Corporate Technology

SIEMENS

BISSAM

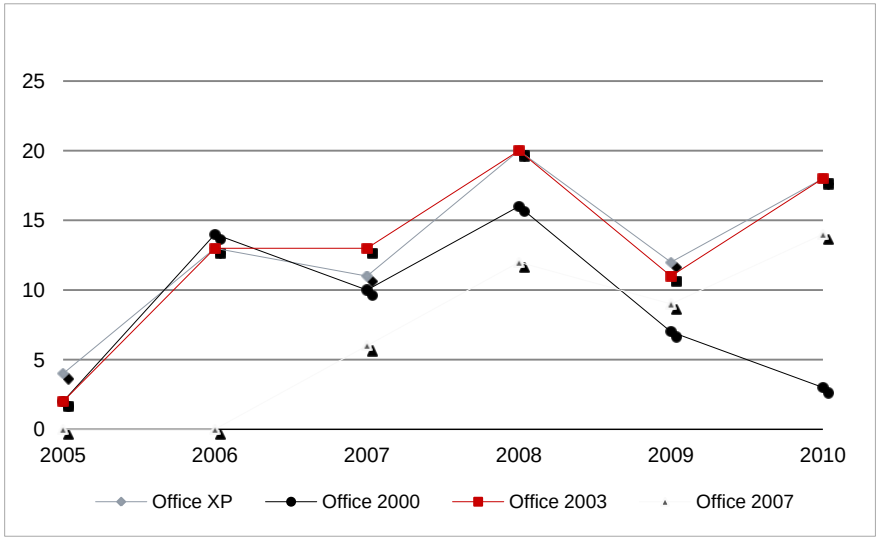
Automatic Vulnerability Identification of Office Documents

Thomas Schreck, Stefan Berger, Jan Göbel
Siemens CERT

DIMVA 2012
27.07.2012

Motivation

- Malware increasingly focuses on client applications
  - Security in Operating Systems is improving
  - Circumventing perimeter security controls
  - Microsoft Office documents are widely used
- Complex file formats lead to vulnerabilities



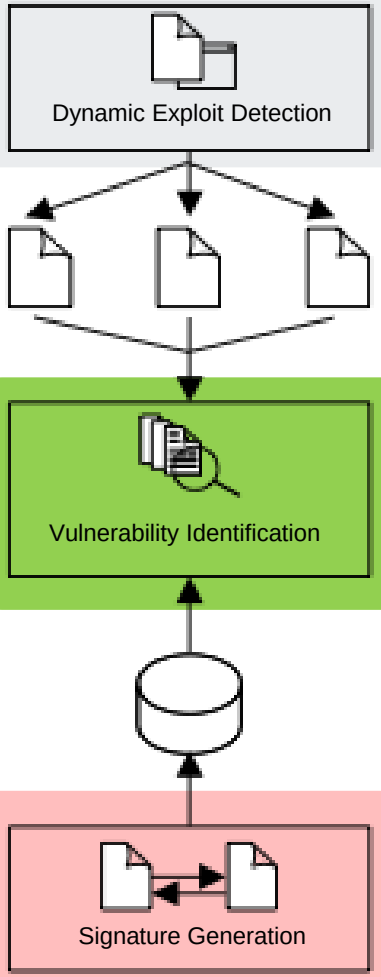
Source: Microsoft TechNet

SIEMENS

Motivation

- During malware-related incidents, the following questions are necessary to answer
  - Is the document malicious at all?
  - Is it exploiting a 0-day or a known vulnerability?
  - If known, which vulnerability is actually using?
  - Which update remediates this security flaw?
- Today's analysis tools either use manually created vulnerability signatures or concentrate on malware behavior

System Overview

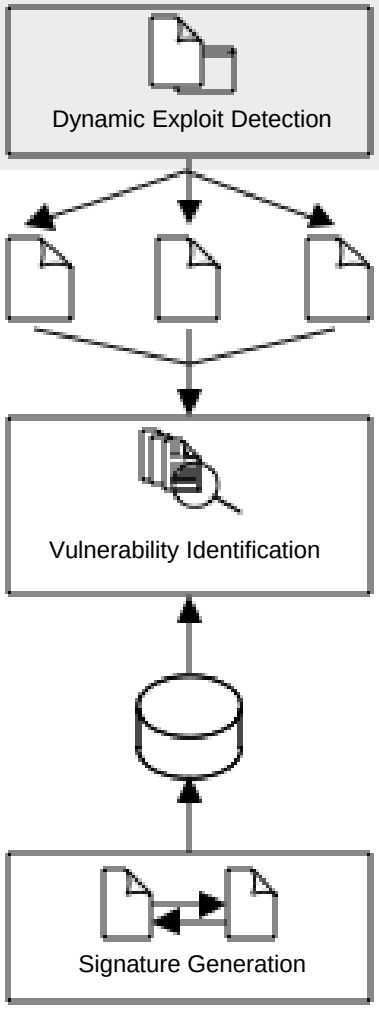


- Multiple Sandboxes
- Running different Microsoft Office Versions
- Detection of “Forbidden Behavior”

- Analysis of “Detection Logs“
- Mapping of “Forbidden Behavior” to Security Patches

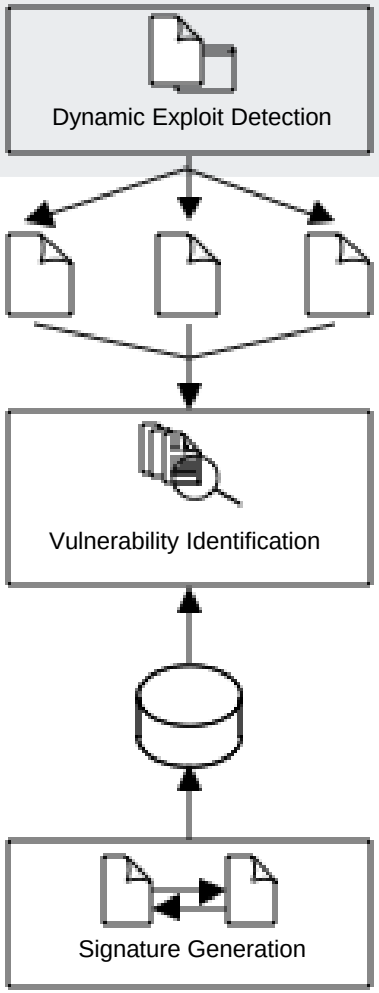
- Signatures automatically generated from Security Patches

System Overview – Automatic Exploit Detection

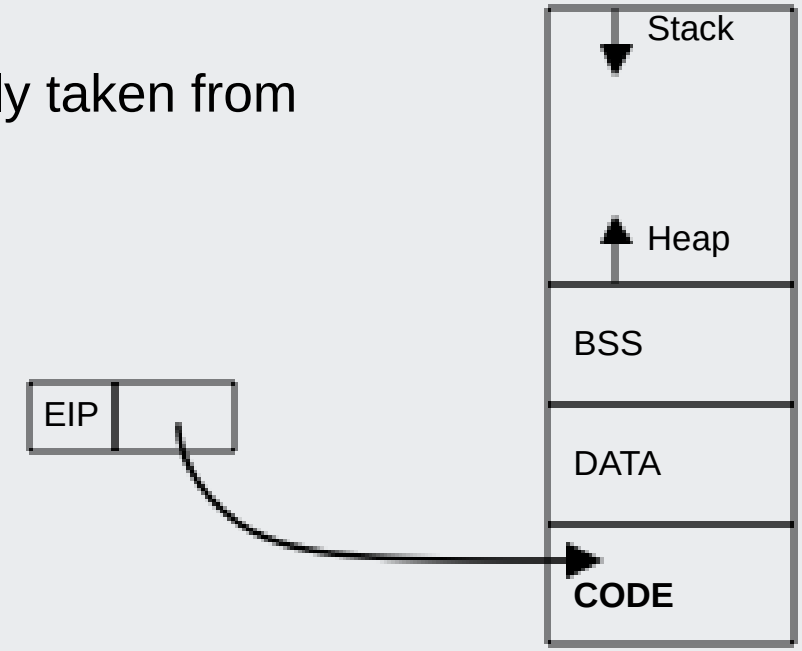


- Document is executed in several sandboxes, currently:
  - Office 2003, SP1, SP2, SP3
  - Office 2007, SP1, SP2
- Documents are deployed to each machine
- The execution of the application is monitored and logged by BISSAM using PIN

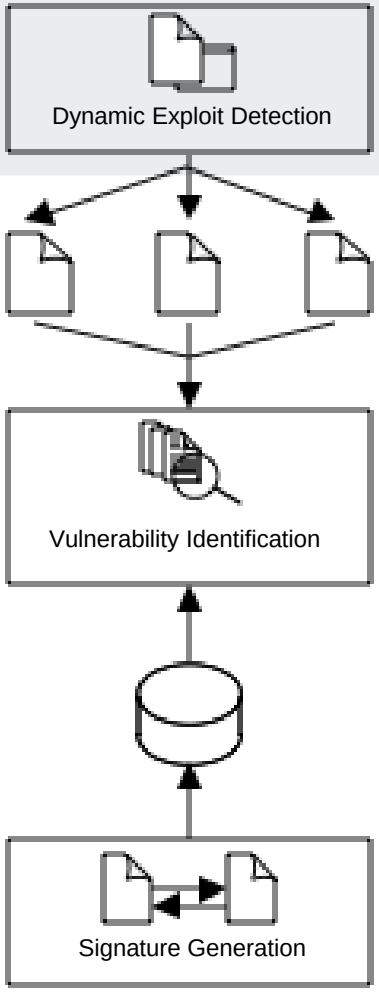
System Overview – Automatic Exploit Detection



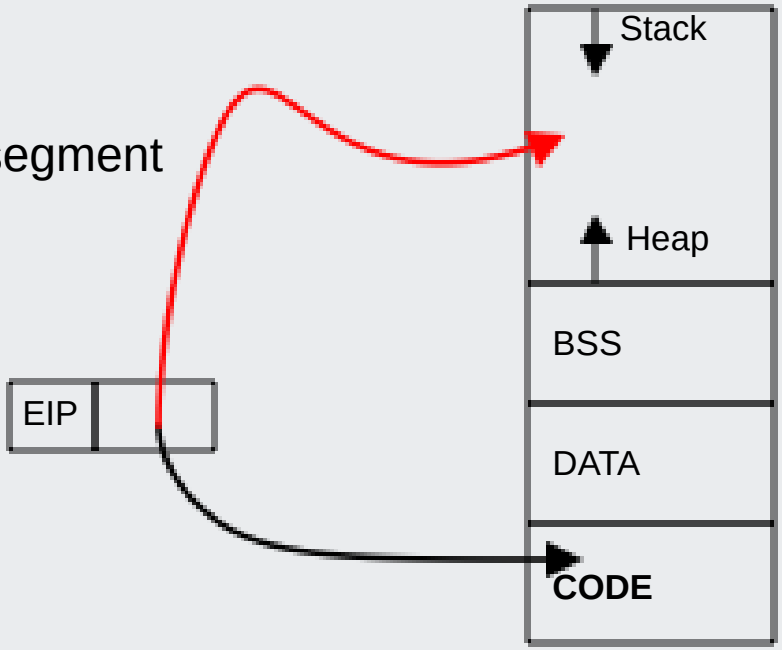
- Exploits can be detected by monitoring the instruction pointer (EIP)
- The EIP holds the address of the next instruction
- Instructions are usually taken from the CODE segment



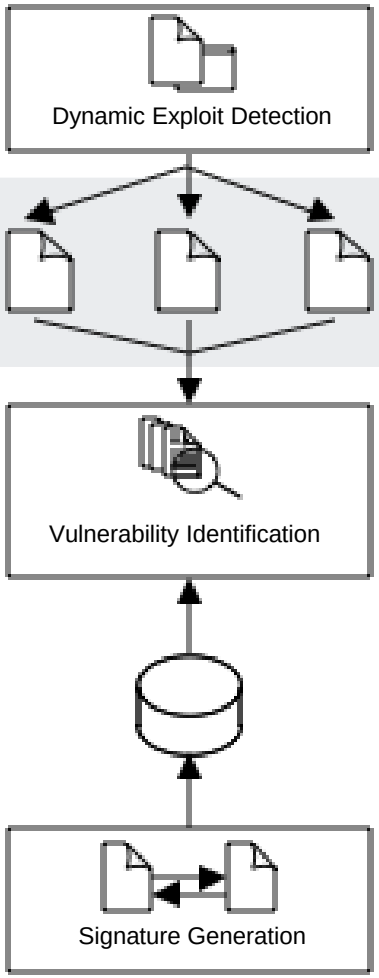
System Overview – Automatic Exploit Detection



- Attackers force the EIP to execute instructions from other segments
- BISSAM detects this by monitoring each instruction
- If the EIP leaves a legal segment BISSAM generates the necessary log files



System Overview – Automatic Exploit Detection



Trace.log

```
...msvcrt.dll:2009363160,msvcrt.dll:2009363171,msvcrt.dll:2009363173,msvcrt.dll:200936348
4,WINWORD.EXE:805331138,WINWORD.EXE:805574942,WINWORD.EXE:810004582,WIN
WORD.EXE:812760928,WINWORD.EXE:812760939,WINWORD.EXE:812760978,WINWOR
D.EXE:812760988,WINWORD.EXE:810004592,mso.dll:818672096,mso.dll:818672122,mso.
dll:818672141...
```

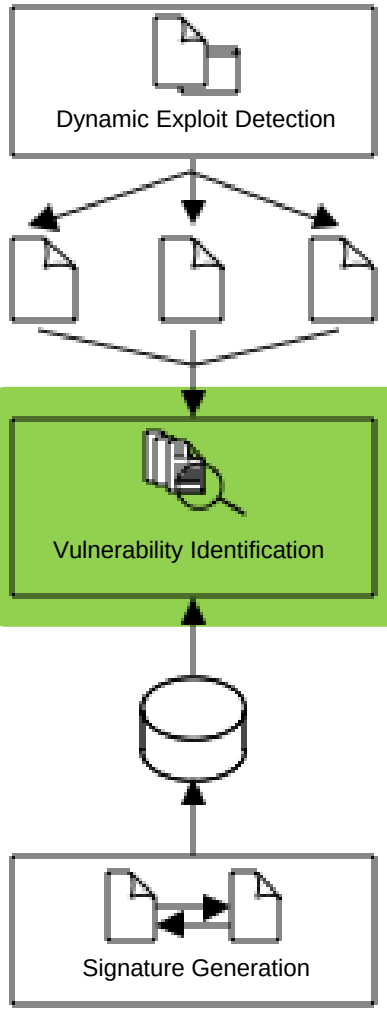
Shellcode.log

```
...
0: 0x044986E1::: 90              :nop
0: 0x044986E2::: 90              :nop
0: 0x044986E3::: 90              :nop
0: 0x044986E4::: db df           :fcmovnu st0, st7
0: 0x044986E6::: d9 74 24 f4     :fnstenv ptr [esp-0xc]
...
```

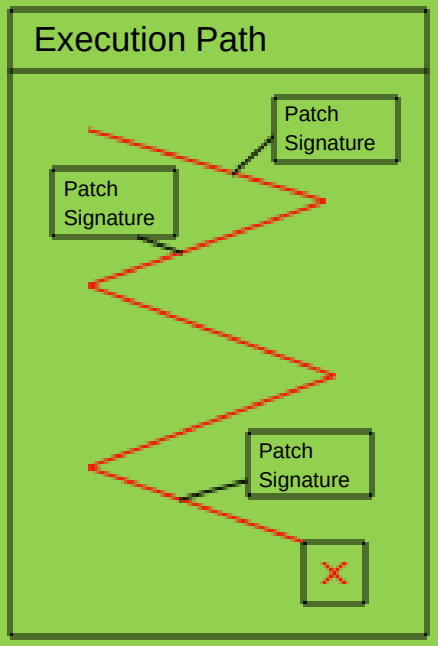
Instructions.log

```
...
0: 0x30003136::WINWORD.EXE 0f 85 8f 93 a6 00    :jnz 0x30a6c4cb
0: 0x3000313C::WINWORD.EXE c3                   :ret
0: 0x3016D46E::WINWORD.EXE 5f                   :pop edi
0: 0x3016D46F::WINWORD.EXE 5e                   :pop esi
0: 0x3016D470::WINWORD.EXE c9                   :leave
0: 0x3016D471::WINWORD.EXE c2 28 00             :ret 0x28
```

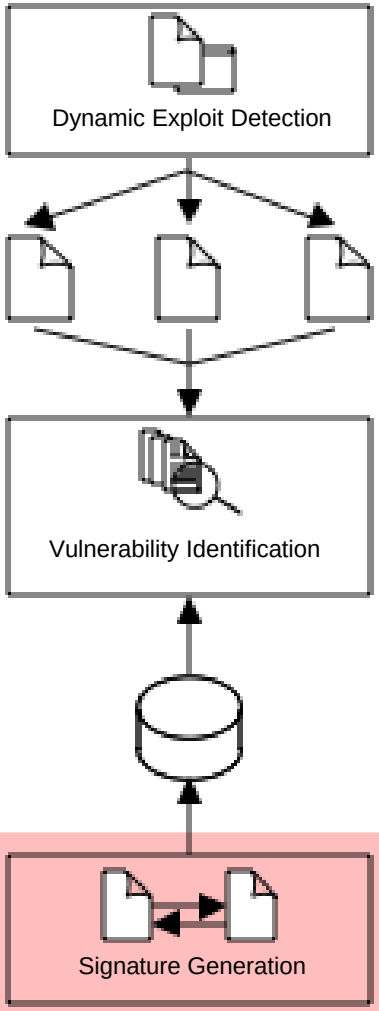
System Overview – Vulnerability Identification



- Uses the logs from the dynamic exploit detection
- The patch is found by matching the execution path to the signatures
- A patch may remediate multiple vulnerabilities

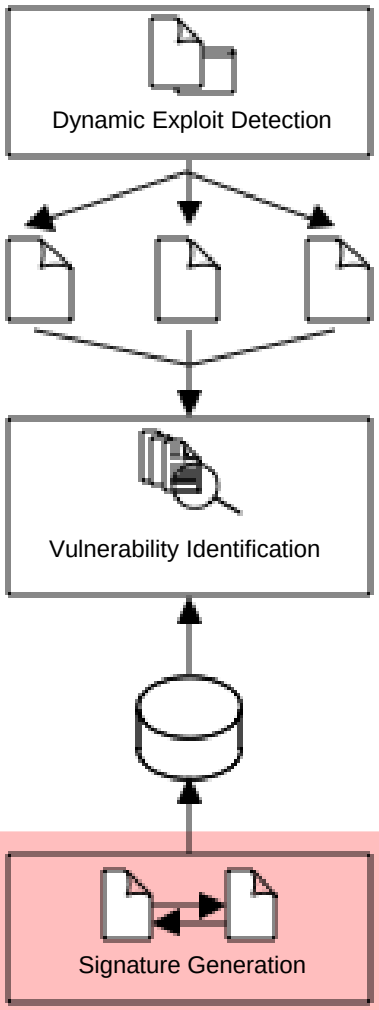


System Overview – Signature Generation

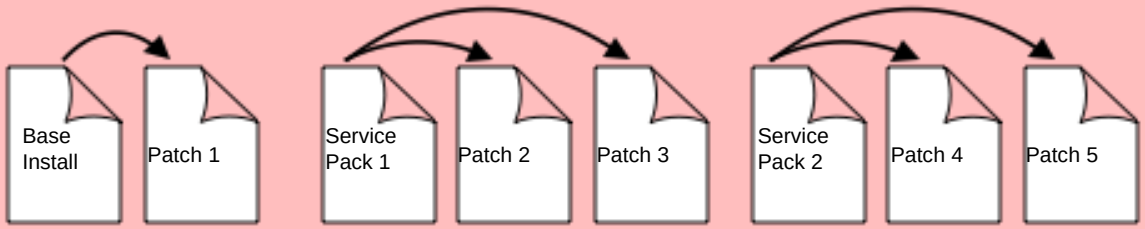


- Signatures must be generated automatically
- Signatures are generated by creating the binary difference between two security patches
- One patch is identified by multiple signatures
- One signature is a changed code block by the patch

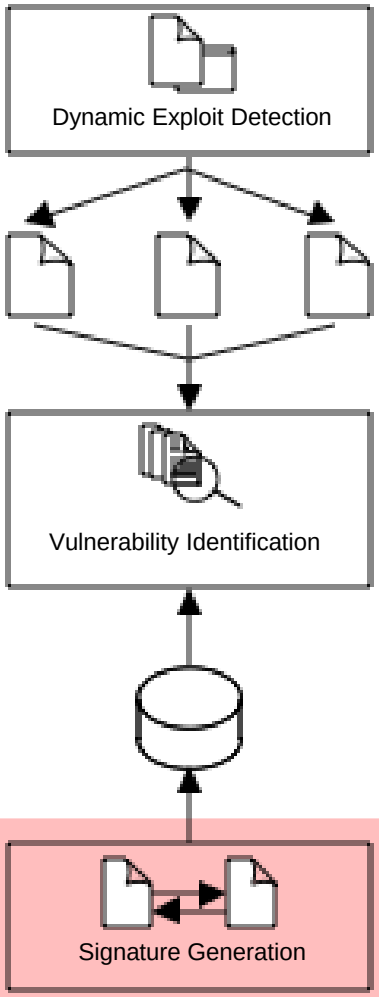
System Overview – Signature Generation



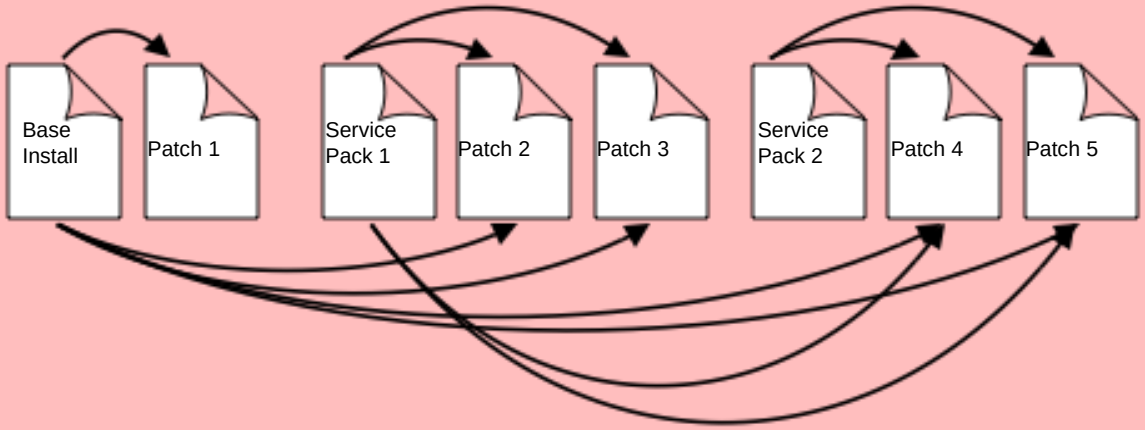
- The implementation uses vendor's security patches (full-file patches)
- The signatures are created by binary comparing each file in the patch to the same file in the base installation



System Overview – Signature Generation



- The implementation uses vendor's security patches (full-file patches)
- The signatures are created by binary comparing each file in the patch to the same file in the base installation



Evaluation

SIEMENS

- For the evaluation 7 documents were analyzed in depth
- Currently around 300 documents were analyzed

Document	Correct Patch	BISSAM	OfficeCat	OffVis
CVE 2006 0022.ppt	*MS06-028*	*MS06-028, MS06-058*	×	✓
CVE 2006 2492.doc	*MS06-027*	×	×	×
CVE 2009 0556.ppt	*MS09-017*	*MS09-017, MS10-004*	×	×
CVE 2009 0563.doc	*MS09-027*	*MS09-027, MS09-068 MS10-036*	×	×
CVE 2009 1129.ppt	*MS09-017*	*MS08-051, MS09-017*	×	×
CVE 2009 3129.xls	*MS09-067*	*MS09-067, MS09-021*	×	×
CVE 2010 3333msf.doc	*MS10-087*	*MS07-015, MS10-087*	×	×

SIEMENS

Limitations & Future Work

- Improve the detection of malicious behavior
- Improve the security rating of binary changes
- Execution path log size affects the identification rate

Conclusion

- System was developed to
  - detect malicious documents
  - identify the vulnerability
- Evaluation showed that the system improves the Analysis compared to today's tools
- Saves a lot of analysis time
- Adaptable to other Applications
- Currently in productive use at Siemens CERT

Some Numbers

There are currently

- **519** Bulletins

mapped to

- **1069** CVE Numbers

for

- **2821** downloaded patches

that create a total set of

- **21.933.889** Signatures in the Database

SIEMENS

Please contact for further information

Thomas Schreck
Siemens CERT

Otto-Hahn-Ring 6
81739 Munich
Germany

Phone: +49 89 / 636 - 41165
Fax: +49 89 / 636 - 41166

E-mail: t.schreck@siemens.com
Internet: http://www.siemens.com/cert