Challenges of CC Evaluations

A vendor's perspective

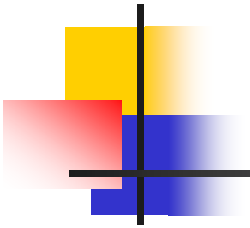
by:
Soheila Amiri

Director
Q/A and Security Certifications

- CyberGuard Corporation
- 350 SW 12th Avenue
- Deerfield Beach, Florida, 33442
- +1 954-375-3611
- samiri@cyberguard.com

Overview

- **A brief history of CyberGuard certifications**
- **CC – Challenges in continually meeting certification requirements:**
  - Security v. Performance – A vendor dilemma
  - Managing software or hardware changes
  - Recertification dilemma
  - Hardware tied to certification
  - Restrictive nature of AC requirements
  - While you were certifying the world passed you by!
- **CC – As a value add:**
  - Meeting requirements v. embracing the methodology
  - CC driven processes
  - Flaw Remediation – Whose watching over you?
  - Designing with certifications in mind
  - Protection Profiles – as marketing requirements documents
  - Testing with certifications in mind
- **Commercial consumer vs. government consumer**
  - Market motivators
  - Education is the name of the game
  - Offering CC requirements as product features
- **Recommendations**
- **Questions and answers**



Challenges of CC Certifications

A brief history of CyberGuard evaluations for perspective

CyberGuard Evaluation History

- Over many years, CyberGuard has certified various products on various platforms under various certification schemes, the most prominent of which are:
- Trusted Computer System Evaluation Criteria (**TCSEC**), a comprehensive United States Department of Defense (DoD) certification criteria for IT products.
- Information Technology Security Evaluation Criteria (**ITSEC**), a multi-national European version of certification criteria for IT products.
- Common Criteria (**CC**) a comprehensive international certification criteria for IT products.
- In each case, CyberGuard has either been the only vendor or the first vendor to go through application of these criterion to existing Commercial, Off the Shelf (COTS) products.

Purpose of Certifications

Why do we continue to certify our products:

- To ensure confidence in customers that our products are qualified adequately to accomplish their specific tasks.
- To provide reduced or manageable risk and assure fewer or no “surprises” when customers buy the product.
- To attach a brand to the product that is reinforcing in and of itself. Certified product, better product and vice versa.
- To give us advantage over the competitors in the market place.
- To open domestic and international markets for us.
- To improve our processes to meet all of the above.

Uses of CC Certifications

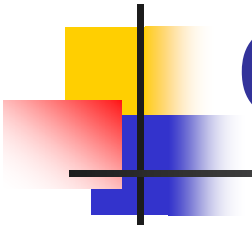
Who benefits from our certifications:

Consumers - as a guide for the **procurement** of products with IT security features:

- Government customers
- Commercial customers

Product Developers and Integrators - as a basis for the **development** of products with IT security features

Auditors, Certifiers, Accreditors - to support their specific needs, regulatory compliance, etc.



CC Certification Challenges

Challenges in continually meeting certification requirements

Security vs. Performance

- We have to design security features and we have to deliver high performance.
- These are contrary objectives. The higher the security level, the lower the performance level.
- We have resolved this by designing with as many configurable options as possible.
- This has made our products highly flexible and configurable. Customer decides what is the right balance.
- This has been an advantage that in significant part is due to our certifications efforts.

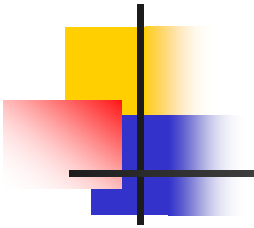
Managing Hardware or Software Changes

- Most high level certifications tie software and hardware together.
- The vendor's objective is to certify the latest software and latest hardware.
- Obviously, development is ongoing while you are certifying.
- With long duration of certifications and short life cycle of commodity hardware, you often end up with certified ancient hardware running old software no one needs.

Recertification Dilemma

Which brings us to this problem:

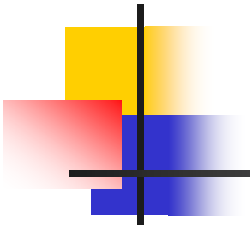
- How often do you recertify? A matter of time, resources and costs for vendor.
- Separating software from hardware certifications eases the frequency.
- We have to enhance the scheme to allow certification of generic hardware. We have proposals in front of the CB and International committee to this effect.
- Assurance Maintenance was one way to manage minor software releases between two major certifications.
- Assurance Continuity is too restrictive and unpredictable from vendor point of view.
- We have offered to partner with the CB and see how the process can work to achieve both goals.



The World Moves On

Meanwhile, the solutions we have found that work for us:

- CyberGuard has previously invested heavily in automating the AMA process and used the mechanism to maintain minor releases.
- Even though AMA is no longer approved by CC, we continue to maintain the software in a certification ready state, using the AMA model, by preserving SEFs and using repeatable, automated testing at each release.
- This makes us ready to go to recertification at every revision of the product.
- We stagger the certifications in multiple planned releases. This way, we have a certified product to hold the customer over while another one is in the works.



Challenges of CC Certifications

Common Criteria as a value add

Meeting or Exceeding Requirements?

- One approach some vendors use is to meet the requirements once, to get the product certified once.
- We have found that unless we turn them into ongoing processes, they will be costly to revamp each time.
- The process enhancements include:
  - Development process – requirements built in at design stage
  - Q/A process – non compliance with requirements ironed early
  - Physical Security – both system and human aspects
  - Shipping practices and product packaging
  - Corporate security policy
  - And many more…

CC Driven Processes

As a direct result of certifications we:

- Design certification requirements early in development cycle.
- Have established an automated testing process with over 1000 functional repeatable tests.
- Have established an end-to-end flaw remediation process with objective of preemptive resolution of vulnerabilities.
- Enhanced the physical security of our headquarters.
- Improved our corporate security policy.
- Improved our shipping practices.
- And many more…

ALC_FLR.3 Flaw Remediation

An example of a CC driven process:

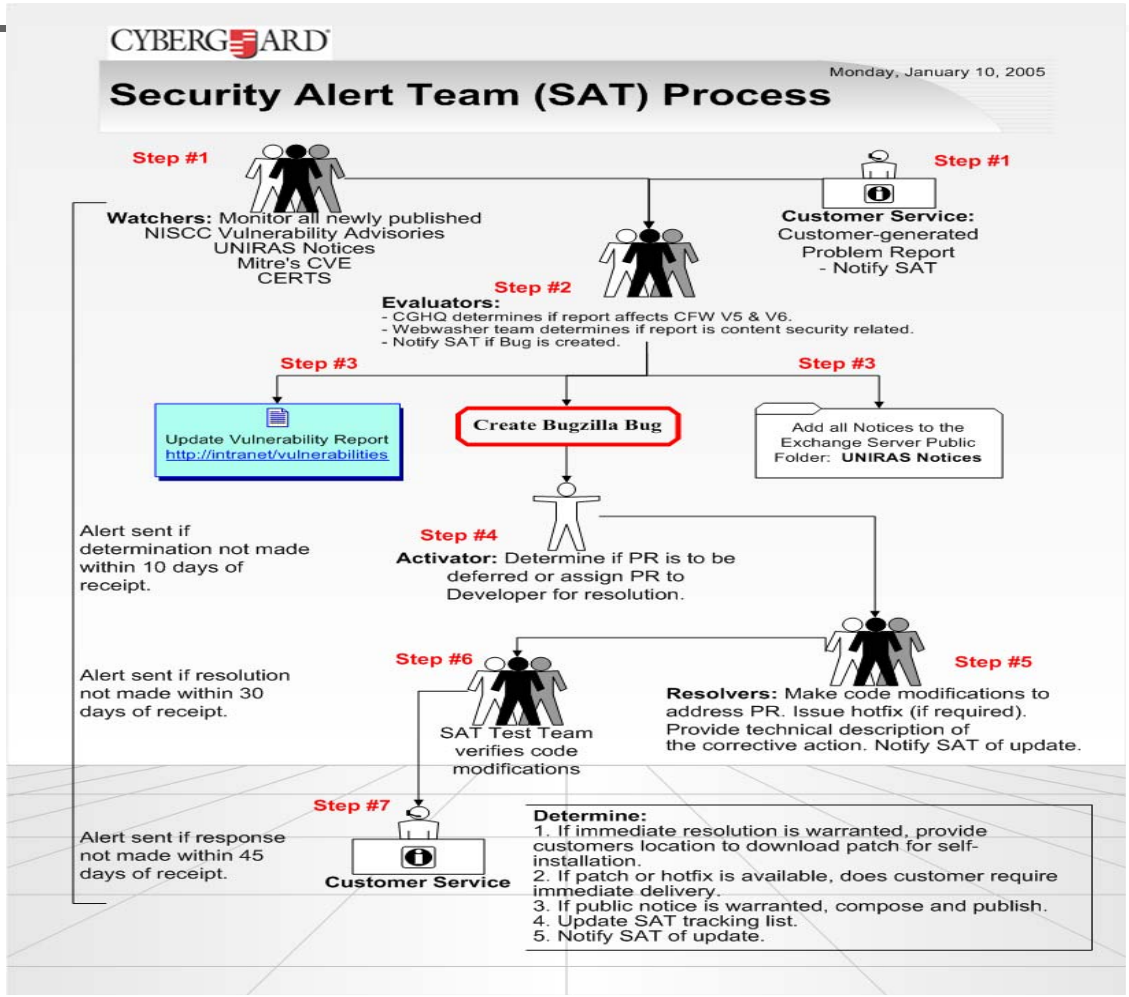
- CyberGuard has achieved the highest level of Flaw Remediation defined in CC (ALC_FLR.3).
- This has mandated a comprehensive end-to-end process to achieve zero public vulnerabilities and maintain this status.
- Process involves at least four distinct groups within CyberGuard to cooperate together.
- This involves Certification, Development, Q/A and Customer Service to find, fix and disseminate vulnerability or best practice information to customers.

ALC_FLR.3 Flaw Remediation

An example of a CC driven process:

- Process has multiple points of input for reporting potential problems.
- Process has automation built into it for resolution and tracking of reported problems.
- Process requires monitoring publicly reported vulnerabilities and testing for them even if not reported against us.
- Point being that the customer community is benefiting from the oversight of certification process, whether they know it or not.

Flaw Remediation Process at a Glance



CC Driven Processes

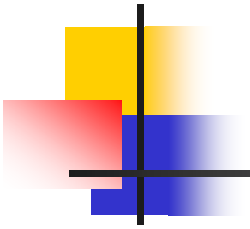
Designing and testing with certification in mind:

- In the beginning, there was no indication what certified security features the customer required.
- Scope of certification at best was a guessing game by the vendor.
- Non-compliant software features were patched long after development was completed.
- With introduction of PPs, we know the requirements of a significant portion of our customer base.
- PPs work the same as marketing requirement documents.

CC Driven Processes

Designing and testing with certification in mind:

- We use PP's and other CC guidance documentation as requirements documents for designing new or enhancing existing features.
- The earlier features are built in, the more time to iron out any lack of conformance.
- This change in approach in design and development is a CC driven process.
- Again an overall benefit to the customer as the best security practices are continually built into the product.



Challenges of CC Certifications

Commercial v. government market

Market Motivators

- It is difficult to sell IT products on their certification merits, because an understanding of the process itself would be required by the customer.
- Government sectors for the most part are familiar with CC, or are mandated by law to deploy CC conformant products.
- CC is an unknown process for the most part in the commercial market.
- The commercial market is however driven by some factors that tie into the certifications process.

Market Motivators

What could drive the commercial market to embrace CC?

- There are privacy and confidentiality concerns for commercial consumer when dealing with private information. These are fuelled by:
  - Laws and regulations requiring protection of user data (example HIPPA regulations in US).
  - Privacy and confidentiality issues and loss of consumer confidence (example regulations in Europe dealing with e-mail privacy).
  - High profile Security breaches resulting in loss of customer data.
  - Regulatory compliance (for example Sarbain-Oxley regulations in US) and others.

Market Motivators

How do we extend the CC protection to commercial markets?

- Educating the consumer is the very first step.
- The burden is on the vendor to educate its potential commercial customer as to the benefits gained from a certified product.
- The burden is similarly on the scheme and its officials to educate the commercial consumers as to its advantages.
- Many of enhancements that CC has introduced in CyberGuard is a selling point for us.
- We capitalize on these by educating our sales force, who in turn educate the potential commercial consumers on how the CC certified components can help them achieve these goals.

Summary and recommendations

- Educating the commercial consumer is the very first step in extending CC to commercial markets.
- Vendors must take advantage of the CC process enhancements and use them as a competitive edge, not just as a stamp of approval, but with detailed benefits to their customers.
- Product features that meet CC requirements must be marketed by vendors with their full CC credentials marketed.
- Vendors must step in when high profile incidents are exposed to educate the consumers which certified features can help resolve the issues.
- If there is any hope of expanding CC to commercial markets, it requires the scheme to step in and resolve some of the age old problems vendors face in certification process. This allows the vendor to keep certifying in the first place.

Challenges of CC Evaluations

A vendor's perspective

by:
Soheila Amiri

Director
Q/A and Security Certifications

- CyberGuard Corporation
- 350 SW 12th Avenue
- Deerfield Beach, Florida, 33442
- 954-375-3611
- samiri@cyberguard.com