David Rook

Agnitio
Security code review swiss army knife

OWASP, Holland

if (slide == introduction) System.out.println("I'm David Rook");

- Application Security Lead, Realex Payments, Ireland
  CISSP, CISA, GCIH and many other acronyms
- Security Ninja (@securityninja)
- Speaker at developer and security conferences
- Microsoft Developer Security MVP
- Developed and released Agnitio

realex
The real time payment exchange

if (slide == introduction && replacement) System.out.println("I'm Steven van der Baan");

- Senior Security consultant, Sogeti Nederland BV, Nederland
  CISSP, OSCP, ASS and someother acronyms
- Not a blogger(@vdbaan)
- Project Leader OWASP CTF
- Dedicated dad
- Commented and contributed on Agnitio

realex
The real time payment exchange

Agenda

- What is static analysis?
- Security code reviews: the good, the bad and the ugly
- Agnitio: security code review Swiss army knife

realex
The real time payment exchange

Static analysis

- What do I mean by static analysis?
  - A review of source code without executing the application
  - Can be either manual or automated through one or more tools
  - Human and/or tools analysing application source code

realex
The real time payment exchange

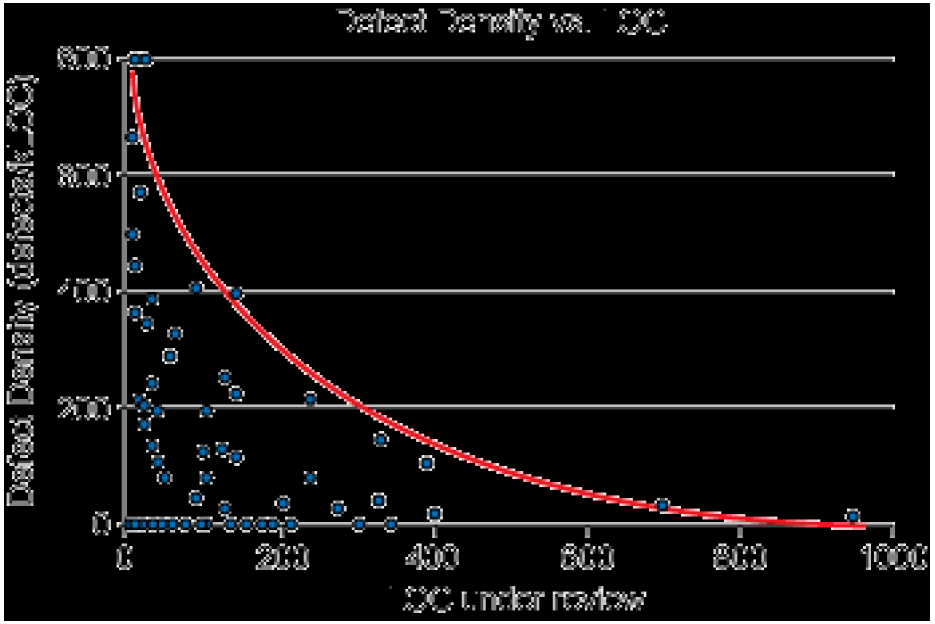
Static analysis

- Wetware or software?
  - Humans are needed with or without static analysis tools
  - The best thing about humans is that they aren't software
  - The worst thing about humans is that they are humans

realex
The real time payment exchange

Static analysis

- Wetware or software?

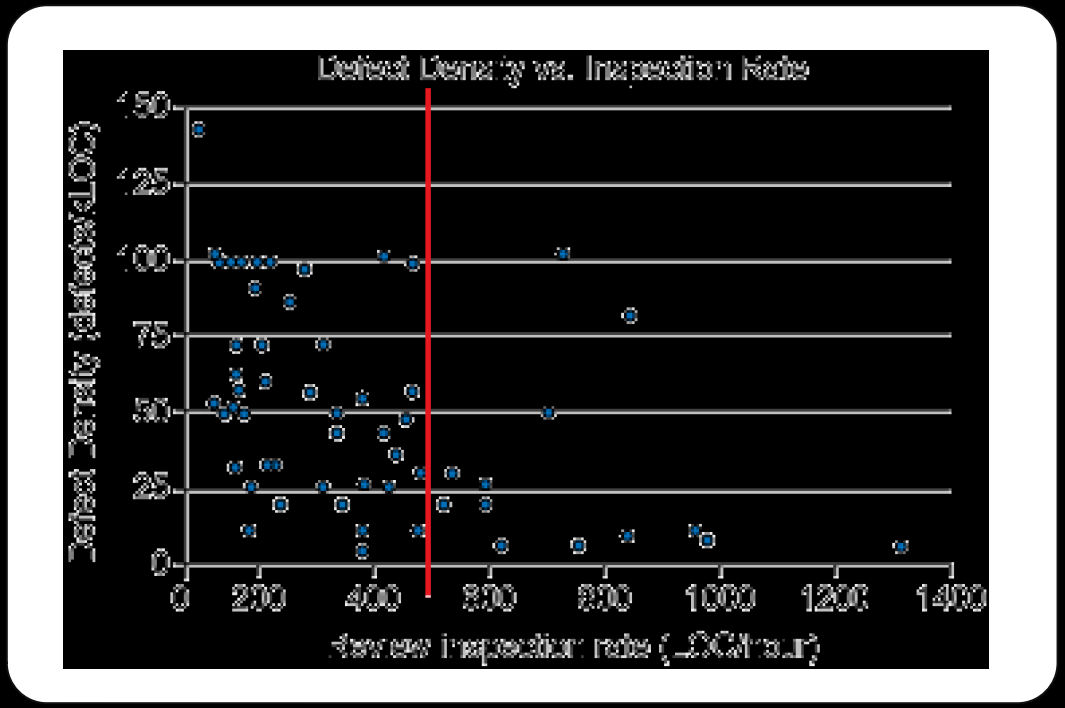


http://www.ibm.com/developerworks/rational/library/11-proven-practices-for-peer-review/index.html?sf1100063=1

realex
The real time payment exchange

Static analysis

- Wetware or software?



http://www.ibm.com/developerworks/rational/library/11-proven-practices-for-peer-review/index.html?sf1100063=1

Static analysis

- Wetware or software?
  - Tools can cover more code in less time than a human
  - The best thing about software is that it isn’t human
  - The worst thing about software is that it’s software

realex
The real time payment exchange

The ugly security code reviews

- “Ugly reviews” implies you do actually review code
  - An unplanned magical mystery tour at the end of the SDLC
  - Unstructured, not repeatable and heavily reliant on $C_8H_{10}N_4O_2$
  - Too late in the SDLC making findings very expensive to fix
  - Completely manual process, no tools used during reviews
  - No audit trails, no metrics.....no security?
  - Better than nothing?

realex
The real time payment exchange

The bad security code reviews

- “Bad reviews” might be fine for some companies
  - A single planned code review in your SDLC
  - Some structure, normally based on finding the OWASP top 10
  - Still too late in the SDLC making findings very expensive to fix
  - Some automation, usually basic code analysis tools
  - Basic audit trails still no metrics so hard to measure “anything”
  - Better than ugly reviews, might be fine for some companies

realex
The real time payment exchange

The good security code reviews

- “Good reviews” don’t happen by accident
  - Multiple reviews defined as deliverables in your SDLC
  - Structured, repeatable process with management support
  - Reviews are exit criteria for the development and test phases
  - Automation used where useful freeing up the reviewer
  - Ability to produce reports, metrics and measure improvements
  - External validation of the review process and SDLC

realex
The real time payment exchange

Agnitio

- What is Agnitio?
  - Tool to help with manual static analysis
  - Checklist based with reviewer & developer guidance
  - Produces audit trails & enforces integrity checks
  - Single tool for security code review reports & metrics

realex
The real time payment exchange

Agnitio

- What is Agnitio?
  - C# open source application, GPLv3 license
  - Five different versions in 12 months
  - 10,000+ downloads from users in over 100 countries
  - Used by SMEs, consulting firms and companies of the NYSE

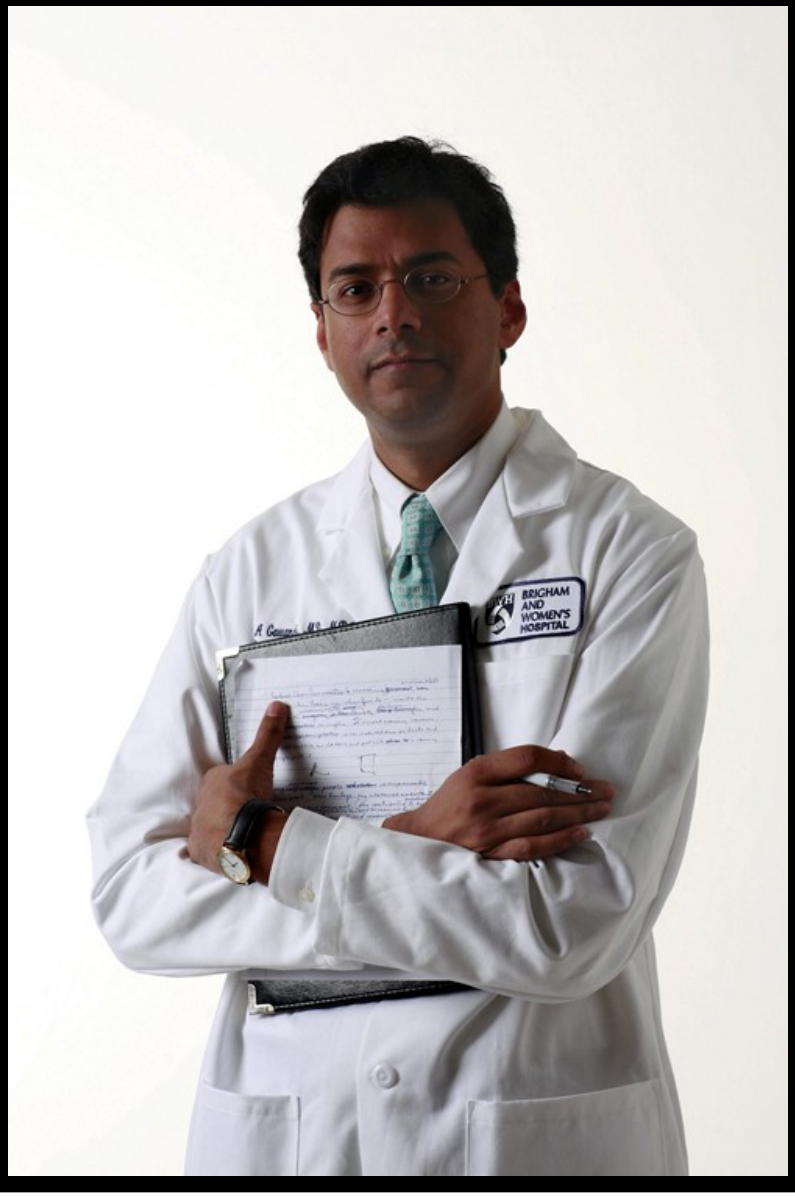
realex
The real time payment exchange

Agnitio

- Checklists?
  - An application for doing checklist reviews? *yawn* how boring!
  - Checklists are for n00bs! I don't need a checklist to review code!
  - I beg to differ, would you say Doctors and Pilots are n00bs?

realex
The real time payment exchange

SECURITY



realex
The real time payment exchange

A CHECKLIST FOR CHECKLISTS

Development → Drafting → Validation

Development

- ❑ Do you have clear, concise objectives for your checklist?

Is each item:

- ❑ A critical safety step and in great danger of being missed?
- ❑ Not adequately checked by other mechanisms?
- ❑ Actionable, with a specific response required for each item?
- ❑ Designed to be read aloud as a verbal check?
- ❑ One that can be affected by the use of a checklist?

Have you considered:

- ❑ Adding items that will improve communication among team members?
- ❑ Involving all members of the team in the checklist creation process?

Drafting

Does the Checklist:

- ❑ Utilize natural breaks in workflow (pause points)?
- ❑ Use simple sentence structure and basic language?
- ❑ Have a title that reflects its objectives?
- ❑ Have a simple, uncluttered, and logical format?
- ❑ Fit on one page?
- ❑ Minimize the use of color?

Is the font:

- ❑ Sans serif?
- ❑ Upper and lower case text?
- ❑ Large enough to be read easily?
- ❑ Dark on a light background?

- ❑ Are there fewer than 10 items per pause point?
- ❑ Is the date of creation (or revision) clearly marked?

Validation

Have you:

- ❑ Trialed the checklist with front line users (either in a real or simulated situation)?
- ❑ Modified the checklist in response to repeated trials?

Does the checklist:

- ❑ Fit the flow of work?
- ❑ Detect errors at a time when they can still be corrected?

- ❑ Can the checklist be completed in a reasonably brief period of time?
- ❑ Have you made plans for future review and revision of the checklist?

Please note: A checklist is NOT a teaching tool or an algorithm

Last updated 1/14/10

Congenital Heart Surgery Check List (Template)

Before Induction
SIGN IN

PATIENT HAS CONFIRMED

- ❑ IDENTITY
- ❑ SITE
- ❑ PROCEDURE
- ❑ CONSENT

DOES PATIENT HAVE A KNOWN ALLERGY?

- ❑ NO
- ❑ YES
  - ❑ DRUGS
  - ❑ LATEX
  - ❑ OTHER

- ❑ **H&P CURRENT (< 30d)**
- ❑ **WEIGHT RE-CHECKED**
- ❑ **ANESTHESIA SAFETY CHECK COMPLETED (Machine and Meds)**
- ❑ **PULSE OXIMETER ON PATIENT AND FUN`CTIONING**

DIFFICULT AIRWAY/ASPIRATION RISK?

- ❑ NO
- ❑ If YES, EQUIPMENT/ASSISTANCE AVAILABLE

- ❑ **INTRAVENOUS ACCESS AND FLUIDS PLANNED**
- ❑ **WARMER (blankets and fluids) IN PLACE**
- ❑ **BLOOD BANK NOTIFIED AND BLOOD PRODUCTS AVAILABLE WHEN NEEDED**

- ❑ **SIGN (NURSING):**_____
- ❑ **SIGN (ANESTH):**_____

Before Skin Incision
TIME OUT

- ❑ **CONFIRM ALL TEAM MEMBERS HAVE INTRODUCED THEMSELVES BY NAME**
- ❑ **SURGEON, ANESTHESIA, PERFUSIONIST AND NURSE VERBALLY CONFIRM**
  - ❑ PATIENT
  - ❑ SITE
  - ❑ PROCEDURE
  - ❑ IMAGING AVAILABLE AND REVIEWED
  - ❑ TRANSESOPHAGEAL ECHO (TEE) OR OTHER ECHO
  - ❑ ANTIFIBRINOLYTICS
  - ❑ ANTIBIOTICS ADMINISTERED (within last 60 min)

PERFUSION STRATEGY:

- ❑ CANNULATION SITES
- ❑ CANNULAE SIZES
- ❑ BYPASS PRIME (blood vs prime)
- ❑ TARGETED CORE TEMP
- ❑ USE OR NON-USE OF DHCA, SELECTIVE CEREBRAL PERFUSION
- ❑ ICE ON THE HEAD
- ❑ OTHER BYPASS CONSIDERATIONS (shunts, collaterals, AR, LV venting, CARDIOPLEGIA, etc)

ANESTHESIA TEAM REVIEWS:

- ❑ ANY FURTHER PATIENT-SPECIFIC CONCERNS?

NURSING TEAM REVIEWS:

- ❑ EQUIPMENT STERILITY CONFIRMED?
- ❑ ARE THERE EQUIPMENT/PROSTHESES ISSUES OR ANY CONCERNS?

- ❑ **SIGN (SURG):**_____

Before Patient Leaves Room
SIGN OUT

NURSE VERBALLY CONFIRMS WITH THE TEAM:

- ❑ NAME OF THE PROCEDURE
- ❑ THAT INSTRUMENT, SPONGE AND NEEDLE COUNTS ARE CORRECT

- ❑ **HOW THE SPECIMEN IS LABELLED**
  - ❑ INCLUDING PATIENT NAME
  - ❑ SENT FOR APPROPRIATE TESTS

- ❑ **WHETHER THERE ARE ANY EQUIPMENT PROBLEMS TO BE ADDRESSED**

SURGEON, ANESTHESIA PROFESSIONAL AND NURSE

- ❑ REVIEW THE KEY CONCERNS FOR POST-OP RECOVERY AND MANAGEMENT OF THIS PATIENT
- ❑ BLOOD PRODUCTS USED
- ❑ BLOOD PRODUCTS STILL AVAILABLE
- ❑ BREAKS IN TECHNIQUE

- ❑ **SIGN (NURSING):**_____
- ❑ **SIGN (SURG):**_____

FUEL INJECTED CESSNA 172 CHECKLIST

- Fuel — CHECK (122.85)

CABIN CHECK

- Ignition Key — ON GLARESHIELD
- Documents (AROW) — CHECK
- Hobbs Meter — CHECK TIME
- Control Lock — REMOVE
- Electrical & Avionics — OFF
- Master Switch — ON
- Avionics Master Switch — ON-CHECK FAN-OFF
- Annunciator Panel Switch — TEST LIGHTS
- Fuel Gauges — CHECK
- Flaps — DOWN
- Exterior Lights — CHECK
- Master Switch — OFF
- Parking Brake — ON

EXTERIOR INSPECTION

- Fuel Sumps — SAMPLE (5)
- Fuselage Left Side — CHECK
- Elevator/Rudder — CHECK
- Tail Tie-down — REMOVE
- Fuselage Right Side — CHECK
- Right Flap & Aileron — CHECK
- Wing Tie-down — REMOVE
- Fuel Sumps — SAMPLE (5)
- Main Wheel Tire/Brakes — CHECK
- Chocks — REMOVE
- Fuel Quantity (Right Tank) — CHECK VISUALLY
- Engine Oil Level — CHECK (MIN. 5 QTS)
- Fuel Strainer/Selector Drains — SAMPLE (2)
- Propeller & Spinner — CHECK
- Alternator Belt — CHECK
- Landing Light — CHECK (CONDITION)
- Engine Air-Intake Filter — CHECK
- Nose Wheel Strut & Tire — CHECK
- Nose Chocks — REMOVE
- Static Source — CHECK
- Fuel Quantity (Left Tank) — CHECK VISUALLY
- Wing Tie-down — REMOVE
- Pitot Tube Cover — REMOVE
- Fuel Tank Vent — CLEAR
- Stall Warning Horn Opening — CHECK
- Left Flap & Aileron — CHECK
- Main Wheel Tire/Brakes — CHECK
- Chocks — REMOVE
- Move Airplane — CHECK TIRES
- Overall Condition — REVIEW

FUEL INJECTED CESSNA 172 CHECKLIST

BEFORE ENGINE START

- Seatbelts/Shoulder Harness — FASTENED
- Brakes — TEST & SET
- Fuel Selector — BOTH
- Fuel Shutoff Valve — ON (IN)
- Circuit Breakers — CHECK
- Beacon — ON
- Avionics Switch — OFF
- Master Switch — ON
- Throttle — OPEN 1/4 INCH
- Mixture — IDLE CUTOFF
- Aux. Pump — ON
- Mixture Rich 3-5 GPH — CUT OFF
- Aux. Pump — OFF
- Propeller Area — CLEAR

AFTER ENGINE START

- Ignition Switch — START
- Mixture (At Engine Start) — RICH
- Engine RPM — 1000 RPM
- Oil Pressure — CHECK
- Mixture — LEANED MAX
- Flaps — RETRACT

TAXI

- Brakes — CHECK
- Magnetic Compass — MOVEMENT FREE
- Flight Instruments — CHECK

BEFORE TAKEOFF

- Parking Brakes — SET
- Flight Controls — FREE & CORRECT
- Flight Instruments — SET
- Fuel Selector — BOTH
- Elevator & Rudder Trim — SET
- Mixture — RICH FOR RUNUP
- Autopilot — CHECK DISCONNECT
- Throttle — 1800 RPM
- Ammeter — CHECK
- Engine Instruments. — CHECK
- Suction — CHECK
- Magnetos — CHECK (125/50)
- Throttle — IDLE CHECK SMOOTH & 600 RPM ± 25 THEN 1000 RPM
- Radios — SET
- Brakes — RELEASE

Final Items

- Door/Windows — CLOSED
- Flaps — AS REQUIRED
- Mixture — RICH (BELOW 3000 FT)

FUEL INJECTED CESSNA 172 CHECKLIST

TAKEOFF

- "LIGHTS" (ALL) — ON
- "CAMERA" (Transponder) — ON
- "ACTION" (RPM, Oil Pres., Time) — FULL POWER
- Climb Speed (172R) — 74 KTS
- Climb Speed (172S) — 79 KTS

BEFORE LANDING

- Seatbelts — ADJUST
- Fuel Selector — BOTH
- Engine Gauges — CHECK
- Heading Indicator — ALIGNED
- Altimeter Setting — CHECK
- Radios — SET
- Autopilot — OFF

Final Items

- Mixture — RICH
- Flaps — DOWN
- Approach Speed — 65-75 KTS

AFTER LANDING CHECK

- "LIGHTS" (Except Beacon) — OFF
- "CAMERA" (Transponder) — OFF
- "ACTION" (Mixture, Flaps)

ENGINE SHUTDOWN

- Throttle — IDLE
- Mags — GROUND CHECK
- Throttle — 1000 RPM
- Avionics/Electrical Equip. — OFF
- Mixture — CUTOFF
- Master/Alternator Switch — OFF
- Ignition Switch — OFF
- Ignition Key — GLARESHIELD

SECURING AIRCRAFT

- Hobbs & Tach — RECORD
- Control Lock — INSTALL
- Tiedowns/Chocks — INSTALL
- Propeller (For Fuel) — VERTICAL
- Fuel — RIGHT TANK

Agnitio

- Checklists?
  - Do you use checklists for your source code reviews?
  - What's the worst that could happen if you don’t?

realex
The real time payment exchange

Ariane 5 flight 501

SECURITY

realex
The real time payment exchange

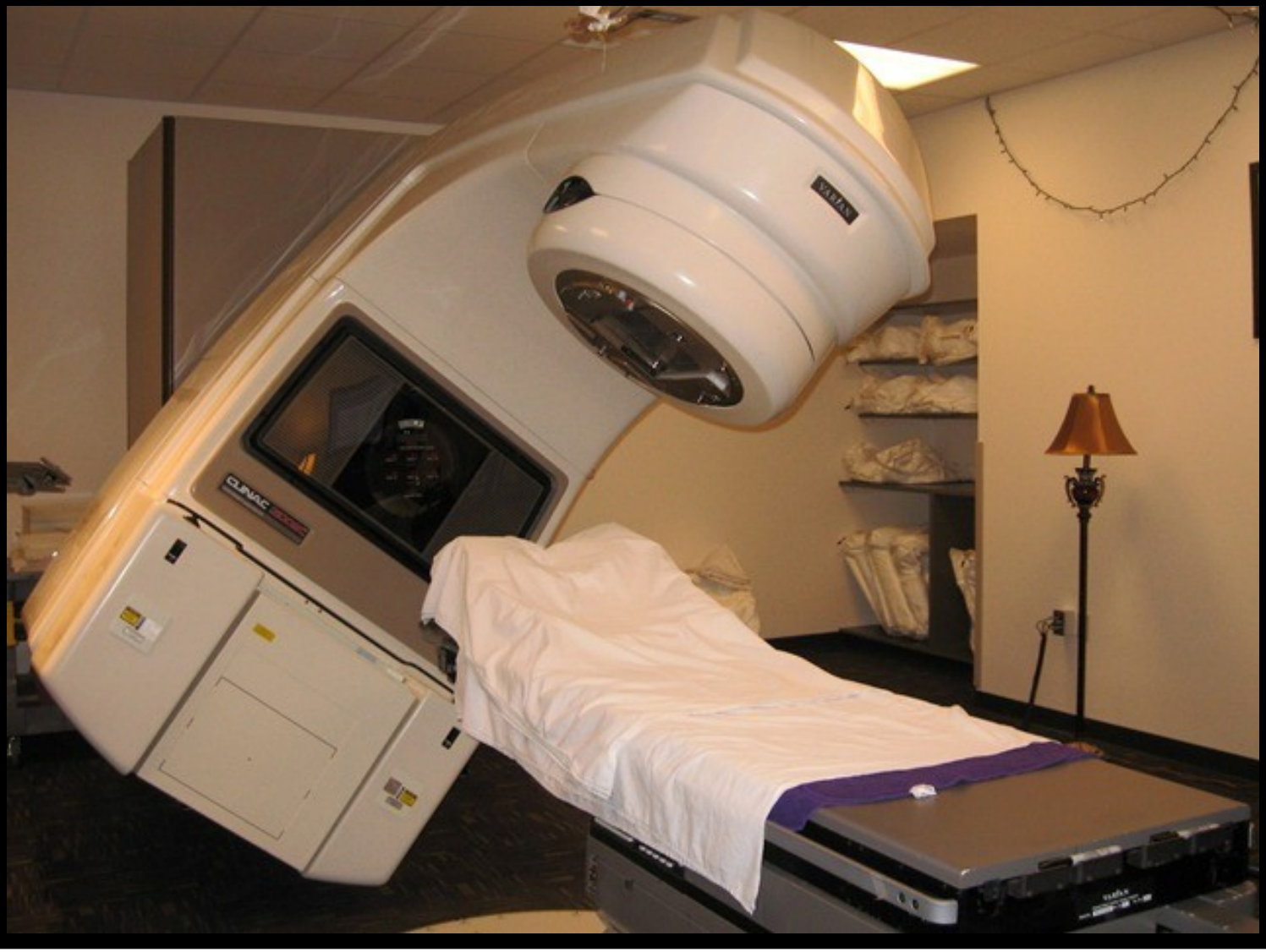
Ariane 5 flight 501

```
L_M_BV_32 := TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) * G_M_INFO_DERIVE(T_ALG.E_BV));

if L_M_BV_32 > 32767 then
        P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
elsif L_M_BV_32 < -32768 then
        P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
else
        P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32);
end if;

P_M_DERIVE(T_ALG.E_BH) := UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) *
G_M_INFO_DERIVE(T_ALG.E_BH)));
```

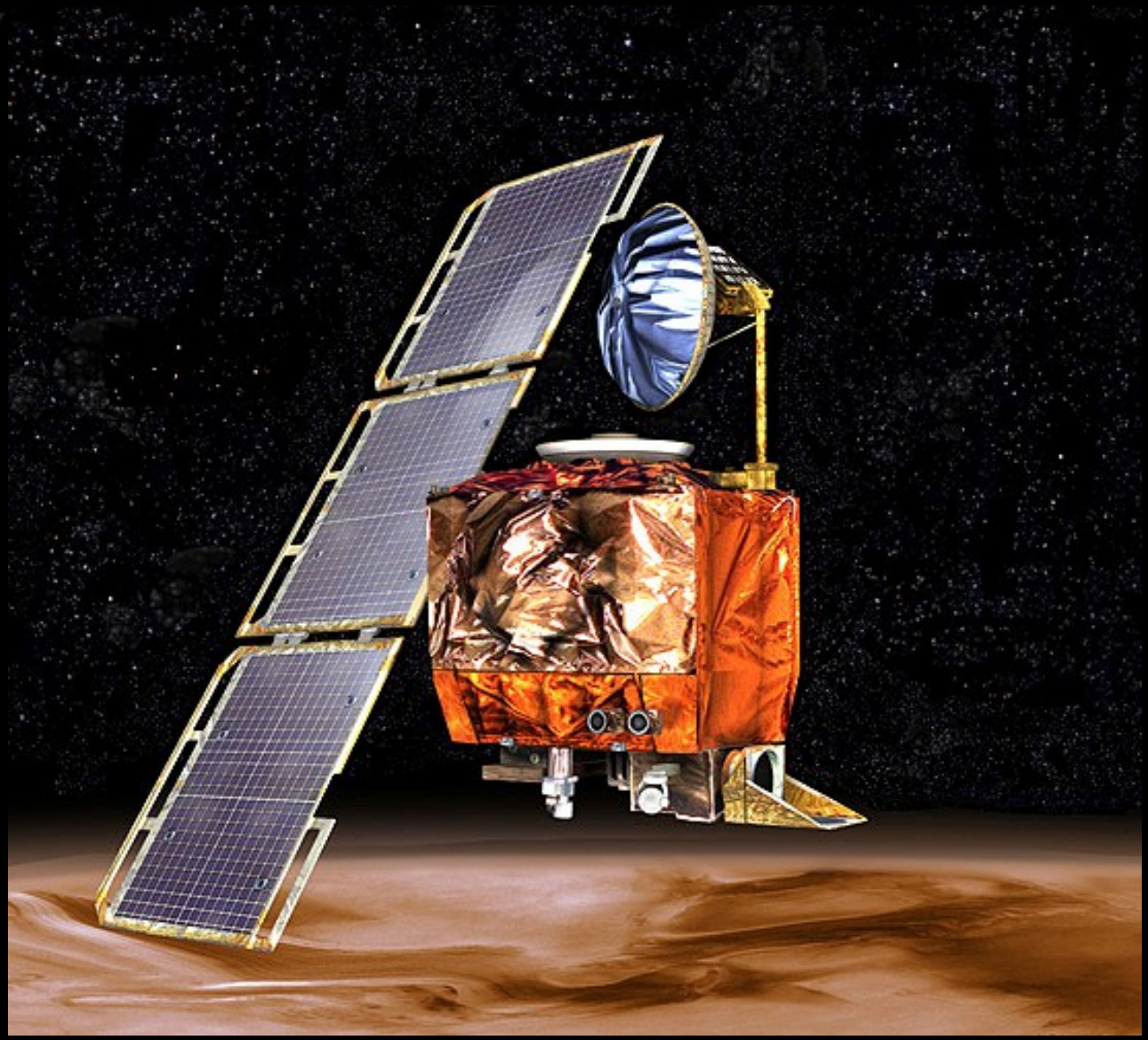
http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf

SECURITY

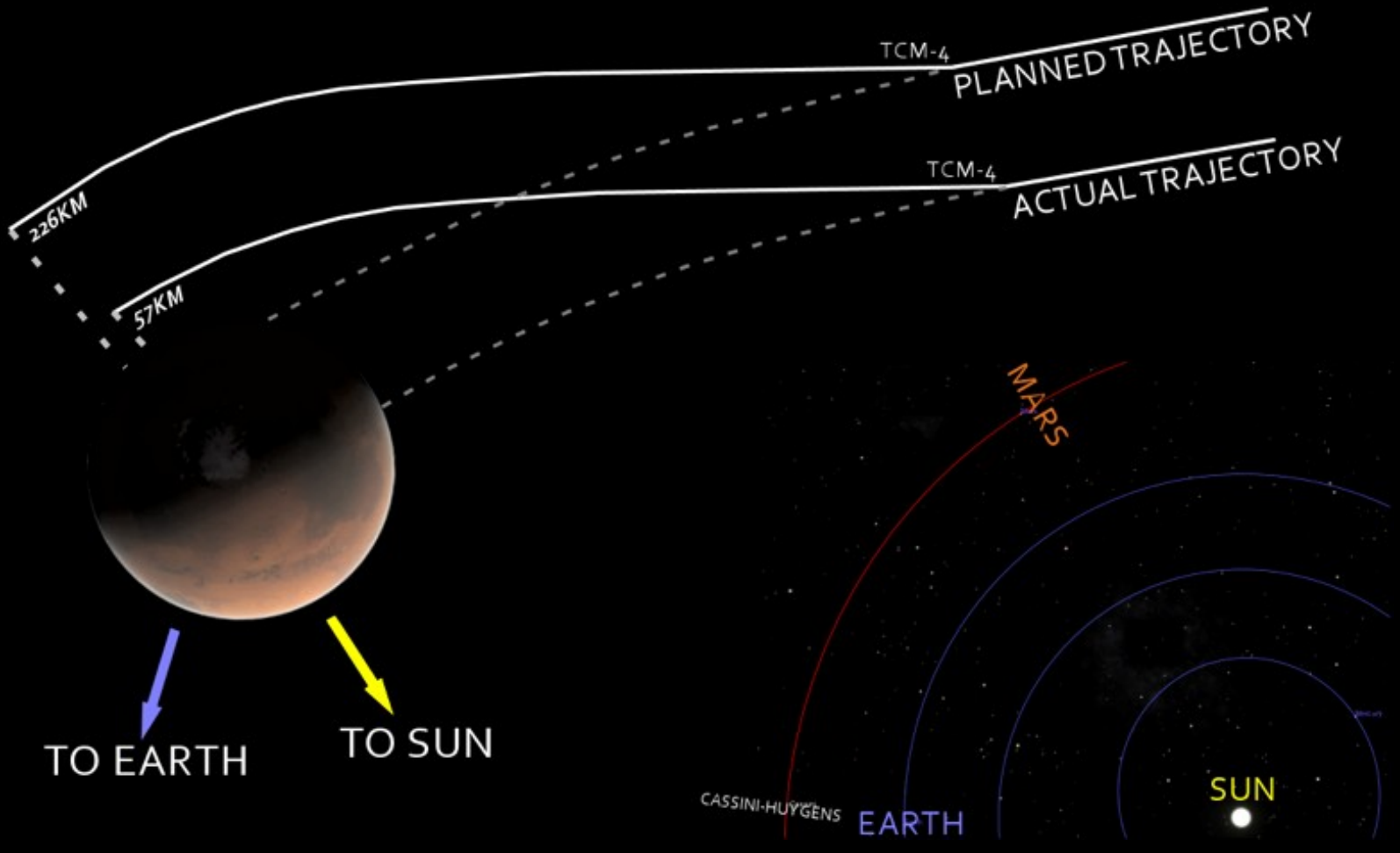
Therac-25



Mars Climate Orbiter



Mars Climate Orbiter



Agnitio

- Checklists?
  - Do you use checklist for your source code reviews?
  - What's the worst that could happen if you don’t?
  - Four people dead and over €700m of equipment destroyed
  - Checklists can be useful to pilots, doctors and code reviewers!

realex
The real time payment exchange

Agnitio

- So, why did I develop Agnitio?
  - I love using checklists for security code reviews!
  - Even if your process is good it might not be smart
  - Is your review process really repeatable and easy to audit?
  - How about producing metrics, useful reports & integrity checks?
  - No? That's why I developed Agnitio!

realex
The real time payment exchange

Why did I develop Agnitio?

- Demonstration: application profiles

realex
The real time payment exchange

Why did I develop Agnitio?

- Demonstration: security code reviews

realex
The real time payment exchange

Why did I develop Agnitio?

- Demonstration: security code review reports

realex
The real time payment exchange

Why did I develop Agnitio?

- Demonstration: application security metrics

realex
The real time payment exchange

Why did I develop Agnitio?

- Demonstration: customise your Agnitio installation

realex
The real time payment exchange

Agnitio hands on

- Create a PHP rule

realex
The real time payment exchange

Agnitio hands on

- Analyse the PHP application

realex
The real time payment exchange

Agnitio v2.2

- Verification records for the code you analyse
- Ability to use open source static analysis tools
- Full screen mode, syntax highlighting etc
- Suggested security test cases for failed items
- Save reviews without completing them
- Plus many more new features!

realex
The real time payment exchange

My “shoot for the moon” vision for Agnitio

“we pretty much need a Burp Pro equivalent for Static Analysis – awesome, powerful in the right hands, and completely affordable!”

http://www.securityninja.co.uk/application-security/can-you-implement-static-analysis-without-breaking-the-bank/comment-page-1

realex
The real time payment exchange

Using Agnitio

- How you can use Agnitio in your reviews
  - Download Agnitio from Source Forge
  - Focus security code reviews on root causes not vulnerabilities
  - Use your language/s in all code examples and checklist items
  - Use Agnitio to conduct principles based security code reviews

realex
The real time payment exchange

QUESTIONS?

www.securityninja.co.uk

http://sourceforge.net/projects/agnitiotool/


@securityninja


/realexninja


/securityninja

/realexninja