Curriculum vitae

PERSONAL INFORMATION

Tal Melamed

Trento (Italy), Tel Aviv (Israel)

+39.328.8491434 (ITA)

career@appsec.it

http://appsec.it

Date of birth 12/1982 | Nationality Israeli | Residence Trento, Italy

PROFESSIONAL EXPERIENCE

2013–Present

Security Academy Director | Principal Security Consultant

AppSec Labs, (Israel)
https://appsec-labs.com

Principal roles

- **Security Academy Director**; responsibility for scientific research and the creation of new content for training courses in Cyber-Security. Delivering training courses and specialized training activities to ethical hackers, developers, designers, and system architects worldwide.
  For more information: https://appsec-labs.com/training/
- **Tech Lead;** technical direction of AppSec Labs security consultants; serving as a focal point for technical knowledge, reviewing official reports for customers. Managing client services scoping, kick-off meetings, presenting reports and meetings with relevant leaderships. Leading and executing security projects for *IoT*, *Hardware, Mobile, Web* and *Desktop* applications.
- **Principal Security Consultant;** providing SDL solutions (software and architecture security, threat-modelling, risk assessment, etc.) for AppSec Labs clients (e.g. *Intel, IBM, HP, CheckPoint*, *CyberArk*, *Verint*, *AVG, TEVA, Amdocs, Motorola, AT&T, NTT, 888, NCR, LivePerson, Akamai).*
  For more information: https://appsec-labs.com/clients/
- **R&D:** carrying out research for new technologies into providing new tools and kits for our security testing platforms and training materials.

Major areas

- **Web/Client Application Security**: Black box and Code Reviews (White-box) Penetration testing and security assessments in accordance with the standards and OWASP and NIST guidelines.
- **Mobile Security**: Hacking, Reversing, Security Testing and Scientific Research for Android and iOS apps. Development of platforms and tools to perform Security Tests for Mobile Applications.
- **IoT and Hardware Security**: PCB, Serials and Firmware Analysis; Flash/Chip manipulation; Hacking of Wireless, Radio Frequency (RF) and Bluetooth.
- **Malware Analysis**: Research and analysis of Malware and Anti-Malware applications and tools. Development and use of static/dynamic analysis tools and Exploits; Production of didactic materials, aimed both at theoretical learning and practical exertion.

2011–2013

Sr. Information Security Analyst

Amdocs Ltd., (Israel)
http://www.amdocs.com

- Performing hands-on penetration testing, according to OWASP recommendations and standards, for applications developed within the organization for internal and external use.
- Bringing application security awareness to the organization developers and managers – presentations and lectures about common vulnerabilities, impact and mitigation and analysing of real attack incidents.
- Working hand in hand with Amdocs developers, project managers and architects in order to implement application security fundamentals and mitigations, according to the organization needs.
- Developing tools for security testing and automation (Python/ Bash), in order to support the security team.

2009–2011 **Security Researcher**

CheckPoint Software Technologies Ltd., (Israel)
http://www.checkpoint.com/products/dlp-software-blade/

- Research, design and implementation of security contents for the DLP (Data Loss Prevention) system in compliance with the standards requirements *PCI, HIPAA, PII*, etc. in order to detect and prevent unauthorized transmission and data leakage of sensitive information.
- Creation of data signatures based on the analysis of algorithms and IOS standards validations; development of the operative model suitable for the control and management of the DLP, to prevent the leakage of in/outgoing organization data, under the HTTP/S, SMTP and FTP protocols.

2006–2008 **Intelligence Analyst**

RSA, The Security Division of EMC, (Israel)
http://www.emc.com/security/rsa-identity-protection-and-verification/rsa-fraudaction.htm

- Prevention of internet frauds for worldwide banking and financial institutions (e.g. *Banco Posta, UniCredit, Intesa Sanpaolo, BofA, HSBC, Barclays, Citigroup,* RBS, *JPMorgan Chase, E-Trade, ING*, *Banco Santander).*
- Analysis and monitoring of fraudulent/ Phishing websites and Trojans targeting client; communication methods, rootkits, attack techniques, data manipulation, etc.
- Forensics analysis for malicious websites and files, in order to retrieve stolen financial data and to trace the events and the causes that led to the internet fraud attack.
- Research for anti-fraud solutions and tools to be integrated into production.

2001–2004 **Security Team Member**

Israel Aerospace Industries (IAI), (Israel)
http://www.iai.co.il/

Enforcing security strategies (both physical and cyber-security) of the company; constant monitoring of correctness of events in order to detect possible threats and efficiently counteract any possible attack or risk.

2001–2004 **Platoon Sergeant**

Israel Defense Force (IDF)
https://www.idfblog.com/

Three-years of Military service lasting three years in the Infantry Corps of the IDF *Golani* Brigade.

- Intelligence collection and analysis; coordination with the intelligence corps, reviewing of target maps aerial photography for course of action.
- Logistics management of operations; delivering weapons, vehicles and other equipment necessary for the operation. Coordinating with other participating forces.
- Preparation training; preparing the platoon for the operation regarding the modes of action, and possible threats in the field; Creation, direction and analysis of critical scenarios and incidents related to the operation and guidance of the platoon resolution strategies.
- Commanders' course sergeant; election for excellence to train future commanders in the Infantry Corps. Responsibility for the preparation, management and delivery of the training program for the role of operative-commander in the Infantry and Paratroopers Brigades.

NOTABLE TOOLS AND PROJECTS

https://github.com/nu11p0inter

* **Microsoft SDL**
https://www.microsoft.com/sdl
Developing SDL training course for Microsoft Developers.

* **ProKSy**
https://appsec-labs.com/proksy
A TCP Proxy with Java KeyStore Handling to Support SSL/TLS connections and bypassing Key-Pinning.

* **AppUse - Android Pentest Platform Unified Standalone Environment**
https://appsec-labs.com/AppUse
A leading, free, platform for mobile application security testing in the android environment. Includes custom-made tools created by AppSec Labs.

* **iNalyzer - iOS Penetration Testing Framework**
https://appsec-labs.com/iNalyzer
A framework for manipulating and tampering with parameters and methods for iOS applications. AppSec Labs iNalyzer targets closed applications by turning a black box testing into an automatic grey-box effort.

PUBLICATIONS

Tal Melamed, "An active Man-in-the-Middle Attack on Bluetooth Smart Devices," *International Journal of Safety and Security Engineering*, Volume 8, Issue 2, 2018
https://www.witpress.com/elibrary/sse-volumes/8/2/2120

CONFERENCES

http://appsec.it/talks

10-14/09/2017 SECUREWARE 2017 - The Eleventh International Conference on Emerging Security Information, Systems and Technologies
Hacking Bluetooth Low Energy Based Applications
http://www.iaria.org/conferences2017/ProgramSECURWARE17.html

06-08/09/2017 SAFE 2017 - 7th International Conference on Safety and Security Engineering
An Active Man-in-the-Middle Attack on Bluetooth Smart Devices
http://www.wessex.ac.uk/conferences/2017/safe-2017

04-08/08/2017 SHA 2017
Hack-a-ble: Hacking BLE Smart Devices
https://sha2017.org/, https://media.ccc.de/v/SHA2017-230-hack-a-ble

28/06/2017 BSidesTLV 2017
Break-a-ble: Hacking Your Smartphone with BLE
https://www.bsidestlv.com/

25-29/06/2017 ICIMP 2017 - The Twelfth International Conference on Internet Monitoring and Protection
Hacking Bluetooth Low Energy Based Applications
https://www.iaria.org/conferences2017/ICIMP17.html

18/01/2017 OWASP Israel January 2017
R U aBLE? BLE Application Hacking
http://sl.owasp.org/melamed17

19/09/2016 OWASP AppSec IL 2016
Java Hurdling: Obstacles and Techniques in Java Client Penetration-Testing
http://sl.owasp.org/melamed16

EDUCATION AND TRAINING

2007–2011 **B.Sc. Software Engineering**

Shenkar College of Engineering and Design, (Israel)

2016 Cryptography I @ Stanford University

Cryptographic systems and how to correctly use them in real-world applications; exam of deployed protocols and analysis of mistakes in existing systems; public-key techniques and more.

2016 Cybersecurity and Its Ten Domains @ University System of Georgia

Governance and risk management, compliance, business continuity and disaster recovery, cryptography, software development security, access control, network security, security architecture, security operations, and physical and environmental security.

2016 Software Security @ University of Maryland

Foundations of software security; analysis of important software vulnerabilities, attacks, exploit and related defences (advanced testing and program analysis techniques).

2016 Cybersecurity and the Internet of Things @ University System of Georgia

Threats, security policies and practices, privacy concerns related to the internet capabilities of some of the most common products of Internet of Things (IoT).

2016 Usable Security @ University of Maryland

Principles of HCI; design and development of secure systems with a human-centric focus.

2016 Cybersecurity and Mobility @ University System of Georgia

New challenges in protecting data, evolvement of threats, critical-data exchange, BYOB, effective cybersecurity, prevention strategies, securing networks, etc.

2012 iOS Hacking @ AppSec Labs

The iOS Architecture, security model, file system, static and dynamic Analysis, reversing and tools.

2012 Android Application Hacking @ AppSec Labs

Android Components, runtime and static analysis, file system, reversing, and common tools.

2011 Advanced Web Application Hacking & Pen-testing @ AppSec Labs

Web application hacking and testing. Methodologies, legal issues, writing security reports, known tools, information gathering and main vulnerabilities exploits and defence techniques.

2010 Network Hacking @ CheckPoint Software Technologies Ltd.

Fundamentals and latest network hacking techniques based on standard security steps and evasion principles (ARP Spoofing, DNS Poisoning, TCP Hijack, SQL Injection, HTTPS Striping, etc.).

2009 Certified Secure Developer @ CheckPoint Software Technologies Ltd.

Input validation, Buffer overflow, Format strings/integer security issues, privileges escalation vulnerabilities, Handling Passwords, Using SSL/TLS securely.

2006 Internet Threats Analysis @ RSA, The Security Division of EMC

Methodologies, detection, tracings, and tools of internet threats (Phishing, Trojans, Viruses, etc.).

PERSONAL SKILLS

Mother tongue(s) Hebrew

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
Italian	B1	B1	B2	B2	B1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user. Common European Framework of Reference for Languages .

Communication skills

Excellent interpersonal and collaborative skills gained both in the private and working sphere, thanks to:

- the planning and design of technical projects within different work groups
- participation in various technical working teams for the management of complex projects
- the role of teacher and tutor in training courses in the field of information security for multidisciplinary professionals
- the role of trainer and educator in the military, responsible for the transmission of ethical, military and cultural knowledge and for the development of the physical, moral of the subordinates
- the excellent relationships maintained with colleagues and customers

Organisational / managerial skills

Great leadership skills and excellent skills in the organization and coordination of teams, acquired in:

- the planning and design of technical projects within different work groups
- the attentive relationships with colleagues and the networking group
- the organization, coordination, tutoring and training addressed to both group and individual professionals
- in the organization of educational materials for the training courses provided and the related work plan

Investigative and analytical problem solving skills to resolve in-depth queries in a methodical manner, independently and with internal and external business partners to find appropriate resolutions, efficiency and high level of quality.

Great team player skills, enjoys sharing knowledge and encouraging development of others to achieve specific team goals.

Digital competence

- Full control upon Windows, Unix\Linux, OS X environments, structure and internals.
- Solid understanding in networking and protocols, such as TCP/IP and Client-Server model.
- Strong understanding of internals of HTTP/S protocol, web servers and web applications.
- Deep knowledge of information security principles, methodologies (OWASP/ WASC), theories and attacks under all platforms (Web/ Client / Mobile / IoT).
- Professional Python, Java, .NET, PHP, C/C++, SQL, Go, NodeJS, JavaScript and Bash/Shell programming skills.
- Advanced experience in the use of common tools for communication monitoring. E.g. Burp, Fiddler, WireShark, tcpdump, Netcat.
- Experience in the use of commercial security scanners. E.g. AppScan, Fortify, Checkmarx, Nessus, Metasploit.
- Experience in the use of Reverse Engineering tools. E.g. OllyDBG, IDA, procmon, processhacker, HxD, apimonitor, ILSpy, Dotfuscator, adb, FFDec, JavaSnoop, apktool, jadx/jd-gui, jbe/reJ, snoop-it.
- Experience in the use of IoT and HW hacking tools. E.g. esptool, inspectrum, gattacker, btljuice, UART, bus pirate, GoodFet, Jtagulator, binwalk, Aircrack-ng.
- Excellent oral and written communication skills including the ability to construct and deliver compelling and succinct presentations, collateral and reports to internal and external teams.
- Good understanding of Information Security and Privacy standards such as ISO27001, PCI, HIPAA, PII, etc.