Information Security Risk Assessment of Smartphones Using Bayesian Networks

Kristian Herland, Heikki Hämmäinen and Pekka Kekolahti

Aalto University, School of Electrical Engineering,
Department of Communications and Networking, Espoo, Finland
Email: {kristian.herland; heikki.hammainen; pekka.kekolahti}@aalto.fi

Received 31 August 2015; Accepted 20 November 2015;
Publication 22 January 2016

Abstract

This study comprises an information security risk assessment of smartphone use in Finland using Bayesian networks. The primary research method is a knowledge-based approach to build a causal Bayesian network model of information security risks and consequences. The risks, consequences, probabilities and impacts are identified from domain experts in a 2-stage interview process with 8 experts as well as from existing research and statistics. This information is then used to construct a Bayesian network model which lends itself to different use cases such as sensitivity and scenario analysis. The identified risks' probabilities follow a long tail wherein the most probable risks include *unintentional data disclosure*, *failures of device or network*, *shoulder surfing or eavesdropping* and *loss or theft of device*. Experts believe that almost 50% of users share more information to other parties through their smartphones than they acknowledge or would be willing to share. This study contains several implications for consumers as well as indicates a clear need for increasing security awareness among smartphone users.

1 Introduction

The global number of smartphone users already surpassed 1 billion in 2012 [18] and in Finland, the share of smartphones relative to all mobile handsets in use exceeded 50% in 2013 [26]. As smartphones have become powerful

Journal of Cyber Security, Vol. 4, 65–86.
doi: 10.13052/jcsm2245-1439.424

enough to fulfil most consumers' computing needs, users are effectively migrating their computing tasks from traditional computers to smartphones. While traditional computer security is common knowledge and end-users typically use security software such as anti-virus on these devices, smartphone security is not as well understood among end-users.

Research concerning specific smartphone vulnerabilities exists in large numbers. Terms such as mobile malware and mobile phishing already return numerous matches in research paper searches. However, comprehensive risk assessments of smartphone use are not readily available. It is not immediately clear how much mobile malware contributes to the information security breaches that occur via smartphones, for example. Moreover, it is unclear how much smartphone use contributes to all information security breaches.

The main objective of this study is to perform a high-level risk assessment of information security related to smartphone usage. As a secondary objective, this study aims to design and implement a practical risk assessment process for eliciting information from multiple experts and consolidating this information into a Bayesian network. The outcome of this risk assessment is a Bayesian network model of information security risks, which can be used for various purposes such as scenario and sensitivity analysis.

2 Bayesian Networks

First documented applications of Bayesian networks in risk analysis include evaluation of terrorism threats by Hudson et al. in 2001 [5] and of structures under fire by Gulvanessian and Holicky in 2002 [4]. Later, Bayesian networks have been used for risk management purposes in various fields such as banking [7], nuclear power plants [6], building fires [10], earthquakes [22] and other natural hazards [23]. Some studies employ fully knowledge-based approaches using only expert interview [6, 8, 9], whereas others combine expert opinion with statistical knowledge [7, 37, 38]. Eunchang et al. [24] describe a study where 252 industry experts were surveyed for risk knowledge concerning a large engineering project. Bayesian network models have also been used for assessing the probability of ship collision [37] and effectiveness of oil combating [38] in the Gulf of Finland.

Peltola and Kekolahti [30] use Bayesian networks and expert knowledge to perform a risk assessment of the Finnish TETRA PSS network, where several risk sources and controls affect the availability of the network. Bayesian networks have been also used in several research papers to model interdependent information security vulnerabilities as attack scenarios

[13–15, 17]. Sommestad et al. [16] present a framework for analysing cyber security using Bayesian statistics and Mo et al. [12] propose a quantitative model for evaluating a firm's cyber security readiness by use of Bayesian networks.

Classical methods of causal and frequency analysis include, in addition to Bayesian networks, Fault Trees [32], Markov chains [33] and Petri nets [34]. Fault trees are commonly used in causal analysis but can be completely replaced by Bayesian networks. Markov chains and Petri nets on the other hand are not suitable for causal analysis [21]. Bayesian networks was chosen in this study as the risk analysis method due to the following reasons:

1. Efficient consolidation of hard data and expert opinion [35].
2. Ability to capture causal knowledge even from domain experts with little or no statistical experience [2].
3. Easily understandable format for visualizing causal relationships between variables [1].
4. Suitability for simple expert elicitation methods [3].
5. Robustness with regards to incomplete information [35].
6. Flexibility and abundance of use cases [3].

However, Bayesian networks also exhibit the following disadvantages:

1. Continuous variables typically must be discretized before use [21]. However, the variables analysed in this study are ordinal and therefore, this disadvantage is irrelevant.
2. Determining quantitative values via expert elicitation is a complex [35] and time-consuming process [1]. However, the number of variables to be elicited can be reduced using for example parameterized methods. A secondary target of this study is to simplify the elicitation by developing an interview process supported by an Excel-based tool for gathering data and deriving Node Probability Tables (NPT).

3 Research Method

Whereas in the data-driven approach the model structure is first learned using either score- or constraint-based methods [39–41] and thereafter the parameters by learning the local distributions implied by the structure, the Bayesian network model in this study is constructed using a knowledge based approach due to the lack of available data. First, relevant a priori information is reviewed from literature in order to determine the known assets and risks related to smartphone use. This information is then utilized as a basis for

interviews with domain experts, where information is gathered in order to construct a Bayesian network model of the risks and consequences. This model is then used for further analysis of the risks.

The expert interviews follow a two-stage expert elicitation process designed in this study. This process aims to collect the data necessary for constructing a Bayesian network model of information security risks and assets related to smartphone use in Finland at the time of this study. The purpose of the first stage is to gather enough information to build a qualitative model of the information security risks and consequences, i.e. the graphical BN structure in which nodes represent risks or consequences, and edges indicate causal relationships. During the second stage, this model is presented and validated with each expert whereafter the strengths of dependencies and impacts are determined, i.e. the quantitative values are elicited. Figure 1 describes this process.

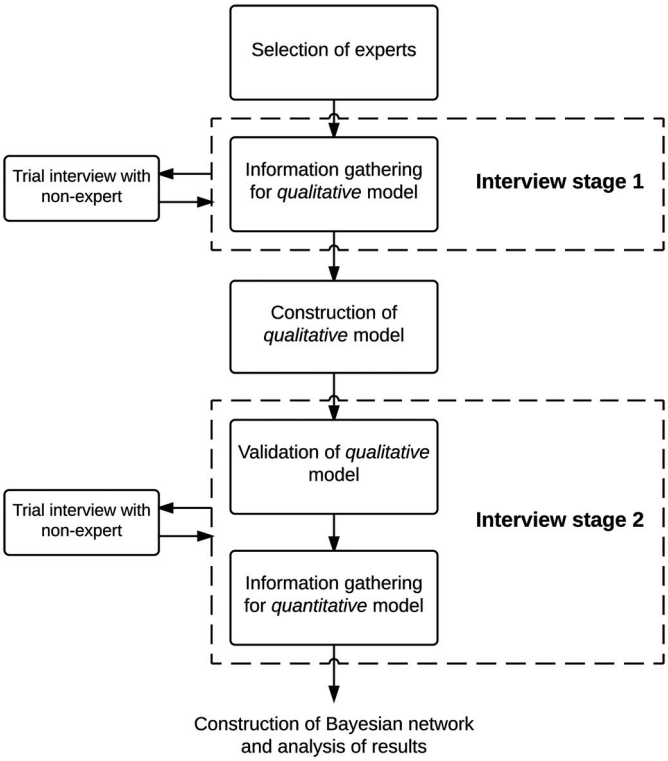

Figure 1 High level overview of expert interview process.

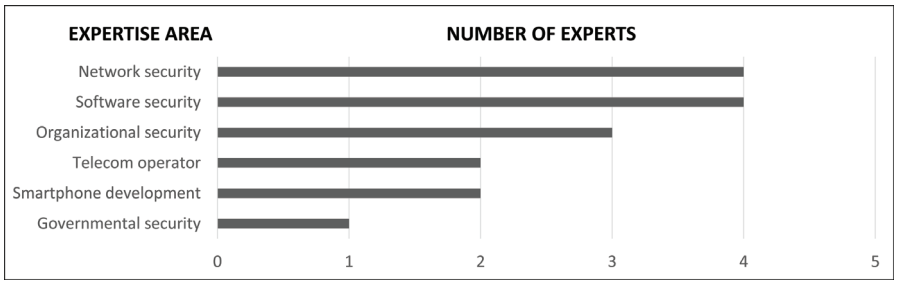

Figure 2 Interviewed experts' areas of expertise.

The experts to be interviewed are chosen based on experience, subject matter knowledge, current employer and position. Two main objectives are taken into account when choosing the experts: (1) the group of experts should include various specializations with partial overlap in order to ensure completeness of the information available and (2) the interviewee's experience and knowledge in the domain and their own viewpoint should be good or very good in order to ensure the quality of the information available. The representation of different expertise areas within the chosen experts is visualized in Figure 2.

3.1 Interview Stage 1

Two different types of techniques are commonly used to capture the information required for building the qualitative Bayesian network from expert interviews. *Structured* techniques involve specific questions about predefined concepts and are thus most suitable for confirming existing knowledge. *Unstructured* approaches focus on exploring new information and are thus well suited for use in domains for which existing knowledge is lacking or non-existent. Prior knowledge in smartphone security is available but in limited extent and due to this lack of completeness, a combination of *structured* and *unstructured* methods are used. The first stage interviews roughly follow the process visualized in Figure 3.

3.2 Interview Stage 2

The main objective of the second stage interviews is to collect the information necessary in order to construct the quantitative Bayesian network model, which is the set of Node Probability Tables (NPT) assigned to the nodes of the

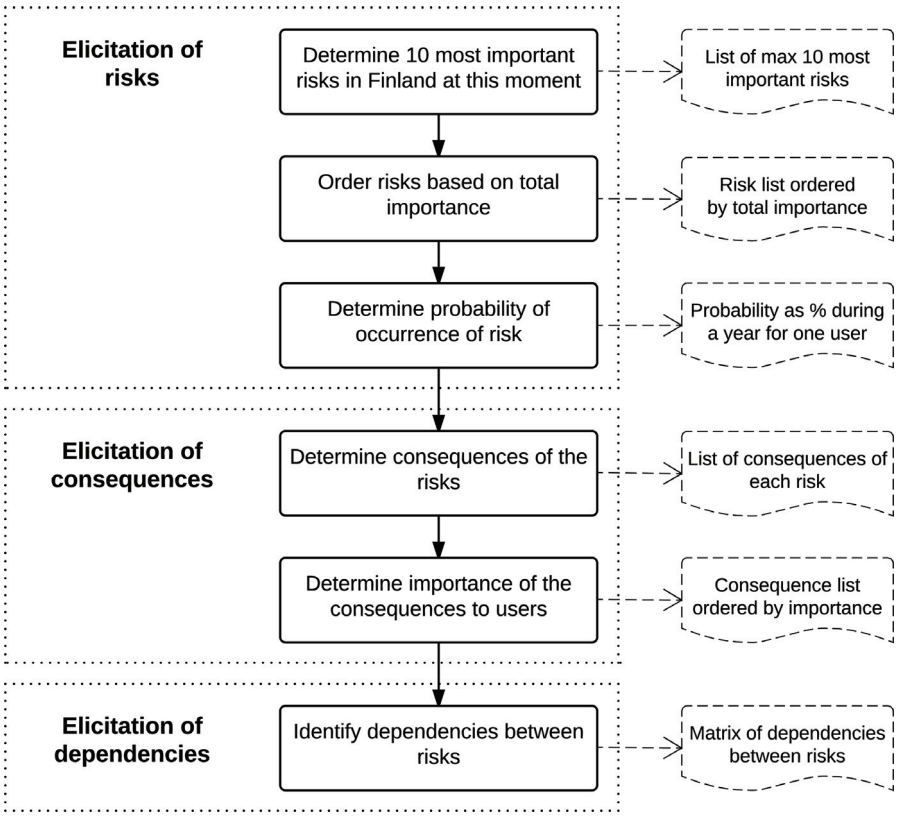

Figure 3 Expert elicitation stage 1 interview process.

qualitative Bayesian network. In this model, each risk is defined as a Boolean node and each consequence as a ranked node with the scale *negligible-low-medium-high*.

Eliciting the content of NPT's from experts can be performed in several ways. Manual elicitation by interview quickly becomes infeasible in non-trivial networks due to the exponential increase in NPT size with the amount of nodes. A less time-consuming alternative is utilizing a parameterized model, where the NPTs are constructed according to a formula whose variables are elicited from experts. Common methods of building parameterized models include using NoisyOR operators [27, 28], their multivalued generalization Noisy-MAX or a truncated normal distribution [25], for instance. However, these methods are not suitable for the purpose of this study due to their

prerequisites, i.e. that either all nodes are Boolean, represent abstractions of continuous variables or have only few parent nodes.

For the purpose of this risk assessment, a method is designed with the objective of being easy to understand even by experts with little or no statistical experience. The resulting method consists of assessing each risk-consequence-pair individually and thereafter combining this information into NPTs using an Excel-based tool. The process is visualized in Figure 4.

This method was easy for experts to understand and follow, minimizing the time and effort required for familiarizing the experts with the process. However, due to the high amount of risk-consequence-pairs, this method was more time consuming than typical parameterized methods. On the other hand, this method is not as prone to the typical loss of accuracy observed when representing large amounts of variables with a simplified function. Compared to manual elicitation of NPTs, this method still provided a nearly hundredfold reduction in variables to be elicited.

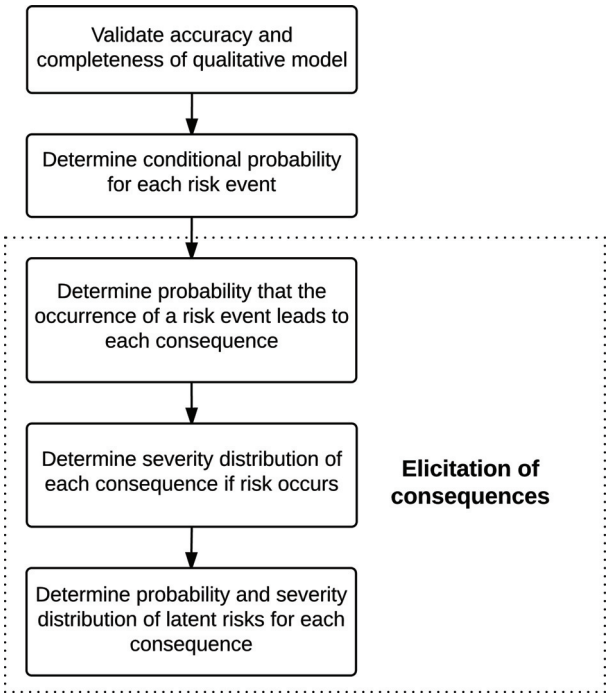

Figure 4 Expert elicitation stage 2 interview process.

4 Results

The Bayesian network constructed in this study describes the most important risk events and consequences related to smartphone use in Finland during year 2015. Probabilities in the network describe the expected probability of an event or consequence for a single smartphone user during one year without any additional knowledge of the user. The probabilities and severity distributions are arithmetic averages of the values given by experts. The choice of identified risks to be included in the network was made based on the interviewed experts' opinions of the risks' importance, taking into account both probability and consequences.

A subset of the complete model be seen in Figure 5, which describes the risks that could cause either the consequence *leakage of personal* or *leakage of confidential data*. This qualitative subset describes the most important risk events identified by the experts but does not include quantitative values such as probabilities of risk events. The qualitative model subsets, such as shown in Figure 5, were used for eliciting quantitative values from the experts during interview stage 2.

Figure 6 shows the complete Bayesian Network structure including the nodes' state probability distributions. For example the risk *shoulder surfing or eavesdropping* can directly cause leakage of confidential or personal data as well as lead to theft of the device, for example in a scenario where a thief steals the device after seeing its passcode. Furthermore, the thief might be interested in accessing the device's information and services, thus realizing the risk *unauthorized physical device access*, as opposed to wiping the device's memory and selling it.

Figure 7 visualizes the probability of occurrence for each risk, which shows that most risks are unlikely to occur during one year. However, based on Figure 7, experts believe that almost 50% of smartphone users become victim to *unintentional data disclosure* during a year, i.e. share more information to other parties through their smartphones than they acknowledge or would be willing to share.

Figure 8 visualizes the possible consequences of each risk. The total bar length indicates each consequence's probability when the respective risk event occurs. In addition, the bars are divided by colour into different consequence severities, wherein each severity has been assigned a probability. Consequences with a negligible probability or severity are omitted from the figure. Based on the figure, the risks *unintentional data disclosure* and *vendor backdoor* are both very likely to cause *leakage of personal* data when they occur but the effects of *vendor backdoor* are more likely to be severe.

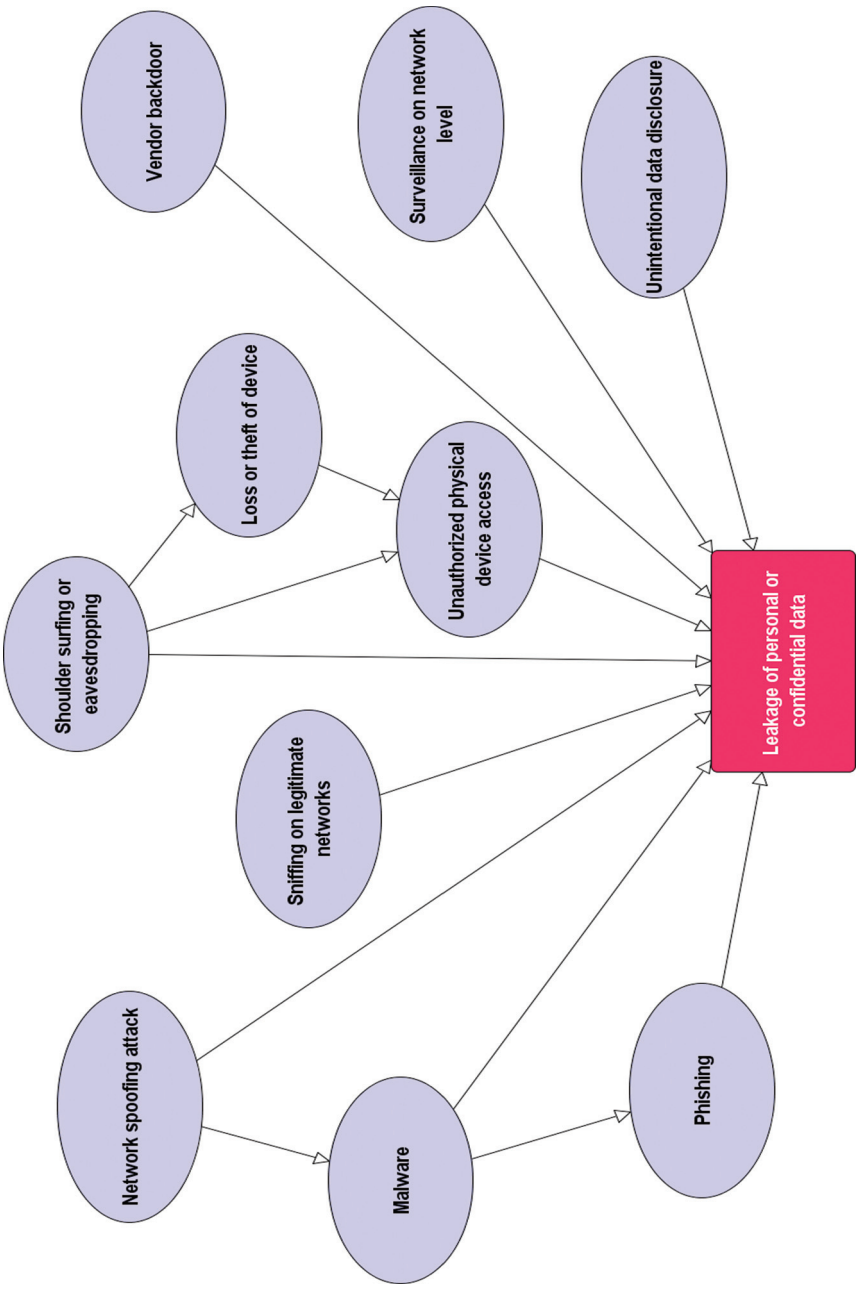

Figure 5 Qualitative model of the risk events which can cause the consequences *leakage of personal data* or *leakage of confidential data*.

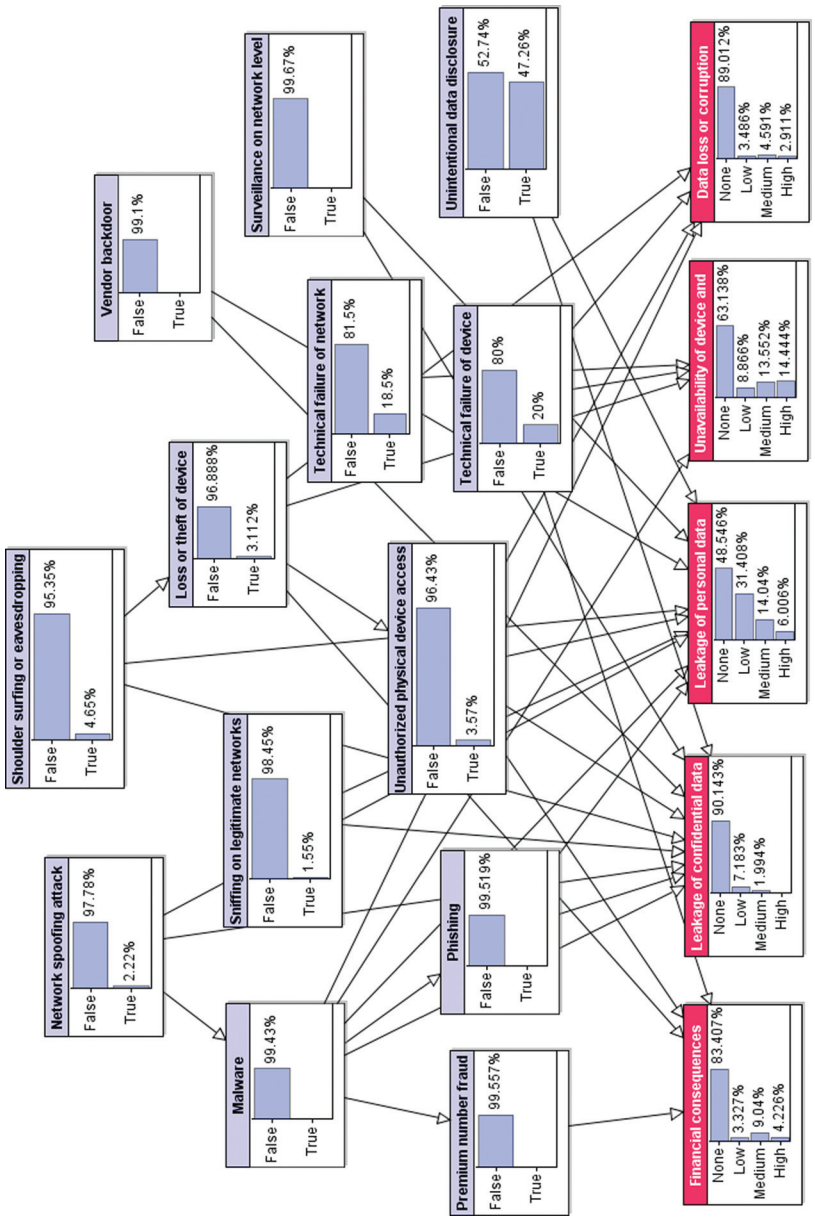

Figure 6 Complete Bayesian network model of information security risk events related to smartphone use, and their respective consequences.

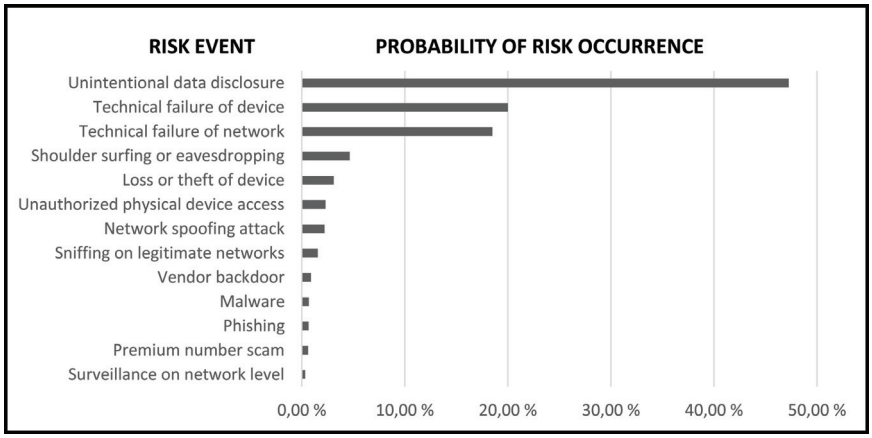

Figure 7 Probability of occurrence for each risk.

From the risk assessment results, it seems clear that a data breach is considerably more likely to concern a smartphone user's personal information than confidential information related to the user's employer. One likely reason is that while businesses and governmental entities have significant incentives to use encryption and strong authentication, consumers' often value price and ease of use more than security.

Figure 9 shows a sensitivity graph describing the effects of individual risk events on medium- or high-severity confidential data leakage. According to the analysis, the consequence is most sensitive to *unauthorized physical device access* or *malware*. This is reasonable as an unauthorized user would have access to all services which do not require additional authentication and malware with elevated rights could access all data on the device and monitor interaction between the device and user. However, most devices used for confidential purposes should require a passcode for unlocking the device, which might not be sufficiently represented in the results.

Figure 10 represents the effects of individual risks on medium- or high-severity personal data leakage. The results resemble those of confidential data leakage in Figure 9. However, two clear differences exist between these results: (1) all risk events have a significantly higher probability of affecting personal data than confidential data and (2) the effect of *unintentional data disclosure* is much higher relative to other risks' effects on leakage of personal than confidential data.

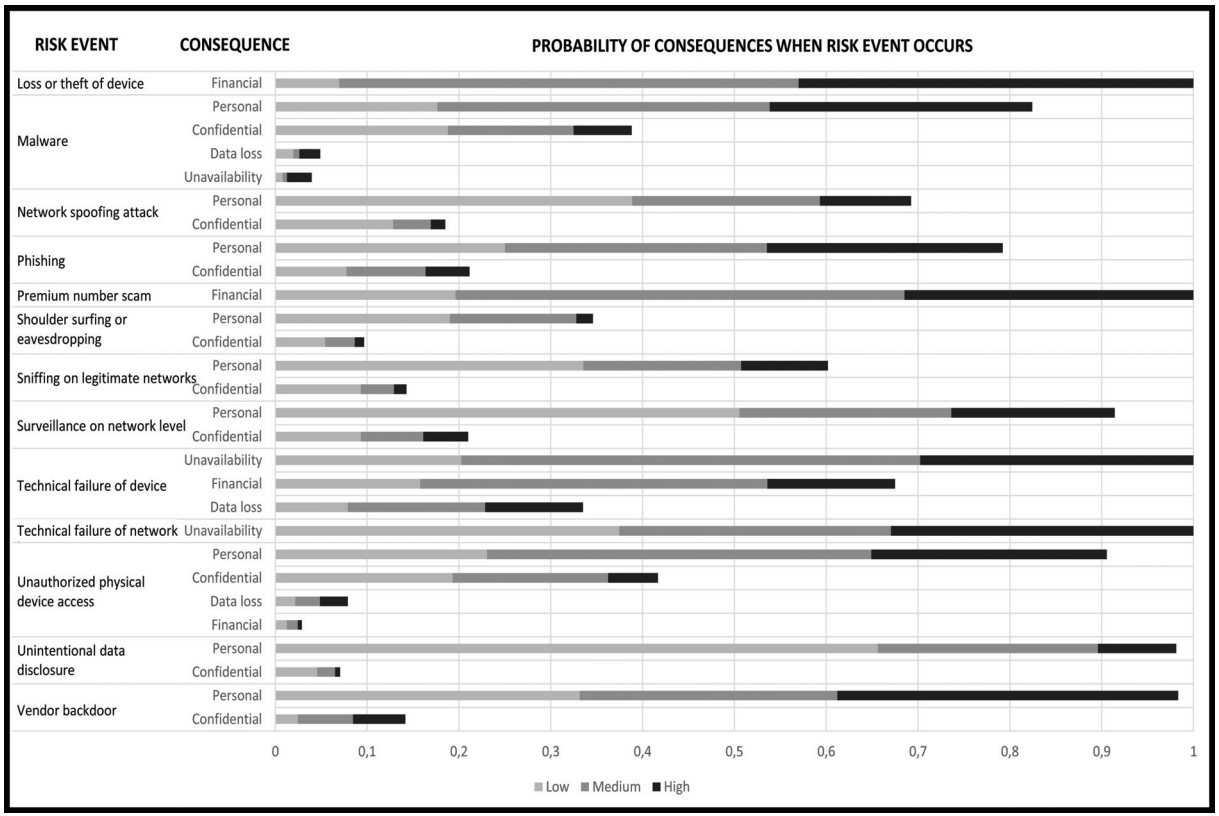

Figure 8 Probability of each risk event's consequences and consequence severities (low-medium-high), when the respective risk event occurs. Risk events ordered alphabetically.

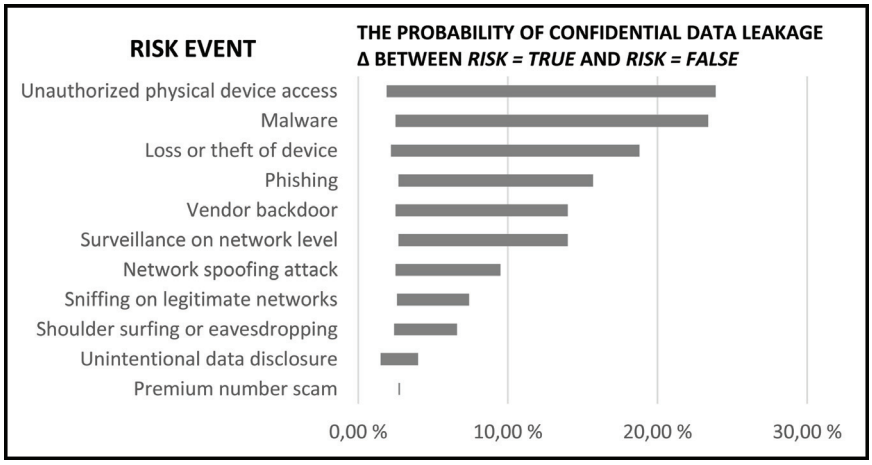

Figure 9 Effect of individual risk events on medium- or high-severity leakage of confidential data.

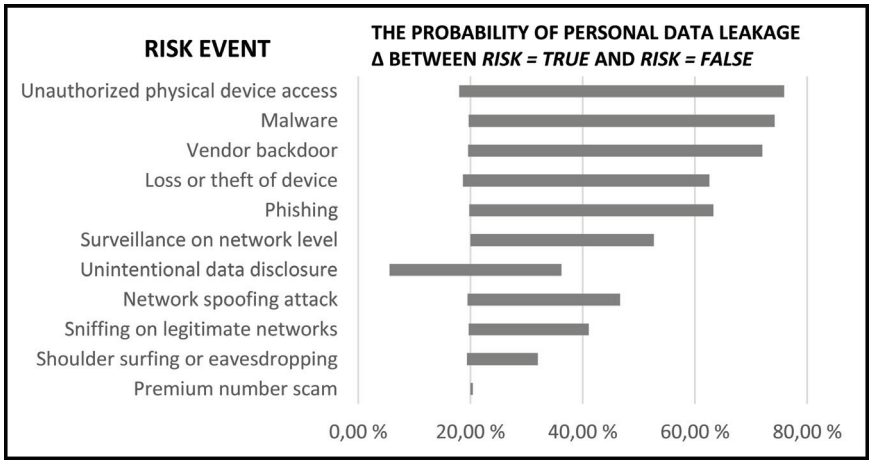

Figure 10 Effect of individual risk events on medium- or high-severity leakage of personal data.

Loss or corruption of data related to smartphone usage seems to be a relatively unlikely scenario and most often caused by *loss or theft of device* or *technical failure of device*. Also, low-severity and medium-severity unavailability is very rarely caused by anything else than technical failures of the device or network. On the other hand, high unavailability is rarely caused by anything else than *loss or theft the device*.

5 Discussion

The Bayesian network model seems realistic as a representation of the actual risk space surrounding smartphone use. The results are logical and offer more insight into the importance of different risks and their consequences. Bayesian networks as a method seems suitable for information security risk assessment as it produces a very flexible model that can be used for various kinds of analysis. However, the process for eliciting information and constructing the network is time-consuming and poses challenges for networks with a large amount of nodes.

The information elicited from experts is mostly well in line with that found in statistics and existing research. For example, the conditional probability that the data stored on a lost or stolen smartphone is accessed, reflects the results of Symantec's Honey Stick Project [36]. The experts' answers also varied significantly for some risks, such as the unintentional data disclosure risk, where estimates of probability ranged from less than 1% to 95%. However, the average of answers received from the 8 experts seem realistic. One special threat that arose in this risk assessment is the speculative vendor backdoor, for which the experts had very different opinions. According to some experts, at least 10% of the smartphones in Finland are likely to include an active backdoor designed by the device vendor or operating system developer, whereas some experts believe that none of the smartphones used in Finland have such a backdoor. Experts' answers were often derived from a real-world assumption, such as that exactly one mid-sized smartphone vendor is inserting backdoors into mobile devices.

Some experts were uncomfortable estimating probabilities without any statistical data. For instance data leaks regarding company confidential information is a topic where experts felt particularly insecure due to lack of hard data, especially as businesses do not necessarily report all data breaches to outside parties due to the possibility of reputational damage.

A common expectation between experts is that the mobile risk space is going to undergo significant changes in the near future. Expectations include increased usage of mobile banking and payment services as well as a respective increase in attacks that target these services. Also, experts expect users to increasingly store sensitive information on their smartphones. The abundance of sensor data on smartphones is still a relatively unexploited resource, for which risks such as *malware* and *vendor backdoor* present a natural threat. Research shows that many mobile services are vulnerable to sophisticated and unsuspicious phishing attacks [29].

The Bayesian network model can be used as is to illustrate the significance of different smartphone risks in different scenarios. Based on this study, the following implications for consumers can be drawn. First, consumers should ensure that their devices' built-in security features are enabled, especially a passcode and restrictions against installing applications from outside the official application store. Second, consumers should familiarize themselves with mobile applications' privacy settings and terms. Third, consumers should regard their smartphones as untrusted devices, wherein a minimal amount of private or confidential information should be stored on them. Also, it is warranted for security stakeholders to place more emphasis on educating users about smartphone security features and pitfalls.

The model could be extended with controls and mitigants, which contribute to the probability or consequences of risk events. Such an extended model could be used for identifying the most dangerous practices of smartphone usage as well as which security measures would be most useful for prevention or mitigation of risks. Further extended with costs of security measures, the model would lend itself to cost-benefit analysis of security measures. Another possible extension of the network would be to add demographic parameters such as age, occupation or income of the user, wherein the network would give more insight into the vulnerabilities and security awareness of each demographic group. The model constructed in this study could be applied to other countries by updating the parameter values and structure as necessary to represent the local environment. In order to ensure validity of the model in any environment, the parameter values as well as the structure should be updated regularly.

6 Conclusion

The purpose of this study is to perform an information security risk assessment of smartphones using Bayesian networks. Most information is gathered during a two-stage expert elicitation process, where the experts represent various experience, knowledge and viewpoints related to information security, thus ensuring the completeness of the elicited information. The expert interviews follow a process designed as part of this study in order to facilitate accurate and simple elicitation.

The outcome of this study is a Bayesian network model which documents the information security risks related to smartphone use and can be extended with new data when available. The model shows that the most important risks in Finland include traditional information security risks such as *malware* and

phishing, very general risks such as *loss or theft of device* and relatively new risks such as *unintentional data disclosure* through legitimate applications. In fact experts believe that almost 50% of smartphone users share more information to other parties through their smartphones than they acknowledge or would be willing to share. Also, the experts raise a concern over more speculative risks such as *surveillance on network level* and *vendor backdoors*. The study contains several implications to consumers as well as highlights a need for increasing security awareness among smartphone users.

Bayesian networks are found to be an effective method for documenting and analysing causal knowledge of domain experts. The model lends itself well to different types of sensitivity analysis, which would be especially useful when analysing potential controls and mitigants for risks. The expert elicitation method designed was easy for experts to understand and delivered accurate results, but however time-consuming. Both Bayesian networks and the expert elicitation method could be applied to other risk assessments as well.

Future research topics include extending the model with controls and mitigants in order to identify causes and preventive measures or with demographic parameters to better identify how risks vary between different age, occupation, income or location groups. Further research is also warranted for developing more effective tools and methods for expert elicitation and consolidation of results to be used in Bayesian networks.

References

[1] Fenton, N., Neil, M. *Risk Assessment and Decision Analysis with Bayesian Networks*. Noca Raton: CRC Press, 2013.

[2] Nadkarni, S., Shenoy, P. *A causal mapping approach to constructing Bayesian networks*. Decision Support Systems, 2004, volume 38, p. 259–181.

[3] Weber, P., Medina-Oliva, G., Simon, C., Iung, B. *Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas*. Engineering Applications of Artificial Intelligence, 2012, volume 25 (4), p. 671682.

[4] Gulvanessian, H., Holicky, M. *Determination of actions due to fire: recent developments in Bayesian risk assessment of structures under fire*. Progress in Structural Engineering and Materials, 2002, volume 3 (4), p. 346–352.

[5] Hudson, L., Ware, B., Laskey, K., Mahoney, S. *An Application of Bayesian Networks to Antiterrorism Risk Management for Military*

Planners, 2002. [Online] Available from: http://www.mathcs.emory.edu/∼whalen/Papers/BNs/KathyLanskey/Antiterrorism.pdf [Accessed 4 March 2015]

[6] Kim, M., Seong, P. *A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants*. Reliability Engineering & System Safety, 2006, volume 91 (5), p. 580–593.

[7] Cornalba, C., Giudici, P. *Statistical models for operational risk management*. Physica A: Statistical Mechanics and its Applications, 2004, volume 338 (1–2), p. 166–172.

[8] Russel A., Quigley J., Van der Meer R. *Modelling the reliability of search and rescue operations with Bayesian Belief Networks*. Reliability Engineering & System Safety, 2008, volume 93 (7), p. 940–949.

[9] Trucco P., Cagno E., Ruggeri F., Grande O. *A Bayesian Belief Network modelling of organisational factors en risk analysis: A case study in maritime transportation*. Reliability Engineering & System Safety, 2008, volume 93 (6), p. 845–856.

[10] Hanea D., Ale B. *Risk of human fatality in building fires: A decision tool using Bayesian networks*. Fire Safety Journal, 2009, volume 44 (5), p. 704–710.

[11] Cheon S-P., Kim S., Lee S-Y., Lee, C-B. *Bayesian networks based rare event prediction with sensor data*. Knowledge-Based Systems, 2009, volume 22 (5), p. 336–343.

[12] Mo, S. Beling, P. Member, Crowther, K. Quantitative Assessment of Cyber Security Risk using Bayesian Network-based model. In *Systems and Information Engineering Design Symposium*, Charlottesville, VA, 2009, p. 183–187.

[13] Noel, S., Jajodia, S., Wang, L., Singhal, A. *Measuring Security Risk of Networks Using Attack Graphs*. International Journal of Next Generation Computing, 2010, volume 1 (1), p. 1–11.

[14] Khosravi-Farmad, M., Rezace, R., Harati, A., Bafghi, A. Network Security Risk Mitigation Using Bayesian Decision Networks. In *4th International eConference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, 2014, p. 267–272.

[15] Dantu, R., Kolan, P. *Risk Management Using Behavior Based Bayesian Networks*. Intelligence and Security Informatics, 2005, volume 3495, p. 115–126.

[16] Sommestad, T., Ekstedt, M., Johnson, P. Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models. In *42nd*

Hawaii International Conference on System Sciences, Big Island, HI, USA, 2009, p. 1–10.

[17] Cie, P., Li, J., Ou, X., Liu, P., Levy, R. Using Bayesian Networks for Cyber Security Analysis. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Chicago, IL, USA, 2010, 211–220.

[18] Strategy Analytics. *Worldwide Smartphone Population Tops 1 Billion in Q3 2012*, 17 Oct 2012. [Online] Available from: http://www.businesswire.com/news/home/20121017005479/en/StrategyAnalytics-Worldwide-Smartphone-Population-Tops-1 [Accessed 4 March 2015]

[19] Strategy Analytics. *Global Mobile Phone Shipments Reach 460 Million Units in Q3 2014*, 30 Oct 2014. [Online] Available from: http://blogs.strategyanalytics.com/WDS/post/2014/10/30/StrategyAnalytics-Global-Mobile-Phone-Shipments-Reach-460-Million-Unitsin-Q3-2014.aspx [Accessed 4 March 2015]

[20] Omlis, *Global Mobile Payment Snapshot 2014*, 5 Aug 2014. [Online] Available from: http://www.omlis.com/omlis-media-room/worldwide-use-ofmobile-payments/ [Accessed 4 March 2015]

[21] Rausand, M. *Risk Assessment: Theory, Methods, and Applications*. New Jersey: Wiley, 2011.

[22] Bayraktarli Y., Ulfkjaer J., Yazgan U., Faber M. On the application of bayesian probabilistic networks for earthquake risk management. In *9th International Conference on Structural Safety and Reliability (ICOSSAR 05)*, Rome, Italy, 2005.

[23] Straub D. Natural hazards risk assessment using Bayesian networks. In *9th International Conference on Structural Safety and Reliability (ICOSSAR 05)*, Rome, Italy, 2005.

[24] Eunchang, L., Park, Y., Shin, J. *Large engineering project risk management using a Bayesian belief network*. Expert Systems with Applications, 2009, volume 36 (3), p. 5880–5887.

[25] Fenton, N., Neil, M., Caballero, J. *Using Ranked Nodes to Model Qualitative Judgments in Bayesian Networks*. IEEE Transactions on Knowledge and Data Engineering, 2007, volume 19 (10), p. 1420–1432.

[26] Vesselkov, A., Riikonen, A., Hämmäinen, H. *Mobile Handset Population in Finland 2005–2013*, Aalto University Department of Communications and Networking, 2014. [Online] Available from: https://research.comnet.aalto.fi/ public/Mobile_Handset_Population_2005-2013.pdf [Accessed 5 April 2015]

[27] Huang, K., Henrion, M. Efficient Search-Based Inference for Noisy-OR BeliefNetworks. In *Twelfth Conference on Uncertainty in Artificial Intelligence*, Portland, OR, 1996, 325–331.

[28] Díez, F.J. Parameter adjustment in Bayes networks: the generalized noisy orgate. In *Ninth Conference on Uncertainty in Artificial Intelligence*, Washington D.C, 1993, 99–105.

[29] Felt, A., Wagner, D. *Phishing on Mobile Devices*, Workshop on Web Security and Privacy (W2SP), 2011. [Online] Available from: http://w2spconf.com/2011/papers/felt-mobilephishing.pdf [Accessed 1.7.2015]

[30] Peltola, M., Kekolahti, P. Risk Assessment of Public Safety and Security Mobile Service. In *International Conference on Availability, Reliability and Security ("ARES")*, Toulouse, France, 2015.

[31] Wang, J., Guo, M. Vulnerability Categorization Using Bayesian Networks. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, USA, 2010, no. 29, p. 1–4.

[32] Fischhoff, B., Slovic, P., Lichtenstein, S. *Fault trees: Sensitivity of estimated failure probabilities to problem representation*. Journal of Experimental Psychology: Human Perception and Performance, 1978, volume 4(2), p. 330–344.

[33] Kemeny, J.G., Snell, J.L. *Finite markov chains*. Princeton, NJ: van Nostrand, 1960.

[34] Murata, T. *Petri nets: Properties, analysis and applications*. Proceedings of the IEEE, 1989, volume 77(4), p. 541–580.

[35] Uusitalo, L. *Advantages and challenges of Bayesian networks in environmental modelling*. Ecological Modelling, 2007, volume 203(3–4), p. 312–318.

[36] Symantec, *The Symantec Smartphone Honey Stick Project*, 2012. [Online] Available from: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf [Accessed 17.7.2015]

[37] Hänninen, M., Kujala, P. *Influences of variables on ship collision probability in a Bayesian belief network model*. Reliability Engineering & System Safety, 2012, volume 102, p. 27–40.

[38] Helle, I., Lecklin, T., Jolma, A., Kuikka, S. *Modeling the effectiveness of oil combating from an ecological perspective – A Bayesian network for the Gulf of Finland; the Baltic Sea*. Journal of Hazardous Materials, 2011, volume 185(1), p. 182–192.

[39] Singh, M., Valtorta, M. *Construction of Bayesian network structures from data*. International Journal of Approximate Reasoning, 1993, volume 12(2), p. 111–131. [Online] Available from: http://www.sciencedirect.com/science/article/pii/0888613X9400016V [Accessed 17.7.2015]
[40] Kjaerulff, U. B., Madsen, A. L. *Bayesian networks and influence diagrams*. New York: Springer, 2008.
[41] Scutari, M. *Learning Bayesian Networks with the bnlearn R Package*. Journal of Statistical Software, 2010, volume 35(3), p. 1–22.

Biographies

K. Herland is a cyber security specialist with an M.Sc. (Tech.) from the Department of Communications and Networking, Aalto University, Finland. He works as a security consultant for various public and private sector clients regarding security-related topics from technical IT security to organization-wide risk management. His special interests lie in the security of mobile devices and related technologies.

H. Hämmäinen is professor of networking technology at Department of Communications and Networking, Aalto University, Finland, since 2003. He received his Ph.D. in computer science from the same university in 1992. His main research interests are in techno-economics and regulation of mobile services and networks. Special topics recently include measurement and analysis of mobile Internet usage, value networks of cognitive radio, and diffusion of Internet protocols in mobile.

P. Kekolahti is a postgraduate student at the Department of Communications and Networking, Aalto University, Finland. His research interest is in the modeling of variety of complex telecommunications business related phenomena using Bayesian Networks. Pekka Kekolahti holds a M.Sc. and Lic.Sc.(Technology) from Helsinki University of Technology.