AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Android Security Product Testing

Maik Morgenstern (CTO) and Andreas Marx (CEO)
AV-TEST GmbH, Magdeburg, Germany

Presented at AVAR 2012 Hangzhou

http://www.av-test.org

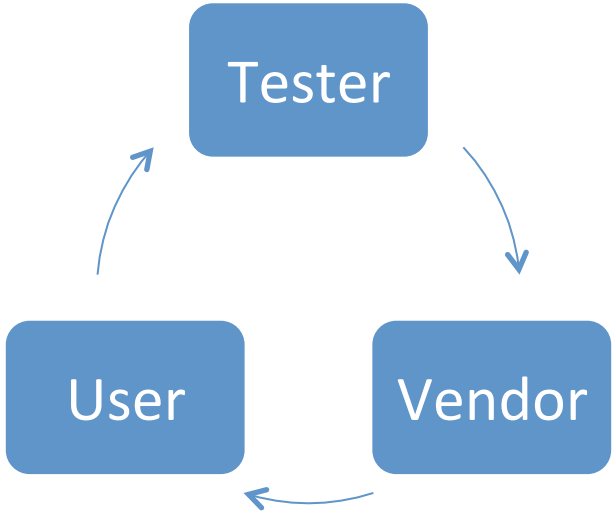
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Content

- Motivation
- Why Android?
- Good and Bad Points of Current Tests
- What really matters
- AV-TEST approach

Motivation

- Three interest groups with conflicting interests and opinions



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Motivation

- Users don‘t know about threat details
- Users don’t care about testing methodologies
- Users just want to be secure and want to know which program they should use
- Many Smartphone users are less technically savvy than many PC users

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Motivation

- Vendors don't want to fail the tests
- Especially not because of errors in the methodology or sample selection
- Vendors want good technical tests (see AMTSO guidelines)
- Vendors want results for technical improvements but also for marketing purposes

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Motivation

- Testers originally wanted to answer users questions
- Testers have to technically improve their tests more and more to meet the strict expectations of vendors
  - For the good tests (from good testers) this doesn't change much to the results, but adds more complexity to the methodology and makes results harder to understand
- Testers have moved the focus from users to the vendor, making many tests virtually useless for the user

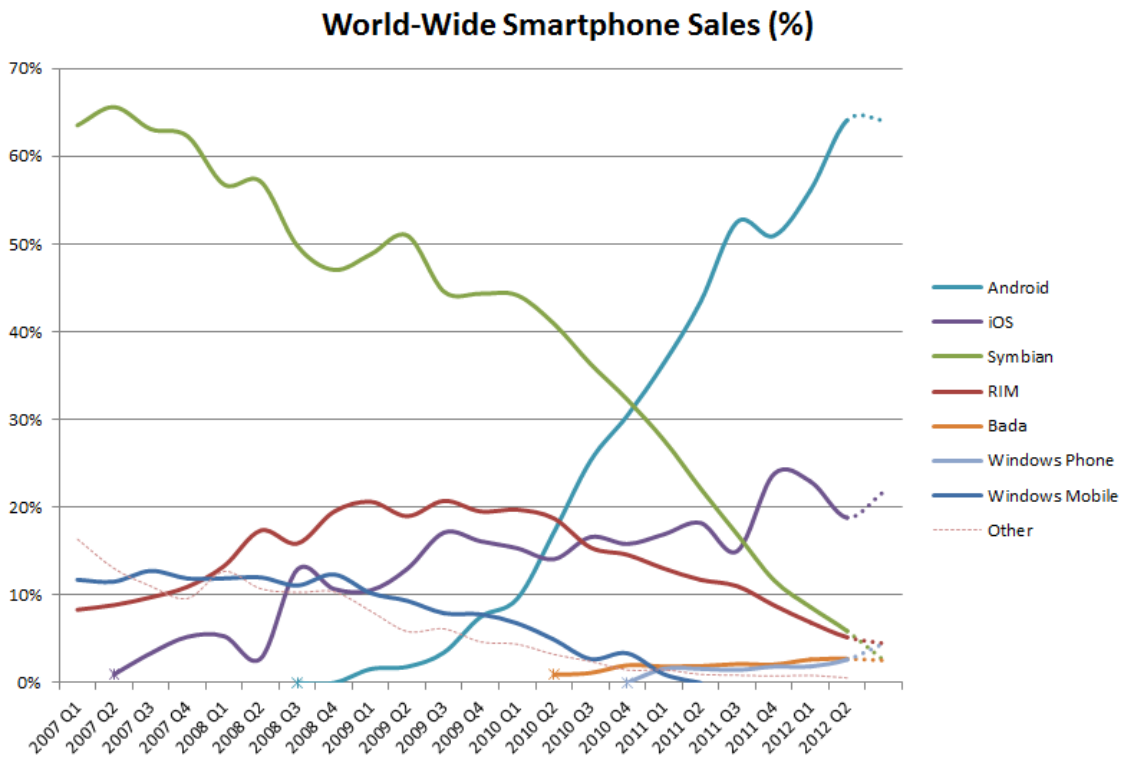
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Motivation

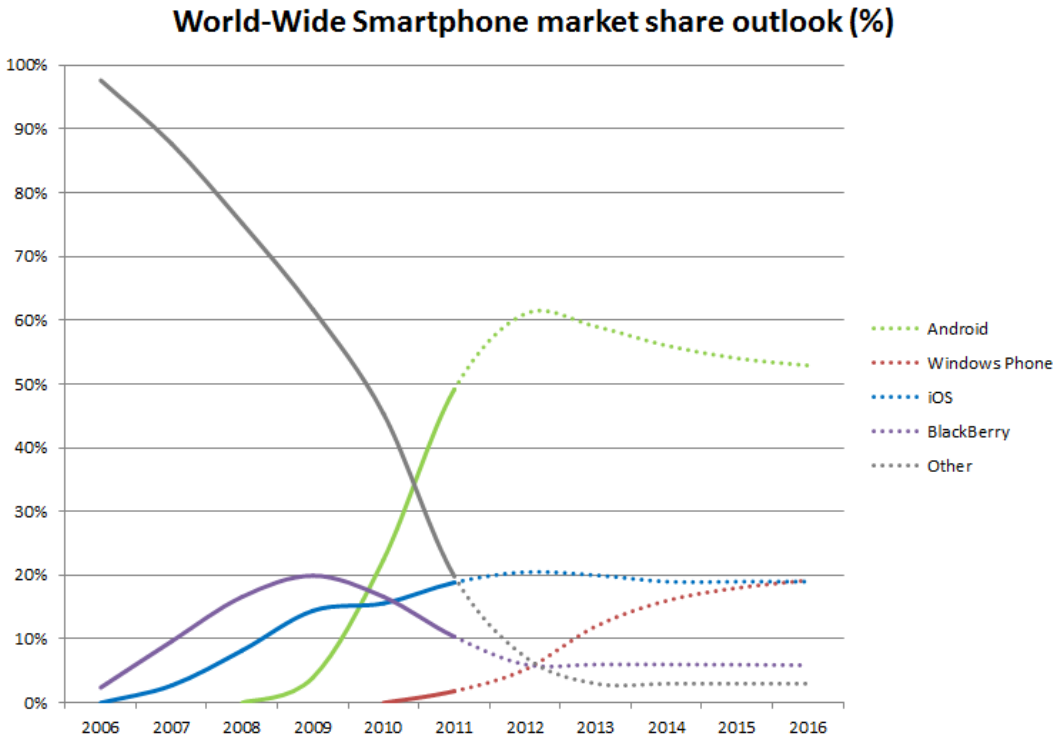
- Changing PC Security testing is difficult to do for historic reasons, only small steps are possible
- Android as a new platform, different user base, with new threats and scenarios is the perfect platform to change testing and make it right
- Answer users questions (and at the same time fulfill technical expectations of vendors)

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Why Android?



Why Android?


World-Wide Smartphone market share outlook (%)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
Android
Windows Phone
iOS
BlackBerry
Other

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Why Android?

- Android is popular because
  - Cheap and easy to use for vendors
  - It is very open and customizable
  - Lots of apps and lots of (regional) markets
- Also popular among malware authors
  - Open markets
  - A huge user base
  - The only modern mobile OS that can be used for their purposes

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- There have already been several tests for Android Security Software
- They have been mostly inspired by the traditional PC testing
  - AV-TEST
    - "Are free Android virus scanners any good?" November 2011
    - "Test Report: Anti-Malware solutions for Android" March 2012
  - West Coast Labs
    - "Custom Test Report - NQ Mobile Inc." October 2011
    - "Mobile Security Technology Report" October 2011
  - AV-Comparatives
    - "Mobile Review" August 2010 [5]
    - "Mobile Review" August 2011 [6]
    - "Mobile Security Review" September 2012 [7]

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Only very few specific questions are answered
  - Which program protects best against malicious apps?
  - Which free security apps are useless?
  - Which apps do have further security features?
- The main question is not answered by any report: Which apps protect me best from all the security threats?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- There are errors or at least problems in the methodology, the sample selection and the display of results for some of the reports
- User questions are not answered and furthermore the data and results are not reliable, sometimes there is not even real data
- But both expectations have to be met:
  - Technical correct tests
  - Tests that are focusing on user demands

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Limited testing criteria
  - Any detection test should be accompanied by a false positive test
  - There is more to test than just malware detection
    - Performance, Anti-Theft, Encryption, Backup etc. are important as well
    - PUA vs. false positive vs. malware problem
  - Wrong focus
    - Is malware detection the most important feature?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Bad testing methodology
  - When testing malware detection, it should be feature independent
    - Some products don't provide an on-demand scan, but still protect the user with
  - Results are meaningless when they are all the same for all products
  - No comparative testing of certain features, instead describing the feature
    - Can these features be tested comparatively at all?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Bad documentation of the test
  - Missing version information or product details
  - Unclear methodology
  - Unclear sample set

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Bad sample set
  - Sample set is too small
  - Samples are too old or not prevalent or both
  - No detailed information about the sample set is given
    - Sample set may be distorted
      - 1000 samples split into 10 families with 100 samples each
      - 1000 samples split into 10 families, where one family has 950 samples and the other 50 samples are distributed among the remaining 9 families
      - If a product detects that one family particularly well it will score good

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

	Samples	Product A	Product B
Fakeinstallers	900	900	0
Other families	100	0	100
Final Result	1000	90%	10%

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

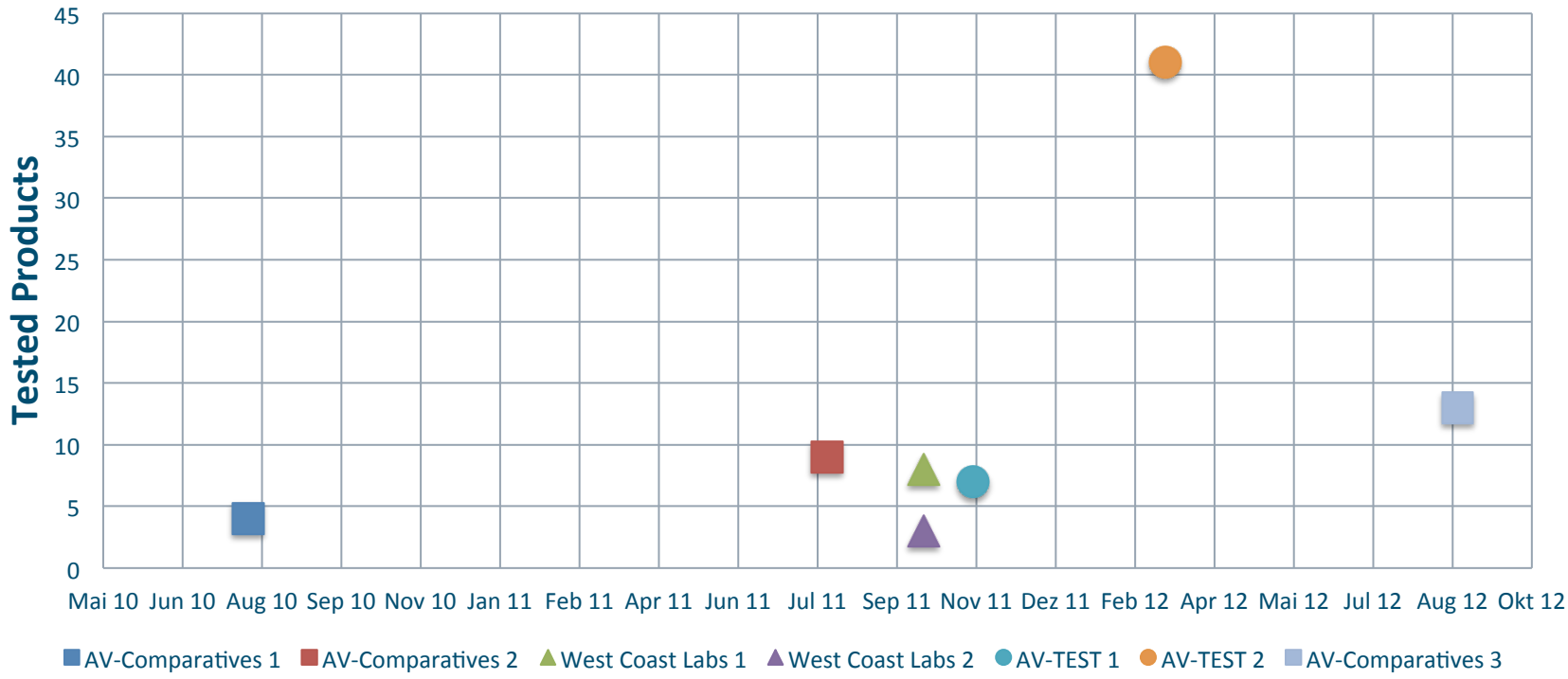
- Wrong product selection
  - Important products are missing
    - The results of the products cannot be realistically rated, as the winner of the test might still be worse than the missing product
  - Too few products tested
    - If the product the user is looking for/using is missing, then the test doesn't help him
  - Comparing apples to oranges
    - A mediocre product will always look good compared to a fake product
    - Different products have different features

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Bad Timing
  - Tests are quickly outdated
    - Threat Landscape and overall mobile landscape changes fast and often
    - Lots of new malware samples evolve daily
    - So the products change fast and often as well
  - Therefore up-to-date tests are necessary as well as regular tests to show the development of the products and to make sure the vendors are able to consistently react to the new problems

Good and Bad Points of Current Tests



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Good and Bad Points of Current Tests

- Results don't help the user to choose the right product
  - Do these tests answer the questions of the user at all?
    - All products achieve more or less the same results
    - There are no comparable results at all, just plain descriptions
    - There are testing criteria missing, only certain features/ scenarios are tested
    - There are too many plain results, interpreting them is hard to impossible for normal user

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- What happens when I lose my phone?
  - Can I get it back?
    - Anti-Theft (Locate Device)
  - Is my data safe?
    - Remote Wipe
    - Remote Lock
    - Encryption
  - Can I get my data back?
    - Online Backup

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- Is my privacy ensured?
  - Which apps spy on me and can security software tell me and protect me?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- Is malware a problem for me?
  - Malware Detection rates
  - I like free games, but they are reported as bad
    - PUA vs. malware

What really matters

- I want to protect my child from inappropriate content on the phone.
  - Parental Control

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- Will the security app eat all my battery or download bandwidth?
  - Measuring impact on battery life and downloads

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- Where do I find recent test results of my product or of all the good important products?
  - Required to perform regular tests to always have up-to-date results of the recent product versions
  - Include as many products as possible

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

What really matters

- Has this product always been so good/bad?
  - Again regular tests, so the user could look through the history and watch the development of a product.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- One obvious approach to solve the problem is quantity:
  - Test as many products as possible
  - Test as many aspects of the products as possible
  - Test as many scenarios/samples as possible
  - Perform the tests as often as possible
- Together with quality in methodology and sample selection

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- That is only half of the story
- Generating all the data is necessary but not enough
- No user could dig through all the raw data
- Interpretation of the data, according to certain real scenarios has to be done

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- Timing
  - We will test and publish results every second month
  - This ensures up-to-date and regular results
- Product Selection
  - The 20-30 most important vendors will be included to cover 99% of the users

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- Basic Information in the report
  - Version information about tested products
  - Description of sample set (size, age, families)
  - Description of methodology

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- Actual testing criteria
  - Malware detection rates
    - Including PUA (e.g. aggressive adware)
  - False positive rates
  - Performance impact
    - Battery drainage
    - Download bandwidth
  - Further security features

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST Approach

- From the different testing criteria it will be possible to derive answers for users questions
- Different user groups and their different demands can be considered

AV-TEST Approach

- Ultimately providing two different answers
  1. AV-TEST certifies products that perform overall good and are a good choice for most of the scenarios
  2. AV-TEST will provide the best fitting products for certain demands
     - Which product is able to help me when my phone is lost?
     - Which product protects my child from inappropriate content on the phone?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Thank you for your attention!
Questions?

Latest test results and news always available on

facebook.com/avtestorg
twitter.com/avtestorg
www.av-test.org