

Research Division

IBM

Increased Information Flow Needs for High-Assurance Composite Evaluations

Paul A. Karger, Thomas J. Watson Research Center
Helmut Kurth, atsec Information Security, GmbH

April 2004

Research Division

IBM

Why isn't the paper in the proceedings?

- Published at Second IEEE International Information Assurance Workshop
 - Subject to IEEE copyright – couldn't get permission to reprint in time for this conference
 - Karger, P.A. and H. Kurth. *Increased Information Flow Needs for High-Assurance Composite Evaluations*. in **Second IEEE International Information Assurance Workshop**. 8-9 April 2004, Charlotte, NC: IEEE Computer Society. p. 129-140.
- Details on downloading at end of talk

Research Division

IBM

Composite Evaluation

- Composite Evaluation was introduced into the Common Criteria in Europe by France, Germany, the Netherlands, and the UK
 - Supplementary documents, not endorsed by all countries
- Introduced to reduce costs of having to re-evaluate hardware many times for each evaluated software product
- Similar to earlier scheme (TCB subsets) used under Orange Book and the Trusted Database Interpretation (TDI)

Research Division

IBM

The old (undesirable) scheme for layered products

```

graph TD
    A[JavaCard applets] --> B[JavaCard]
    B --> C[Native Applications]
    C --> D[Secure OS<br/>crypto]
    D --> E[hardware]
    
```

evaluations and re-evaluations

Research Division

IBM

Layered products under Composite Evaluation

```

graph TD
    A[JavaCard applets] --> B[JavaCard]
    B --> C[Native Applications]
    C --> D[Secure OS<br/>crypto]
    D --> E[hardware]
    
```

evaluation

Research Division

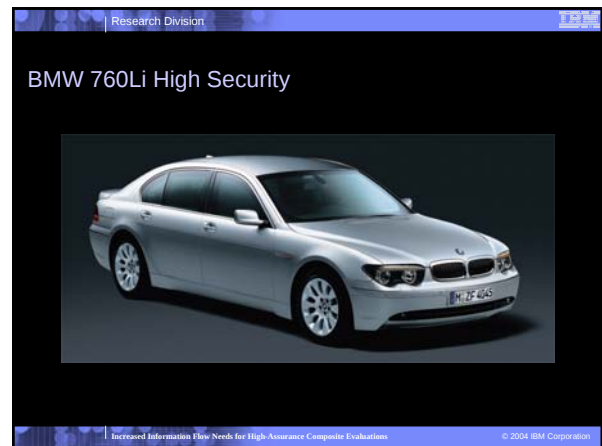
IBM

Limited Information Flow

- Composite evaluation scheme limits information flow from hardware evaluator to software evaluator
- Concern about proprietary information for both the hardware developer and the hardware evaluator's methods
- Concern about national security
 - France did not want ETRs to leave the country
- ETR-lite
 - Censored version of evaluation technical report
 - Compromise solution to meet French concerns, yet allow some information flow
 - Supposed to be sufficient to meet needs of software evaluator
 - Actually practice has shown major gaps in some certified ETR-lite reports

Document Title	Hardware Developer	Hardware Evaluator	Hardware Certifying Body	Software Evaluator	Software Certifying Body	Software Developer
Security Target (ST)	O	R	R	R	R	R
ST-Lite	O	R	R	R	R	R
Data Sheet	O	R	R	R	R	R
Guidance Manual	O	R	R	R	R	R
Developer Docs such as FS, HLD, AVA, etc.	O	R	R	X	X	X
ETR-Lite	R	O	R	R	R	X
Full ETR (incl. all reports)	R	O	R	X	X	X
Certificate	R	R	O	R	R	R

O = Originator
 R = Receiver (may need NDA)
 X = no access



- ### BMW 760Li High Security withstands armor-piercing bullets, grenade blasts and gas attacks
- certified to meet B6/B7 requirements of German Federal Crime Office
 - source: www.carat-duchatelet.be/s-class/hallb7.htm
 - withstands fire from weapons as powerful as an M16 or Kalashnikov AK47 rifle
 - can travel a long distance at 80 kmph (50 mph) even if tires are burst by rifle fire
 - withstands the detonation of two hand grenades under the driver and rear passenger seats
 - if attacked with tear gas, the cabin is hermetically sealed and its passengers supplied with oxygen
 - remote control engine start ensures no explosives are wired up to the ignition
 - automatic or manual actuation of onboard fire extinguishers
 - distinguishable only to the trained eye by its toughened glass and wider tires

- ### BMW 330i Security – EAL5+ counterpart
- 
- Ballistic protection level B4
 - Bullet resistant
 - Run-flat tires
 - No tear-gas protection
 - No bomb or grenade protection

- ### BMW and DuPont (real life, not hypothetical)
- DuPont is the supplier of windshields for the BMW 760Li High Security
 - BMW performs tests on the window glass
 - DuPont = Hardware Developer
 - BMW = Software Developer
 - User Guidance:
 - Our security glass is impermeable to tear gas when used with our adhesive part number DA1896-PXT
 - Our security glass
 - withstands B7 ballistic attacks
 - does not break within the temperature range specified

- ### DuPont has more information that it does not share with BMW (hypothetical)
- ATE: DuPont adhesive part number DA1896-PXT deteriorates in humidity lower than 25% over prolonged periods of time.
 - AVA: DuPont safety glass has shattered once at an indoor stadium in Canada where the heat was left off overnight and was struck the next morning by a hockey puck. We don't know how cold it got overnight. It did not break purely as a result of the cold.
 - DuPont does not know that one of BMW's primary markets is the Middle East, where humidity is low for prolonged periods.
 - BMW has no way to find out (during design) that DuPont's user guidance is wrong.
 - BMW cannot tighten its specifications to account for low humidity, because BMW is not aware of this attribute of adhesives.
 - If BMW knew about the failure of the hockey screen, they might run additional tests using bullets (instead of hockey pucks) over a range of low temperatures.

Research Division IBM

Computer Security is a Systems Engineering Issue

- Analyzing individual components in isolation and assuring that they are secure is not necessarily sufficient to assure that the overall system itself is secure
- Inconsistent or unstated assumptions can easily lead to vulnerabilities falling through the cracks
- A hardware evaluator cannot necessarily anticipate all potential threats to the hardware without a detailed understanding of the software
- Systems engineering was developed in the aerospace industry to deal with these types of problems in complex aircraft design
- Software developers and evaluators must know ALL assumptions made in the hardware evaluation – not just those that are mentioned in ETR-lite

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division IBM

Case Studies from the Literature

- How invalid hardware assumptions can lead to serious vulnerabilities in practice
- Only a few examples here – lots more in the paper

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division IBM

Flaws in Hardware Implementation

- Is the instruction set and memory protection mechanism implemented correctly?
 - Failures could be exploited
- Back in 1960s, concern that random hardware failures could result in security violations
 - ADEPT-50 work at SDC
 - Multics subverter programs
- Goal is to systematically test ALL the boundary conditions in the hardware architecture to ensure that instructions correctly follow the hardware security policy
- Example: GE-645 processor
 - Execute instruction in odd machine location
 - Executes instruction in word zero of another memory segment
 - Target instruction uses index register but not base register modification
 - Processor allows target to execute with NO protection checking

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division IBM

Potentially Huge Number of Test Cases

- Solutions developed independently at DEC and at IBM
- Random test case generators – run for thousands of hours
- Check results
 - By knowing what correct results should be
 - Hard to achieve for huge number of cases
- Compare results on two different implementations
 - Much easier!
 - If mismatch, then either system A has a flaw, system B has a flaw, or the test program has a flaw
 - Very powerful technique – finds LOTS and LOTS of processor bugs
- Software developer and evaluator need to know what level of testing was done – do they have to fill in gaps that the hardware evaluator missed?

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division IBM

Covert Channel Issues

- Serious problem for software that implements any kind of information flow policy between applications
 - Covert channels are only exploitable in the presence of Trojan horses
 - Side channel analysis of traditional smart cards (with all applications in a single protection domain – ie: mutually trusting) is NOT covert channel analysis
- Covert channel analysis is required at EAL5 by Common Criteria
 - If an information flow policy exists
- Covert channel analysis of software requires an intimate knowledge of the hardware implementation – cannot be transferred between two different models of same processor

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division IBM

Disk Arm Covert Channel

- KVM/370 discovered covert channel in the software implementation of the elevator algorithm in disk drivers
 - State variable of the direction of disk arm motion is exploitable
- Solved problem by eliminating elevator algorithm from disk driver
- More modern disk controllers implement the elevator algorithm in hardware!
 - Not mentioned in hardware interface specification
 - Hardware designer and evaluator may have no idea that there could be a problem from this, yet O/S designer needs to know if this is done and whether it can be turned off
- DEC's VMM Security Kernel for the VAX had to deal with this problem in its A1 Orange Book evaluation
 - Had to have in-depth information about the hardware implementation
 - Elevator algorithm could NOT be turned off
 - Required major re-design of VMM disk drivers to batch all disk requests to conceal the effects of the elevator algorithm – patented result
 - ETR-lite on disk controller would likely have not revealed the problem!

Increased Information Flow Needs for High Assurance Composite Evaluations © 2004 IBM Corporation

Research Division

IBM

Covert Channel in SMP Memory Interlock

- VAX hardware architecture (data sheet) states that any location in memory can be separately interlocked in multi-processor operation
- VAX 8800 implemented this with a single memory interlock for the entire memory unit – functionally equivalent, but...
 - Exploitable as 1000bps covert channel on 5 MIP processor
 - Undocumented
 - Could only be identified with in-depth knowledge of the hardware implementation
- Analogous problem in shared memory bus on modern SMP processors can easily result in a covert channel in the megabit per second range
- Essential that the implementation issues be totally exposed, so that the OS designer can develop countermeasures

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Research Division

IBM

Instruction Pre-Fetch Queue Length

- Software developed for IBM Series/1
- Contained code that modified the instruction stream
 - Explicitly permitted by hardware architecture
- New model of Series/1 deployed
 - Supposedly 100% software compatible
 - But undocumented instruction pre-fetch queue was increased in size
 - Instruction stream modifications no longer worked, because instructions were stored in the undocumented pre-fetch queue
- Software developer needed in-depth hardware implementation information that would not have been disclosed in ETR-lite

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Research Division

IBM

How do BMW and DuPont solve this problem? Could hardware and software developers use the same approach?

- We know that BMW performs testing on DuPont's products.
- Software developer cannot afford to perform hardware tests.
- Hardware and software developers cannot rely solely on evaluation to find problems
 - cost of delayed specification changes
 - cost of delayed failure
 - cost of evaluations on spec revisions

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Research Division

IBM

What can we do to succeed?

- Recognize that achieving high assurance requires closer cooperation between developers (hardware and software) and evaluators (hardware and software)
- Share information within limits (NDAs and no disclosure of third party IP)
- The old TCB-subset approach under the Orange Book recognized the need for extensive information sharing

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Research Division

IBM

Desired hardware document sharing

Document Title	Hardware Developer	Hardware Evaluator	Hardware Certifying Body	Software Evaluator	Software Certifying Body	Software Developer
Security Target (ST)	O	R	R	R	R	R
ST-Lite	O	R	R	R	R	R
Data Sheet	O	R	R	R	R	R
Guidance Manual	O	R	R	R	R	R
Developer Docs such as FS, HLD, AVA, etc.	O	R	R	NDA	NDA	NDA
ETR-Lite	R	O	R	R	R	NDA
Full ETR (incl. all reports)	R	O	R	NDA	NDA	NDA
Certificate	R	R	O	R	R	R

O = Originator
 R = Receiver (may need NDA)
 X = no access
 NDA = Receiver under NDA

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Research Division

IBM

Why Use NDAs?

- Big debate on full disclosure of security vulnerabilities
- Full disclosure is generally better
 - "security through obscurity" doesn't work most of the time
 - Only the "bad guys" know about problems
- Hardware security countermeasures
 - Often probabilistic
 - Secrecy sometimes is the only option – depending on difficulty of hardware probing, rather than logical defenses
 - Knowledge of where and how to probe surface could be deadly
 - In this case, "security through obscurity" is actually important
- Software developer cannot always dictate confidentiality policy to hardware vendor

Increased Information Flow Needs for High Assurance Composite Evaluations

© 2004 IBM Corporation

Recommendations

- Composite Evaluation can save lots of time and money
- Need more information flow to make it work at high assurance levels (EAL6 and above)
- Mandate that software developers and software evaluators get access to the full evaluation technical report (ETR) (and all supplementary reports)
 - Permit ETR-lite only at lower assurance levels (EAL4 and below)
 - Recognize that some, but not all, hardware evaluation data may need protection under NDA
 - Permit, but do not require, the use NDAs in these cases
 - EAL5 is a borderline case – AVA_VLA.4 is a good indicator of need for full ETR

For further information

- Read the paper
 - Karger, P.A. and H. Kurth. *Increased Information Flow Needs for High-Assurance Composite Evaluations*. in **Second IEEE International Information Assurance Workshop**. 8-9 April 2004, Charlotte, NC: IEEE Computer Society. p. 129-140.
 - Also available (for a short time) as: RC 22950 (W0310-168), Revision 2, 30 October 2003, IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, NY. URL: <http://domino.watson.ibm.com/library/CyberDig.nsf/home>
- Contact the authors for a copy by email
 - karger@watson.ibm.com
 - kurth@atsec.com