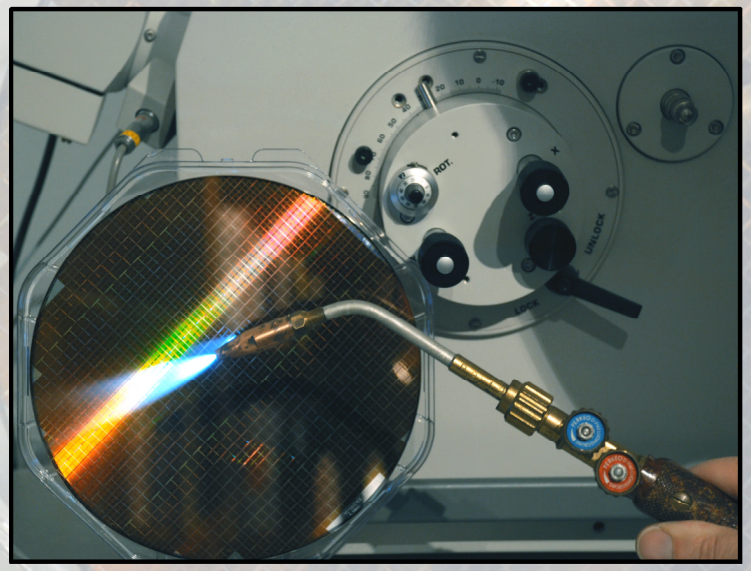
Hardware-Trojaner in Security-Chips

Eine Reise auf die dunkle Seite



Peter Laackmann
Marcus Janke

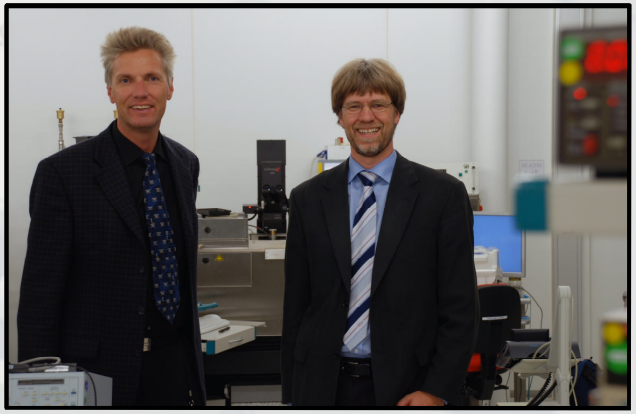
1989

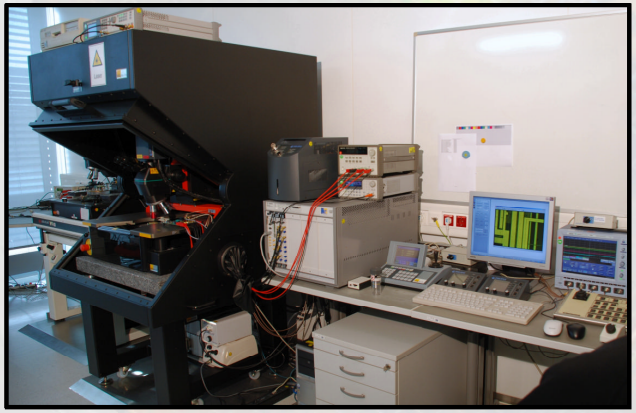
- Seit 1989: Chipkarten-Forscher
- Brunsbüttel, Kiel, Hamburg
- Fachautoren für Chipkartensicherheit
- Beratung Datensicherheit und Datenschutz
- Sicherheitsschwächen aufgedeckt:
  z.B. Krankenversichertenkarte, ec-Karte
- 1999 von Headhunter kontaktiert

Pictures: Private Archive M.Janke, P.Laackmann

2015

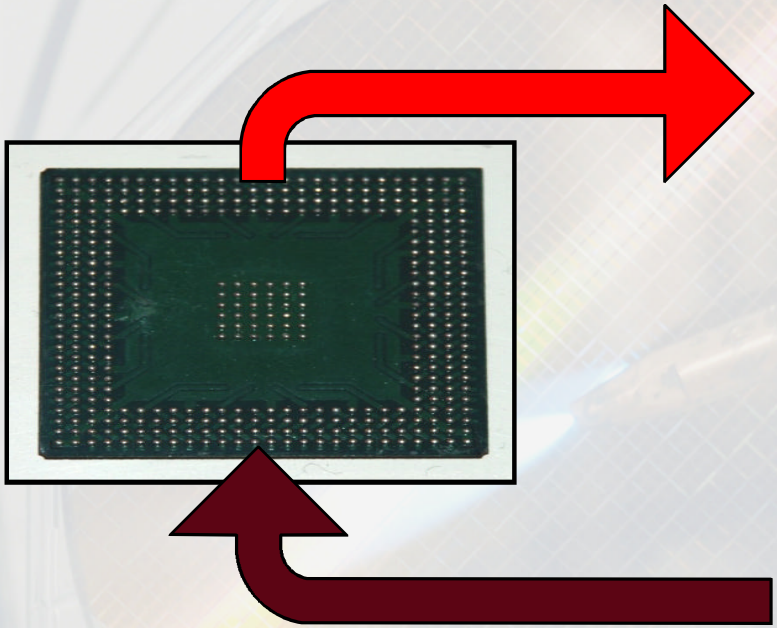
- Seit 1999: Mitarbeiter der Infineon Technologies AG
- München
- Chipsicherheit (Operativ&Strategisch)
- Leitung der internen Experten(“Hacker")gruppe
- Entwicklung neuer Angriffsmethoden
- Projektion teurer Angriffsmethoden auf Amateurmittel
- Private Forschung läuft weiter…





Pictures: M.Janke/P.Laackmann (Infineon)

Der gefährliche “Zweck” von Hardware-Trojanern



EXFILTRATION
- Daten (Betriebsdaten, persönliche Daten, Parameter, Logs)
- Kryptografische Schlüssel oder Teile davon
- Startwerte für Pseudo-Zufallszahlengeneratoren
- Identität (Chip-ID, System-ID, Personen-Identität, Verhalten)
- Code (Firmware, OS, Apps, FPGA-Netzlisten)

INFILTRATION
- Code (Malware)
- Daten (modifizierte Parameter)
- Bekannte oder schwache Schlüssel für Kryptografie
- Bekannte Startwerte für Pseudo-Zufallszahlengeneratoren
- “Kompromat” (belastendes Material)

Pictures: Private Archive M.Janke, P.Laackmann

Die Begriffe – Von der “Bugdoor” zum “Trojaner”

HORIZONTE
SERIE: VERBRECHEN DER ZUKUNFT

Foto: Adam Voorhes, Sydney Robin Tribe

Böse Überraschung

Gegen Software-Schädlinge schützen sich heutzutage selbst Computer-Laien mit Firewalls und Virenscannern. Aber was ist, wenn die Angreifer schon **in der Hardware lauern?**

VON CLAUDIA WESSLING

Was wäre, wenn? Wenn Ihr Büro verwanzt wäre? Der Kopierer die Konstruktionspläne für den neuen Motor heimlich nach China schickt? Oder die nagelneue Videokonferenz-Anlage die vertraulichen Vertragsverhandlungen mitschneidet und den Mitschnitt heimlich in die USA sendet? Unmöglich, sagen Sie? Das Firmennetz ist mit Firewalls gesichert, überall laufen die neuesten Virenscanner? Das wird nichts nützen. Denn möglicherweise ist der Spion ganz woanders: tief in den Eingeweiden der Hardware versteckt wie die Larve der Mehlmotte in der Müslipackung.

Ausländische Mächte oder kriminelle Datenhändler, die elektronische Hintertüren in Computerchips einbauen, könnten persönliche Daten oder Firmengeheimnisse ausspähen. Sie könnten sensible militärische Ausrüstung kopieren oder Waffensysteme gezielt sabotieren. Klingt paranoid? Deutsche Wissenschaftler erforschen diese neue Bedrohung. „Wir haben gezeigt, dass sich das Problem schon auf der untersten Ebene der Chipherstellung stellt“, sagt Georg Becker vom Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum.

Seitdem das Defense Science Board, eine Forschungsabteilung des Pentagons, 2005 erstmals vor den Gefahren manipu-

42 TECHNOLOGY REVIEW | JULI 2015

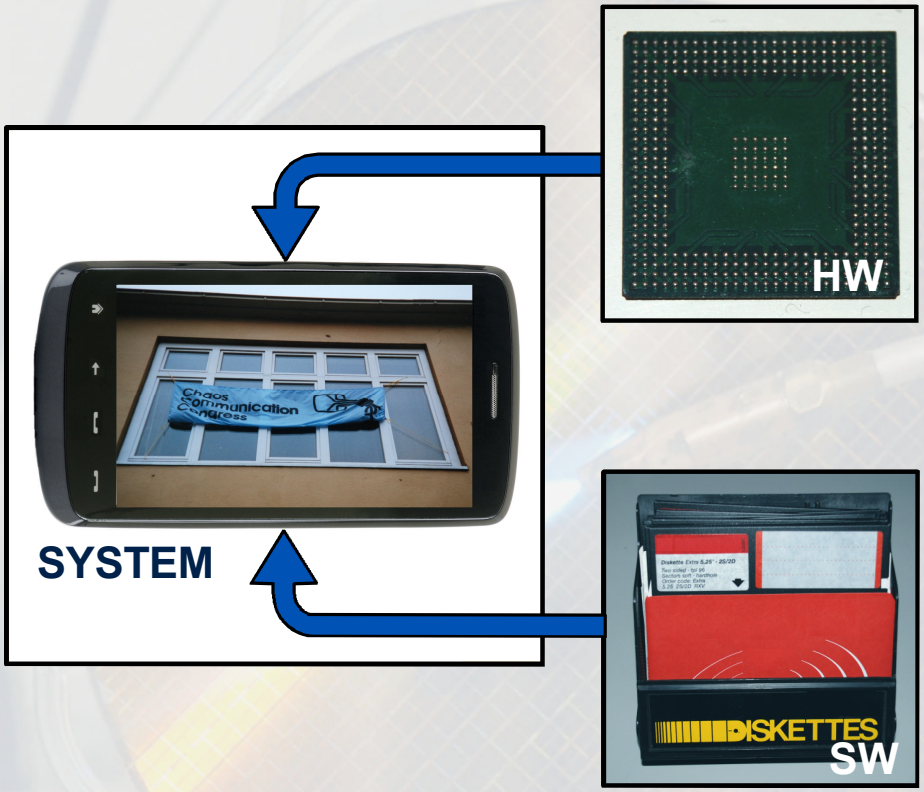
BUGDOOR
- Unbeabsichtigt implementiert
- Basiert auf schlechter Programmierung („Bug“+“Door“)
- Kann von jedem genutzt werden, der die Bugdoor kennt

BACKDOOR
- Beabsichtigt implementiert
- Speziell entwickelt, für genau diese Funktion
- Kann von einem Trojaner installiert und kontrolliert werden

TROJANER
- Beabsichtigt implementiert
- Täuscht oft eine andere, ungefährliche Funktion vor
- Kann eine Backdoor installieren und kontrollieren

→ Die Begriffe „Trojaner“ und „Backdoor“ werden oft vermischt

Wo können sich Trojaner verstecken ?



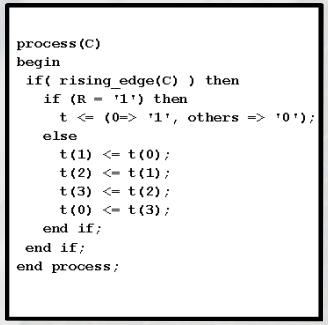
HARDWARE
- Implementierung des Trojaners aufwändig & teuer
- Identifizierung schwierig
- Beweis aufwändig

SYSTEM
- Ist der Wirkungsort der Trojaner
- Besteht aus Hardware und Software
- Manipulationsmöglichkeiten multiplizieren sich

SOFTWARE
- Implementierung des Trojaners einfach & billig
- Identifizierung oft einfach, manchmal aufwändig
- Beweis einfach

Pictures: Private Archive M.Janke, P.Laackmann

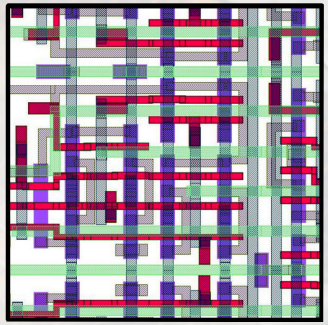
Normaler Fertigungsablauf der Chipherstellung



```
process(C)
begin
 if( rising_edge(C) ) then
   if (R = '1') then
     t <= (0=> '1', others => '0');
   else
     t(1) <= t(0);
     t(2) <= t(1);
     t(3) <= t(2);
     t(0) <= t(3);
   end if;
 end if;
end process;
```

VHDL
(Schaltungsbeschreibung)

Die gewünschte Funktion des Chips wird in einer Hardware-Beschreibungs-Sprache definiert.

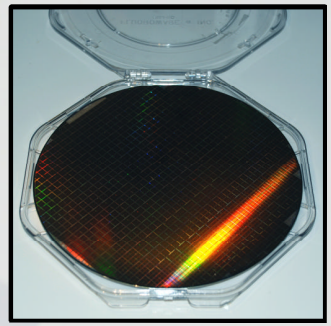


Layout
(Schaltungsanordnung)

Mittels Compiler wird eine Netzliste erstellt, daraus entstehen die Schaltelemente und Verdrahtungen.

Maskensatz
(Belichtungsvorlagen)

Aus dem Layout wird ein Satz von optischen Vorlagen für die einzelnen Schichten der Chips erzeugt.



Wafer
(fertige Chips)

Nach einigen zehn Prozess-Schritten ist ein Wafer fertig und wird anschliessend in einzelne Chips getrennt.

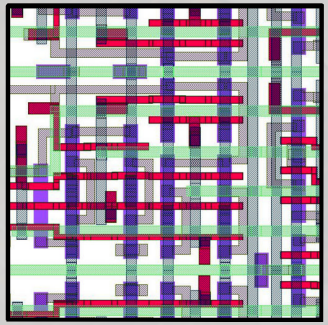
Pictures: Private Archive M.Janke, P.Laackmann

Trojaner lassen sich in jeder Fertigungsstufe einbauen

```
process(C)
begin
 if( rising_edge(C) ) then
   if (R = '1') then
     t <= (0=> '1', others => '0');
   else
     t(1) <= t(0);
     t(2) <= t(1);
     t(3) <= t(2);
     t(0) <= t(3);
   end if;
 end if;
end process;
```

VHDL

- Insider ändern die Funktion direkt im VHDL Code und bringen dadurch Hardware-Trojaner ein
- Implementierung einfach
- Entdeckung ist normalerweise einfach

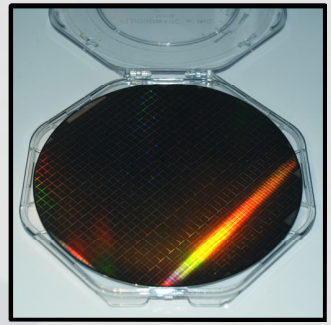


Layout

- Insider ändern die Schaltungselemente und Verdrahtungen im Layout
- Implementierung mittelschwer
- Entdeckung ist normalerweise mittelschwer

Maskensatz

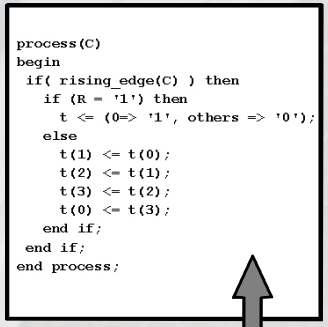
- Insider ändern die Masken und damit auch die Strukturen des Chips
- Implementierung schwierig
- Entdeckung ist normalerweise schwer



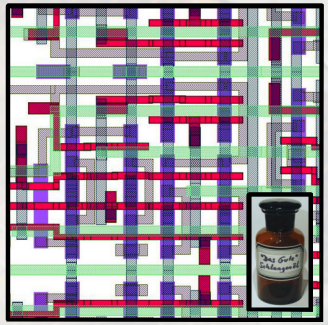
Wafer

Pictures: Private Archive M.Janke, P.Laackmann

Schlangenöle können Trojaner stark begünstigen

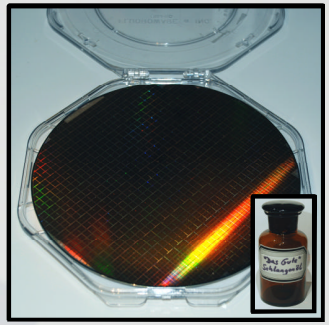


VHDL

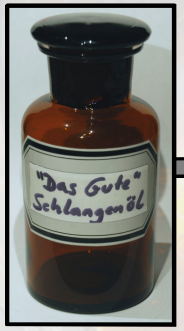


Layout

Maskensatz



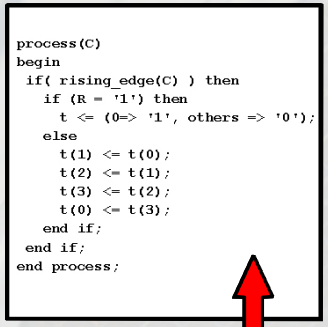
Wafer



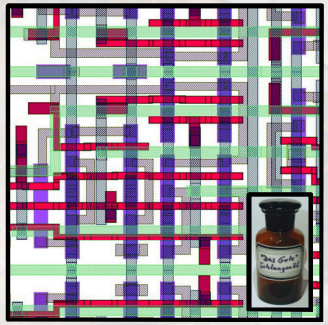
Zweifelhafte “Sicherheitsfeatures”, auch “Snake Oil” oder “Schlangenöl” genannt, können eine erhebliche Gefahr für die Sicherheit der Hardware darstellen:
Sie können den Einbau von Trojanern stark vereinfachen und deren Entdeckung extrem erschweren.

Pictures: Private Archive M.Janke, P.Laackmann

Schlangenöle können Trojaner stark begünstigen

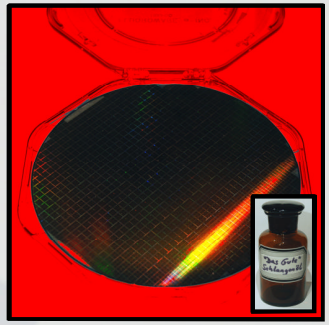


VHDL



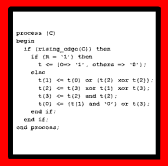
Layout

Maskensatz



Wafer

Bei Anwesenheit von Snake Oil Features können Trojaner unbemerkt bereits in den Quellcode der Hardware eingebracht werden. Dadurch kann die Detektion stark erschwert werden.

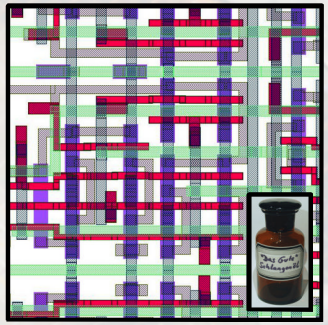


Pictures: Private Archive M.Janke, P.Laackmann

Beispiel: “White-Box Kryptografie”

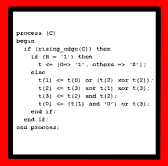
```
process(C)
begin
 if( rising_edge(C) ) then
   if (R = '1') then
     t <= (0=> '1', others => '0');
   else
     t(1) <= t(0);
     t(2) <= t(1);
     t(3) <= t(2);
     t(0) <= t(3);
   end if;
 end if;
end process;
```

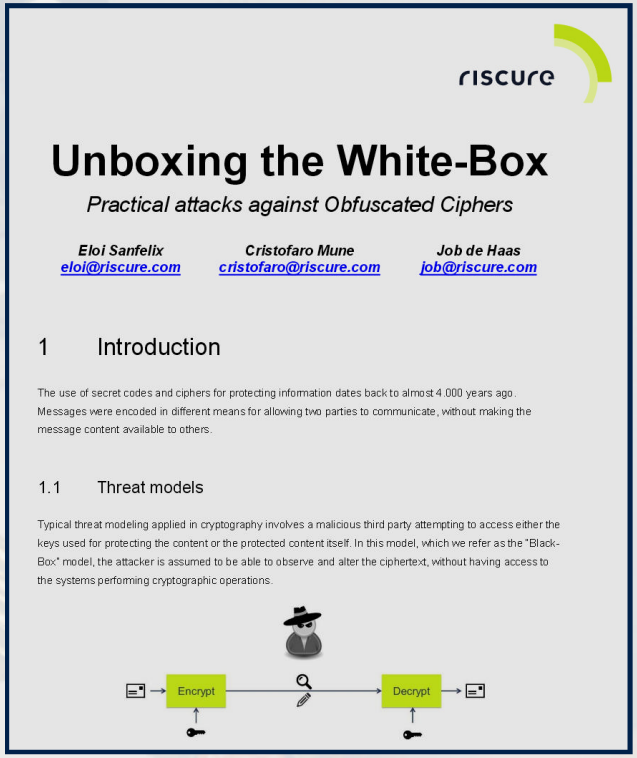
VHDL



Layout

“White-Box Kryptografie” übersetzt kryptografische Keys in unterschiedliche möglichst komplexe Software-Codes. Hier könnten schwer erkennbare Trojaner eingeschleust werden.





riscure

Unboxing the White-Box

Practical attacks against Obfuscated Ciphers

Eloi Sanfelix eloi@riscure.com
Cristofaro Mune cristofaro@riscure.com
Job de Haas job@riscure.com

1 Introduction

The use of secret codes and ciphers for protecting information dates back to almost 4.000 years ago. Messages were encoded in different means for allowing two parties to communicate, without making the message content available to others.

1.1 Threat models

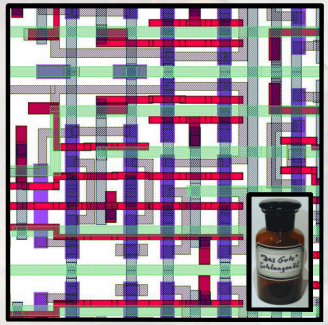
Typical threat modeling applied in cryptography involves a malicious third party attempting to access either the keys used for protecting the content or the protected content itself. In this model, which we refer as the "Black-Box" model, the attacker is assumed to be able to observe and alter the ciphertext, without having access to the systems performing cryptographic operations.

Pictures: Private Archive M.Janke, P.Laackmann

Schlangenöle können Trojaner stark begünstigen

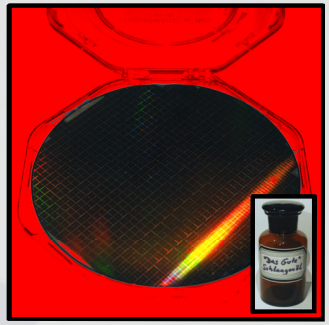
```
process(C)
begin
 if( rising_edge(C) ) then
   if (R = '1') then
     t <= (0=> '1', others => '0');
   else
     t(1) <= t(0);
     t(2) <= t(1);
     t(3) <= t(2);
     t(0) <= t(3);
   end if;
 end if;
end process;
```

VHDL

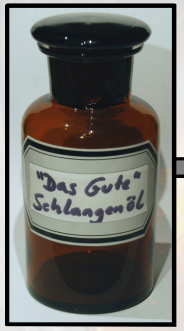


Layout

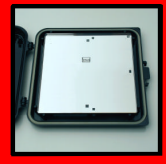
Maskensatz



Wafer



Snake Oil Features können das Einbringen von Trojanern auch im letzten Schritt der Chipherstellung erleichtern: So könnte eine einfache zusätzliche Maske für die Manipulation ausreichen.



Pictures: Private Archive M.Janke, P.Laackmann

Beispiel: “Physical ‘Unclonable’ Functions”

Cloning Physically Unclonable Functions

Clemens Helfmeier*, Christian Boit
Semiconductor Devices,
Dept. of High-Frequency and Semiconductor System Tech.,
Technische Universität Berlin,
Berlin, Germany
{clemens.helfmeier,christian.boit}@.tu-berlin.de

Dmitry Nedospasov*, Jean-Pierre Seifert
Security in Telecommunications,
Dept. of Software Eng. and Theoretical Computer Science,
Technische Universität Berlin,
Berlin, Germany
{dmitry,jpseifert}@sec.t-labs.tu-berlin.de

* These authors contributed equally to this work

***Abstract*—As system security demands continue to evolve, Physically Unclonable Functions (PUFs) are a promising solution for secure storage on Integrated Circuits (ICs). SRAM PUFs are among the most popular types of PUFs, since they require no additional circuitry and can be implemented with on-die memories such as caches and data memory that are readily available on both ASICs and FPGAs. This work demonstrates that SRAM PUFs are not well suited as PUFs, as they do not meet several requirements that constitute an ideal PUF. The compact nature of SRAM, standard interconnects and resiliency to environmental effects make SRAM PUFs particularly easy to clone. We consider several ways in which SRAM PUFs can be characterized and demonstrate a Focused Ion Beam circuit edit with which we were able to produce a physical clone of our Proof-of-Concept SRAM PUF implementation. As a result of the circuit edit, when challenged, the physical clone produced an identical physical response to the original device. To the best of our knowledge, this is the first work in which a physical clone of a Physically Unclonable Function was produced.**

I. Introduction

Secure storage is a critical component of any secure system and is often delegated to dedicated hardware. In many cases dedicated security Integrated Circuits (IC) are incorporated into the designs of secure systems specifically to take care of such tasks. Secret data can be programmed into a secure IC during production by the vendor or personalization by the end-user [1]. In systems lacking Non-Volatile Memory (NVM), key storage and distribution can be particularly difficult.

However, even with NVM, an attacker can utilize any number of techniques to read-out on-die memories [2]. One especially promising avenue to solve the problems of key storage are Physically Unclonable Functions (PUFs) since intrinsic process variations can be used to implement unique challenge/response pairs for every IC [3], [4]. When implemented correctly, a key does not have to be stored at all, but is instead derived from the characteristic response of a PUF. Ideally, the characteristic response changes whenever the IC is altered, i.e. when the device is depackaged. Such behavior provides an additional layer of tamper-resistance [5].

One of the most researched and popular classes of PUFs are memory-based PUFs [6]. Such PUFs utilize the settling state of volatile memory, such as Static Random Access Memory (SRAM), to implement unique challenge/response pairs. Such memories are already present on secure ICs and offer hardware vendors substantial flexibility during manufacturing. Memories can be partially or completely re-purposed to temporarily or permanently act as a PUF at startup. SRAM is commonly included in such solutions, making SRAM-based PUFs especially popular [7]. SRAM and SRAM-based PUFs are also particularly resilient to temperature variations and are generally more compact than many other memory-based PUFs [8].

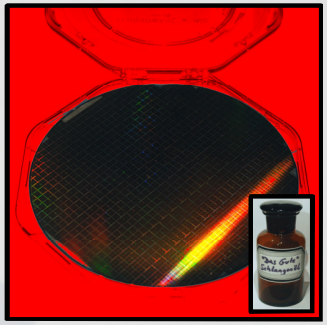
Though several works to date have described the characteristics of an ideal PUF, this work focuses on the original definitions introduced in [3]. This work demonstrates that SRAM PUFs violate at least the following characteristics of an ideal PUF:

- **Manufacturer resistant -** It should be infeasible to create a second PUF that generates the same response.
- **Hard to characterize -** It should be infeasible to characterize the response of a PUF.
- **Controlled -** The PUF should be difficult to access for the attacker and implement some tamper-resistance.

The main contributions of this paper are: (1) *First successful physical clone.* We successfully reproduced the “unique” response of our Proof of Concept (PoC) SRAM PUF implementation in a second identical device. We used a Focused Ion Beam (FIB) circuit edit (CE) to produce a fully-functioning second instance of the device with an identical physical response to that of the target device. To the best of our knowledge this is the first successful hardware-based cloning attack against a PUF. (2) *Several strategies to read out SRAM.* If the entire contents of the SRAM can be extracted, an SRAM PUF can be fully-characterized. We review several techniques with which the contents of SRAM at startup can be extracted allowing an attacker to recover the unique response of the IC. (3) *Discussion and Countermeasures.* We discuss several inherent weaknesses of memory-based PUFs as compared to other classes of PUFs. We also introduce several mitigation techniques with which hardware vendors can make our attack significantly less cost-effective for the attacker.

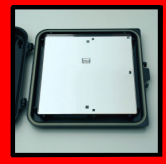
The rest of this paper is structured as follows: In Section II we provide additional necessary background information on the 6T-SRAM cell circuit as well as SRAM PUF implementations. The FIB CE is explained in Section III. In Section IV we

Maskensatz



Wafer

SRAM-PUF Speicherzellen liefern beim Einschalten individuelle Werte, aus denen Keys erzeugt werden können. Das Einschaltverhalten ist aber mit einer zusätzlichen Maske manipulierbar.



Pictures: Private Archive M.Janke, P.Laackmann

Beispiel: “Camouflage Chip Design”

Stealthy Dopant-Level Hardware Trojans *

Georg T. Becker[1], Francesco Regazzoni[2], Christof Paar[1,3], and Wayne P. Burleson[1]

[1]University of Massachusetts Amherst, USA
[2]TU Delft, The Netherlands and ALaRI - University of Lugano, Switzerland
[3]Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum, Germany

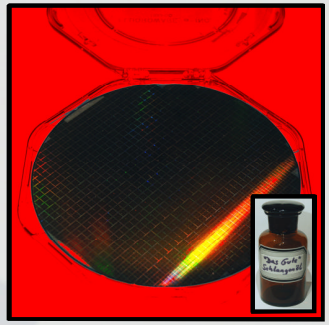
Abstract. In recent years, hardware Trojans have drawn the attention of governments and industry as well as the scientific community. One of the main concerns is that integrated circuits, e.g., for military or critical-infrastructure applications, could be maliciously manipulated during the manufacturing process, which often takes place abroad. However, since there have been no reported hardware Trojans in practice yet, little is known about how such a Trojan would look like, and how difficult it would be in practice to implement one.
In this paper we propose an extremely stealthy approach for implementing hardware Trojans below the gate level, and we evaluate their impact on the security of the target device. Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors. Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), our family of Trojans is resistant to most detection techniques, including fine-grain optical inspection and checking against “golden chips”. We demonstrate the effectiveness of our approach by inserting Trojans into two designs — a digital post-processing derived from Intel’s cryptographically secure RNG design used in the Ivy Bridge processors and a side-channel resistant SBox implementation — and by exploring their detectability and their effects on security.

Keywords: Hardware Trojans, malicious hardware, layout modifications, Trojan side-channel

1 Introduction

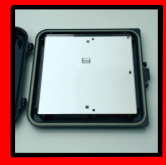
Integrated circuits (ICs) are the heart of virtually all modern applications. This includes sensitive and safety critical devices, such as medical devices, automotive, industrial control systems, power management or military devices. Often circuit blocks in a single IC are designed by different parties, manufactured by

Maskensatz



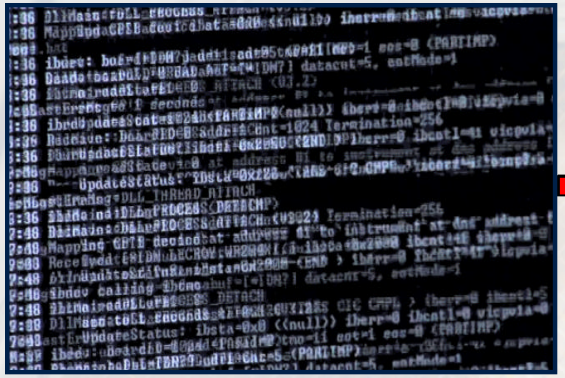
Wafer

Universelle Logikelemente werden in vielen “Camouflage” Designs nur durch eine Maske letztlich funktional festgelegt. Solche Elemente sind daher ebenso mit einer zusätzlichen Maske manipulierbar.

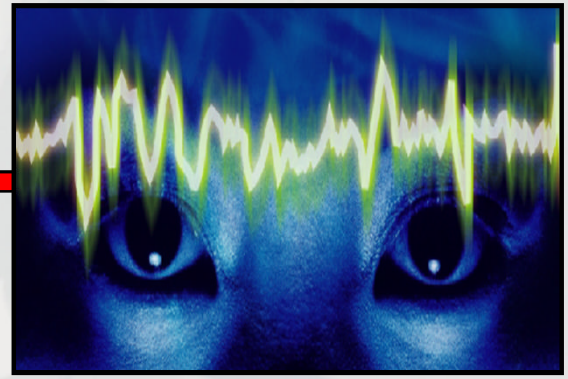


Pictures: Private Archive M.Janke, P.Laackmann

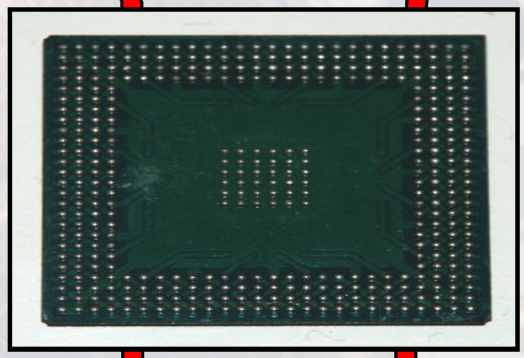
Backdoors – Mittel zur versteckten Kommunikation

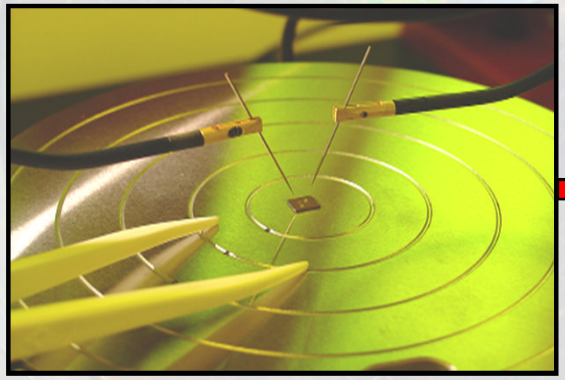


Protokoll-Backdoors



Seitenkanal-Backdoors

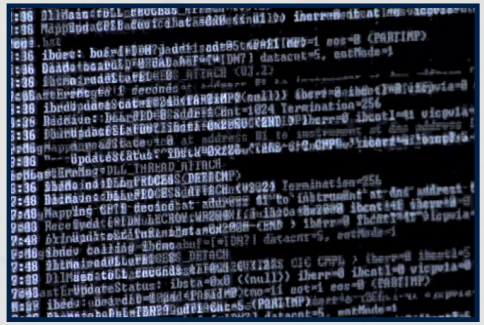




Manipulations-Backdoors

Fehlerinduktions-Backdoors

Beispiele: Protokoll-Backdoors



Undokumentierte Befehle/Sequenzen
• Versteckte, nicht beschriebene Befehle erlauben Zugriff auf interne Daten oder Code

Geschwächte Krypto-Funktionen
• Verschlüsselungs-Algorithmen sind absichtlich in ihrer Stärke beeinträchtigt

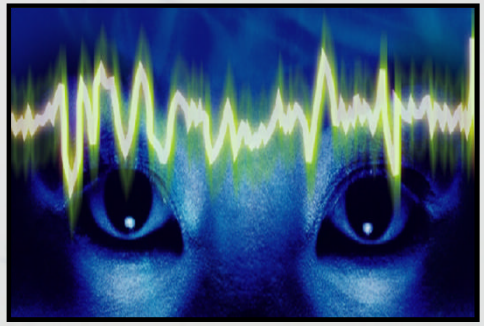
Watermarking/Undokumentierter Output
• In den vom Chip ausgegebenen Daten sind Zusatzinformationen versteckt

Generalschlüssel
• Nicht dokumentierte übergreifende Schlüssel erlauben den unbemerkten Zugang

Beispiel-Quellen

Y. Dodis, C. Ganesh, A. Golovnev, A. Juels, T. Ristenpart, *A Formal Treatment of Backdoored Pseudorandom Generators*, EUROCRYPT, Sofia, Bulgarien, 27.04.2015.
A. L. Young, *Building Robust Backdoors in Secret Symmetric Ciphers*, BlackHat, Las Vegas, USA, 28.07.2005.
A. Mishra, *Cryptographic Backdoors: Subverting the RSA*, COCON, Kochi, Indien, 22.08.2014.
S. Bhasin, J. L. Danger, S. Guilley, T. Ngo, L. Sauvage, *Hardware Trojan Horses in Cryptographic IP Cores*, FDTC, Santa Barbara, USA, 29.08.2013.
J. P. Aumasson, *SHA1 Backdooring and Exploitation*, BSIDES, Las Vegas, USA, 05.08.2014.
D. Kern, *Understanding and Implementing Encryption Backdoors*, CSC7002 Project Paper, 31.03.2012.

Beispiele: Seitenkanal-Backdoors



Stromprofil
• Auf den Stromverbrauch des Chips werden absichtlich Daten aufmoduliert

Elektromagnetische Abstrahlung
• Gezielt beeinflusste elektromagnetische Abstrahlung des Chips sendet Daten

Lichtabstrahlung
• Bewußt manipulierte Schaltungselemente senden Photonen aus, um Daten zu übermitteln

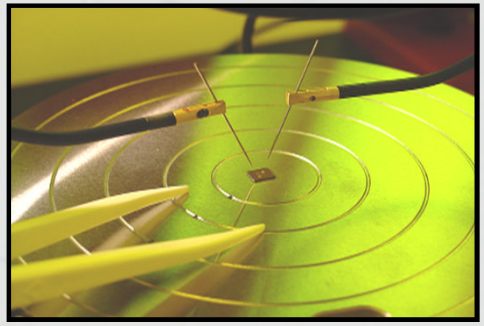
Potential der Signalleitungen
• Signalleitungen mit kritischem Inhalt werden vorsätzlich so gelegt, daß das Potential gemessen werden kann

Temperaturwerte
• Schaltungselemente mit hohem Energieverbrauch werden datenabhängig geschaltet, die Erwärmung wird beobachtet

Beispiel-Quellen

M. G. Kuhn, R. J. Anderson, *Soft Tempest - Hidden Data Transmission Using Electromagnetic Emanations*, Information Hiding, LNCS 1525, Springer-Verlag, Berlin, 1998.
R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, S. Capkun, *Thermal Covert Channels on Multi-core Platforms*, 24th Usenix Security Symposium, Washington, USA, 12.08.2015.
M. Kasper, A. Moradi, G. T. Becker, O. Mischke, T. Güneysu, C. Paar, W. Burleson, *Side Channels as Building Blocks*, J. Cryptogr. Eng., 2, 3, Springer Verlag, Berlin, 2012,143-159.
F. Kiamilev, R. Hoover, R. Delvecchio, N. Waite, S. Janansky, R. McGee, C. Lange, M. Stamat, *Demonstration of Hardware Trojans*, DEFCON 16, Las Vegas, USA, 09.08.2008.
L. Lin, M. Kasper, T. Güneysu, C. Paar, W. Burleson, *Trojan Side-Channels - Lightweight Hardware Trojans through Side-Channel Engineering*, CHES, LNCS 5747, 2009, 382–395.
A. Cui, *Emanate Like A Boss – Generalized Covert Data Exfiltration With Funtenna*, BlackHat, Las Vegas, USA, 05.08.2015.

Beispiele: Manipulations-Backdoors



Undokumentierte Anschlüsse
• Chip-Anschlüsse mit nicht beschriebener Funktion erlauben Zugang

Debug-Schnittstellen
• Zweckentfremdete Diagnose-Schnittstellen zum Lesen & Schreiben von Daten oder Code

Zur Manipulation bestimmte Signalleitungen
• Vorbestimmte Leitungen auf dem Chip werden verbunden oder getrennt, um Funktionen zu aktivieren

Dauerhaft veränderbare Schaltungselemente
• Mittels Ionenimplantation (lokale Bestrahlung) wird die Funktion einer Schaltung oder werden Daten verändert

Beispiel-Quellen

G. T. Becker, F. Regazzoni, C. Paar, W. P. Burleson, *Stealthy Dopant-Level Hardware Trojans*, CHES, Santa Barbara, USA, 22.08.2013.
J. Zaddach, *Exploring the Impact of a Hard Drive Backdoor*, RECON, Montreal, Kanada, 29.06.2014.
A. A. Ortega, S. Muniz, *Hardware Trojans and Malicious Logic*, RSA Conference, San Francisco, USA, 25.02.2014.
G. T. Becker, *Planting and Detecting Hardware Trojans*, ECRYPT Summer School: Challenges in Security Engineering, Bochum, Deutschland, 04.09.2012.
S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, Y. Zhou, *Designing and Implementing Malicious Hardware*, USENIX LEET, San Francisco, USA, 15.04.2008.

Beispiele: Fehlerinduktions-Backdoors

Temporär veränderbare Schaltungselemente
• Beeinflussung mittels Licht (Laser) aktiviert vorbestimmte Schaltungselemente

Extern beeinflußbare Speicherzellen
• Schreiben oder Löschen von Speicherzellen von außen (z.B. durch UV-Licht)

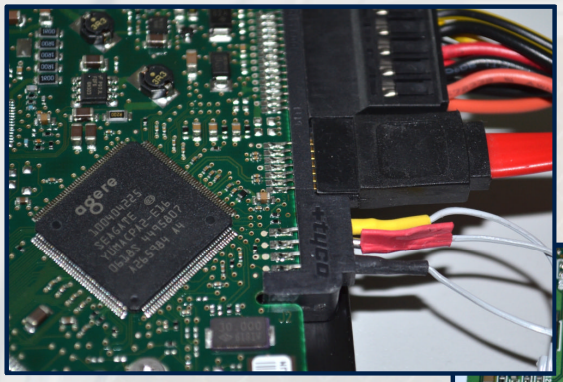
Störbarer Zufallszahlengenerator
• Schwächung der Zufallszahlen durch Einprägung einfacher oder bekannter Werte von außen

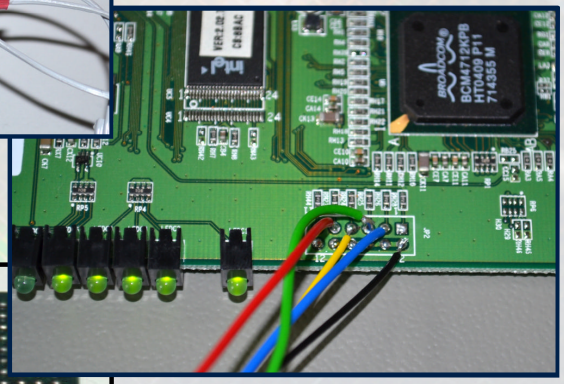
Sensoren mit absichtlicher Schutzlücke
• Sicherheits-Sensoren mit absichtlich lückenhafter Funktion erlauben gezielte Fehlerinduktion

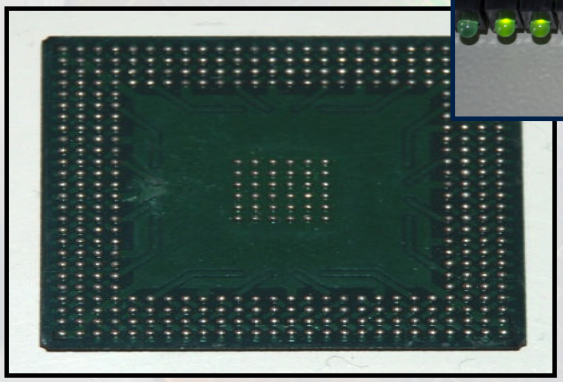
Beispiel-Quellen

R. Kumar, P. Jovanovice, W. P. Burleson, I. Polian, *Parametric Trojans for Fault-Injection Attacks on Cryptographic Hardware*, FDTC, Busan, Korea, 23.09.2014.
N. Tihanyi, *Fault-Injection Based Backdoors in Pseudo-Random Number Generators*, Studia Scientarium Mathematicarium Hungarica 52 (2), 2015, 233-245.
A. T. Markettos, S. W. Moore, *The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators*, CHES, Lausanne, Schweiz, 09.09.2009.
P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, *Contactless EM Active Attack on Ring Oscillator Based TRNG*, COSADE, Darmstadt, Deutschland, 04.05.2012.
X. T. Ngo, Z. Najm, S. Bhasin, D. B. Roy, J. L. Danger, S. Guilley, *Integrated Sensor - A Backdoor for Hardware Trojan Insertions*, EUROMICRO, Madeira, Portugal, 27.08.2015.

Analyse-Schnittstellen als mögliche Backdoor







Beispiel: FESTPLATTE
Debug-Port in PC-Festplatte,
erlaubt Einbringen von Trojanern in Firmware
oder direkten Zugriff auf die Platten-Daten

Beispiel: WLAN ROUTER
JTAG-Port in WLAN Router,
erlaubt Einbringen von Trojanern in Firmware
oder Erzeugung von „Rogue Access Points“

Beispiel: SICHERHEITSCHIP
Analyse-Port in Security Controller,
erlaubt Einbringen von Trojanern
oder Zugriff auf interne Daten und Software

Pictures: Private Archive M.Janke, P.Laackmann

Analyse-Schnittstellen als mögliche Backdoor

Türspion Innenseite
Viele Wohnungstüren sind “aus Sicherheitsgründen” mit einer solchen Optik ausgestattet.

Der Blick nach Aussen
Vorgesehene Funktion ist eine Analysemöglichkeit durch die Tür hindurch von Innen nach Aussen.

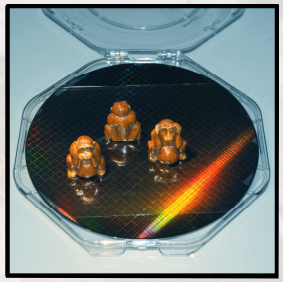
Türspion Aussenseite
Die stark gekrümmte Linse soll den Blick von Aussen nach Innen verhindern. Man sieht nur einen Punkt.

Der Blick nach Innen
Eine Türspion-Umkehroptik kehrt den Analyseweg um und erlaubt den Blick von Aussen nach Innen.

Pictures: Private Archive M.Janke, P.Laackmann

Warum gibt es Trojaner und Backdoors ?

Böser Wille



Ignoranz

Dummheit

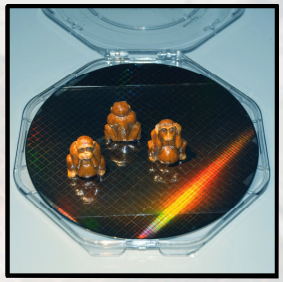
Guter Wille

Gründe	**Sabotage Erpressung Politische Motive**	**Verdrängung Zeitdruck Hierarchien**	**Bildungsmangel Fach-Idiotie Überforderung**	**Debugging Service Politische Motive**
Wirkung	**Auswirkungen sind bekannt und erwünscht**	**Auswirkungen sind teils bekannt und werden ignoriert**	**Auswirkungen sind nicht bekannt**	**Auswirkungen werden falsch eingeschätzt**

Pictures: Private Archive M.Janke, P.Laackmann

…und was kann man dagegen tun ?

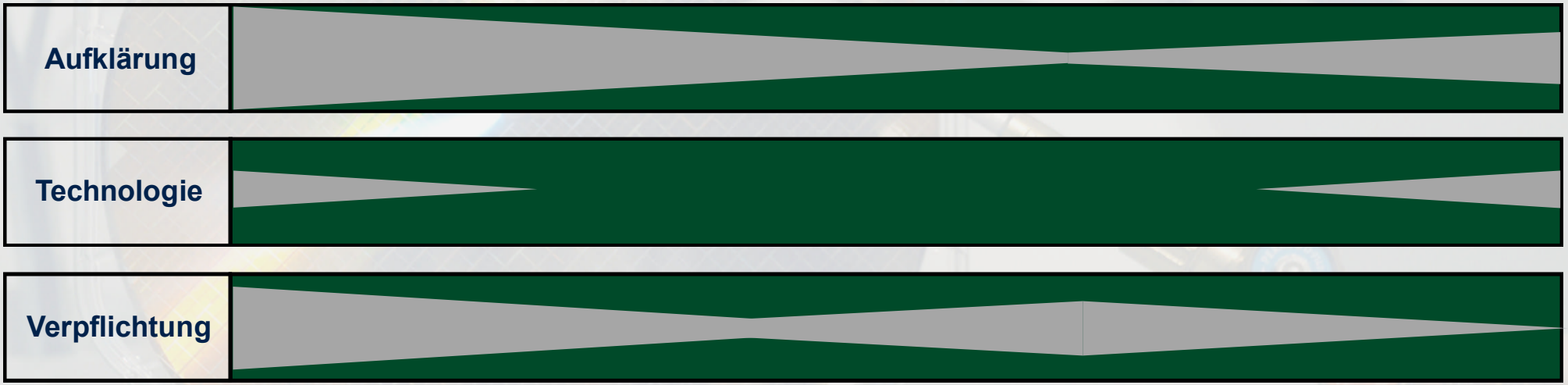
Böser Wille



Ignoranz

Dummheit

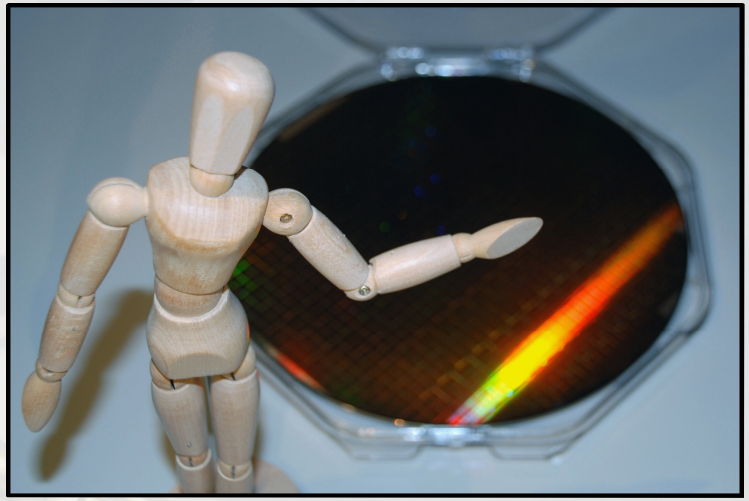
Guter Wille



Pictures: Private Archive M.Janke, P.Laackmann

Aufklärung gegen Trojaner und Backdoors

Technische Aspekte
- Gut gemeint ist noch lange nicht gut gemacht
- Security by Obscurity darf nicht das Ziel sein
- Debug-Schnittstellen passen nicht zu Sicherheitschips
- Entwickler denken nicht wie Hacker



Politische Aspekte
- Trojaner und Backdoors sind in der Praxis unkontrollierbar
- Trojaner/Backdoors können sich gegen ihren Urheber richten
- Politische Situationen können sich jederzeit ändern

Ethische Aspekte
- Backdoors können Personen in tödliche Gefahr bringen
- Backdoors zerstören Vertrauen in neue Technologien
- Generell: "*The Road to Hell is Paved with Good Intentions*"*

Abgeleitet von: Saint Bernard de Clairvaux ca. 1150, *"L'enfer est plein de bonnes volontés ou désirs"

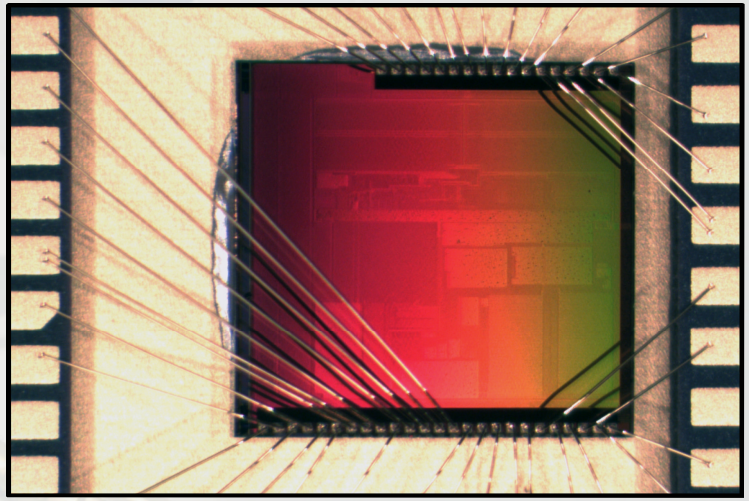
Pictures: Private Archive M.Janke, P.Laackmann

Technologie gegen Trojaner und Backdoors

Prophylaxe
- Keine Backdoor-fördernden Technologien einsetzen !
- Design muß eine Backdoor Implementierung erschweren
- Erkennung von Backdoors muß durch Design vereinfacht sein
- Security by Obscurity darf nicht das Ziel sein
- Auf Debug-Schnittstellen verzichten

Selbst-Tests
- Korrekte Funktion des Chips für den Nutzer überprüfbar machen
- Vorsicht: Ein Insider könnte solche Tests manipuliert haben

Erkennung
- Externe Tests am Chip zur Detektion von Manipulationen
- Vorsicht: Wirksamkeit meist sehr zweifelhaft

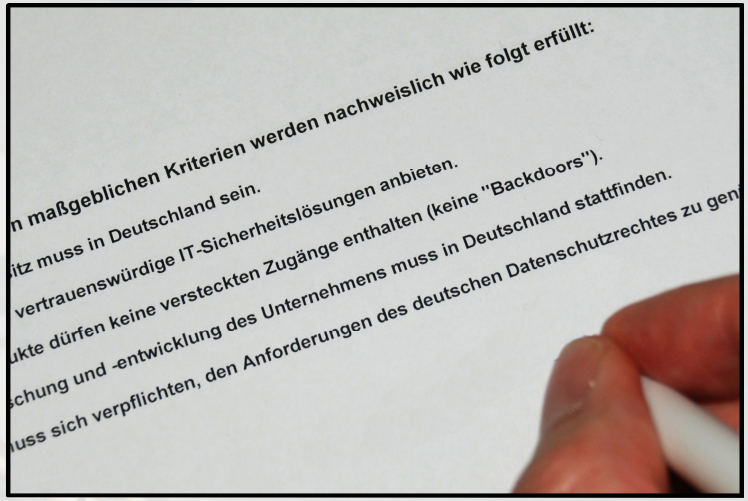


Pictures: Private Archive M.Janke, P.Laackmann

Verpflichtung gegen Trojaner und Backdoors

Auferlegte Verpflichtung
- Durch Anwender, die “No-Backdoor” Chips fordern
- Durch Gesetze oder Richtlinien
- Wer setzt durch ? Wer überprüft ?
- Realitätsabgleich nötig !

Selbstverpflichtung
- Backdoors sind für den Hersteller dadurch kein Vorteil mehr
- Backdoors werden damit zum ökonomischen Risiko
- Die Abwesenheit von Backdoors wird nun zum Vorteil
- Koppelung an weitere ethische Werte möglich
- Hersteller-Unternehmen wird zum Vorbild für Andere
- Schlüsselpunkt bleibt die zentrale Frage:
  “Warum soll sich ein Hersteller selbst verpflichten ?”



Beispiel für Selbstverpflichtung
(hier: Kriterien des TeleTrust e.V.)

Pictures: Private Archive M.Janke, P.Laackmann

Weitere Literatur

J. P. Anderson, *Computer Security Technology Planning Study ESD-TR-73-51*, Hanscom AFB, Air Force Electronic Systems Division, Bedford, USA, 1972.

M. Tehranipoor, H. Salmani, X. Zhang, *Integrated Circuit Authentication, Hardware Trojans and Counterfeit Detectors*, Springer Verlag, Cham 2014, ISBN 978-3-319-00815-8.

C. Wessling, *Böse Überraschung*, Technology Review, Juli 2015, 42-44.

A. Iqbal, *Understanding Integrated Circuit Security Threats*, MIT SDM Systems Thinking Webinar, 10.02.2014.

C. Helfmeier, D. Nedospasov, C. Boit, J.-P. Seifert, *Cloning Physically Unclonable Functions*, Proceedings HOST2013, 6th Annual IEEE International Symposium on Hardware-Oriented Security and Trust, Austin, USA, Juni 2013.

E. Sanfelix, C. Mune, J. de Haas, *Unboxing the White-Box - Practical attacks against Obfuscated Ciphers*, BlackHat EU, Amsterdam, Niederlande, 12.11.2015.

P. Rogaway, *The Moral Character of Cryptographic Work*, University of California, Davis, USA, 04.12.2015.

Have Fun Researching

Pictures: Private Archive M.Janke, P.Laackmann