Kyberturvaa ohjelmistollisella diversifioinnilla, Tekes Challenge Finland –projekti

Ville.Leppanen@utu.fi

Hilla: Meriteollisuus ja IoT Growth Mill –seminaari, Salo 31.8.2016

Turun yliopisto
University of Turku

Here: Looking for participants to the project

- Aim of Challenge Finland project is to make _real_ industrial Tekes application
- Target group: IoT and critial infrastructure companies (with software based products)
- Application DL: end of October

Past research from us

We: A security research group of about 8 persons

Publications on the topic: 15 – 20

Software implementations for Linux kernel, libraries, web-layer, SQL-layer, command shell layer
For Linux, ThingSee OS, Raspbian OS, ...

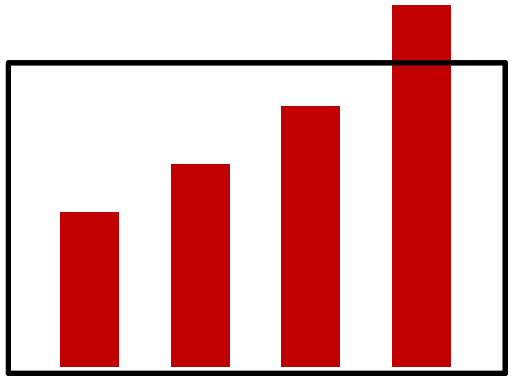
Programs and projects

Part of Cyber Trust SHOK; PreKOD (Challenge Finland Tekes funded project on diversification); past Matine funded project on diversification

Motivation

The amount of malware is growing
at an alarming rate

”[…] more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before.” - Symantec



Motivation

Situation

There are a few different execution platforms

Software monoculture

platforms are using identical internal structure!

Result

Single malware works on millions of machines!

Remedy

Break the monoculture *(how?)*

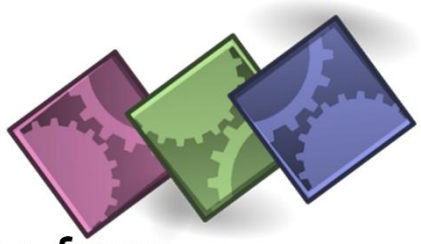
Solution: Diversification

Change the inner workings of a system to be based on changed internal interfaces (changing done after development at deployment phase)

Car analogy

The same feeling, the same performance, but engine room parts and their connections are different + engine hood welded shut

Diversification continued



- Goal: Deployed systems are made unique from each other
  - System = software, platform, libraries, OS, network protocols, …
  - Unique = Internal structures changed, no changes to user
- Some resemblance to cryptography
  - A secret key is used…
  - …but there is no decryption in the traditional sense

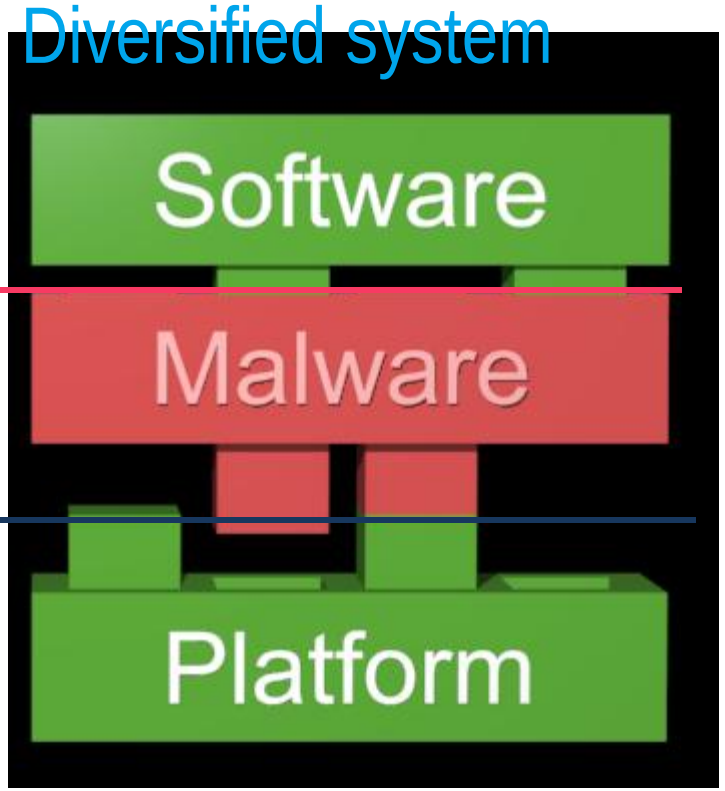
Diversification: Meaning of solution

Even after injection, malicious code is unable to perform anything

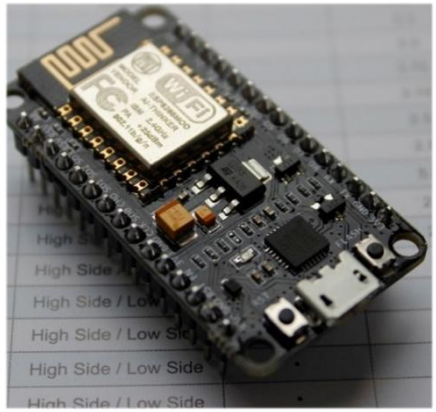
Exploited vulnerability

Internal diversified interfaces

Specifics not known to the malware



For internet of things



Add diversification as additional defense against mass exploitation

Advantages

- Low or no performance/storage penalty
- No hardware changes necessary
- Multilayer defense: Can be used with other security solutions
- A bug discovered later: attacker can't use the security hole …

Reading material

Book: Internet of Things - Chapter: Software Obfuscation and Diversification for Improving the Security in Internet of Things

Picture of NodeMCU © Vowstar

Questions?

Further reading

From us

S. Rauti, S. Laurén, S. Hosseinzadeh, J.-M. Mäkelä, S. Hyrynsalmi, V. Leppänen: Diversification of system calls in Linux binaries, Proceedings of the 6th International Conference on Trustworthy Systems (InTrust 2014), Revised Selected Papers, pages 15–35, LNCS 9473, Springer, 2015.

S. Hossenzadeh, S. Rauti, S. Hyrynsalmi, V. Leppänen: Security in the Internet of Things through Obfuscation and Diversification, Proceedings of International Conference on Computing, Communication and Security (ICCCS), pages 1–5, IEEE, 2015, DOI: 10.1109/CCCS.2015.7374189.

J. Uitto, S. Rauti, V. Leppänen: Practical implications and requirements of diversifying interpreted languages. Proceedings of 11th Annual Cyber and Information Security Research Conference (CISRC), pages 14:1-14:4, Oak Ridge, ACM, 2016.

S. Rauti, J. Teuhola and V. Leppänen, Diversifying SQL to prevent injection attacks, Proceedings of The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, pages 344–351, IEEE, 2015.

S. Hosseinzadeh, S. Hyrynsalmi, M. Conti, V. Leppänen: Security and Privacy in Cloud Computing via Obfuscation and Diversification: a Survey, Proceedings of IEEE 7th International Conference on Cloud Computing Technology and Science, (WS on Enterprise Security), pages 529–535, Vancouver, Canada, IEEE, 2015. DOI: 10.1109/CloudCom.2015.29.

S. Lauren, S. Rauti, V. Leppänen: An Interface Diversified Honeypot for Malware Analysis, Proceedings of Workshop on Monitoring and Measurability of Software and Network Security (MeSSa), 6 pages, to appear, 2016.

S. Rauti, V. Leppänen, A Proxy-Like Obfuscator for Web Application Protection, International Journal on Information Technologies & Security, 6:1, pp. 39–52, 2014.

MORE publications ON NEXT SLIDE.

From other universities

Larsen, Per, et al. "SoK: Automated software diversity." *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014.

Baudry, Benoit, and Martin Monperrus. "The multiple facets of software diversity: Recent developments in year 2000 and beyond." *ACM Computing Surveys (CSUR)* 48.1 (2015): 16.

- S. Hosseinzadeh, S. Rauti, S. Laurén, J.-M. Mäkelä, J. Holvitie, S. Hyrynsalmi, V. Leppänen: A Survey on Aims and Environments of Diversification and Obfuscation in Software Security, Proceedings of International Conference on Computer Systems and Technologies (CompSysTech), Palermo, Italy, ACM Press, ACM ICPS, 2016, to appear.
- J. Uitto, S. Rauti, J.-M. Mäkelä, V. Leppänen: Preventing malicious attacks by diversifying Linux shell commands, Proceedings of 14th Symposium on Programming Languages and Software Tools (SPLST'15), pages 206–220, CEUR workshop proceedings 1525, 2015.
- S. Laurén, P.Mäki, S. Rauti, S. Hosseinzadeh, S. Hyrynsalmi, V. Leppänen: Symbol diversification of Linux binaries, Proceedings of World Congress on Internet Security (WorldCIS-2014), pages 75–80, London, IEEE, 2014.
- S. Rauti and V. Leppänen: Man-in-the-Browser Attacks in Modern Web Browsers. Chapter 28 (pages 469 – 480), in book "Emerging Trends in ICT Security" (Babak Akhgar et al), Morgan Kaufman Publishers (Elsevier), 2014.
- S. Hosseinzadeh, S. Hyrynsalmi and V. Leppänen: Chapter "Obfuscation and Diversification for Improving the Security in Internet of Things (IoT)" In: Rajkumar Buyya, Amir Vahid Dastjerdi (Eds.), "Internet of Things: Principles and Paradigms", 259 – 274, Elsevier, 2016.
- S. Hosseinzadeh, S. Lauren, S. Rauti, S. Hyrynsalmi, M. Conti, V. Leppänen: Chapter Obfuscation and Diversication for Securing Cloud Computing, In book "Enterprise Security Springer Book", 30 pages, Springer, to appear, 2016.