Trends in Information Security

Topic Description:
The Economics of Threat Analysis for Cyber Security

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introduction

Functional requirements can be verified through conventional forms of testing so that it is possible to determine whether or not a requirement has been satisfied. Non-functional requirements include safety and security – they pose greater challenges because conventional testing cannot be used to show that a system is totally safe or totally secure. In consequence, companies have to ensure that their systems are acceptably secure. This is a subjective assessment given that opinions may differ about how much to spend on cyber security. Risk assessment techniques can be used to identify the probability and consequences of potential threats. Resources can be allocated to the greatest risks; hence these techniques are often used to demonstrate that companies have acted in a responsible manner to mitigate future attacks.

Different Perspectives

Risk assessment techniques were originally developed to support the design and implementation of safety-critical systems. They include HAZOPS, Fault Trees and FMECA. Versions of these tools have been developed to support security threat assessments [Brooke and Paige, 2003]. As mentioned, they tend to focus on ranking threats in terms of their likelihood and consequence. Other factors may also be considered including an estimate of the company's vulnerability to a threat or their ability to detect that an attack has been launched. The UK Government continues to recommend risk assessment as a key tool in cyber-security [BIS, 2012], similar initiatives have been started in the US [NIST, 2014]. There are a host of specialist tools – ISF-RAM, ETSI TISPAN, approaches in ISO 31010, NIST-SP800-30 etc.

There are very few objective studies to assess the reliability of different risk assessment techniques being applied in a range of different companies. Very often research papers present the initial application of an approach by the team who originally developed the idea. Hence, it can be difficult for end users to identify which method might provide the greatest benefits to their organisation. Clearly, if a risk assessment technique places undue emphasis on particular threats then finite design and development resources as well as security policy decisions may be misdirected.

Open Research Questions

The following list provides a partial summary of open research questions in this area:

- **Qualitative vs Quantitative Approaches?**

In safety-critical systems, it is common to provide quantitative assessments of the probability and consequences of particular risks. For example, operational data can be used to measure the frequency of certain types of failure and also to assess the costs when these failures occur. This is only possible if the data exists. In security, many attacks are never made public so it is very hard for analysts to know the probability that they might be attacked or the costs of mitigating a threat by relying on information about previous attacks on their competitors. The European Commission issues a proposed Cyber-Security directive including a requirement to report cyber incidents in critical information infrastructures during 2013, this is intended to ensure we have better data about previous event so that we are better able to assess future threats. Even if we have this information, there is a danger that we may focus too much on the last attack and fail to identify the next one. In consequence, many security risk assessment techniques use qualitative assessments of probability, consequence and vulnerability using terms like "Frequent" and "High impact" rather than using numeric probabilities or monetary values.

- **How to Characterise the Risks from Human Error/Violations?**
  Cyber security risk assessment is difficult because it has to consider human behaviour. This can lead to technical and organizational conflict – for example, in assessing the likelihood tht an employee might forget or deliberately ignore a security policy. If a risk assessment said that the probability of such a violation was zero then this could indicate complacency. Equally if a security manager considered such a violation to be likely then it would indicate that they had failed in their own responsibilities. Audit and monitoring techniques can be used to provide data on violations but in general it is extremely difficult to assess the probability and consequences of an insider threat.

- **Can we Estimate the Probability that Software Contains Security Vulnerabilities?**
  The probabilistic aspects of risk assessment were derived from the analysis of hardware. Most components can be characterised in terms of their failure rate over time. During an initial burn-in period the probability of failure is high then it falls as components are tested in operation. After the working life of the hardware component, the probability of failure rises again during the 'burn-out' phase. Unfortunately, these techniques cannot be applied to software, which does not age in any conventional sense. It is also impossible to derive an accurate assessment of the total number of bugs in code – following the Dijkstra maxim that testing proves the presence of bugs and not their absence. By analogy, we cannot then know if we have identified every security vulnerability in a complex system. Not simply because we cannot exhaustively test millions of lines of control statements, but also because the methods of attack change over time.

- **How to Assess the Probability of Configuration and Maintenance Issues?**
  Configuration and patch management are arguably the two areas of greatest concern for security managers. A system that is initially secure may be compromised by mistakes during routine maintenance. Rom this it follows that security is not something that can be 'proven' at design time. It is an attribute that must be continually monitored over the operational lifecycle. Techniques for ensuring that security continues to be maintained remain an active

are of research – especially given that the teams, which develop a complex system might not be responsible for its subsequent installation and maintenance;

- **How to Maintain a Cyber Risk Assessment within a Security Management System?** Security risk and threat assessments will change over time. If a company suffers an attack or an incident is reported in another comparable organisation then this may reveal new threats that were not considered during an initial analysis. Similarly, the detection or response to a threat may provide new insights into the consequences of an attack. It is for this reason that risk assessments must be linked to incident reporting within a security management system. Methods for supporting this feedback are an area of research – it is unclear how knowledge of an attack might be use to update the quantitative and qualitative approaches to cyber risk assessment.

References

O.H. Alhazmi, Y.K. Malaiya, I. Ray, Measuring, analyzing and predicting security vulnerabilities in software systems, Computers & Security, (2006) 1–10

Ross Anderson, Rainer B¨ohme, Richard Clayton, and Tyler Moore. Security Economics and the Internal Market. January 2008. http://www.enisa.europa.eu/act/sr/reports/ econ-sec/economics-sec.

Rok Bojanc, Borka Jerman-Blažič, An economic modelling approach to information security risk management, International Journal of Information Management, Volume 28, Issue 5, October 2008, Pages 413–422.

Phillip J. Brooke and Richard F. Paige, Fault trees for security system design and analysis, Computers & Security, Volume 22, Issue 3, April 2003, Pages 256–264

K.J. Soo Hoo, How Much Is Enough? A Risk-Management Approach to Computer Security, School of Engineering, Stanford University, June 2000.

US NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4. Available on: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf accessed January 2014.

US NIST, Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37 Revision 1. Available on: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf, accessed January 2014.

W. Jansen/NIST, Directions in Security Metrics Research, NISTIR 7564, Gaithersberg MD, USA, 2009.

T. Peltier, Information Security Risk Analysis, Taylor and Francis/CRC Press, Boca Raton, Fl.2005.

P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb, Cyber security risk assessment for SCADA and DCS networks, Elsevier International Society of Automation Transactions, Volume 46, Issue 4, October 2007, Pages 583–594.

Chris Salter, O. Sami Saydjari, Bruce Schneier, Jim Wallner, Toward a Secure System Engineering Methodology, http://www.schneier.com/paper-secure-methodology.pdf

UK Department for Business Innovation and Skill, Cyber Risk Management – A Board Level Responsibility, London, UK, 2012. Available on: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf