OVERVIEW OF SELECTED PROJECTS

Ongoing: Consulting Projects

Overview:

Includes structured technical audits and due diligence of technology companies on behalf of boards of directors and venture capital funds, diverse R&D projects, some involving ML,AI/LLM, transformer models, etc.

For reasons of confidentiality, more details are not available at this moment.

2020 – 2025: Principal Software Architect — Fortinet, Herzliya, Israel.

Overview of some projects and activities:

2022 – 2025: Cloud workload protection. Research, definitions and prioritization (in close collaboration with Product and Research teams), design, and hands-on development of the EDR ("Endpoint Detection and Response") product to protect Kubernetes workloads in major public clouds (AWS, Azure, GCP). The EDR/XDR software runs in a privileged container in a DaemonSet on every cloud node. Events are generated in the node's kernel using eBPF ("extended Berkeley Packet Filter") hooks, tracing system call invocation, scheduler events, socket events, etc. Infrastructure to generate system call event tracing with minimal coding has been developed. Userspace infrastructure to provide detailed information for "threat hunting" while resolving process, filesystem, user data in each protected container in an integral part.

2020 – 2025: Linux EDR. Design, development, and troubleshooting the kernel module and the userspace part of the Linux EDR product for a large number of distributions. *From 2024:* unification of Linux EDR with cloud workload protection (cf. above) using eBPF.

2024: Linux ransomware detection. Participated in definitions (joint with Security Research), design, and development of ransomware detection PoC, to be integrated into Linux EDR and cloud protection products (see above).

2020 – 2022: MacOS EDR. Created the macOS EDR product utilizing "system extensions" (in macOS 10.16 and later versions). Gathered requirements, designed and developed the full endpoint product for both Intel and Apple's M-series ARM CPUs, including next generation antivirus (NGAV), filesystem scanning, interfaces and protocols with other system components, malware signature update infrastructure, packaging and installation, support for MDM (Mobile Device Management, including Jamf and VMware Workspace ONE), etc. Leading support and troubleshooting activities opposite major customers on a regular basis. *Presently working closely with the R&D and QA teams in a consulting capacity.*

2018 – 2020: CTO — TrapX Security, Tel Aviv, Israel.
2014 – 2018: Director, Product Architecture.

Overview of some projects and activities:

Emulation traps and appliances. Definitions, design, and hands-on development of virtual and physical appliances hosting hundreds of emulation-based malware traps of various kinds: servers, workstations, network devices, VoIP systems, IoT and OT devices, industrial systems (SCADA), financial systems (PoS, SWIFT, ATM), ERP systems (SAP), medical devices, etc. Each trap provides a complete emulation of all the layers of the corresponding real system: OS fingerprint in the network, relevant application level protocols, filesystems, fake data, etc. Traps can be deployed on a massive scale and may be configured manually or automatically.

BotNet Detector. A sensor deployed on an appliance (see above) that analyzes outgoing traffic and detects suspicious activity including communications with BotNets' Command and Control servers, suspicious user activity (connections to infected servers or TOR), etc.

"FullOS" traps. A real server installed and configured by the customer and running arbitrary services, instrumented to serve as a trap capable of engaging a human attacker for a long time in order to gather intelligence, profile the activities, analyze procedures, techniques, and tactics. Emulation traps that can be deployed on a large scale (see above) may redirect attacks to the high interaction traps transparently.

Linux High Interaction Traps. A "jailed" fully fledged Linux server running on a TrapX appliance (see above) — a trap capable of engaging a human attacker for a long time without the need to provision, install, and configure a separate server.

"Deception Tokens". "Baits" installed on organization's computers (workstations or servers) that lure malware and human attackers to deployed traps, increasing the probability of detection.

TSOC: TrapX SOC management server. A server that manages the full lifecycle of traps and tokens, receives, stores, and analyzes security events, provides monitoring capabilities, issues alerts, communicates with various elements of the ecosystem (sandboxes, SIEM, NAC, etc.), generates detailed reports, etc.

Automatic trap configuration. Automatic configuration of emulation traps based either on active asset discovery or external inventory (obtained from Active Directory data or from custom or 3rd party asset management systems). Reconfiguration is possible at any time, driven by scheduled changes, overall system orchestration, arbitrary external events, etc. Autonomous configuration decisions are made by configurable algorithms.

Custom trap creation. A "build your own trap" mechanism allowing customers to define their own malware traps that are not provided out of the box by the system. Patent issued.

2018 – 2020: CTO — TrapX Security, Tel Aviv, Israel (cont.)
2014 – 2018: Director, Product Architecture (cont.)

Overview of some projects and activities (cont.):

REST API. Covering all the functionality of the system, allowing event retrieval and passing through to integration and analysis systems, dynamic (including event-driven) orchestration of trap provisioning and configuration at scale, custom trap creation and deployment, etc.

Cloud appliances and traps. Emulation and high interaction traps may be adapted to all the major cloud environments: AWS, Azure, GCP, OpenStack, etc., including highly customized ones.

Ecosystem. Numerous integrations with firewalls, sandboxes, SIEM/SOAR tools, NAC, EDR, asset management, compliance systems, etc.

Coverage analysis. A system providing customers with visibility into deceptive coverage of the entire network, globally and on a per subnet basis, as well as coverage of the entire relevant attack surface.

2009 – 2013: Director, Research — TraderTools Inc., Raanana, Israel.

Overview of some projects and activities:

Optimal execution and smart order routing for spot FX. Created and implemented in production a sophisticated algorithm that optimizes routing and execution of orders against multiple liquidity providers with different business rules of engagement. The optimized solution typically yields a price improvement of $50-100 per $1M of flow for the company's customers, compared to any alternative method. The algorithm is the foundation of the Smart Order Router (SOR) and is also utilized in the trading stations and the pricing engine.

Smart Order Router architecture. Designed a SOR architecture separating the order/book matching and execution optimization engine from the event handling and communication infrastructure. Led technology research and provided business and technology guidance for design, and development of a new technological foundation of connectivity to liquidity providers, liquidity aggregation, and smart order routing components for the latest generation of the product.

FX swap and forward trading. Designed and developed a prototype swap and forward execution management system, including FIX (Financial Information Exchange) protocol communication with multiple liquidity providers for streaming market data, RFQ (request for quotes), and dealing.

2009 – 2013: Director, Research — TraderTools Ltd. (cont.)

Overview of some projects and activities (cont.):

Trading in synthetic cross currency pairs. Customers needed a system to trade in "synthetic" (i.e., not directly quoted) currency pairs. Led requirement gathering from customers, provided the initial specifications as well as design guidelines for implementation. Developed all the relevant algorithms, including efficiency optimizations and performance analysis. Designed and developed a complete reference implementation that serves, among other purposes, as a benchmark for testing. Provided detailed guidance for design and implementation to R&D and for development of a detailed testing plan to QA.

Performance analysis, monitoring, and alert infrastructure. Designed and implemented a completely automated infrastructure to comprehensively monitor the company's products' business performance in production. Deal flow and execution quality are monitored on a daily, weekly, and monthly basis, with automated statistical analysis and a break-down by currency pair and liquidity provider. Periodic reports are automatically generated for internal analysis and for delivery to customers, and provide a basis for tuning price feed subscriptions, tier management, bandwidth management, etc. The system notifies of significant events, e.g., of drops or increases of execution quality against a particular counterparty, changes in price competitiveness from liquidity providers, etc. The system tracks and provides statistical analysis of the system's performance, e.g., latency at different stages.

Price improvement and ROI analysis. Developed a methodology and designed and implemented a system for analyzing price improvement compared to competition, and the associated ROI. The results of the analysis serve as an essential part of periodic reports to customers and an important marketing/sales tool.

Spread analysis. Developed a tool to analyze price spreads per liquidity provider, currency pair, and amount, depending on the hour of the day. The results were cross-referenced against trading patterns (e.g., order sizes) for various customers, and served as an important input for analysis of efficacy of trading.

Pricing engine algorithmics. Developed a set of algorithms that allow constructing multi-tiered raw, core, and customer spot prices in an optimal manner (with the tightest core spread) very efficiently. A different set of algorithms pertains to creation of forward prices. The algorithms have been incorporated into the company's Pricing Engine.

NDF price creation and publishing. Specified and designed a product allowing customers to create and publish non-deliverable forward (NDF) prices in various currencies.

Real-time position management and hedging. Conceived, specified, and designed a system that allows traders to automatically monitor, manage, and hedge their positions in real time. The event-driven system utilizes a Complex Event Processing engine that handles events that occur both inside and outside the TraderTools product.

2009 – 2013: Director, Research — TraderTools Ltd. (cont.)

Overview of some projects and activities (cont.):

Generic trading strategy engine. Designed a generic platform allowing customers and third parties to build customized event-driven trading strategies in a variety of programming languages. The strategies are seamlessly integrated into the company's automated trading engine and can be applied, stopped, and monitored through a unified user interface. The most common application is (selective) automated hedging engine. However, the platform is completely generic and sophisticated strategies have been implemented on it.

2007 – 2009: Director, System Architecture — Voltaire Ltd., Herzliya, Israel.

Overview of some projects:

High performance low latency 10 Gbps Ethernet director switch and fabric. Led requirements formulation, silicon vendor selection, detailed product and system level specifications for a 288 port 10 Gbps Ethernet director switch suitable for building highly scalable and efficient data center interconnects. Led development of L2 multipathing technology providing high utilization of large scale Ethernet fabrics compatible with legacy Ethernet environments.

324 port QDR InfiniBand director switch. Led requirements formulation and detailed specifications for a 324 port QDR InfiniBand switch delivering 26 Tbps of non-blocking bandwidth at 300 ns port-to-port latency. The system is scalable up to 648 and 1296 ports.

36 port QDR and DDR InfiniBand switches. Led requirements formulation and detailed specifications for the world's first generally available quadruple data rate (QDR) 1U, 36 port InfiniBand switch delivering 2.88 Tbps of non-blocking bandwidth with 100 ns of port-to-port latency. A double data rate (DDR) InfiniBand switch utilizing the same hardware and software design was also developed.

Unified device and chassis management software. Led requirements formulation and detailed specifications of chassis management software for all the company's products from 1U to multi-board InfiniBand and Ethernet director switches. The software includes inventory and device management, signal optimization, high availability, health monitoring, event and alarm management, CLI, GUI, SNMP, security and user management, logging, etc.

Unified fabric management software. Led work on architectural specification for Voltaire's Unified Fabric Management software facilitating monitoring and management of InfiniBand and Ethernet fabrics, including topology discovery, provisioning, InfiniBand subnet management, health and performance monitoring, congestion management, fabric virtualization, etc. Today similar systems are dubbed Software-Defined Networks (SDN) and Software-Defined Data Centre (SDDC).

2002 – 2007: Research Staff Member — IBM Research, Haifa, Israel.

Overview of some projects:

2002–2007: Job management and scheduling system for the Blue Gene/L supercomputer. Led research and analysis of the properties of the interconnect architecture and the novel "multi-toroidal" topology of Blue Gene/L, its impact on the machine performance and resource utilization. Participated in the design of Blue Gene/L's open resource and job management architecture and software, parallel job scheduling policies and algorithms. Published 5 peer-reviewed papers and filed patent applications. Blue Gene/L was the fastest supercomputer in the world until the advent of LANL/IBM Roadrunner in June 2008 (see above). The successors, Blue Gene/P and Blue Gene/Q, remain among the fastest and most scalable supercomputers today, running parallel applications on more than a million cores concurrently.

2003–2006: "IP-Only Server". Led design and implementation of a novel server architecture that has a single I/O channel — the IP network. All the I/O devices — disks, keyboard, video, mouse, USB, etc., are remote, the "IP-only server" has no I/O devices or controllers on the board. An FPGA-based hardware/firmware component dispatches the I/O commands and data to the remote devices transparently to the software stack from BIOS to OS to applications. The server architecture is simplified, the power consumption is reduced, the reliability is improved, and the system management is improved greatly, even when the main server software and/or hardware are not operational. In addition, the new architecture has important potential for I/O virtualization. Published a paper, a research report, and filed patent applications.

2005–2006: "Encompass" — a functionality-centric system provisioning and management mechanism for enterprise data centers. Led design and development of the system based on a repository of bootable software stacks that reside on shared (SAN or NAS) storage and can be cloned, customized, and deployed on physical or virtual machines. The focus of system management is shifted from the computational resources (machines, CPUs, memory) to business functionality represented by software and data in the storage system. The mechanism forms the basis of system provisioning in the novel "Commercial Scale-Out" architecture developed at IBM Research, and has been incorporated into IBM's mainstream system management software products. Published a paper and filed a number of patent applications.

2006–2007: Collaborative Driving Systems. Leading an "adventurous research" project focusing on improving safety and efficiency of intelligent transportation systems incorporating communication between vehicles and road infrastructure, and on driver-vehicle interface. A patent application was filed.

2001 – 2002: Director of Development — DataZoo Ltd., Raanana, Israel.

Overview:

The company started as a platform for interacting AI-driven "intelligent agents" (today called "agentic AI", though the term didn't exist then and the technological capabilities of the time were inadequate, performance-wise).

Later the company pivoted to applying data mining/AI/ML algorithms for real time analysis of IP network traffic on a per packet basis to protect networks against DDoS attacks. Participated in application and algorithmic research, legal research, customer relations. Led requirement specification, design, and implementation of the software. The protection mechanism, implemented in userspace and in the Linux kernel, produced excellent results in lab and field-test experiments.

2000 – 2001: Head of Algorithm Development — Comgates Ltd., Herzliya, Israel.

Overview:

To improve quality of service (QoS) of real time (VoIP) applications an overlay network of specialized routers that continually measure conditions (latency, jitter, loss, etc.) in autonomous systems comprising the Internet and route packets optimally to minimize cost while providing the required QoS was designed and developed. Led research of policies, algorithms, and protocols, and software design and development by geographically separated teams of algorithm researchers and programmers.

1996 – 2000: Financial Analyst — Bloomberg L. P. (BFM), Tel Aviv, Israel.

Overview:

Led development of a number of financial analysis and information products related to pricing options, warrants, and other derivative securities, from financial analysis to mathematical models to numerical algorithms to design, implementation, and integration of software. Coordinated product development and maintenance with geographically separated teams of financial analysts, application specialists, programmers, sales representatives, and help desk personnel. Formed and maintained close relationships with customers in many of the world's leading financial institutions. The option and warrant pricing products were recognized as industry standard and recommended to clients by world's largest investment banks. Published a number of papers on financial modeling and option pricing.