Fotios (Fotis) Chantzis

Website	sock-raw.org	**Email**	chantzis.fotios@gmail.com
LinkedIn	profile	**Twitter**	@ithilgore

Personal Profile

Computer security engineer with strong background in software development and a research focus on network exploitation (TCP Exploitation - Phrack, Nmap developer & creator of Ncrack) and IoT. Presenter at notable security conferences including DEF CON. Lead author of ”Practical IoT Hacking” book - to be published soon by No Starch Press.

Experience

Mayo Clinic Nov 2016 - Present

Principal Information Security Engineer

Managing and conducting manual security assessments, Red Team operations, penetration tests and vulnerability research on medical devices, clinical support systems and critical healthcare infrastructure.

- Have completed manual assessments on more than 35 complex systems (minimum of 3 weeks testing), developing proof of concept exploits to demonstrate critical risk vulnerabilities.
- Leading the security design, architecture and technology governance oversight for mission critical large-scale infrastructure, including cloud platforms, and acting as information security liaison to business units, IT, clinical practice and medical device vendors.

No Starch Press Oct 2018 - Jan 2020

Lead Book Author

Led the authorship of the upcoming ”Practical IoT Hacking” book.

Packt Publishing Nov 2016 - March 2017

Mastering Nmap author

Authored and published a video course on Mastering Nmap. Focused on showing ways to effectively utilize Nmap, NSE and Ncrack to conduct extensive and refined scans, including how to deal with very large networks.

CENSUS SA Dec 2015 - Sep 2016

IT Security Engineer / Computer Security Researcher

Conducted manual security assessments and penetration tests on infrastructure and devices for clients around the world.

- Researched and developed tools for exploitation of special-purpose network protocols such as NFC, WS-Discovery and DICOM.
- Developed fully-working 0-day exploits for specific vulnerabilities to demonstrate high impact of findings.
- Tested security of critical web applications and mobile apps for financial institutions.

Cyber Defense Directorate, Hellenic National Defense General Staff Mar 2015 - Dec 2015
Information Security Engineer

Researched and developed a variety of network security projects (mainly C/C++). Performed large-scale penetration tests on mission critical infrastructure. Conducted malware analysis and consulted on threat intelligence.

PrimaVista Jan 2013 - Mar 2015
Cloud Engineer / Software Engineer

- Designed and implemented the back-end cloud infrastructure based on Amazon Web Services (EC2, S3). Built an internal REST API on Tornado Web Server and crafted a custom queuing mechanism for load balancing worker tasks using RabbitMQ and Redis.
- Developed a synchronization algorithm tailored for sheet music files and metadata, offering functionality similar to Dropbox/Evernote.
- Designed and developed the Android application.

Was also responsible for securing and hardening all cloud infrastructure.

Lesspaper Aug 2012 - Dec 2012
Cloud Engineer / Software Engineer

- Developed the Android application demo for snapping pictures out of a printed page or book, sending them to the back-end server for image processing (Optical Character Recognition) and returning the text back to the user.
- Implemented minimal back-end service by leveraging Parse (parse.com) and Amazon Web Services in addition to building on Tornado Web Server and RabbitMQ.

Demo was accepted in first round of YCombinator.

Nmap / Ncrack Apr 2009 - Sep 2010
Software Developer / Network Security Researcher

Designed and developed Ncrack (in C/C++), the network authentication cracking tool of the Nmap project. Funding was provided by Google, as a student participant in Google Summer of Code 2009 and 2010. Was also mentor for Google Summer of Code 2016 and 2017. Still maintaining Ncrack in free time.

- Wrote the first working RDP cracker for all modern Windows editions by inspecting captured network data and reverse engineering the protocol.
- Implemented full SSH support by hacking the OpenSSH client code and converting part of it into a library tailored for Ncrack's non-blocking architecture.
- Improved overall network speed and authentication accuracy by programming a dynamic, optimized timing engine and using reconnaissance probes to collect metrics.

Computer Engineering & Informatics Department, University of Patras Sep 2005 - Jun 2012
Computer & Information Engineer

Administered a large variety of computer servers used as the infrastructure of the Computer Engineering and Informatics Department. Conducted penetration tests on mission critical servers and worked with the principal engineers to harden the systems.

Education

2018-now PhD candidate on Information Security
University of Piraeus

2005-2012 Master of Engineering (MEng) -
Computer Engineering and Informatics Department, University of Patras, Greece
Grade: 8.46/10 (scholarship for 3rd highest score)

2002-2005 High School - 19.6/20 (two scholarships for highest grade)

Selected Research

Exploiting TCP and the Persist Timer Infiniteness
Phrack

Discovered an inherent vulnerability in Transmission Control Protocol (TCP) by exploiting the TCP Persist Timer mechanism. Developed a proof of concept tool to demonstrate the attack by using a variety of network techniques: statelessness, client SYN cookies and TCP Timestamp time-keeping.

Abusing Network Protocols
AthCon security conference

Invented a new stealthy port-scanning attack by abusing XMPP.

Hacking the OpenSSH library for Ncrack
Nmap

Analysis of how the OpenSSH-based library was tailored for Ncrack's SSH module.

SOCK_RAW Demystified

In-depth analysis of the raw socket mechanism on the Linux 2.6 and FreeBSD 7.0 network stacks.

Resiliency testing of cardiac implantable electronic devices (pending review)

Results of systematic hacking of defibrillators, pacemakers, and remote monitoring systems

Network Exploitation of IoT Ecosystems

Conferences: GrrCon, OWASP Latam 2019, LayerOne

Skills

Reverse Engineering	- *IDA Pro, Ghidra, WinDbg*	**C/C++**	- most experienced with ANSI C
Penetration Testing	- over 100 assessments	**Python**	- scripting language of choice
Security Architecture	- over 80 reviews	**Java/Android**	- done a lot of development
Cloud Security	- *AWS, Azure, Docker*	**JS, PHP, Perl**	- working knowledge

Certifications

- **OSCE** - Offensive Security Certified Expert - License: OS-CTP-17601
- **OSCP** - Offensive Security Certified Professional - License: OS-101-034495
- **CISSP** - Certified Information Systems Security Professional - License: 635441

Languages

- **English** - Full professional proficiency (Cambridge/Michigan Proficiency)
- **German** - Limited working proficiency (Mittelstufe)
- **Japanese** - Elementary proficiency (Level 4 Japanese Language Proficiency Test)
- **Greek** - Native

Interests

ninjutsu, guitar, pen-and-paper RPGs, biohacking, cognitive science