

Security Metrics

Measuring Operational Security

Felix C. Freiling
Lehrstuhl für Praktische Informatik 1
Universität Mannheim

PI1 @ UMA

- Felix Freiling
- Sabine Braak (admin)
- Jürgen Jaap (tech. admin)
- Michael Becher
- Zina Benenson
- Thorsten Holz
- Martin Mink
- Lucia Draque Penso



Dependability

- “A system is **dependable** if trust can justifiably be placed in the service it delivers.” [Avizienis 2004]
 - Necessary prerequisite: Quantifiable attributes of dependability
- Research agenda: Contribute to **sound engineering methods to construct dependable systems**
 - Systems which are safe and secure
- This talk: **Focus on security**
 - Part of Dependability Metrics Project

Motivation: How Secure is your Network?



SME FAQ

- How secure is my system at the moment?
- How secure will it be in one year?
- Are my current security investments sufficient?
- How much should I invest to keep my current level of security?

- For most of these questions there is **no answer**
 - This talk: Survey approaches towards (partial) answers

Overview

- The Usual Approach:
 - Risk Analysis and Reliability Theory
- Interesting Avenues from Different Areas:
 - Mathematics: Formal Methods and Crypto
 - Law: Standards and Compliance
 - Economics: Security Markets and Exploit Derivatives
- New Approach (Freiling et al.):
 - Security Testing

Security is “CIA”

- Classic security properties [Voydock and Kent 1983, Common Criteria 1999]:
 - **C**onfidentiality: Absence of unauthorized information flow
 - **I**ntegrity: Absence of unauthorized information modification
 - **A**vailability: Readiness for usage
- (Attempted) violation of security properties for a system: **Security incident**

Overview

- The Usual Approach:
 - **Risk Analysis and Reliability Theory**
- Interesting Avenues from Different Areas:
 - Mathematics: Formal Methods and Crypto
 - Law: Standards and Compliance
 - Economics: Security Markets and Exploit Derivatives
- New Approach (Freiling et al.):
 - Security Testing

Risk Analysis

- Classical approach
- Assume that security incidents follow some **probability distribution**
 - Estimate the distribution (by measuring the past)
- **Risk** = probability of incident * expected loss
- Raise awareness for and then manage risks of the system
- **Estimating probability distributions** is similar to reliability theory
 - Sample many events
 - Easy with exponential distribution and constant incident rate

Examples

- ROSI: Return on Security Investment
 - Measure how much your security investment reduces the risk
- Calculation:
 - Cost = cost of security investment
 - Annual Rate of Occurrence of an incident ARO
 - Single Loss Expectancy SLE per incident (in Euro)
 - Annual Loss Expectancy ALE = SLE * ARO
 - $ROSI = ALE[\text{year0}] - ALE[\text{year1}] - \text{Cost}$

Overview

- The Usual Approach:
 - Risk Analysis and Reliability Theory
- Interesting Avenues from Different Areas:
 - **Mathematics: Formal Methods and Crypto**
 - Law: Standards and Compliance
 - Economics: Security Markets and Exploit Derivatives
- New Approach (Freiling et al.):
 - Security Testing

Verification

- Use **formal methods** to verify that system satisfies security properties
 - Model security properties as safety/liveness properties (linear logic, process algebra)
 - Model possibilities of attacker
- Difficulties:
 - What is a **good attacker model**?
 - Deal with **covert channels**/information flow
 - Either define away (perfect crypto and access control)
 - Employ complex formalisms
- Practically impossible to eliminate all forms of covert channels

Crypto Metrics

- Classically **focussed on confidentiality**
- Important distinction:
 - Unconditional security
 - Computational security
- Applies information theory
 - **One-time pads** are unconditionally secure
- Other ciphers like RSA are computationally secure
 - Assumes it is hard to factor large numbers
 - Probabilistic polynomial-time adversary can only perform brute force attacks
- Important contribution: **Security measured in effort** (not probabilities)

Overview

- The Usual Approach:
 - Risk Analysis and Reliability Theory
- Interesting Avenues from Different Areas:
 - Mathematics: Formal Methods and Crypto
 - **Law: Standards and Compliance**
 - Economics: Security Markets and Exploit Derivatives
- New Approach (Freiling et al.):
 - Security Testing

Best-Practices and Standards

- Document describing **what should be done** to secure the system
 - Usually includes obligation for **comprehensive documentation**
- Examples:
 - **ISO 17799**: Tells how to set up processes and access control, no detailed security technologies
 - Baseline protection (**BSI Grundschutz**): Detailed technical and organizational recommendations
- Related are **laws** that prescribe organizational measures
 - Examples: Sarbanes Oxley Act, Basel II
- Experience: Companies following standards are in general more secure than others (hard to quantify)

Overview

- The Usual Approach:
 - Risk Analysis and Reliability Theory
- Interesting Avenues from Different Areas:
 - Mathematics: Formal Methods and Crypto
 - Law: Standards and Compliance
 - **Economics: Security Markets and Exploit Derivatives**
- New Approach (Freiling et al.):
 - Security Testing

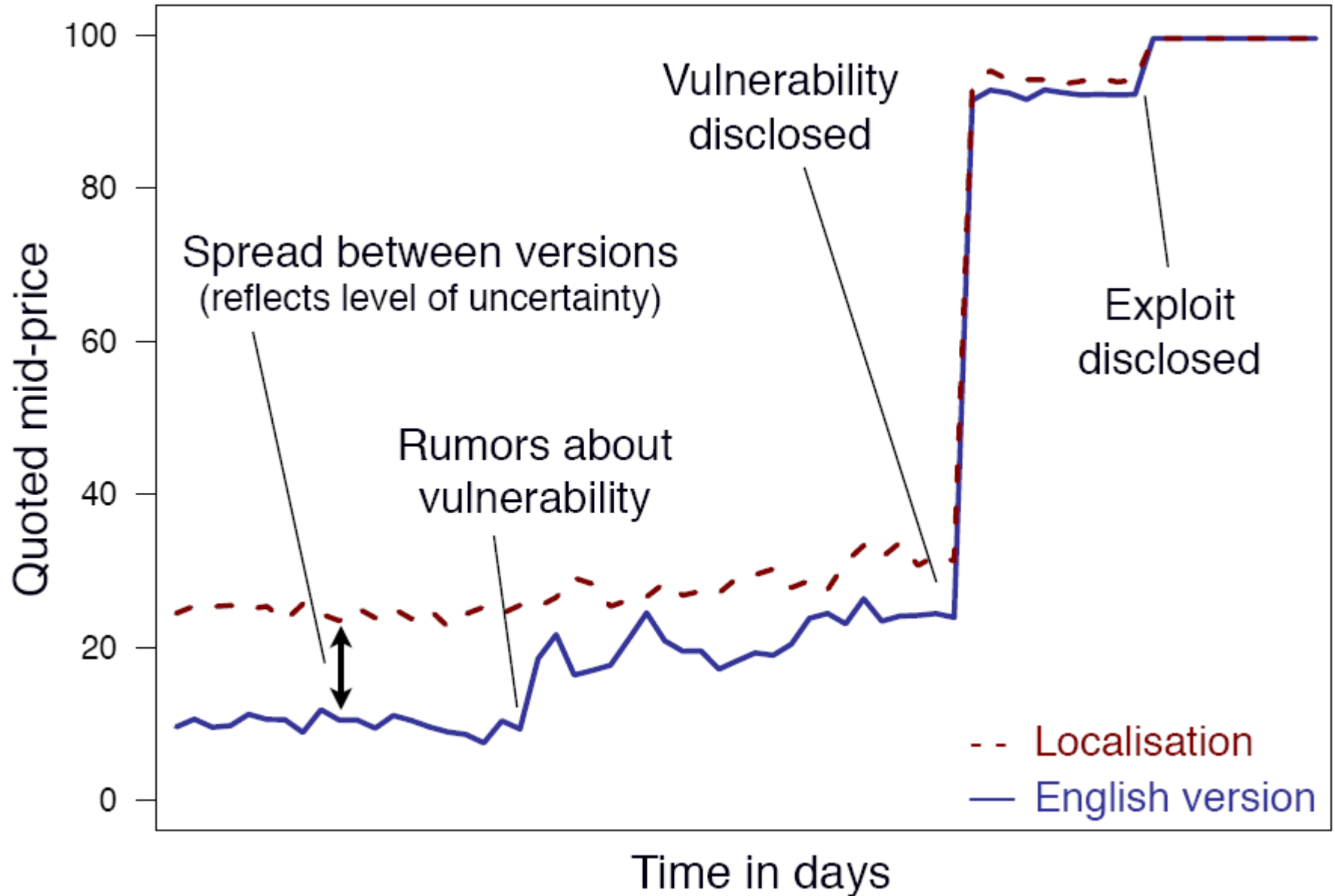
Market-based Mechanisms

- Market price of vulnerability (MPV) [Schechter 2004]
 - Lower bound on the **cost to break a system**
- **Create markets** to measure costs of vulnerabilities:
 - Bug challenges in Mozilla Bug Bounty
 - RSA factoring contest
 - Companies like iDefense (they buy vulnerabilities and offer protection against them to their customers)
- Problems:
 - No real market, low liquidity
 - Can reward be high enough for software with large installation bases?

Exploit Derivatives

- Idea of **binary options** (stock market)
 - Pair of contracts: C and inverse contract C'
 - Example C = "Authority X pays 100 Euros to the holder of this contract if a remote root exploit for ssh is submitted to X by the end of 2007."
- Selling both (C, C') is risk free
 - Market maker sells bundles
 - Offers a platform for trading
 - Ratio of value of C to value of C' is **indicator for probability that exploit will exist**
- Assumes enough market participants (software vendors and their competitors, bug hunters, ...)

Example [Böhme and Nowey 2008]



Overview

- The Usual Approach:
 - Risk Analysis and Reliability Theory
- Interesting Avenues from Different Areas:
 - Mathematics: Formal Methods and Crypto
 - Law: Standards and Compliance
 - Economics: Security Markets and Exploit Derivatives
- **New Approach (Freiling et al.):**
 - **Security Testing**

Penetration Testing (Pentesting)

- “... is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.” [NIST 2003]
- Explicitly take **viewpoint of an attacker**
 - Experience/skill-wise
 - Effort-wise
- **Measure effort** to break (parts of) the system
 - Use effort to assess the security and partially predict future
- Increasing market in practice, almost **no academic echo**

Mobile Device Security

[Becher, Freiling, Leidner 2007]

- How secure are **mobile devices** like smart phones against mobile malware (worms)?
- Estimate effort for **Windows Mobile Version 5**
- **600 work hours** to build constant part
 - Skilled single individual
 - Up to date software engineering tools and methods
- **44 work hours** spent on finding buffer overflow in WLAN stack of Windows Mobile 5
 - Unsuccessful

Use of Google Hacking [Freiling, Kröner 2007]

The screenshot shows a Mozilla Firefox browser window with the title "WS_FTP.log - Google-Suche - Mozilla Firefox". The address bar contains the URL "http://www.google.de/search?hl=de&q=WS_FTP.log&btnG=Suche&meta=". The search bar contains the text "WS_FTP.log" and the search button is labeled "Suche". Below the search bar, there are radio buttons for "Das Web" (selected), "Seiten auf Deutsch", and "Seiten aus Deutschland".

The search results are displayed under the heading "Web" and show "Ergebnisse 1 - 10 von ungefähr 847.000 für WS_FTP.log. (0,09 Sekunden)".

The first result is titled "ws_ftp log" and shows a log entry: "LOG 2004.09.09 14:34 B C:\Dokumente und Einstellungen\Carsten Müller\Eigene Dateien\Homepages\Fachschaft\WWW\bilder\nav\WS_FTP.LOG <- Fachschaft ...". The URL is "www.fs-chemie.uni-hd.de/bilder/nav/WS_FTP.LOG - 5k - Im Cache - Ähnliche Seiten".

The second result is also titled "ws_ftp log" and shows a log entry: "104.02.24 10:33 B D:\Linux\Linux IBP-WT-PC15\home\web\images\divers\bild1.gif <- ibp /home/web/images/divers bild1.gif 104.02.24 10:33 B D:\Linux\Linux ...". The URL is "www.ibp.fraunhofer.de/images/divers/WS_FTP.LOG - 3k - Im Cache - Ähnliche Seiten".

The third result is titled "NEOHAPSIS - Peace of Mind Through Integrity and Insight" and shows a file named "ws_ftp.log". The text says: "file with name ws_ftp.log. This file holds sensitive data such as file source/destination and file ... Please remove ws_ftp.log file from website after data ...". The URL is "archives.neohapsis.com/archives/fulldisclosure/2004-08/0663.html - 7k - Im Cache - Ähnliche Seiten".

The fourth result is titled "99.09.17 11:07 B X:\Public-Relation\www_new\html\images\maps ..." and shows a log entry: "LOG --> info /home/httpd/html/www-new/images/maps WS_FTP.LOG 99.09.17 11:38 B X:\Public-Relation\www_new\html\images\maps\anfahrt_b.gif --> info ...". The URL is "www.isit.fraunhofer.de/images/maps/WS_FTP.LOG - 5k - Im Cache - Ähnliche Seiten".

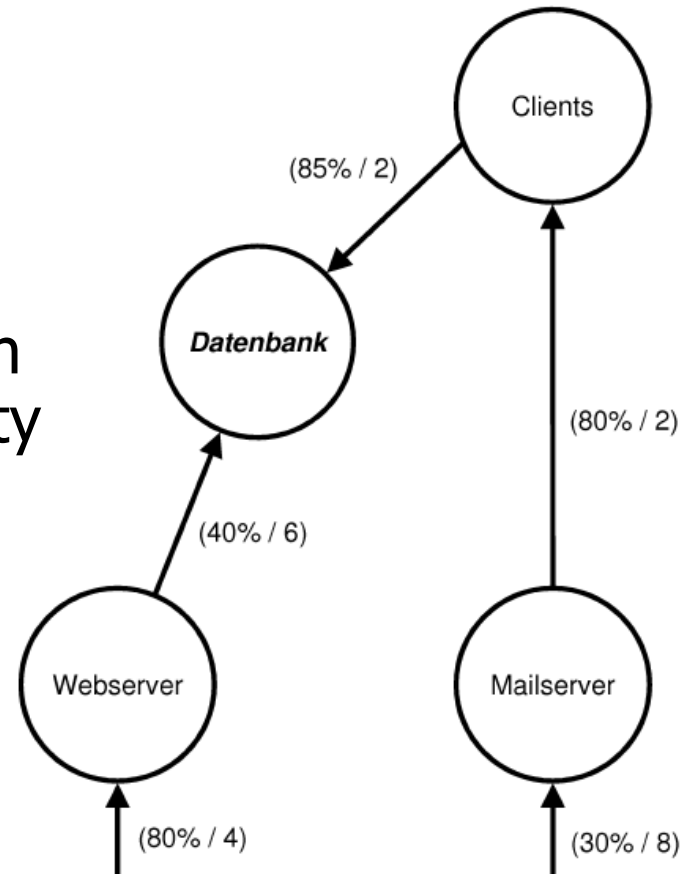
The fifth result is titled "2002.07.24 12:58 B C:\transfer\internet\ng\adenauer\laera.htm ..." and shows a log entry: "... 15:23 A C:\transfer\internet\ng\adenauer\WS_FTP.LOG --> www.uni-stuttgart.de /serv/ser/v/apache/www.uni-stuttgart.de/UNLuser/hi/ng/adenauer WS_FTP. ...". The URL is "www.uni-stuttgart.de/hing/adenauer/WS_FTP.LOG - 3k - Im Cache - Ähnliche Seiten".

The sixth result is titled "100.03.01 13:21 B W:\www\images1\maps\iwu_anfahrt.gif --> iwu ...".

The status bar at the bottom of the browser window shows "Fertig".

Pentest Effort Estimation Method [Freiling, Liebchen 2007]

- Estimate **total effort of a pentest**
- Begin with model of the network assets
- Add estimated team effort (in hours) and success probability to follow path
- Steadily refine estimation of final effort
- Formally reducible to Steiner tree problem



Source: Liebchen, Diplomarbeit

Security Testing vs. Software Testing vs. Security Audits

- Unlike software testing, security testing is **not** reducible to checking an input/output relation
 - Security testing also tests operational procedures, administrators' resistance against social engineering, robustness of software engineering method
- Unlike audits, security testing does **not** follow a predefined route
 - Every pentest needs an individual approach
 - High amount of creativity
- **Security testing** offers to look back and **partially ahead**



RedTeam Pentesting GmbH - Seeing your network from the attacker's perspective

[Home](#)[RedTeam
Pentest](#)[FAQ](#)[Advisories](#)[Publikationen](#)[Presse](#)[Kontakt](#)[Impressum](#)

 **Noch Fragen?**
+49 241 963-1300

RedTeam Pentesting bietet individuelle Penetrationstests, kurz Pentests, durchgeführt von einem Team spezialisierter IT-Sicherheitsexperten, an. Hierdurch werden Sicherheitslücken im Unternehmensnetzwerk aufgedeckt und können anschließend behoben werden.

Da in diesem Bereich zur Zeit nur sehr wenige Experten vorhanden sind, möchte RedTeam die Wissensvermittlung auf diesem Gebiet vorantreiben und mit aktueller Forschung im Bereich von sicherheitsrelevanten Themen unterstützen. Die zur Zeit veröffentlichten Ergebnisse sind unter [Advisories](#) hinterlegt und fanden national und international [Beachtung](#).

Im Unterschied zu vielen anderen Firmen ist RedTeam auf die Durchführung von Pentests spezialisiert. Eine ausführliche Beschreibung von Pentests finden Sie auf der [Pentest](#)-Seite, Antworten auf häufig gestellte Fragen finden Sie in den [FAQ](#).

Gerne beantworten wir Ihnen weitere Fragen per [E-Mail](#), [Fax](#) oder [Telefon](#).

Aktuelles



Summary: Why Security is Different

- Many approaches to measure operational security
- Why is it so difficult?
- Attacker always looks for the weakest link in system
 - Includes system, system design, defender, defender's goals, ...
 - Attacker can always attack outside the defender's model
 - Similar to diagonalisation in undecidability theory



<http://www.syslog.com/~jwilson/pics-i-like/kurios119.jpg>

Outlook

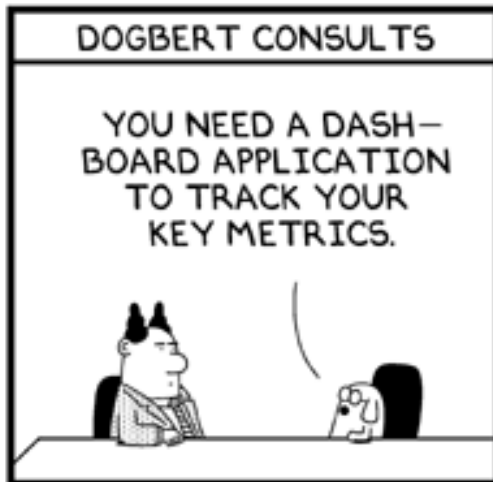
- Only **total effort** can bound the attacker
 - Effort measured in motivation, time, money
- Security testing = practical way to measure real effort
- Currently gives **qualitative measures** at most
- Aim: Estimate **time-dependent coverage** of test results based on experience/empirical measurements

References

- Avizienis, Laprie, Randell, Landwehr: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable and Secure Computing, 1 (1), 2004
- Voydock, Kent: Security mechanisms in high level network protocols. ACM Computing Surveys, 1983.
- Common Criteria for Information Technology Security Evaluation, 1999.
- Schechter: Computer Security Strength & Risk: A Quantitative Approach. PhD Diss., Harvard Univ., 2004.
- Böhme, Nowey: Economic security metrics. In: Dependability Metrics, to appear, 2007
- NIST: Guideline on network security testing. Publication 800-42, 2003
- Becher, Freiling, Leidner: On the effort to create smartphone worms in Windows Mobile. Information Assurance Workshop, 2007.
- Freiling, Kröner: Corporate Google Hacking. to appear 2007.
- Freiling, Liebchen: Zur Theorie und Praxis von Penetrationstests. to appear 2007.

Abstract

- Quantitative measures for operational security have long been termed the "holy grail" of information security. We review the state of the art in this area, including approaches from formal methods, economics and law. We then present a practical approach which allows to assess the security of a system using a qualitative effort-based metric. The approach is based on the notion of security testing (also known as penetration testing).



www.dilbert.com scottadams@aol.com

5-4-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.