Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia - Social and Behavioral Sciences 57 (2012) 163 – 169

Procedia Social and Behavioral Sciences

International Conference on Asia Pacific Business Innovation and Technology Management

Can We Assess and Monitor Privacy and Security Risk for Social Networks?

Mehmet Sahinoglu[a], Aysen Dener Akkaya[b], David Ang[c]

[a]*Auburn University Montgomery, Informatics Institute, Montgomery, AL 36124, USA,*

[b]*METU, Department of Statistics, Ankara, Turkey 06531*

[c]*Auburn University Montgomery, Department of ISDS, Montgomery, AL 36124, USA*

Abstract

With the advent and unprecedented popularity of the now ubiquitous social networking sites such as Google Friend, Facebook, MySpace, Twitter etc. in the personal sphere, and others such as LinkedIn in business circles, undesirable security and privacy risk issues have come to the forefront as a result of this extraordinary rapid growth. The most salient issues are mainly lack of trustworthiness; namely, those of security and privacy. We will address these issues by employing a quantitative approach to assess security and privacy risks for social networks already under pressure by users and policymakers for breaches in both quality and sustainability; and will also demonstrate, using a cost-optimal game-theoretical solution, how to manage and monitor risk. The applicability of this research to diverse fields from security to privacy and health care, as well as the currently popular social networks is an additional asset. A number of real people (not simulated) were interviewed and the results are discussed. Ramifications of this quantitative risk assessment of privacy and security breaches in social networks will be summarized.

Keywords- privacy, security, assessment, risk, cost

1. Introduction

The social networks and their related services have grown rapidly, but so has unwanted security and privacy challenges [1], [2], [3]. A major reason social network security and privacy lapses exist simply results from the astronomical amounts of information the sites process each and every day that end up making it that much easier to exploit a single flaw in the system. Features that invite user participation -- messages, invitations, photos, open platform applications, etc. -- are often the avenues used to gain access to private information, especially in the case of Facebook. A Ph.D. candidate at Berkeley made small headlines last year when she exposed a potentially devastating hole in the framework of Facebook's third-party application programming interface (API) which allows for easy theft of private information. This candidate and her co-researchers found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the application (http://www.fastcompany.com/articles/2008/10/social-networking-security.html). The problems now plaguing social networks, e.g.: security and privacy issues, can only be resolved if users take a more careful approach to what they share and how much privacy they value.

1877-0428 © 2012 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of the Asia Pacific Business Innovation and Technology Management Society (APBITM)
doi:10.1016/j.sbspro.2012.09.1170

With the growth of social networks, it's becoming harder to effectively monitor and protect site users and their activity because the tasks of security programmers become increasingly spread out. This brings us to the difficult task of how to measure risk and mitigate it within a certain budget in a cost-effective manner.

Risk assessment methods may be classified as conventionally qualitative and newly quantitative, and recently hybrid [4], [5]. Such a quantitative approach for software assurance (the confidence in being free from intentional or accidental vulnerabilities) is used to determine and even manage security risk and has the advantages of being objective in terms of dollar figures [6]. A well-known management proverb says that "what is measured is managed" and another says, "Yes, you can quantify risk" balanced against reasons such as the difficulty in collecting trustworthy data regarding security and privacy breaches [7]. The Security Meter technique provides a quantitative alternative to the currently used purely qualitative models [4, 5], a method which has been theoretically validated [9]. This method, currently not addressed in the literature in the way proposed for the typical social networks we plan to study, is computationally intensive. The core of the matter is to come up with a set of effective risk quantification and management techniques so as to help alleviate problems arising from lack of security and privacy due to mushrooming social networks as well their connect services..

2. Methods

Innovative quantitative risk measurements are greatly needed to objectively compare risk alternatives and manage existing risks [5]. The proposed Security Meter (SM) design provides the means in a quantitative manner that is imperative in the security world [4]. For a practical and accurate statistical design, security breaches will be recorded so as to estimate the model's input probabilities using the risk equations developed. Undesirable threats (with and without bluffs) that take advantage of hardware and software vulnerabilities can break down availability, integrity, confidentiality, nonrepudiation, and other aspects of software quality such as authentication, privacy, and encryption [6]. We must collect data for malicious attacks that have been either prevented or not prevented [5]. Figure 1 below illustrates the constants in the SM model as the utility cost (dollar asset) and criticality constant; the probabilistic inputs are vulnerability, threat, and lack of countermeasure, all valued between 0 and 1 [4]. See Figure 1. SM is described as follows:

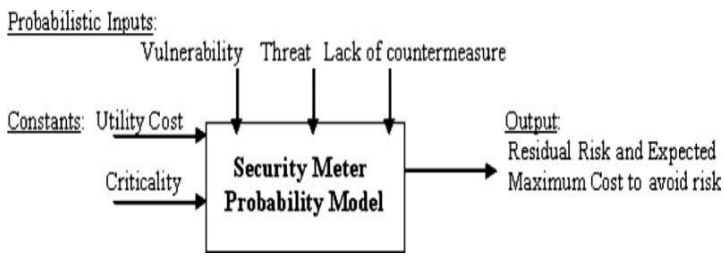


Figure 1 Security Meter Model with probabilistic, deterministic inputs, calculated outputs.

Probabilistic Tree Diagram: Given that a simple sample system or component has two or more outcomes for each risk factor, vulnerability, threat, and countermeasure, the following probabilistic framework holds for the sums Σ vi = 1 and Σ tij = 1 for each i, and the sum of LCM + CM = 1 for each ij, within the tree diagram structure in Figure 2. Using the probabilistic inputs, we get the residual risk = vulnerability x threat x lack of countermeasure, where x denotes multiplication. That is, if we add all the residual risks due to lack of countermeasures, we can calculate the overall residual risk. Then we apply the capital investment cost to the final risk to determine the expected cost of loss (ECL), which helps to budget for avoiding (before the attack) or repairing (after the attack) the entire risk where the final risk = residual risk x criticality, whereas ECL ($) = final risk x capital cost.

Algorithmic Calculations: Figure 1 leads to the probabilistic tree diagram of Figure 2 in the Appendix to perform the calculations. For example, out of 100 malware attempts, the number of penetrating attacks not prevented will give the estimate of the percentage of LCM. One can then trace the root cause of the threat level retrospectively in the tree diagram. A cyber-attack example: 1) A hacking attack as a threat occurs. 2) The firewall software does not detect it. 3) As a result of this attack, whose root threat is known, the 'network' as vulnerability is exploited. Out of those cyber-attacks that are not prevented by a certain countermeasure (CM), how many of them were caused by threat 1 or 2,

etc., to a particular vulnerability 1 or 2, etc.? Residual Risk (RR) = Vulnerability x Threat x LCM, for each branch and then proceed by summing the RRs to obtain the total residual risk (TRR) [11] .

3. Application Of The Propose Method For Privacy /Security Risk In Social Networks

Here are some threats listed respectively from the above listed vulnerabilities regarding social networks. The major privacy/security related vulnerabilities in typical social networks vary from i) Correspondence, ii) Internet Connectivity, iii) Personal Identity, iv) Health, v) Career, vi) Legal, vii) Personal Software to viii) Password.

That is for i) Correspondence: 1) VoIP Calls, 2) Phishing, 3) E-Mail Hijacking, 4) Internet Chat, 5) Cell-Phone Software, 6) Blue Tooth Devices, 7) Electronic Commerce; for ii) Internet Connectivity: 1) Cookies, 2) HTTP, 3) Browsers, 4) Search Engines, 5) Spam; for iii) Personal Identity: 1) ISP, 2) Social Sites,3) Social Engineering; for iv) Health: 1) Prescription Tracking, 2) Medical Office Website Records; for v) Career related: 1) Job applications(Sites and Applications), 2) HR Department records, 3) Benefits Records; for vi) Legal related: 1) Personal Documents, 2) Lawyer related files; for vii) Personal Software (Facebook style): 1) Index.dat, 2) Software Purchased, 3) Freeware-Shareware and viii) Password Theft: 1) Keystroke Listening, 2) Monitor Glow, 3) Guess Online, 4) Encrypted Password, 5) Dictionary Attack, 6) Easily Guessed Passwords, 7) Insider Intrusion, 8) Outsider Intrusion, 9) Picture Taking, 10) Shoulder Surfing, 11) Social Engineering, and 12) Using Bugs (Microphones).

4. Clarifications For Applications In Figure 2 and Table 2 and Table 1 (Appendix) on Privacy and Security Risk Survey

Seven graduate students were surveyed at METU (Middle East Technical University) in Ankara during April 2011. Only their first names were used by consent. Their risk scores ranked were as follows: Gul(.23), Sipan(.24), Fidan (.27), Tugba(.35), Sibel(.52), Fatih(.56), Konul (.57). An arithmetic average of 40% risk was recorded. Since no such average real person exists as representative of the sample, the median with 35% was taken as a measure of central tendency. However, the maximum and minimum cases were considered with 57% and 23% respectively so as to execute the worst- and best case risk management scenarios to see extent of precautions. The risk analyses that belong to the median score (by Tugba) are tabulated in Table 1, including cost-optimal risk management.

Now, to mitigate Median student: Tugba's privacy/security risk from 34.5% down to 24%, i) increase the CM capacity for the threat of "E-Mail hijacking" in the vulnerability of "Correspondence" from 85% to 100% for an improvement of 15%, ii) increase the CM capacity for the threat of "E-Commerce" in the vulnerability of "Correspondence" from 69.5% to 100% for an improvement of 30.50% iii) increase the CM capacity for the threat of "Easily guessed passwords" in the vulnerability of "Password" from 50% to 64.36% for an improvement of 14.36 A total cost of $841.76 is allocated. We can recursively continue to mitigate the present risk of 24% (down from an initial 35%) to lower target values such as 10% if we have sufficient budget remaining for further improvement. This is to say that Median: Tugba will implement the above clarified countermeasures by purchasing the services needed to mitigate her privacy/security risk from 35% to a low of 24%. She will do that by simply referring to the CM questions as cited, and converting the negative (No) responses to positives (Yes) by taking countermeasures. While doing so, she will optimize her costs by following the optimal allocation plan suggested by the Security Meter's game-theoretical solutions as explained in Section IV and Table I inspired by Figure 2, both placed in the Appendix respectively.

5. Discussion and Conclusions

Given the rising popularity of social networks, it is little surprise that there have been numerous high profile breaches of security and privacy on sites such as MySpace and Facebook. With over 500 million members combined, all it takes is one single person to cause major damage. But security issues and privacy issues are entirely two different topics. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues, those involving the unwarranted access of private information, don't necessarily have to involve security breaches. Someone can gain access to confidential information by simply watching you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches

a site's security network opens the door to easy access to private information belonging to any user. But the potential harm to an individual user really stems from how much a user engages in social networking sites, and especially the amount of information they're willing to share.

In brief, the proposed Security Meter (SM) technique is a practical tool for assessing overall risk quantitatively and then minimizing the cost to mitigate risk to a desired level applied to the now ubiquitous social networks with ever rising risk factors. It is an adaptable framework that can be customized and configured by the analyst with no custom coding (XML inputs). In contrast to the current quantitative approaches such as the CVSS (NIST) ranking systems, the SM provides objective and scientific guidance in allocating budgetary resources for managing risk in accordance with the provider's budget, which the proposed SM may aid in planning and forecasting. The SM, which possesses an avenue for eliciting data from expert opinion if numerical data are not available, therefore shifts from the current subjective and crude risk evaluation mechanisms to a verifiable and quantitative methodology of risk assessment and management. This may positively result in an optimized expenditure of security/privacy remediation dollars. This way, much contested social networks can be risk-quantified by providing the right set of input data, categorical and numerical, as demonstrated in the above sections.

Even more importantly, what to do next, and in what priority order by minimizing cost to mitigate the risk to a tolerable level are very significant points to consider. The purported goal is to supervise and control software systems that influence our lives by reducing the risks to privacy and security affecting hundreds of millions of people today from all walks of life [10]. For further research, an updated new tree diagram combining the two existing tree diagrams of security and privacy into one large scenario would be worth considering for typical and popular social networks. Protecting social networks at the interface of the two disjoint fronts of security and privacy issues is a first wise step to take. The ultimate goal is to face the collective challenge of quantifying and managing the adversarial risk of security and privacy together due to pervasive malware and malicious users that attack the cyber system from all corners. The surveyed data acquired from a sample of 7 college students at METU, Ankara indicated (40%) that on the average one of two are adversely affected by privacy/security breaches of some sort whether it be social or health or any privacy/security related network. As in medical science, if you can diagnose the malady, then you can attempt to cure it. This is what this research purports to achieve by further mitigating the risk from an undesirable percentage to a tolerable lower level concurrently minimizing the cost of optimized countermeasures employing the game-theory essentials. Another valid application area for this method is the banks proper where billions of monetary losses due to breach of privacy is already damaging economic progress [8].

The validity of this research endeavor will be enhanced the more users go on line and make their opinions heard. An independent third party can be hired by social networks to process these opinion surveys as illustrated. This auditing type of activity will help not only the social networks to improve their services to alleviate breach of privacy and security but also the mainstream public user majority. This way, the users by the millions will be aware of the shortfalls and can correct their usage of the social networks, and can mitigate risk by self-disciplining and monitoring as shown by the proposed algorithm. After all, it is not all fun and games because incorrect and unscrupulous socializing may damage relations, bank accounts, and friendships. Why do not we start now by first identifying soft spots, then taking measures, rather than worrying non-stop about the social networks' privacy risks?

References

[1] M. N. Ko, G. Cheek, M. Shehab, and R. Sandhu, Social-Networks Connect Services, IEEE Computer (Cover Feature), Vol. 43(8), August 2010.

[2] A. C. Squicciarini, M. Shehab, and J. Wede, Privacy Policies for Shared Content in Social Network Sites, VLDB Journal, 2010.

[3] M. Shehab, G. Cheek, H. Touati, A. C. Squicciarini, and P. C. Cheng, User Centric Policy Management in Online Social Networks, Policy'10: IEEE Symposium on Policies for Distributed Systems and Networks, Fairfax, VA, USA, July 2010.

[4] M. Sahinoglu, "Security Meter - A Practical Decison Meter Model to Quantify Risk," *IEEE Security and Privacy,* vol. April-May, pp. 18-24, 2005.

[5] M. Sahinoglu, *Trustworthy Computing - Analytical and Quantitative Engineering Evaluation*. Hoboken, New Jersey: J. Wiley & Sons Inc., August 2007.

[6] M. Sahinoglu, "An Input-Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk," *IEEE Trans on Instrumentation and Measurement,* vol. 57(6), pp. 1251-1260, June 2008

[7] P. Lindstrom, "Yes, You Can Quantify Risk*", For Pete's Sake - ISSA Journal (Information Systems Security Association)*, www.issa.org, p.9, April 2008

[8] M. Sahinoglu, "Can We Quantitatively Assess and Manage the Risk of Software Privacy Breaches", IJCITAE – International Journal of Computers, Information Technology and Vol. **3**, No. 2, pp. 189-191, December 2009

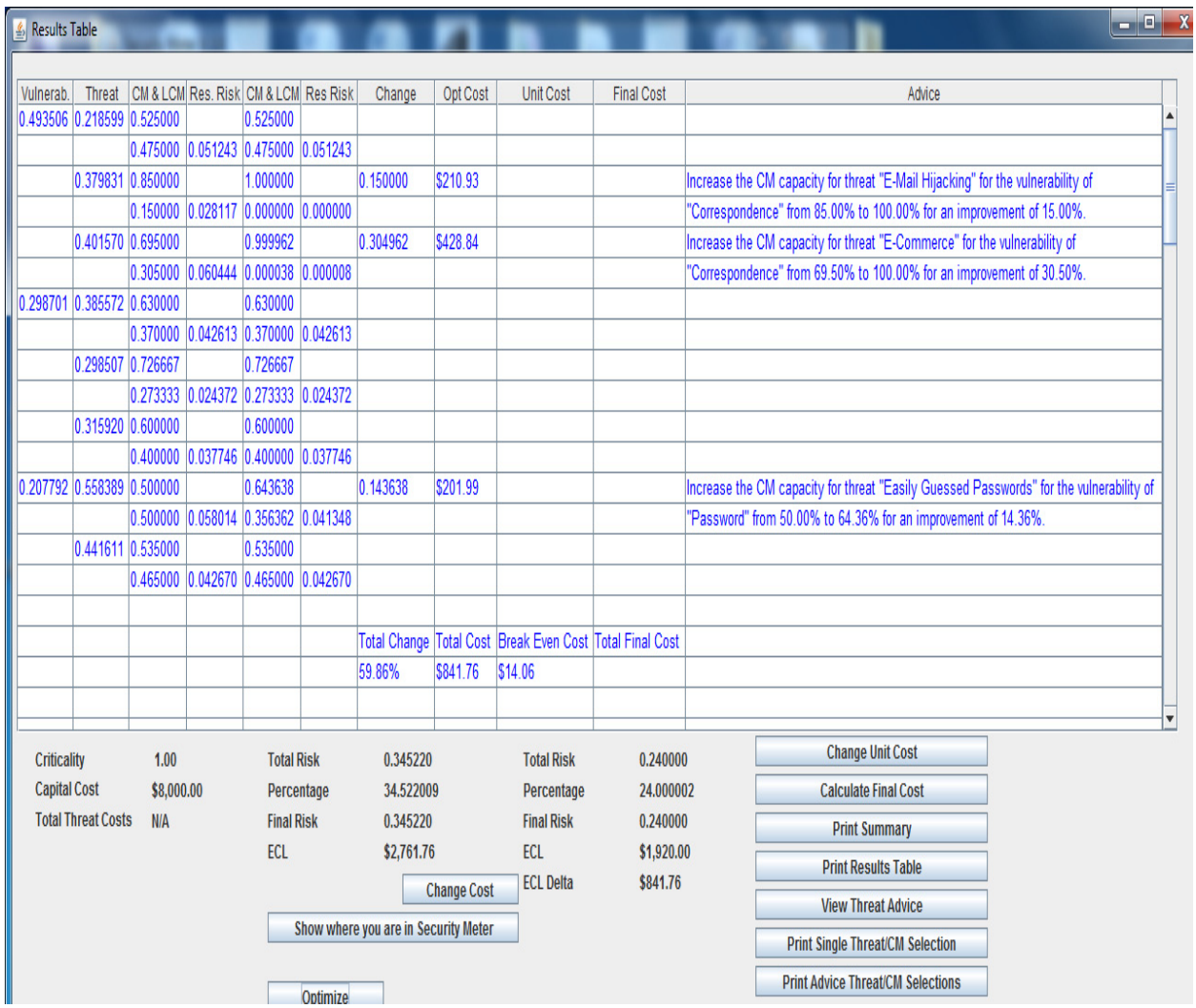
[9] M. Sahinoglu, Y.-L. Yuan, D. Banks, "Validation of a Security and Privacy Risk Metric Using Triple Uniform Product Rule," IJCITAE - International Journal of Computers, Information Technology and Engineering, Vol. **4**,No. 2, pp. 125–135, December 2010.

[10] A. D. Akkaya, M. Sahinoglu, S. Morton, V. Phoha, "A Quantitative Security and Privacy Risk Assessment and Management Method for Social Networks", ISI'11, IPS#18,Invited Session, Dublin, Ireland, Aug. 2011

[11] Tseng M.L. Using a hybrid MCDM method to evaluate firm environmental knowledge management in uncertainty, Applied Soft Computing 11(1), 1340~1352, Jan. 2011.

APPENDIX

TABLE I. EXAMPLE OF A GAME-THEORETIC COST OPTIMAL RISK ASSESSMENT AND MANAGEMENT ANALYSIS FOR FIGURE 2



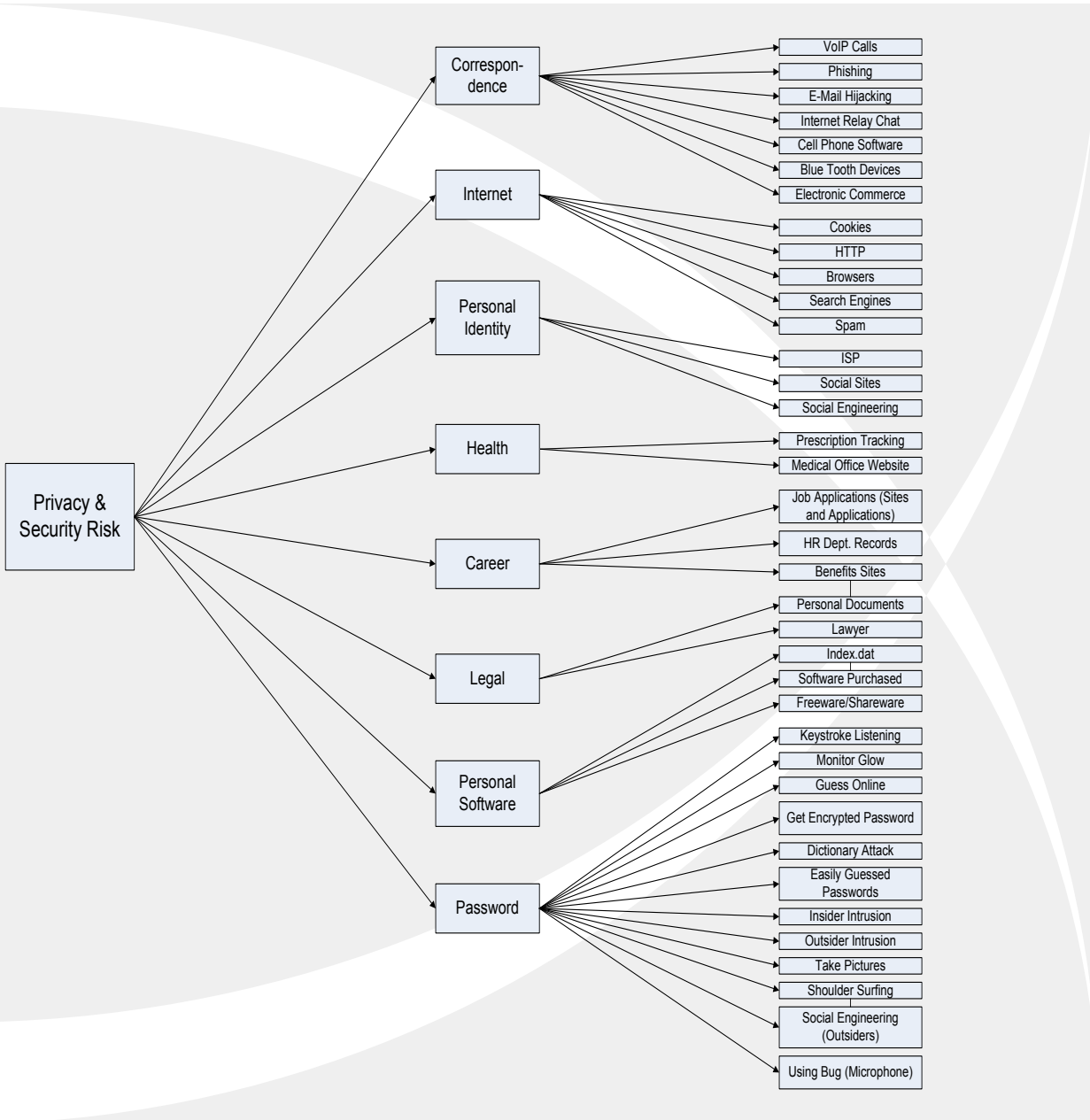


Figure 2. An Example of Privacy/Security Risk Meter Tree Diagram.