UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Title:	Bringing Memory Forensics and Virtual Machine Introspection to Production Environments
Student:	Benjamin Taubmann
PhD stage:	Third year, finisher
Advisor:	Prof. Dr. Hans P. Reiser
Affiliation:	Assistant Professorship of Security in Information Systems University of Passau
Research Area:	System Security, Memory Forensics, Virtual Machine Introspection
Projects:	DINGfest (BMBF), ARADIA (DFG)

DFG Deutsche Forschungsgemeinschaft

DINGfest
Detektion, VisualisieruNG, ForEnsische Aufbereitung von SicherheITsvorfällen

Bundesministerium für Bildung und Forschung

"Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer's iPhone" - CNBC, 2017

What is the problem?

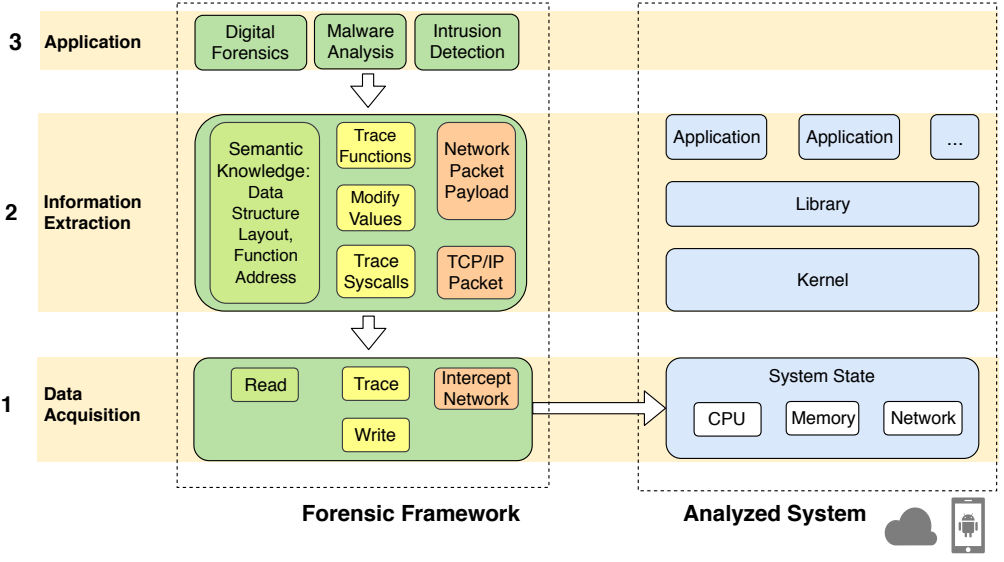
- **Missing interface** for memory access on production systems (cloud, mobile devices)
- **Performance** of current memory forensics and virtual machine introspection tools is too slow for use cases in production environments

Why is it a problem?

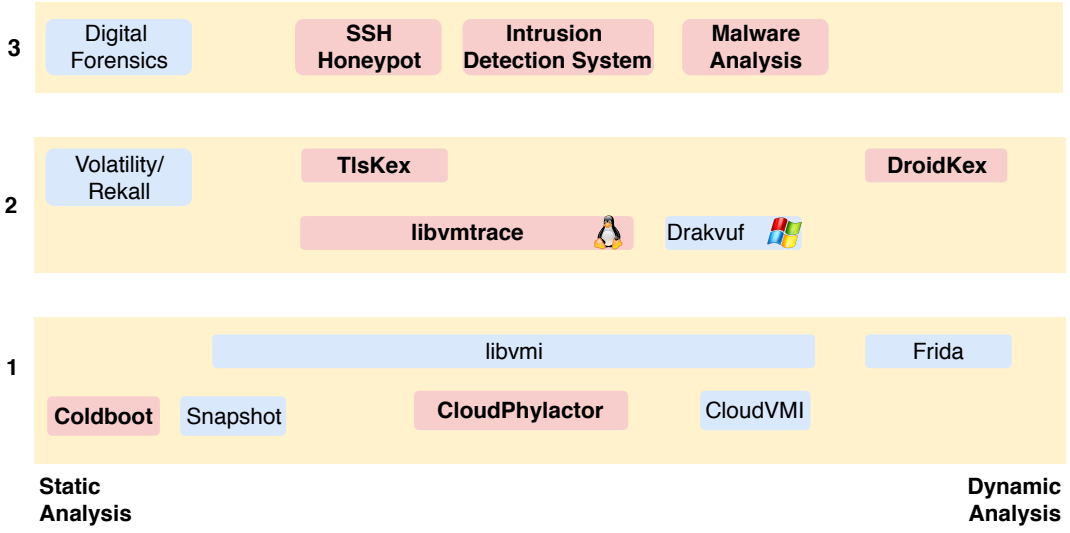
- Forensic investigators and common users cannot do memory based forensics on (their) VMs and mobiles devices
- Cloud customers cannot benefit from the **advantages of memory forensics and VMI-based security approaches**: a higher level of isolation, stealthiness and forensic soundness than traditional in-guest security solutions.

1. **Data Acquisition:** How to get **access** to the memory of production systems such as cloud environments or mobile devices?
2. **Infomation Extraction:** How to **locate and extract** high level information efficiently from main memory?
3. **Applications:** How to deploy and adapt VMI methods to the **requirements of real world use cases and modern computing systems**?

Overall Architecture



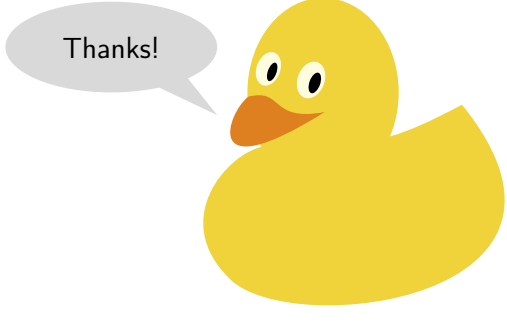
Contributions (bold red)



The main contributions of the thesis are:

1. A generic architecture for digital forensics on production systems
2. Data acquisition architecture for digital forensics in cloud environments and on mobile devices
3. Efficient TLS session key extraction from main memory of applications
4. Adapting resource intensive VMI-based tracing to the requirements of different use-cases that require minimal overhead such as intrusion detection systems

Extended slide set:
`http://www.uni-passau.de/fileadmin/files/lehrstuhl/reiser/publications/taubmann_introduction.pdf`


Thanks!

Publications

[1] Taubmann, Benjamin, Noëlle Rakotondravony, and Hans P. Reiser. "CloudPhylactor: Harnessing Mandatory Access Control for Virtual Machine Introspection in Cloud Data Centers." In: *IEEE TrustCom-16*. 2016.

[2] Taubmann, Benjamin, Christoph Frädrich, Dominik Dusold, and Hans P. Reiser. "TLSkex: Harnessing virtual machine introspection for decrypting TLS communication." In: *DFRWS EU*. 2016.

[3] Taubmann, Benjamin, Manuel Huber, Lukas Heim, Georg Sigl, and Hans P. Reiser. "A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices." In: *ARES*. 2015.

[4] Andres Fischer, Thomas Kittel, Bojan Kolosnjaji, Tamas K Lengyel, Waseem Mandarawi, Hans P. Reiser, Taubmann, Benjamin, Eva Weishäupl, Hermann de Meer, Tilo Müller, and Mykola Protsenko. "CloudIDEA: A Malware Defense Architecture for Cloud Data Centers." In: *C&TC 2015*. 2015.

[5] Taubmann, Benjamin and Bojan Kolosnjaji. "Architecture for Resource-Aware VMI-based Cloud Malware Analysis." In: *SHCIS'17*. 2017.

[6] Taubmann, Benjamin, Omar Al Abduljaleel, and Hans P. Reiser. "DroidKex: Fast Extraction of Ephemeral TLS Keys from the Memory of Android Apps." In: *DFRWS USA*. 2018.

[7] Stewart Sentanoe, Taubmann, Benjamin, and Hans P. Reiser. "Virtual Machine Introspection Based SSH Honeypot." In: *SHCIS'17*. 2017.

[8] Taubmann, Benjamin and Hans P. Reiser. "Secure Architecture for VMI-based Dynamic Malware Analysis in the Cloud." In: *DSN fast abstract*. 2016.

[9] F. Menges, F. Böhm, M. Vielberth, A. Puchta, B. Taubmann, N. Rakotondravony, T. Latzo. "Introducing DINGfest: An architecture for next generation SIEM systems." In: *GI Sicherheit 2018 (Short Paper)*.