The Vulnerability Marketplace

WabiSabiLabi

The art of continuous improvement of imperfect security

DEFINITION OF A MARKET

WabiSabiLabi
CLOSER TO ZERØ RISK

From Wikipedia, the free encyclopedia

“A market is a social arrangement that allows buyers and sellers to discover information and carry out a voluntary exchange of goods or services. It is one of the two key institutions that organize trade, along with the right to own property. In everyday usage, the word "market" may refer to the location where goods are traded, sometimes known as a marketplace, or to a street market.

The function of a market requires, at a minimum, that both parties expect to become better off as a result of the transaction. Markets generally rely on price adjustments to provide information to parties engaging in a transaction, so that each may accurately gauge the subsequent change of their welfare.”

DEFINITION OF A MARKET

WabiSabiLabi
CLOSER TO ZERØ RISK

From Wikipedia, the free encyclopedia

"A market is a social arrangement that allows buyers and sellers to discover information and carry out a voluntary exchange of goods or services. It is one of the two key institutions that organize trade, along with the right to own property. In everyday usage, the word "market" may refer to the location where goods are traded, sometimes known as a marketplace, or to a street market.

The function of a market requires, at a minimum, that both parties expect to become better off as a result of the transaction. Markets generally rely on price adjustments to provide information to parties engaging in a transaction, so that each may accurately gauge the subsequent change of their welfare."

THE PHILOSOPHY BEHIND

WabiSabiLabi
CLOSER TO ZERØ RISK

ワビサビラビ

Wabi-sabi (in Japanese katakanaワビサビ) represents a comprehensive Japanese world view or aesthetic centred on the acceptance of transience. The phrase comes from the two words wabi and sabi. The aesthetic is sometimes described as one of beauty that is "imperfect, impermanent, and incomplete". It is a concept derived from the Buddhist assertion of the Three marks of existence — Anicca, or in Japanese, 無常 (mujyou), impermanence.

Wabi-sabi nurtures all that is authentic by acknowledging three simple realities: nothing lasts, nothing is finished, and nothing is perfect."

In this view, Wabi-sabi is the perfect term to represent the implicit imperfection of the IT security, as well as the scope of our project, which is to contribute to its improvement. This goal is achieved by completely re-designing the traditional security research cycle, introducing for the first time ever a market-driven approach to correctly value the security researchers contributions.

Nothing lasts, but everything can always be improved in its life-cycle.

A BIT OF HISTORY…

WabiSabiLabi
CLOSER TO ZERØ RISK

- Early 90s Legal threats, no disclosure
- 1993 - 2003 Full disclosure and still legal threats
- 2003 - 2007 Full disclosure, less legal threats
- 2002 -2007 Vulnerability purchasing projects
- 2007 WabiSabiLabi

CURRENT STATUS OF THE SECURITY MARKET

The security researcher's work is exploited for free due to:

- Ethical blackmailing
- Wrong set of laws
- Abused “de-facto” position
- Misconception of the security researcher’s role

HACKER = SECURITY RESEARCHER

http://tools.ietf.org/rfc/rfc4948.txt

2.1. The Underground Economy

As in any economic system, the underground economy is regulated by a demand and supply chain. The underground economy, which began as a barter system, has evolved into a giant shopping mall, commonly running on IRC (Internet Relay Chat) servers. The IRC servers provide various online stores selling information about stolen credit cards and bank accounts, malware, bot code, botnets, root accesses to compromised hosts and web servers, and much more. There are DDoS attack stores, credit card stores, PayPal and bank account stores, as well as Cisco and Juniper router stores that sell access to compromised routers. Although not everything can be found on every server, most common tools used to operate in the underground economy can be found on almost all the servers.

OUR BUSINESS MODEL VS. THE REST

WabiSabiLabi
CLOSER TO ZERØ RISK

	WSL
SINGLE SALE (AUCTION)	YES
MULTIPLE SALES	YES
DUTCH AUCTIONS	YES
BUY NOW	YES
EXCLUSIVE SALE	YES

OUR BUSINESS MODEL VS. THE REST

WabiSabiLabi
CLOSER TO ZERØ RISK

	WSL	OTHERS
MULTIPLE SALES	YES	NO
REVENUE SHARING	YES	NO
RESPONSIBLE DISCLOSURE	NO	YES
FREE PUBLIC WARNING	YES	NO
360° INTEREST	YES	NO

OUR BUSINESS MODEL VS. THE REST

WabiSabiLabi
CLOSER TO ZERØ RISK

SQUEEZING THE LEMON TWICE

IS IT ETHICAL?

WabiSabiLabi
CLOSER TO ZERØ RISK

RESPONSIBLE DISCLOSURE ???

WabiSabiLabi
CLOSER TO ZERØ RISK

LEGAL ASPECTS OF A SECURITY MARKETPLACE

WabiSabiLabi
CLOSER TO ZERØ RISK

	WabiSabiLabi	Researcers
Illegal possession of access codes	✔	✔
Wrongful purchase	✔	
Possession of stolen goods	✔	
Money laundering	✔	
Property theft		✔
Reverse engineering		✔
Terrorism	✔	✔
Wrong use of E.U.L.A.		✔
Blackmailing	✔	

CAVEAT EMPTOR

WabiSabiLabi
CLOSER TO ZERØ RISK

caveat emptor

(kah-vee-ott emptor) Latin for "let the buyer beware." The basic premise that the buyer buys at his/her own risk and therefore should examine and test a product himself/herself for obvious defects and imperfections. Caveat emptor still applies even if the purchase is "as is" or when a defect is obvious upon reasonable inspection before purchase. Since implied warranties (assumed quality of goods) and consumer protections have come upon the legal landscape, the seller is held to a higher standard of disclosure than "buyer beware" and has responsibility for defects which could not be noted by casual inspection (particularly since modern devices cannot be tested except by use and many products are pre-packaged).

CAVEAT EMPTOR

WabiSabiLabi
CLOSER TO ZERØ RISK

http://en.wikipedia.org/wiki/Caveat_emptor

Under the doctrine of Caveat Emptor, the buyer could not recover from the seller for defects on the property that rendered the property unfit for ordinary purposes. The only exception was if the seller actively concealed latent defects.

CAVEAT VENDITOR

WabiSabiLabi
CLOSER TO ZERØ RISK

Caveat venditor is Latin for "let the seller beware".

It is a counter to caveat emptor, and suggests that sellers too can be deceived in a market transaction. This forces the seller to take responsibility for the product, and discourages sellers from selling products of unreasonable quality.

THE BIG DILEMMA

WabiSabiLabi
CLOSER TO ZERØ RISK

"…to disclose or not to disclose?"

REPORT ON THE FIRST 3 MONTHS OF ACTIVITY

WabiSabiLabi
CLOSER TO ZERØ RISK

- 1,000 subscribers

- 93 (*) submitted vulnerabilities of which
  - WEB APPLICATION 24
  - LINUX 17
  - WINDOWS 45
  - MAC 2
  - OTHER 5 (iphone, network appliances, etc)
  - INVALID or REJECTED 33

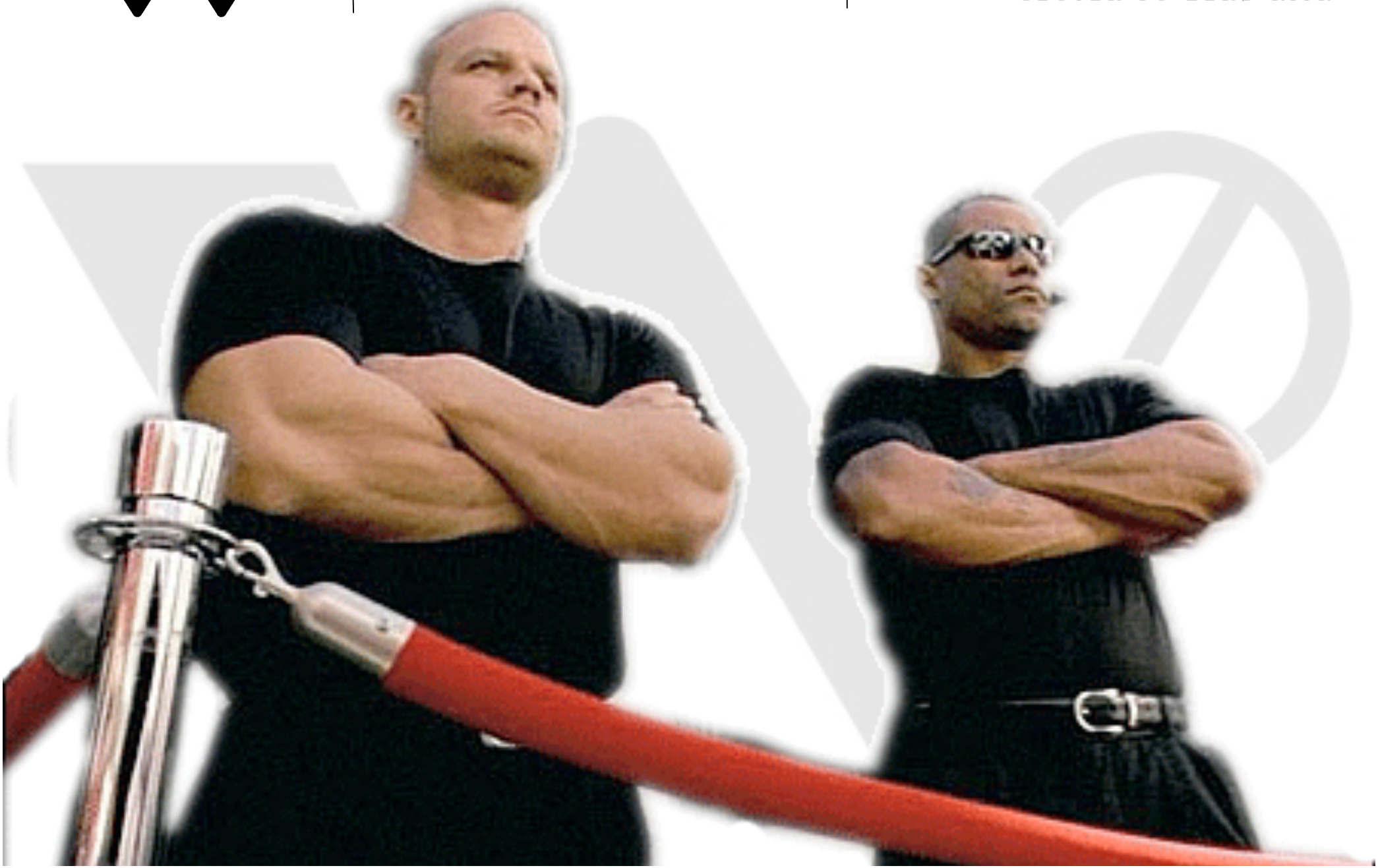
(*) at Aug. 27th 2007

WHAT KIND OF RESEARCH DID WE REJECT?

WabiSabiLabi
CLOSER TO ZERØ RISK

HOW DID WE VET BUYERS AND SELLERS?

WabiSabiLabi
CLOSER TO ZERØ RISK



HOW IS OUR RELATIONSHIP WITH VENDORS?

WabiSabiLabi
CLOSER TO ZERØ RISK

HOW IS OUR RELATIONSHIP WITH VENDORS?

WabiSabiLabi
CLOSER TO ZERØ RISK

WHAT ALLIANCES DID WE ESTABLISH?

WabiSabiLabi
CLOSER TO ZERØ RISK

- PRIVATE SECURITY RESEARCHERS
- SECURITY COMPANIES (RESEARCH)
- HARDWARE MANUFACTORERS
- CONSULTANCY COMPANIES
- COMPETITORS

WHAT WE WISH FOR THE FUTURE

WabiSabiLabi
CLOSER TO ZERØ RISK

Open source hardware and software codes, eventually patent covered

WabiSabiLabi
CLOSER TO ZERØ RISK

Q&A