Security Testing, Research, Counsel & Leadership

How to build a Software Assurance program using sneak and stealth

Trustworthy Development Process and Criteria for Testing

The Security Consortium

Better Knowledge - Better Decisions - Better Security

Disclaimer

- TSC was formed by a group of world class security professionals who wanted to work together sharing a common brand and business infrastructure

- TSC is privately held, founded in 2007 and based in San Jose California

(This is our logo and yes, Djenana it will be on every slide)

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Objective

- Evangelize ongoing certification for development *process* and not the product
- Help vendors build, use, and grow a workable and cost effectiveSA program

Observations

- Security testing tools are worthless if:
  - Management doesn't understand why there is value in using them
  - Management isn't interested in producing a trustworthy product
  - There is no process framework for them to work within

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Observations

- Once management sees the benefits of SA, they drink the Kool-Aid
  - They enforce the process
  - Creates a culture of security
  - Creates a vacuum for tools to eventually fill

Observations

- Scoring systems aren't effective
  - Score should change for each patch
  - Underlying host system has its own vulnerabilities
  - Brings vendors back to testing well for each major product release
  - Can be very expensive for complex products

Success Criteria

- Device Under Test (DUT) MUST:
  - Not create a security hazard when deployed
  - Operate as advertized
  - Not contain hidden functionality
  - Fail in a safe manner

No product that TSC has examined has completely passed this set of criteria

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Methodology

- Testing Framework
  - 3 Test Phases
    - Safety to Deploy
    - Fit for Purpose
    - Destructive Product Test
  - STD & FFP feed Battle Plan for Destructive Test
    - Multiple staff
    - Specialists in appropriate fields

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Testing Framework

- Iterative Process
  - Observe, theorize, test (repeat)
  - More like investigative reporting
- Starts as "black box" Testing
  - We start with the "Out of the box" experience
  - Customer's people think we're real customers
- Moves to "gray box" Testing
  - We've connected with support folks
- Moves to "white box" Testing
  - We have documentation and access to developers

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Test Telemetry

- Provides detailed information about:
  - Product security and performance
  - Documentation accuracy and effectiveness
  - Support (in)effectiveness
  - Development environment maturity
- End result is to slowly modify development process by pointing out where cost savings *could have* been made

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

The Results

- Telemetry is analyzed and correlated
- Based on our knowledge of development environments we:
  - Postulate where the failure occurred
  - Recommend a mitigation or change in process

No product has ever initially passed the STD test

How Customers React

- Some very well!
  - Processes change
  - Products improve
- Some not so well….

But that's why we have lawyers!

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Case Study 1

- Appliance vendor
- Security product
  - Enterprise unit & satellite unit
- Wanted to know what was in the box
  - Entire engineering department quit
  - Shinny new CEO and Sr VP of Engineering
  - Only executive staff and some support
- Trying to get more funding

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Case Study 1 Results

- Failed Safety to Deploy Test
  - Anyone could change product configs
- Failed Fit for Purpose Test
  - Claims of functionality not present *at all*
- Failed Destructive Product Test
- Discovered interesting things about product too….

A large portion of the product's functionality was based on unlicensed open source code

CEO and VP eventually left company

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Case Study 2

- Appliance vendor
- Security product
  - VPN based on MS products (IAG)
  - Multiple "sized" versions
- Was worried about latency
- Only opted to pay for DPT

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Case Study 2 Results

- We tested anyway
- Initially Failed STD
  - No passwords on default network connection
  - No requirement to change them either
- Initially Failed FFP
  - Didn't meet claims of performance
- Failed DPT
  - Killed it with a 5 year old Dell and a 10Mb/s net
  - Leaked tunnel information
  - When product dies it hoses firewall and web server
- Modified build process and enforced version control
- Changes to build process has to pass security review

Case Study 3

- Appliance vendor
  - Restart mode after missing market opportunity
- Security product
  - Firewall, VPN, IDS, Flow monitor
  - Small brick like device
- Worried about functionality
- Customer evals were tanking
- Looking for more funding

Case Study 3 Results

- Failed STD
  - Same as #2 (make install easy)
- Failed FFP
  - Products had incompatible modes
  - Documentation was just wrong
- No DPT done…not needed
- Champion was CTO and new CEO
- Antagonists were legacy directorate
- CTO couldn't get recommendations implemented
- VCs found out about product and process flaws and declined to invest
- Company folded and sold IP

Case Study 4

- Shinny new start-up!
- Software product
- Wanted to know if they had a good idea
  - Can't tell you what it is but it's scary cool!
- Wanted to ensure that they "got it right"
- Wanted to be able to show VCs that they understood all aspects of security

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Case Study 4 Results

- Instituted a fledgling security review process
- Working with engineers to:
  - Vet use cases
  - Institute SA Program
  - Generate documentation frame work
- Driven by Angels
- VCs are listening
- More at the next meeting

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security

Trustworthy Development Aliance

- Goals
  - To demonstrate to potential customers that the processes used to gather requirements and turn them into product is secure and worthy of their trust
  - To educate the universe that the first question that should be asked of any vendor is "Why should I trust you or your stink'n product?"
  - No Djenana, none of our customers are in it…yet.

TSC The Security Consortium
Better Knowledge - Better Decisions - Better Security