BeeWise

A Futures Market for Fostering Security by Design

Slide-deck reconstruction. This document reconstructs the presentation delivered by Alfonso De Gregorio as an invited talk at IFIP TM 2013 (“Security by Design: From Theory to Practice”), Málaga, June 2013, and — in substantially the same form — as *Software Security’s Futures Plural* at MiniMetricon 5.5 (San Francisco, 2011) and RSA Conference Europe (London, 2011).

Provenance and method. Reconstructed from the original Prezi Desktop (Adobe AIR) export. Content is presented in the exact order of the presentation path (73 steps). On-screen text and the raster diagrams are reproduced from the source package; a small number of vector elements authored inside Prezi (6 Flash/SWF objects) and the continuous zoom transitions are not reproduced. This is a faithful record of the deck’s content and sequence, not a pixel facsimile of its canvas.

Pwnshow investigation series · INV-001 (BeeWise) · artefact deposit copy

STEP 01

BeeWise:

A Futures Market for Fostering Security by Design

STEP 02

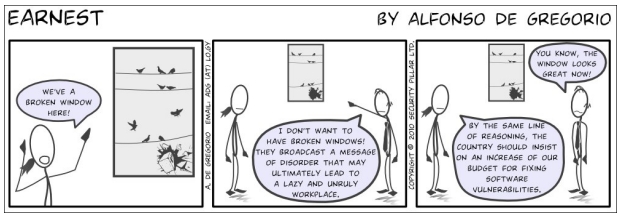
> *"Security metrics are the servants of risk management, and risk management is about making decisions. Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk"*

- Dan Geer, foreward to Andrew Jaquith's Security Metrics

STEP 03

Today, security stakeholders face a challenging task in assessing the risks they are exposed to, as they have incomplete information about the number and the severity of vulnerabilities affecting their systems.

STEP 04



STEP 05

Homeland Security Strategy for Critical Infrastructure Protection

in the Financial Services Sector, May 2004

> *"software products have among the highest levels of defects of any product sold today, and there is very little accountability on the part of producers and software products"*

STEP 06 · OVERVIEW

M&Ms

Bees & Crowds

Perverse Incentives

Configuration

Patching

Features and Information Asymmetry

STEP 07

Back To The Future

STEP 08 · OVERVIEW

Bugs & Carrots

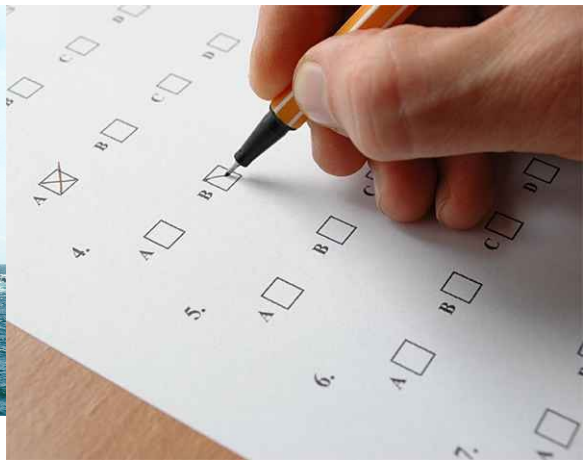
Perverse Incentives

Configuration

Patching

Features and Information Asymmetry

Tragedy of Commons



STEP 09

Patching

Software Maker Cost

Perverse Incentives

Patch Cost to Buyer

'Patching allows software manufacturers to optimize market and legal protections by "re-negotiating contract terms buyers could not negotiate in the first place' - David Rice

Well intentioned actions can have unintended consequences

Configuration

Information

Buyer's Knowledge

Seller's Knowledge

- RESULT: A depth spiral - High quality, secure software is driven from the market - Lower-quality, feature-rich software tends to dominate - Less scrupulous parties enter the market (software pirates) - Individual behavior makes everyone worse off

Features and Information Asymmetry

Software manufacturers will not forgo markets share Software buyers will not forgo features Cyber attackers will not forgo attacking tens of millions of vulnerable systems

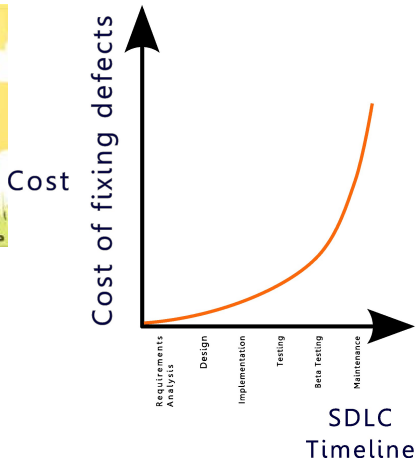
What is Security Today, from an Economic Perspective

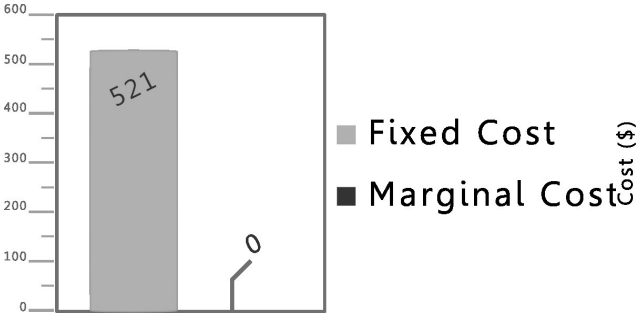
SUPPLY: Lemons market suggests that vendors under-supply security to the market; DEMAND: The tragedy of commons tells us that users demands less security than appropriate;

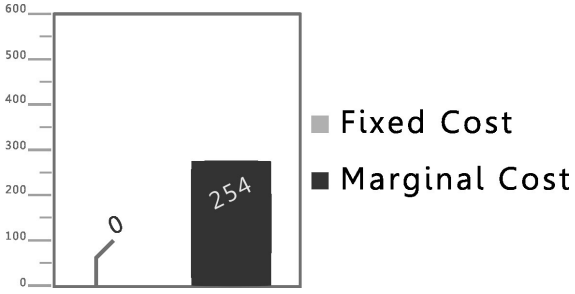
Market Failure, at present

How to invert it? How do we change?

Both risks and benefits are socialized between all the elements of the population, individuals lack the incentive to unilaterally invest in security. (see Garrett Hardin’s tragedy of commons)







STEP 10

"Due to several economic reasons, namely network externalities and information asymmetries, neither vendors have incentives to build sound security technology into their products nor are users willing to spend extra money on security technology"

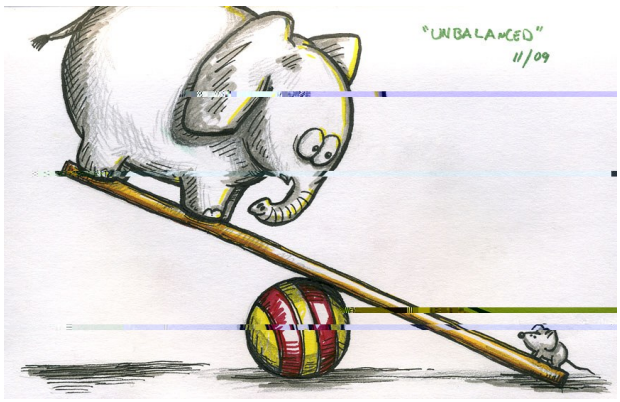
Ross Anderson, Why Information Security is Hard

STEP 11

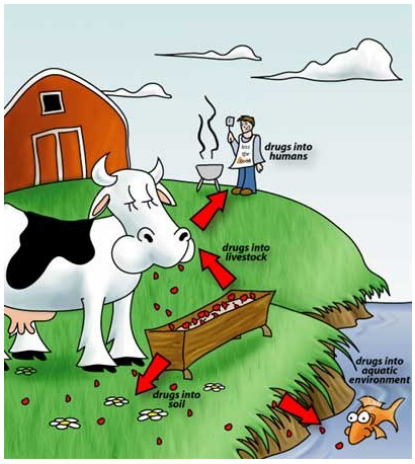
Information

Buyer's Knowledge

Seller's Knowledge



STEP 12



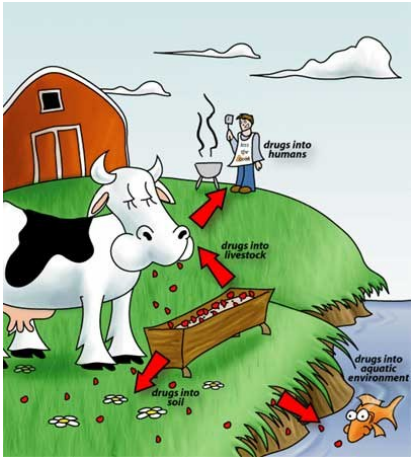
STEP 13

What is Security Today, from an Economic Perspective

SUPPLY: Lemons market suggests that vendors under-supply security to the market; DEMAND: The tragedy of commons tells us that users demands less security than appropriate;

Market Failure, at present

How to invert it? How do we change?



STEP 14

Software manufacturers will not forgo markets share

Software buyers will not forgo features Cyber attackers will not forgo attacking tens of millions of vulnerable systems

STEP 15

What is Security Today, from an Economic Perspective

SUPPLY: Lemons market suggests that vendors under-supply security to the market; DEMAND: The tragedy of commons tells us that users demands less security than appropriate;

Market Failure, at present

How to invert it? How do we change?

STEP 16 · OVERVIEW

M&Ms

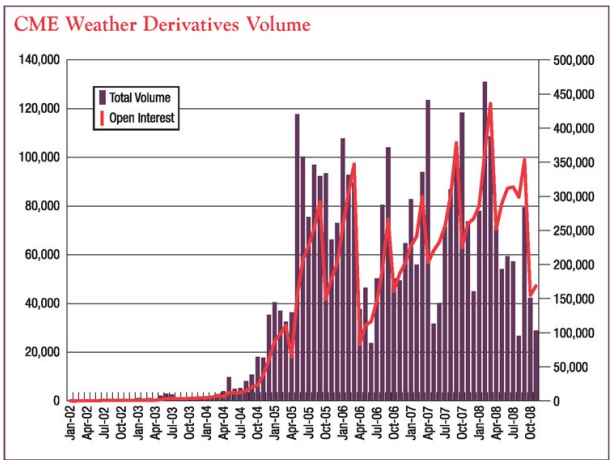
Exploit Derivatives: Investors

New Incentives

Internalize the Externalities

Economic Security Metrics

Two Perspectives



STEP 17

New Incentives

when people engage in activities that impose high social costs, it usually means that private cost is too low... ... to change behavior then, requires raising the private cost of a particular activity.

STEP 18

Internalize the Externalities

Establishing laws and regulations in the information security area (i.e., fixing liability models, security will not be perceived as an externality anymore); Establishing new markets with feedback mechanisms (i.e., balancing information between buyers and sellers, hence mitigating the problems at their source)

STEP 19

Economic Security Metrics

Two main areas of research in economic approaches for security metrics: One has its roots in investment and decision theory and is mainly pursued in the field of information technology-oriented business administration. It has yielded a number of quantitative metrics that can be applied as guidelines in investment decisions as well as for the evaluation of existing security measures. The second area of research has ancestors in micro-economics. It deals with market concepts to gather security-relevant information and extract quantitative indicators on information security properties.

STEP 20

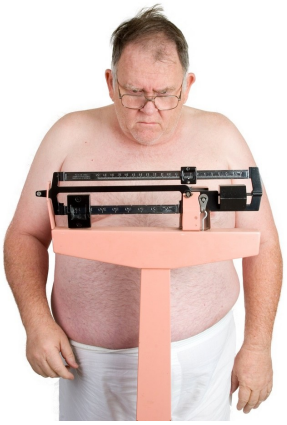
Metrics for IT Security Investments

A number of Investment Metrics has been suggested and adapted to the IT Security context. They include: ROSI; Risk Leverage; NPV (Net Present Value); IRR (Internal Rate of Return); VAR (Value at Risk) - adapted by Juninger et al. Limitations exist and also challenges...

STEP 21

Challenges in Applying Investment Metrics in IT Security

Reliable data: risk management metrics require estimations for severity and probability of loss events. In traditional risk management those values are often deducted from historical data. This is barely feasible at the moment; Quantification: Historical data is scarce even within organisations that have been using IT technology for a long time because it is hard to quantify data or for a lack of rigor of methodological collection; Complexity: it is hard to really get a comprehensive picture of possible threats to an organisation's security.



STEP 22

Metrics Based on Market Mechanisms

Metrics based on market mechanisms are not necessarily employed in an economic or business context, but that their way of measurement is based on economic principles; The observation of economic agents' decisions yields useful indicators for their expectations and can eventually be used to construct operable metrics; Market prices are not always accurate for different reasons (eg., low liquidity, transaction volumes, false estimations); They provide a good approximation; These kind of metrics are forward-looking because market prices are based on expectation about the future rather than on historical data.

STEP 23

Metrics Derived From Existing Markets

Using standard approach in finance research called event study, a number of studies analyzed the impact of computer security (and privacy breaches) related news on financial market prices, typically the stock price of affected or involved publicly traded firms; Assuming the absence of a publication bias, particularly those event studies with large samples provide evidence for a market impact of information security news; There are limits to the adoption of stock market prices as a direct metric for security properties, namely the inability to capture medium and long-term losses (only short term ones get captured) and dependance on the occurrence of extreme events; They are merely a Post-HOC indicator for insecurity, rather than a metric for security in a state where no incident happens.

STEP 24

Design of Specific Information Security Market

Even though the actual extent of the security market failure and the relative contribution of technology and policy are difficult to gauge, many of the countermeasures proposed in the literature stimulate new markets and therefore are not only good tools to align incentives, but also to obtain a new class of security metrics.

STEP 25

Vulnerability Markets: A Taxonomy

The basic idea: Vulnerabilities are errors in computer systems which can be exploited to breach security mechanisms. As a security-related information, vulnerabilities can be traded. Bug challenges; Bug auctions; Vulnerability brokers; InfoSec insurance; exploit Derivatives.

STEP 26

How Vulnerability Markets Compare?

An ideal vulnerability market fulfill three, plus one, functions: Information function – the ability to use market prices as forward-looking indicators of security properties (i.e., countering the lemons effects); Incentive function – allow monetary compensation for security research and development (high priority to security issues!); Risk-balancing function – the market provides instruments to hedge against large information security risks (i.e., mitigate the impact of occasional security breaches); Efficiency – orthogonal to the other functions and characterized in terms of: low transaction costs, liquidity, transparency, accountability.

STEP 27

How Vulnerabilities Market Compare?

With Bug Challenges and Auctions there is no possibility to do risk-balancing at all; moreover the information obtained about the market price is only a lower bound; Brokers gives questionable incentives and not always disclose vulnerability (i.e., information) to the public; Exploit Derivatives and cyber Insurances looks both promising. The former provide a timely indicator, while insurances can be less efficient due to high transaction costs, bad portfolio balancing/high correlation risk.

	Information	Incentives	Risk Balancing	Efficiency
Bug Challenges	-	+	- -	-
Bug Auctions	-	+	- -	-
Vuln. Brokers	- -	+ -	- -	- -
Security-Events Derivatives	+ +	+	+	+
Cyber Insurance	+	+ +	+ +	-

STEP 28

Exploit Derivatives

Transfer the mechanism of binary options from finance to Information security; No sensitive vulnerability information gets traded; The market is build around contracts that pays out a defined sum in case of security events;

STEP 29

Exploit Derivatives: Contracts

Consider a pair of contracts (C; C'), where C pays a fixed amount of money, say 100 EUR, if there exists a remote root exploit against some specied server software X on platform Y at date D in the future; The inverse contract, C' pays out the same face value if there is no remote root exploit submitted to a market authority before date D; It is evident that the value of the bundle (C; C') is 100 EUR at any time and that selling and buying it is risk-free

STEP 30

Exploit Derivatives

Assume that there is an exchange platform, where the contracts C and C' can be traded individually at prices determined by matching bid and ask orders. The platform settles the deals, and publish the price quotes from the order book; Then the ratio of the market price of C and its face value approximately indicates the probability of software X being compromised before date D; Of course liquidity, and thus a high number of market participants as well as low transactions costs, are a prerequisite for this mechanism to provide timely and accurate estimates.

STEP 31

Exploit Derivatives: Market Participants

A larger number of interest groups get attracted! Software Users; Cyber-Insurance companies; Investors; Software-vendors; Security experts and vulnerability researchers.

STEP 32

Exploit Derivatives: Software Users

Software users would demand C in order to hedge the risks they are exposed to due to their computer systems in place.

STEP 33

Exploit Derivatives: Cyber-Insurance Companies

The same applies for cyber-insurance companies underwriting their customers' cyber-risks.

STEP 34

Exploit Derivatives: Investors

Investors would buy contracts C' to diversify their portfolios.

STEP 35

Exploit Derivatives: Software Vendors

Software vendors could demand both types of contracts: contracts C that pay if their software remains secure as a means to signal to their customers that they trust their own system; or contracts C_comp that pay if their competitors' software gets compromised. One could even think of software vendors using exploit derivatives as part of their compensation schemes to give developers an incentive to secure programming.

STEP 36

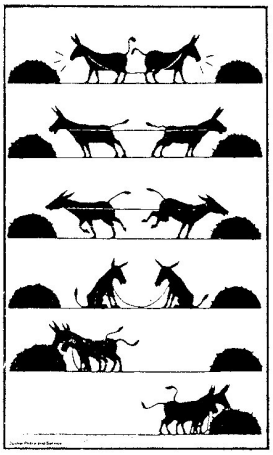
Exploit Derivatives: Security Experts

could use the market to capitalize efforts in security analyses. If, after a code review, they consider a software as secure, they could buy contracts C' at a higher rate than the market price. Otherwise they buy contracts C and afterwards follow their preferred vulnerability disclosure strategy.

STEP 37

Exploit Derivatives: Remarks

No co-operations of the vendor is needed; The number of different contracts referring to different pieces of software, versions, localisations, etc., is solely limited by demand; They are expectation-based and forward-looking since almost all markets are settled in money, the often-dicufficult quantication is inherently implied in the market mechanism; On the downside, while most existing markets are good at predicting future states in the long run, the advantages go along with short-term frictions and, in the terms of metrics, with measurement error

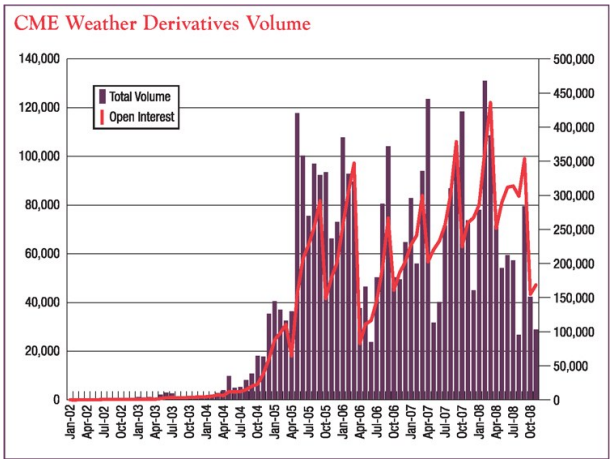


STEP 38

Weather Derivatives

First apperead in 1996 and 1997 US energy industry They allows businesses and other organizations in insure themselves against fluctuations in the weather Hedging with weather derivatives reduces the year-to-year volatility of trading companies,

In turn, low volatility in profits can often reduce the interest rate at which companies borrow money; in publicly traded companies, usually translates into low volatility of the share price, and less volatile shares are valued more highly; low volatility in profits reduce the risk of bankruptcy.



STEP 39

Exploit Derivatives: Criticalities

The Exploit Derivatives market requires a Market Authority to test candidate exploits at the end of each contract and announce the results; The Market Authority can be asked to publish the exploits with the announcements, providing verifiability and countering fraud; The Market Authority role can be distributed to different actors; Modeling contracts (eg, the importance of reliability growth models, understanding defect density, distribution, and nature) Weather derivatives were first traded by companies accustomed to trading contracts based on electricity and gas prices in order to hedge the prices risk of their utilities. How to bootstrap exploit derivatives?

STEP 40 · OVERVIEW

Bees & Crowds

Prediction Markets

What Does it Take...

Relation of events and price quotes of hypothetical exploit derivatives (security-event futures)

The Road Ahead

Heterogeneous user base; Liquidity; Low transaction costs

STEP 41

Prediction Markets: Basic Idea

virtual stocks on an electronic market whose pay-offs are tied to the outcome of uncertain future events; Although the final pay-offs of stocks are unknown during the trading period, rational and risk neutral traders sell stocks if they consider the stocks to be overvalued and buy stocks if they consider the stocks to be undervalued; As a result, the trading price reflects the traders' aggregated beliefs about the likelihood of the future event. Market prices can thus be interpreted as predictions; Hayek hypothesis, theoretical justification: asymmetrically dispersed information is best aggregated using a price mechanism.

STEP 42

Prediction Markets

Historical incarnations of prediction markets - Wagering on Presidential Elections Although election betting was often illegal, the activity was openly conducted by “betting commissioners” and employed standardized contracts that promised a fixed dollar payment if the designated candidate won office

Hayek hypothesis: asymmetrically dispersed information is best aggregated using a price mechanism.

1868-1940

1945

Prediction markets outperformed forecasts by experts and opinion polls, in: sports politics business related fields enterteinment current events

1975

John Brunner publishes a science fiction novel, Shockwave Rider, with a description of a prediction market that he called the Delphi Pool

DARPA "Terrorism Market" Affair

2001 - DARPA Information Awareness Office research the possibility of using prediction markets in policy analysis; 2002 - demonstration markets about the spread of SARS and security threat level; 2003 - Policy Analysis Market Program gets cancelled, after critics savaged DARPA for proposing "Terrorism Features"

1990s - today

mid 1990s

2001-2003

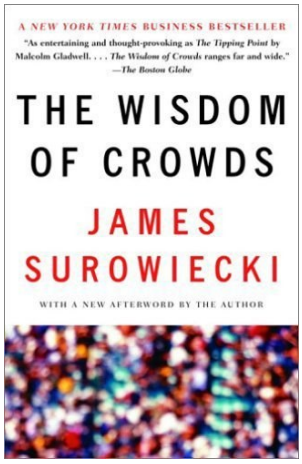
2004

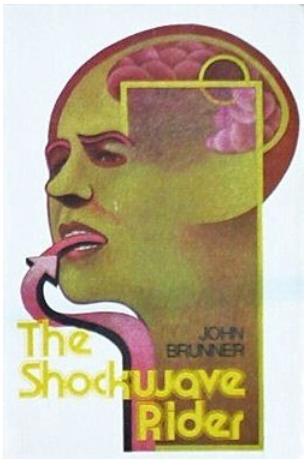
Prediction markets starts to be available online to the general public, in both real-money (gambling) and play-money (game)

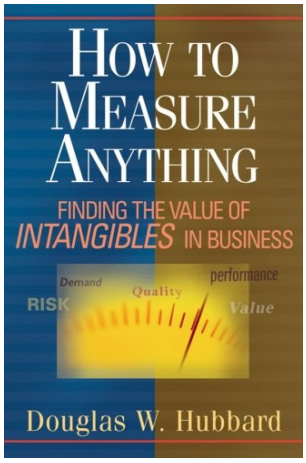
2006

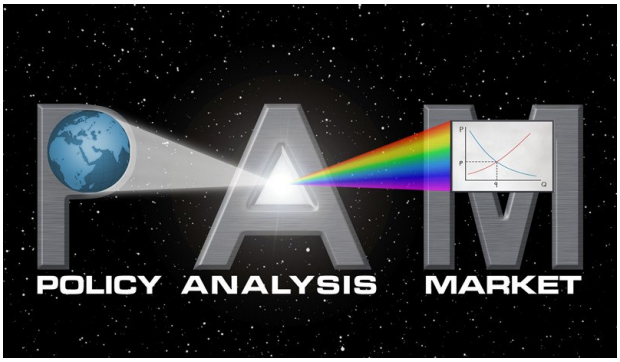
Prediction markets are introduced to a much wider audience by the popular book The Wisdom of Crowds by James Surowiecki

How to measure Anything - Finding the Value of the Intangibles in Business - by Douglas W. Hubbard









STEP 43

Exploit Derivatives vs

Play Money Prediction Market

	Exploit Derivatives	BeeWise Security Event Futures
Currency	Real Money	Play Money
Contracts	(C, C')	C, Lon&Sho
Awarding	Authority	VDB+CVSS
Award. Crit.	fixed	flexible
Exchange	Exch / OTC	Web
Information f	Yes	Yes
Incentive f	Yes	No
Risk Balancing f	Yes	No
Efficiency	Good	Good

STEP 44

Prediction Markets: Does Money Matter?

psychological importance of hard currency; Geographical, financial, technical, fiduciary, regulatory, and, perhaps, ethical obstacles to the establishment of real-money predictions markets; Does the play-money alternative compromise accurancy?

STEP 45

Does Money Matter? Two Studies

Prediction Markets: Does Money Matter?, Justin Wolfers, Emile Servan-Schreiber, David Pennock and Brian Galebach, Electronic Markets, 14(3), September 2004; An Empirical Investigation of the Forecast Accuracy of Play-Money Prediction Markets and Professional Betting Markets, Slamka, C.; Luckner, S.; Seemann, T.; Schröder, J., European Conference on Information Systems (ECIS), 2008

STEP 46

Two Real-World Experiments

real-world online experiment contrasted the predictions of TradeSports.com (real money) against those of NewsFutures.com (play money) regarding American Football outcomes during the 2003–2004 NFL season; Empirical study that compares the forecast accuracy of a play-money prediction market for the FIFA World Cup 2006 to predictions derived from odds issued by two professional betting companies;

STEP 47

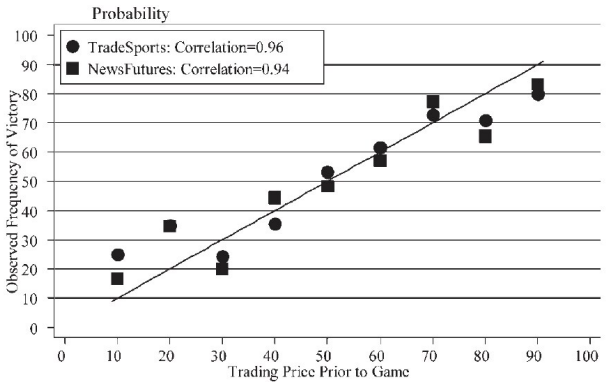
Does Money Matter?

Both types of markets exhibited significant predictive powers, and remarkable performance compared to individual experts; Play-money markets performed as well as the real-money markets (neither type of market was systematically more accurate than the other); play-money prediction markets about as accurate as betting market; real-money markets may better motivate information discovery (i.e., incentive function); play-money markets may yield more efficient information aggregation (i.e., efficiency);

STEP 48

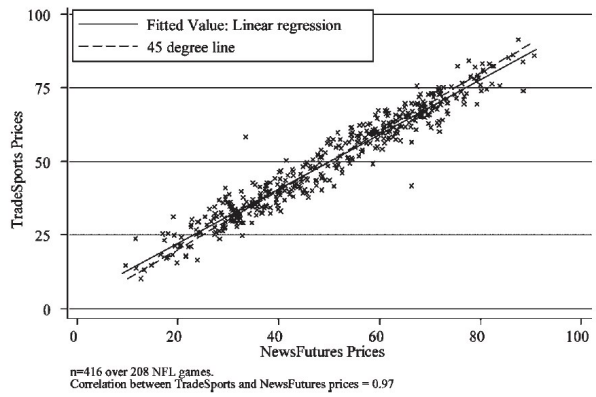
Prediction Markets: Does Money Matter?

Prediction accuracy: market forecast winning probability and actual winning probability with play-money and real-money - src: SERVAN-SCHREIBER et al.



STEP 49

Prediction Markets: Does Money Matter?



STEP 50

Exploit Derivatives vs

Play Money Prediction Market

STEP 51

What Does it Take...

Heterogeneous user base; Liquidity; Low transaction costs

STEP 52

STEP 53

Market Types

Two market types are supported: Binary markets: where contracts pay the maximum settlement value to the holder, or nothing, depending on the occurrence of the underlying event by the contract closing date; Index based markets: contracts pay a variable amount, depending on the pay-off function, taking the index as its input.

STEP 54

Pay-offs Functions

p(x) = min(L$, max(D(x - K), 0))

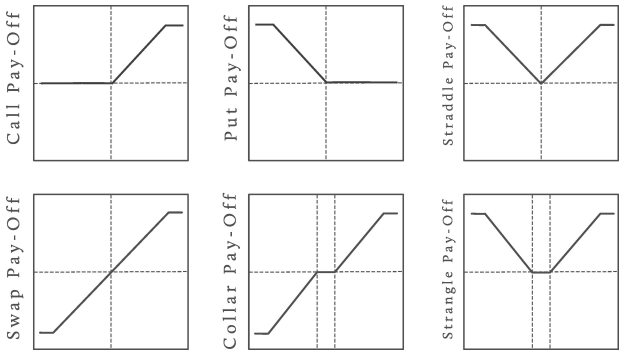
p(X) = min(L$, max(D(K - x), 0))

p(X) = min(L$, max(D(K - x), min(D(x - K), L$)))

p(X) = max(-L$, min(D(x - K), L$))

p(X) = max(-L$, min(D(x - K1), max(0, min(D(x - K2), L$))))

p(X) = min(L$, max(D(K1 - x), max(0, min(D(x - L), L$))))



STEP 55

Market Types: Examples

Binary Markets A contract may be created that pays one dollar to the holder depending on whether the Linux kernel will be found to be vulnerable to a remote code execution by the end of the month. Index-based Markets: A contract may be created that pays 1 BEE/USD cent for every data breach disclosed by a Fortune 1000 in the next year. Index-based markets: A contract may be created that pays 1$ BEE/USD for every point the Index of Cybersecurity values above/below a strike K.

STEP 56

BeeWise Symbols

BEE Symbol: - -

Examples:

DNET4x-6.13-AC:H-RC:C GLIBC-6.13-AC:H-RC:C LNX2.6.x-6.13-A:C-RC:C OBSD-6.13-Au:N-C:P,C-RC:C OSX-6.13-A:C-RC:C WIN7-6.13-AV:N-RC:C

STEP 57

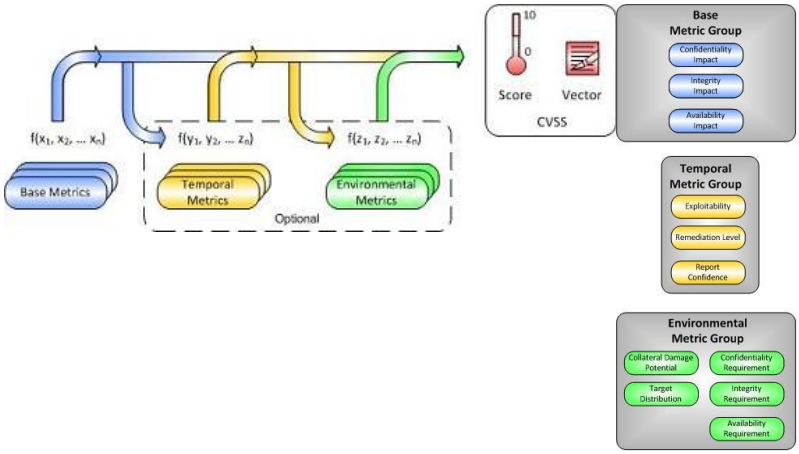
Common Vulnerability Scoring System

Metric Value

Description

Base Temporal Environmental

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]



STEP 58

BeeWise Symbols

BEE Symbol: - -

Examples:

DNET4x-6.13-AC:H-RC:C GLIBC-6.13-AC:H-RC:C LNX2.6.x-6.13-A:C-RC:C OBSD-6.13-Au:N-C:P,C-RC:C OSX-6.13-A:C-RC:C WIN7-6.13-AV:N-RC:C

STEP 59

DNET4x-6.13-AC:H-RC:C

The contract pays $100 BEE dollars to the holder, if a vulnerability requiring specialized access conditions (AC:H) - as defined by CVSS - is found to affect the Microsoft .NET Framework 4.x by June 30th 2013 (6.13). This contract requires (RC:C) the vulnerability to have been acknowledged by the vendor, or confirmed from an external event such as the publication of functional or proof-of-concept exploit code or widespread exploitation.

STEP 60

OBSD-6.13-Au:N-C:P,C-RC:C

There are allegations about an FBI-planted back door in the OpenBSD IPSEC stack: http://marc.info/?l=openbsd-tech&m=129236621626462&w=2 The contract pays $100 BEE dollars to the holder, if the allegations will be confirmed (RC:C), by June 30th 2013 (6.13). The contract is related to vulnerabilities: not requiring the attacker to authenticate in order to exploit them (Au:N), and partial or complete impact on confidentiality (C:P,C), and acknowledged by the vendor or software authors, or confirmed from an external event such as the publication of functional or proof-of-concept exploit code, or widespread exploitation

STEP 61

BeeWise Symbols

BEE Symbol: - -

Examples:

DNET4x-6.13-AC:H-RC:C GLIBC-6.13-AC:H-RC:C LNX2.6.x-6.13-A:C-RC:C OBSD-6.13-Au:N-C:P,C-RC:C OSX-6.13-A:C-RC:C WIN7-6.13-AV:N-RC:C

STEP 62

Markets Selection Criteria

	Open Closed	Main Stake-holders	Type	Scrutiny	Maturity	Defect Freq
OBSD	open source	E, V	SYS	HIGH	HIGH	LOW
WIN7	closed source	C, E, V	CONS	MED	MED	H/MED
GLIBC	open source	E, V, C	TCB	HIGH	HIGH	LOW
OSX	closed source	C, E, V	CONS	MED	M/LOW	M/HIGH
.NET	closed source	C, E, V	TCB	MED	M/HIGH	MED
LNX	open source	E, V, C	SYS	HIGH	M/HIGH	MED

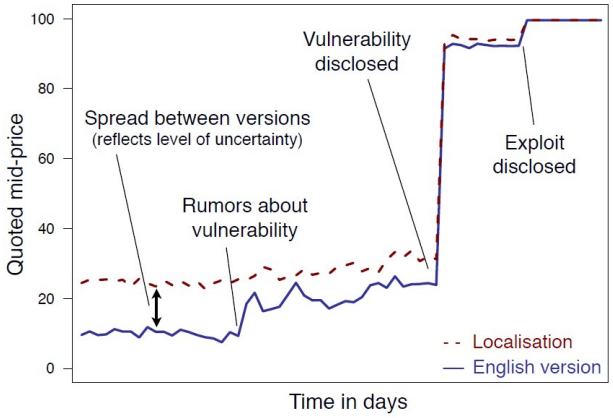
STEP 63

Relation of events and price quotes of hypothetical exploit derivatives (security-event futures)

Combining information from more than one contract allows for even more interesting metrics. Using Spreads: Price differences between related contracts can be directly attributed to distinctions in security (or public scrutiny) due to underlying technical differences (Boheme).

joint probabilities of failure can be computed from pairs of contracts to measure the total security of layered defense mechanisms. How much survivability we get with defense-in-depth?

source: Rainer Bohme, A Comparison of Market Approaches to Software Vulnerability Disclosure

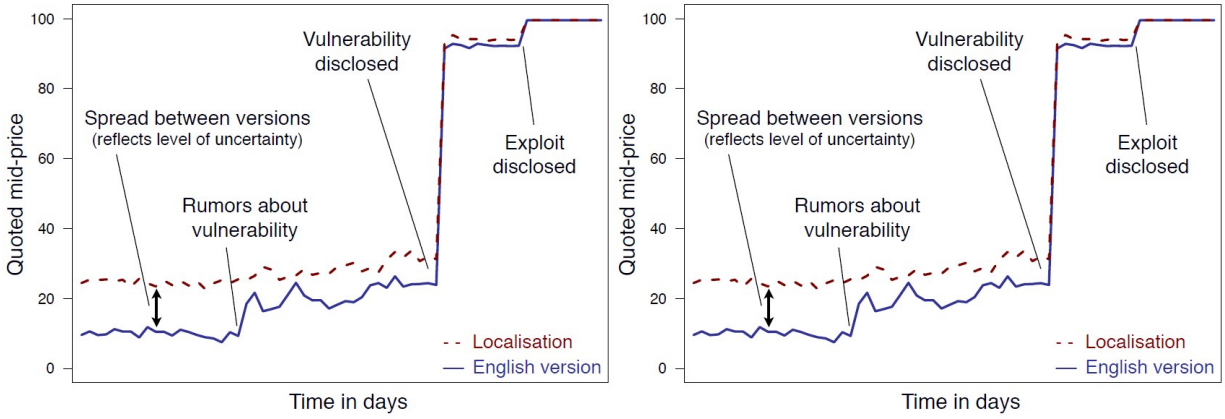


STEP 64

Combining information from more than one contract allows for even more interesting metrics. Using Spreads: Price differences between related contracts can be directly attributed to distinctions in security (or public scrutiny) due to underlying technical differences (Boheme).

STEP 65

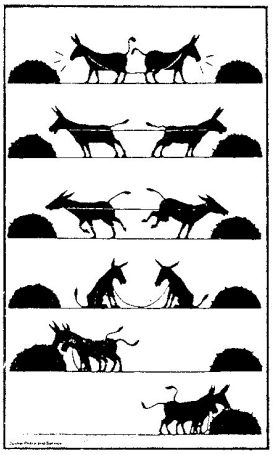
joint probabilities of failure can be computed from pairs of contracts to measure the total security of layered defense mechanisms. How much survivability we get with defense-in-depth?



STEP 66

Security-Event Futures: Remarks

No co-operations of the vendor is needed; The number of different contracts referring to different pieces of software, versions, localizations, etc., is solely limited by demand; They are expectation-based and forward-looking; since almost all markets are settled in money, the often-difficult quantification is inherently implied in the market mechanism.



STEP 67

The Road Ahead

Experiments, Experiments, Experiments: including: non-negligible bid-ask spread, liquidity, pay-off functions, short-term frictions; BeeWise traders competition; Platform Development - a lot still to be done. Few topics: usability, mobile, ...; Call for Participation: researchers, developers, investors. Interested? Please, be in touch.

STEP 68

Back To The Future

STEP 69

What will be the future for software security?

what will be its place over the next 10-20 years? Will we find the way to balance the information between buyers and sellers in the security market? Which incentives will we manage to provide to manufacturers to build security in?

STEP 70

There is not only one possible place for software security, tomorrow. our society will live only the future it will choose to live into.

STEP 71

I believe the understanding of how humans behave, from an economic and psychological perspective, to be key to holistically address the security challenges and make the software the new foundation our society can rely on.

STEP 72

This is why when we talk about the future of software security we should correct ourselves and say 'futures' (plural!). This is why I believe security-event futures might contribute towards establishing information symmetry.

STEP 73 · OVERVIEW

BeeWise:

Bugs & Carrots

M&Ms

Bees & Crowds

A Futures Market for Fostering Security by Design

Back To The Future