CHAPTER 26
SYSTEM EVALUATION AND ASSURANCE
AZMI ABU AHMAD
WHAT ARE ASSURANCE AND EVALUATION..?

• Assurance - whether the system will work
• Evaluation- how to convince other people of this
ASSURANCE

• Assurance - our estimate of the likelihood that a system will fail in a particular way

• This estimate can be based on a number of factors
PERVERSE ECONOMIC INCENTIVES

• The big missing factor in the traditional approach to evaluation is usability
• The incentives are also often adrift in that the customers and the vendors want different things
SECURITY TESTING

• Security testing usually comes down to reading the product documentation, reviewing the code, and then performing a number of tests.

• Architectural flaws

• Implementation flaws (using fuzzers)

• Less common flaws
FORMAL METHODS

• BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both

• The military purchasers seek more

• Proofs can have errors too. If something is provably secure it probably isn’t.
Who shall watch the watchmen?

Once you have a mature product, you should have a good idea of the rate at which bugs will be discovered.
PROCESS ASSURANCE

• Less emphasis on the assurance measures of the product, and more on who developed the system (some programmers produce code with less bugs than others)

• In the 1980s, many organizations interpreted the waterfall model of system development
PROCESS ASSURANCE

The Seven Principles of ISO 9001:2015

- Customer focus
- Leadership
- Engagement of people
- Process approach
- Improvement
- Evidence-based decision making
- Relationship management

Level 1: Initial
- Processes unpredictable, poorly controlled and reactive

Level 2: Repeatable
- Processes characterized for projects and is often reactive

Level 3: Defined
- Processes characterized for the organization and is proactive

Level 4: Managed
- Processes measured and controlled

Level 5: Optimizing
- Focus on process improvement
• An overlooked point is that assurance schemes should support revocation (they don’t for the following reason)

• The problem in here is that vendors aren’t willing to spend money on something they might lose
ASSURANCE GROWTH

• Most software nowadays is developed by continual evolutionary enhancement rather than in a one-off project

• Poisson distribution: \( p = e^{-Et} \)

• This includes a proof of a version of ‘Murphy’s Law’: that the number of defects which survive a selection process is maximized.
EVOLUTION AND SECURITY ASSURANCE

- Evolutionary growth of reliability for the security engineer causes trouble
- Ahmad (Ben Laden) VS Brian (Assurance guy)
EVALUATION

• Evaluation can be defined by the process of assembling evidence that a system meets, or fails to meet, a prescribed assurance target

• Problems occur when the party that provides the protection and the party that relies on it are different

• Evaluations are broken down into 2 cases
EVALUATIONS BY THE RELYING PARTY

• The insurance industry operates laboratories where tests are conducted
• This process may fail because the system doesn’t always respond well enough to progress in attack technology
• The Orange Book wasn’t the only evaluation scheme running in America.
• A number of European countries developed the Information Technology Security Evaluation Criteria (ITSEC)
THE COMMON CRITERIA

• The Defense Department began to realize that the Orange Book wasn’t making evaluation any easier, different evaluations in different countries

• A PP (protection profile) is a combination of threats, EAL (Evaluation Assurance Levels), security objectives, security assurance requirements and rationales
THE COMMON CRITERIA

• The smartcard industry has been a huge fan of evaluation
• There’s a big choice and it’s not easy to understand what an evaluation certificate actually means
Let’s look at some Protection Profile examples:

So the first question a customer should ask when he understands that a product has a Common Criteria Evaluation is: ‘against what protection profile?’

EAL (Evaluation Assurance Level) isn’t a good indicator..
WHAT CAN’T THE CC DO?

• Hint: A LOT

• No such thing as re-evaluation

• The Common Criteria doesn’t cope well with change

• A lot of commercial products have an evaluation that’s essentially meaningless
CORRUPTION, MANIPULATION AND INERTIA

• There are also perverse incentives and political failures.

• Common Criteria evaluations are done by CLEFS—contractors who are ‘Commercial Licensed Evaluation Facilities’.

• The biggest problem is it’s the vendor who pays the CLEF
• The protection profiles might be great, but the way they’re mapped into the real life isn’t... → Electronic signatures didn’t take off
• No sanctions for misbehavior → the incentive will be for CLEFs to race to the bottom and compete to give vendors an easy ride
• The Common Criteria is responsible for lousy, defective products
• The suppliers are free to describe a defective product as ‘CC evaluated’ and even ‘CC Approved’, as long as they don’t call it ‘CC certified’
A PIECE OF ADVICE

• When presented with a security product, you must always keep in mind that the salesman might be lying; ask questions

• Who is the CLEF behind the evaluation?

• You should also consider how your rights are eroded by the certificate
MOVING FORWARD

• Usability is ignored by the Common Criteria, but is in reality all important

• You probably have enough methods to cheat the system. For the remainder of the presentation we are making an effort to protect the system.
HOSTILE REVIEW

• Friendly reviews aren’t as important as hostile reviews of people who are trying to break the system

• The classic ways of doing hostile review are contractual and conflictual

• We can also combine the two ways
OPEN SOURCE SOFTWARE

• Many security products have publicly available source code, the first was the PGP email encryption program.

• Eric Raymond: With many eyeballs, all bugs are shallow

• Different testers find different bugs as their test focus is different

• Will the attackers or the defenders be helped more?
• THANKS FOR LISTENING!!
• QUESTIONS?