DeepSec 2017 Training: The ARM IoT Exploit Laboratory

Posted on **August 29,2017** by **lynx**

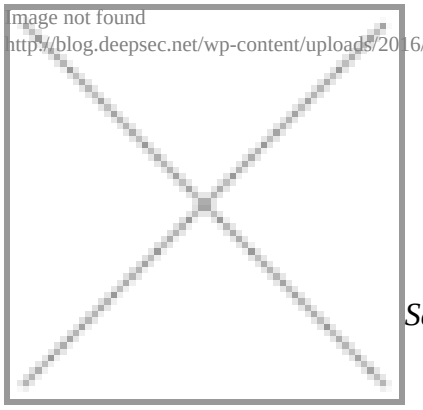
If the Internet of Things (IoT) will ever leave puberty, it has to deal with the real world. This means dealing with lies, fraud, abuse, exploits, overload, bad tempered clients (and servers), and much more. Analysing applications is best done by looking at what's behind the scenes. IoT devices, their infrastructure, billions of mobile devices, and servers are powered by processors using the Advanced RISC Machine (ARM) architecture. This design is different from the (still?) widespread Intel® x86 or the AMD™ AMD64 architecture. For security researchers dealing with exploits the change of design means that the assembly language and the behaviour of the processor is different. Developing ways to inject and modify code requires knowledge. Now for everyone who has dealt with opcodes, registers and oddities of CPUs, this is nothing new. Grab the documentation, ready the tools, and start experimenting. There is another way. Let your lab work be guided by an expert who has extensively done this for x86/x86-64 already. This is why we invited Saumil Shah to conduct the training *The ARM IoT Exploit Laboratory* at DeepSec 2017. Saumil has developed the training to be completely tailored for the ARM architecture.

The all new ARM IoT Exploit Laboratory is a fast paced 3-day intermediate level class intended for students who want to take their exploit writing skills to the ARM platform. The class covers everything from an introduction to ARM assembly all the way to Return Oriented Programming (ROP) on ARM architectures. Our lab environment features hardware and virtual platforms for exploring exploit writing on ARM based Linux systems and IoT devices.

The class concludes with an end-to-end "Firmware-To-Shell" hack, where we extract the firmware from a popular SoHo router, build a virtual environment to emulate and debug it, and then use the exploit to gain a shell on the actual hardware device. The goal is to give you an understanding on how the following topics work on ARM:

- Introduction to the ARM CPU architecture
- Exploring ARM assembly language
- Understanding how functions work on ARM
- Debugging on ARM systems
- Exploiting Stack Overflows on ARM
- Writing ARM Shellcode from the ground up
- Introduction to Exploit Mitigation Techniques (XN/DEP and ASLR)
- Introduction to Return Oriented Programming
- Bypassing exploit mitigation on ARM using ROP
- Practical ROP chains on ARM
- An introduction to firmware extraction
- Emulating and debugging an IoT device firmware in a virtual environment
- Case Study: From Firmware to Shell - exploiting an ARM router's embedded firmware

This three day training definitely will save you from the frustration of spending three months with the architecture and compiler manuals on your lap (or second a screen). Plus you can see how to attack an actual firmware from an actual device. Just like in the movies! ? We recommend this training for anyone dealing with smartphones or devices in the very near future. You are already surrounded by ARM architecture processors and very definitely use them on a daily basis. So why not do some hard-core testing. Best you do this before the other side does!*Important:***Pleasebook** as**early as possible** and bear in mind that this is the only three-day training! Three as in 0,1,2 or 1,2,3. This means the training start one day earlier than the other DeepSec training, i.e. the ARM Exploit Laboratory starts on 13 November 2017, Monday. Remember: Three days.



Saumil Shah is the founder and CEO of[Net-Square](), providing cutting edge information security services to clients around the globe. Saumil is an internationally recognized speaker and instructor, having regularly presented at conferences like Blackhat, RSA, CanSecWest, PacSec, EUSecWest, Hack.lu, Hack-in-the-box and others. He has authored two books titled "Web Hacking: Attacks and Defense" and "The Anti-Virus Book".

Saumil graduated with an M.S. in Computer Science from Purdue University, USA and a B.E. in Computer Engineering from Gujarat University. He spends his leisure time breaking software, flying kites, traveling around the world and taking pictures.

Posted in:Conference,Security,Training | Tagged:ARM,Attack,DeepSec,Exploit,Hacking,IoT,Training | With 0 comments