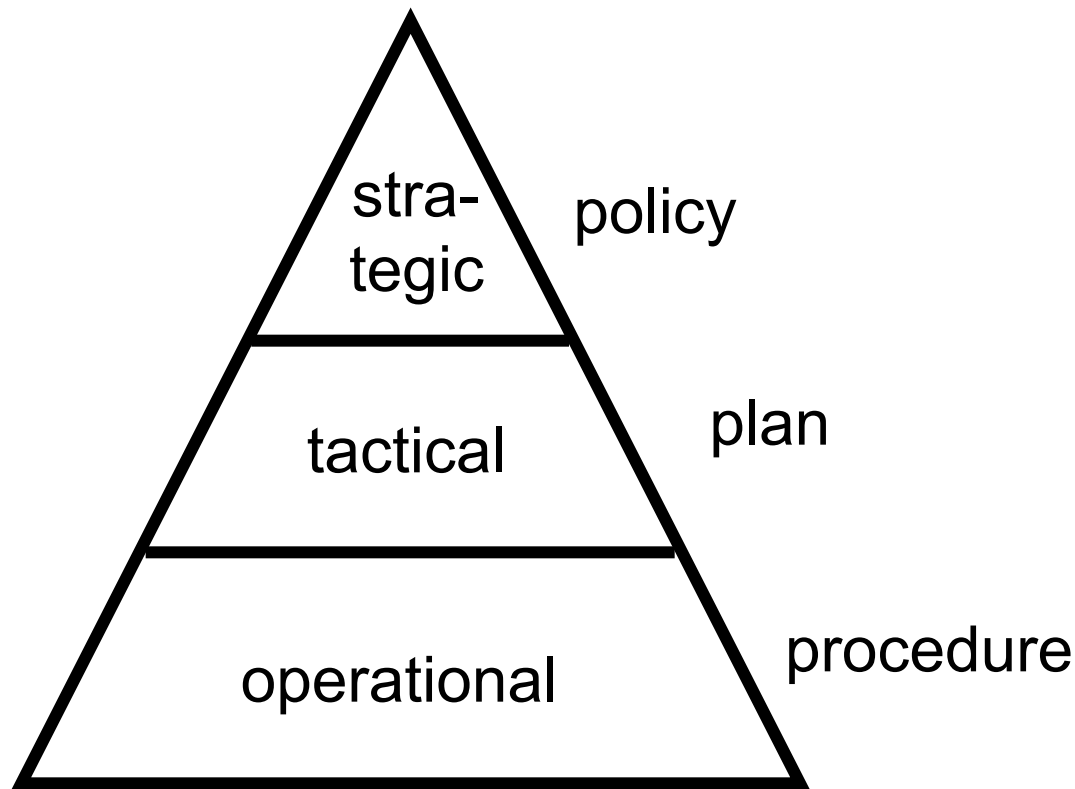
- ▼ Smart cards, SIM card, RFID chips
- ▼ DECT, GSM, UMTS phones
- ▼ VoIP, Skype
- ▼ Wifi, Bluetooth
- ▼ Digital Pay TV, DVD, BluRay
- ▼ iPod (DRM = Digital Rights Management)
- ▼ SSL – Secure Web Servers
- ▼ Electronic carkeys
- ▼ Electronic banking, voting, auctions

Information Security

- ▼ A very broad topic

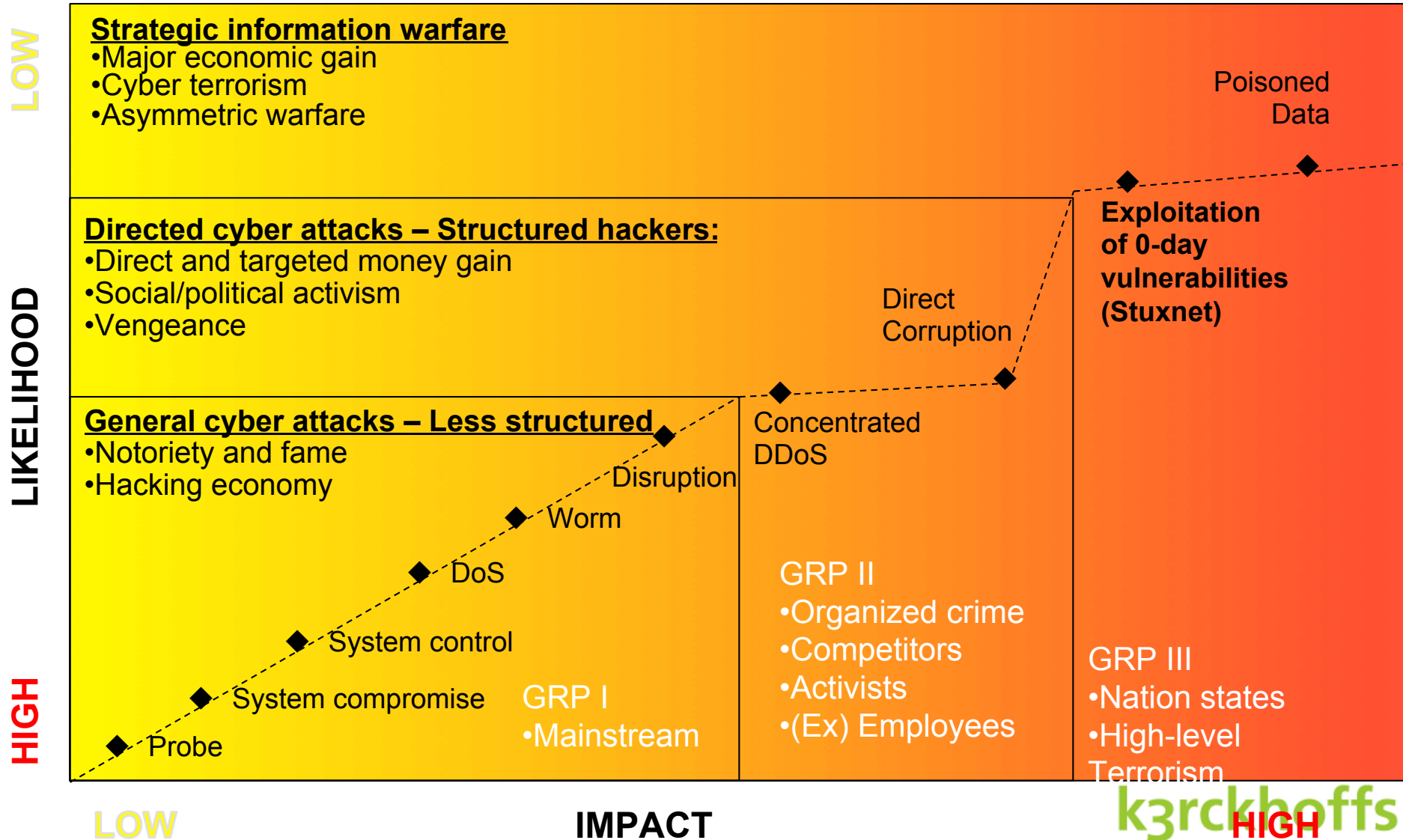


Information security - levels



balancing **risk against cost**

Security Trends





Eindhoven Institute for
the Protection of Systems
and Information

▼ Since 2008

▄ Coding and crypto (Math)

- *coding theory*
- *hash functions*
- *e-voting*
- ...

▄ Security (Computer Science)

- *trust management & access control*
- *physical aspects of security*
- *side-channel attacks*
- ...

▼ Young, big and dealing with hot topics



Eindhoven Institute for the Protection of Systems and Information

- [General information](#)

- [Staff](#)

- [SYMPOSIUM:
First anniversary of
EIPSI](#)

- [Seminars / Courses](#)

- [Publications](#)

- [Education](#)

- [Press releases](#)

- [Upcoming /
Past events](#)

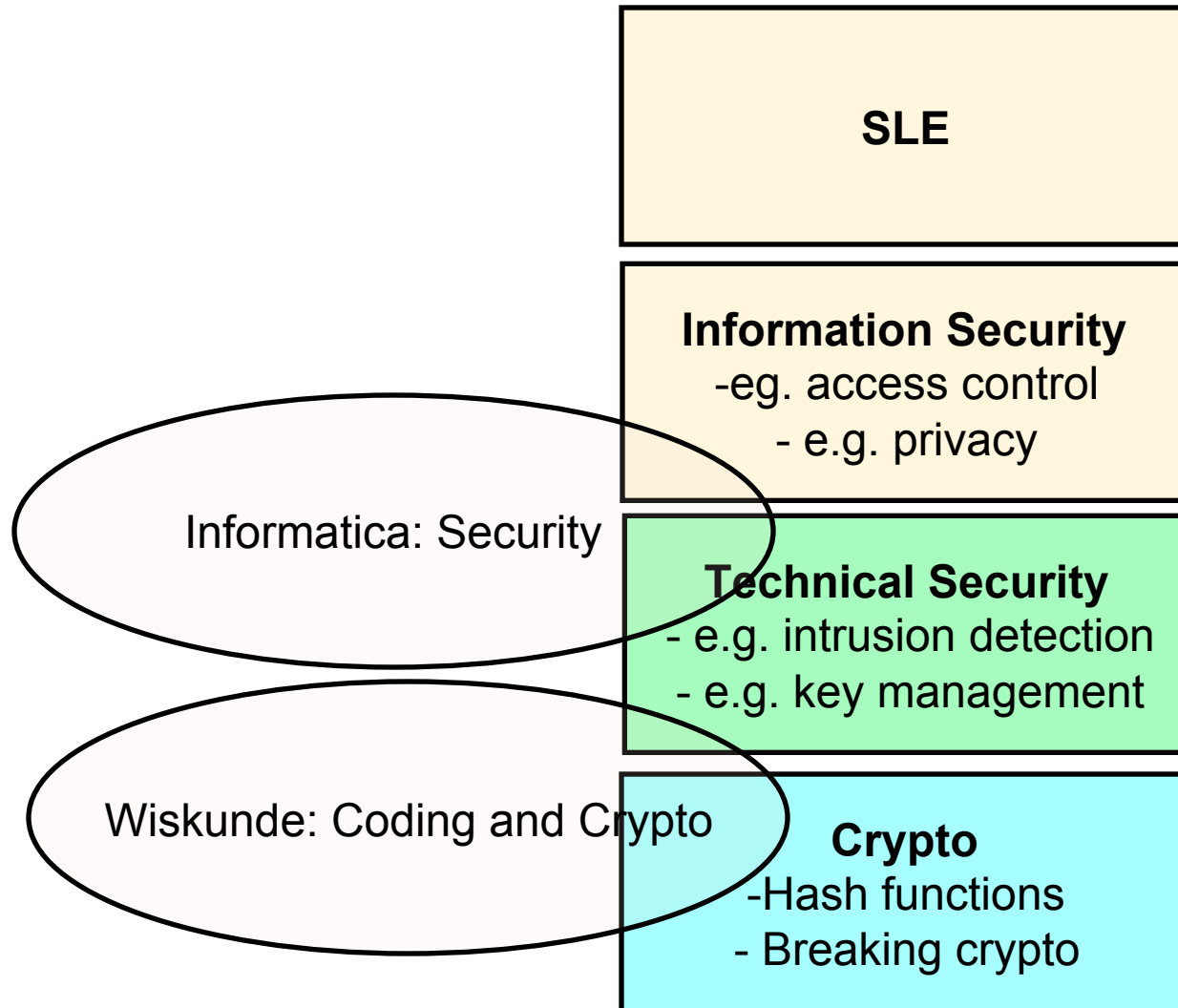
Press releases

December 30, 2008

Experts uncover weakness in Internet security

Independent security researchers in California and researchers at the Centrum Wiskunde & Informatica (CWI) in the Netherlands, EPFL in Switzerland, and EIPSI (TU/e) in the Netherlands have found a weakness in the Internet digital certificate infrastructure that allows attackers to forge certificates that are fully trusted by all commonly used web browsers. As a result of this weakness it is possible to impersonate secure websites and email servers and to perform virtually undetectable phishing attacks, implying that visiting secure websites is not as safe as it should be and is believed to be. The results were presented at the 25C3 security congress in Berlin on the 30th of December 2008. It has already led to an increased adoption of more secure cryptographic standards on the Internet and therewith increased the safety of the Internet.

Security vs Cryptography



Network/computer security vs. cryptography

- ▼ Breach of security:
 - ▄ try to get direct access to the secret key rather than breaking the cryptography
 - ▄ try to bypass the cryptography altogether
 - ▄ try to influence/break random number generation
 - ▄ e.g., viruses, Trojan horses, Denial of Service, buffer overflows, password sniffing, Tempest (or, van Eck phreaking)
- ▼ In between: side-channel attacks such as Kocher's Differential Power Analysis (usually, for smart cards)



Kerckhoffs' Principle

Auguste Kerckhoffs (1835-1903) was a Dutch linguist and cryptographer

- ▼ Formulated 6 principles of practical cipher design:
 1. The system should be, if not theoretically unbreakable, unbreakable in practice.
 2. **The design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents**
 3. The *key should be memorable* without notes and should be easily changeable
 4. The cryptograms should be transmittable by telegraph
 5. The apparatus or documents should be portable and operable by a single person
 6. The system should be easy, neither requiring knowledge of a long list of rules *nor involving mental strain*

Master Thesis (1)

▼ Concrete examples:

- // @Chipper: Differential Power Analysis, get hold of a secret key from a smart-card
- // @Interpay: use of smart cards for anonymous payments
- // @British Telecom: electronic voting
- // @AIVD: cybersecurity
- // @Chess: secure communication in ad-hoc sensor networks
- // ...

Afstuderen (2)

- // **VoIP SPAM**
- // **Quantum cryptography:**
 - *using photons for transmitting data securely*
- // **Digital Rights Management:**
 - *limits and possibilities of **code obfuscation***
- // Study of **algebraic attacks** on block ciphers such as AES (Advanced Encryption Standard)
- // Implementation of **Byzantine agreement** for a secure broadcast channel
- // **Fox-IT** (digital forensics).

Potential Employers

- ▼ **CMG, Origin, CAP Gemini, IBM, ...**
- ▼ **Certicom, Entrust, RSA Security, Verisign, Cryptovision, Cryptomathic, Sectra, ...**
- ▼ **Accenture, PWC, KPMG, Ernst&Young, ...**
- ▼ **Intertrust, Philips: copyright protection, watermarking, digital right management (DRM)**
- ▼ **Overheid (NSA, NBV), universiteit, instituten**
- ▼ **Banken, Interpay, ...**
- ▼ **Militaire industrie, TNO, ...**
- ▼ **Multinationals Shell**
- ▼ **Telecoms: KPN, BT, AT&T, ...**

Contact details

www.securitymaster.nl or
www.kerckhoffs-institute.org

Prof. dr. Sandro Etalle, s.etalles@tue.nl

Security Group

dr. ir. L.A.M. (Berry) Schoenmakers, berry@win.tue.nl

Coding and Crypto group

Dept. of Math. and CS

Eindhoven University of Technology

P.O. Box 513

5600 MB Eindhoven

Netherlands

<http://www.win.tue.nl/~setalle/> <http://www.win.tue.nl/~berry/>

cloakware® Secure software... from the inside out®

how to buy
site map
contact

customers & partners

A few of Cloakware's
[customers](#) and [partners](#):

home

industry

products & services

support

partners

about us

news & events

careers

From smart phones to computers to weapons systems...

Cloakware solutions are on hundreds of millions of devices, protecting the assets of some of the world's largest, most recognizable and technologically advanced companies. As the global leader in software protection, we have a track record in each of the industries below, protecting software, media, passwords and data from unauthorized use, access, analysis, tampering, copying and reverse engineering.

Select your industry to learn how we can help you solve your security challenges.



Try the [CSPM Savings Calculator](#) to see how much your organization could save while protecting your customer or citizen data from internal attack. It could be millions!

Under pressure to deliver secure consumer electronics devices? The whitepaper [Sustainable Device Security](#) explains how.

news

[February 13, 2007](#)

Cloakware Position Paper Reveals Crucial Password Security Measures for FISMA Compliance

[February 5, 2007](#)

Cloakware Position Paper Delivers Comprehensive Password Management Plan For PCI Compliance

[January 29, 2007](#)

New Cloakware Server Password Manager is First to Eliminate Application-to-Application and Privileged Password Risks



upcoming events

[February 27th, 2007](#)

Register today to attend a complimentary webcast: "The Hidden Application Password Problem"

[March 29th, 2007](#)

The Financial World of Information Technology

cloakware server password manager

cloakware robustness solutions

cloakware security suite

professional services