Foreword

Security comes as a second thought, or even a nice-to-have add-on? At least you can get this impression thinking about *when* security is considered in the development of many devices, systems and applications. Have a look at the evolution of cars. In the first place the purpose of a car was to transport you from one location to another. Having solved this somehow, the engineers started to think about safety – especially because vulnerabilities caused severe problems. Some of the "additional" car features were safety belts, ABS and airbags. At least some car manufacturers have seen these as extra features for a long time. This is where I start to be really puzzled. Security as an extra feature? Is it so irrelevant that we can neglect it?

This would support my initial hypothesis – security comes as an afterthought. Considering modern IT networks, IT systems and IT applications, we can see no difference. The primary goal is to enhance functionality and performance but not to mitigate risk. Security and dependability comes later if at all.

In contrast to traditional engineering domains it is, however, very difficult to add security features seamlessly as a new "module." Adding security afterwards is difficult if not impossible. Ad hoc security solutions usually introduce new, unforeseen problems and you suddenly find yourself in a vicious circle.

Somehow new technologies such as Wireless LAN, Internet Telephony or Instant Messaging seem to follow that way. We can identify severe flaws – both in design and implementation – that inevitably lead to severe vulnerabilities. This can't be the right way. We can't always try to catch up with the wily hacker and think about security *after* an incident has occurred.

Based on our experience in teaching, research and development in the areas of digital watermarking, copyright protection in wide-area video-on-demand, firewalls, security in media gateways, vulnerabilities in Internet Telephony, the Darmstadt Hacker Contest and public key infrastructures, I must emphasize: it is time for a new security paradigm. Security must be a mandatory feature, considered from the very first line on the drawing board. Certainly, there is no (and will never be) 100 percent security. Nevertheless, a user should be able to take security for granted, i.e., it should be possible to operate a system with an acceptable residual risk.

A common counterargument is that such a proactive security approach is too expensive. I don't believe this. Certainly, the development process and the resulting product will be more complex. Certainly, developers have to have a broad knowledge in several engineering domains (including security). In the sense of quality of service, we have to determine whether a system works or not. And only a secure system can work as intended. Thus I think that the initial efforts on behalf of security are more than compensated for, as a proactive approach will stop the repair-service behavior observed today.

Recently a very promising solution toward such a way of engineering security has been developed: *Security Patterns* capture proven solutions for recurring security problems in a structured way. Due to an organized peer-review process the quality of such solutions can be taken for granted. As security patterns are best practices that are codified by security experts and refer to related problems, the user can also be sure to proactively solve the overall problem – not only parts, no longer in a repair-service mode.

Dr. Markus Schumacher is already known as the driving force of and a leading worldwide authority on security patterns. In this book he provides a thorough introduction to security patterns. Due to his profound security knowledge he has been able to establish security patterns as a complementary approach for seamless security engineering. Based on his model for security patterns, security novices are now in a position to understand how experts solve problems and can basically act like them.

Once again: Does security come as a second thought? It shouldn't. However, I cannot answer this question once and for all. Nevertheless, security must and will be mandatory for all modern IT systems. Second-class solutions will always be offered and used. Hence, first-class hackers will carry out successful attacks. The earlier we start to treat security as an equivalent requirement with a high priority, the quicker our know-how and skills with seamless security solutions will evolve. This would considerably reduce the residual risk involved in using IT systems in more and more sensitive environments. I believe that this is a feasible approach. We can have secure systems and we have to do it without patchwork – security patterns are a very important step in this direction.

Darmstadt, June 2003 Ralf Steinmetz

Preface

To improve on the unsatisfactory security level we can observe today, we have to close a gap between the theory and the code of security practice. We also have to close a gap in the security knowledge process and make proven solutions available in a suitable way before an incident occurs. This book is considered as a contribution to this problem.

Abstract

We develop a systematic security improvement approach based on the pattern paradigm. *Security Patterns* can be used especially when the people in charge of security have no security expertise or when security aspects are not considered as primary requirements. The basic idea of patterns is to capture expert knowledge in documents with a particular structure. Basically, they contain proven solutions for recurring problems in a given domain.

Using patterns as a means of improving security, we first examine a set of commonly used security techniques. The result is that a pattern-based security approach features many advantages compared to the other approaches, e.g., side-effects can be considered appropriately and the expertise required to use patterns is rather low. Furthermore, patterns can be found at different levels of abstraction and for different life-cycle phases. Thus, they can also be integrated into the regular engineering process serving as a complement to other security techniques. A requirement when using patterns as a security engineering tool is a thorough understanding of security patterns. Thus, we clarify the key concepts of security patterns, define their semantics as well as their syntax, and show how they can be used. This approach is summarized in the following paragraphs.

We introduce the structure of security patterns and their distinguishing features in comparison to traditional patterns in the software domain. In particular, we conclude that the problem statement of security patterns deals with threats and attacks whereas the solution provides the corresponding countermeasures. We also discuss security-related forces and how they are resolved when a particular pattern is applied. Hereby we see that security always has an impact on other, perhaps contradictory requirements. The solution has to balance such forces according to the code of practice. Based

on that, we identify basic approaches for capturing security knowledge with patterns.

Having introduced the meaning of security patterns, we derive a theoretical model for them. Hereby we rely on definitions of key security concepts and relations between them, which builds an extensible security core ontology. Based on the definitions of security patterns and their relations, we are in a position to prove that the application of a security pattern leads to a state of security. Specifying the intuitive and commonsense knowledge, we clarify the internals of the security patterns, i.e., the theoretical model contributes to an intersubjective understanding of security patterns within the community. Furthermore, such a model is an important prerequisite for any kind of tool support. The theoretical model defines the syntax of the security patterns and security pattern systems. With this rather loosely structured meta-information model we are, however, able to make the advantages of security patterns usable.

In order to show the conclusiveness of our approach, we develop a prototype of a security pattern search engine. That way we can present new applications of security patterns, e.g., simulating how potential flaws in the implementation of a pattern affects other patterns, or maintaining a security pattern system. This proof of concept shows that our theoretical model makes patterns useful as a security engineering approach. All applications of security patterns described in the thesis are codified with an ontology and can be used via a Web interface.

Acknowledgements

This book captures the results of the most interesting years of my professional career so far. In particular, working for several years for major IT and software companies within an academic environment was an endeavor with a shaping influence. This is the time to thank those who helped and supported me.

I want to thank my supervisor Prof. Dr.-Ing. Ralf Steinmetz. He supported my decision to work on a Ph.D. and gave me the freedom to choose my environment on my own. His continuous support – in good and especially the critical times – helped me to find my own way. His steady monitoring of my progress was also very appreciated and helpful. I also want to thank Prof. Dr. rer. nat. Claudia Eckert for her willingness to be the second reader of my thesis. She gave me valuable feedback during all stages of this document and gave me confidence that it would succeed eventually.

Furthermore, I express my thanks to Prof. Alejandro Buchmann, Ph.D., for the considerable, valuable advice he gave me. He helped me to always remember the human aspect in many situations. In addition, thanks belong to Prof. Dr.-Ing. Peter Kammerer, one of the founders and “old school” (in the best sense) professors of the IT Transfer Office where I worked. It was always nice to have the backing from such competent and nice people.

The feedback of colleagues and friends was also very appreciated. First of all, I want to thank Dr.-Ing. Utz Roedig for discussing and shaping core ideas of my pattern approach in the context of security for two years. Furthermore, thanks go to Dr.-Ing. Felix Gärtner. The discussions with him were a valuable exchange between the theory (him) and the code of practice (me). He also was the first proofreader of my thesis and gave me motivation for the last mile. I also want to thank Dr.-Ing. Roger Kilian-Kehr who provided feedback on the essential chapters. In addition, the ontology-related meetings with Andreas Faatz were very illuminating. Another thank you to Ralf Ackermann who was the first person to listen to my ideas in Venice.

I had (and have) also a very pleasant time with the guys of the steadily growing security pattern community. Thanks go to Ben Elsinga for giving me the trigger to initiate our thriving movement and for telling countless jokes and riddles at Kloster Irsee. Accordingly, I have to thank Aaldert Hofmann for driving the pattern stuff forward. Last, but not least, I'm happy to have had the chance to work/talk/write with Prof. Eduardo Fernandez, Duane Hybertson and Sasha Romanosky. Generally, I'm glad to have joined the pattern community as far as I know it – everyone should participate in a *PLoP conference at least once in his/her life.

I also won't underestimate the importance of a pleasant working environment. Thus, thanks go to the ITO crew who accompanied me through the last few years: Lars Brückner, Peer Hasselmeyer, Marios Padelis, Jan Steffan and Marco Voss. A joint "thank you" goes to my colleagues at the Database and Distributed Systems Group (DVS) and the Multimedia Communications (KOM) people.

Fundamental support (for the last 30 years) came from my parents. They always gave me the freedom to realize myself. I guess that I owe them the better parts of my personality. Very, very special thanks go to my sister Heike. Besides lowering many educational hurdles for me, she edited the manuscript of this thesis.

I wish to express my biggest gratitude to Anette Mai – my partner and best friend. Thank you for all the love, faith and support you gave me throughout the last decade. I'll never forget this! My family and my friends, both at home and at work, helped me to keep my feet on the ground and to maintain a satisfying life.

Darmstadt, June 2003 Markus Schumacher