

Mr. Nitikorn Sriautha

Mobile: 089-813-2136

E-mail: nitikorn@kdts.co.th

Portfolio Website: <https://korn.nitksoft.com>

Address: Nonthaburi, Thailand

Education

- **Master of Science (M.Sc.) in Information Technology** | King Mongkut's University of Technology Thonburi (KMUTT) | 2003
- **Bachelor of Engineering (B.Eng.) in Control System and Instrumentation Engineering** | King Mongkut's University of Technology Thonburi (KMUTT) | 2001

Professional Summary

A highly accomplished **Principal Software Engineer** with **over 20 years of deep expertise in low-level systems programming**, specializing in **Windows OS Internals (C/C++) and advanced cybersecurity solutions**. Proven track record in designing, developing, and optimizing critical system components that deliver robust security and performance.

- **Pioneered real-time system monitoring:** Designed and implemented a system for real-time screen and resource capture/playback to detect and deter unauthorized user operations.
- **Integrated advanced authentication:** Developed a framework for seamless integration of fingerprint systems into core security products, including Windows login and virtual drive solutions.
- **Secured data at rest:** Created a real-time data encryption/decryption driver to ensure comprehensive data protection on hard disk drives.
- **Forward-looking:** Eager to leverage extensive low-level knowledge, combined with modern **Web Technologies (Blazor, gRPC)** and emerging **Machine Learning (ML) techniques**, to drive innovation in next-generation cybersecurity products.

Work Experience

Principal Software Engineer | KDTS Thailand | May 2001 – Present

Spearheaded the design, development, and implementation of core low-level security and system components for enterprise-level products. Served as the lead technical authority on Windows OS internals, driving innovation from kernel-mode driver development to full-stack application architecture.

- **Pioneered Advanced Endpoint Protection & Data Security Solutions:**
 - **Illegalview (2002-Present):** Designed and developed a core endpoint monitoring product, enabling real-time recording of on-screen activities and granular control/alerting for file access, application usage, and removable drive operations.

- **PAN (2020-Present) & PAN RT (2022-Present):** Designed and implemented a standalone CUI tool for sensitive data (e.g., credit card number) discovery across various databases (MySQL, MSSQL, SQLite) and file types (Office, TXT, CSV), with hash-based change detection. Extended this with a client-server real-time scanning and reporting system (PAN RT).
- **File Lock (2003-2005):** Created a virtual drive solution to provide secure, encrypted data storage.
- **WorkReport (2005-2006):** Designed a client-server application to track application usage activity and generate detailed usage and focused task reports.
- **Datawall (2007-2010):** Engineered a full-disk encryption solution utilizing a **file filter driver** for on-the-fly data encoding/decoding, effectively preventing data leaks from stolen drives.
- **FILE CHECK (2019):** Developed a client-server file integrity monitoring system with a web UI, using SSH for remote command execution (e.g., CRC32 checks) and providing alerts/reports on detected file changes.
- **RDP View (2019-2020):** Developed a Windows desktop application for live screen viewing of RDP sessions on the same server, enhancing monitoring capabilities.
- **Led Innovation in Authentication & Identity Management:**
 - **KTSS Security Suite (2004-2009):** Architected and developed a centralized controller for security services.
 - **KTSS Controller:** designed to manipulate and coordinate all KTSS family services.
 - **KTSS Login:** Implemented a custom **GINA module** to enable fingerprint logon for Windows.
 - **KTSS Finger Print:** Developed a system for fingerprint registration and provided APIs for other products to identify users.
 - **SPIDER (2014-Present):** Designed and developed a web-based privileged identity management system, allowing users to request login accounts and administrators to approve/manage Windows/Linux accounts based on requested periods, including automated account creation/deletion and password updates via CSV scheduling.
 - **USB-AUTH (2022-2023):** Engineered a custom USB drive-based authentication solution for Windows 10/11, intercepting **Credential Providers** to enable login, lock screens upon USB unplug, and log off users if the USB does not match.

Tools & Methodologies:

Microsoft Visual Studio, IDA (Pro), WinDbg, Wireshark, Process Monitor, Sysmon, Virtualization (VMware/VirtualBox), Git, Agile (Scrum), DevOps, CI/CD.

Technical Skills

- **Programming & Core Systems:** C/C++ (Visual C/C++), C#, Java, JavaScript (JS), Assembly (x86), Windows OS Internals (Kernel/User-Mode), Linux (Basic/Intermediate), Data Structures & Algorithms, Performance Optimization.
- **Low-Level & System Programming:**
 - **Windows Driver Development:**
 - **Network Drivers:** Win98 (VXD) and Win2000/XP (SYS) drivers to modify data in transit, including Network Protocol Drivers and Miniport Adapter Drivers.
 - **File System Filter Drivers:** Developed for on-the-fly data encryption/decryption, preventing unauthorized file access, and creating kernel-mode file mappings for user-mode data scanning.
 - **Keyboard Drivers:** Developed to intercept and alter keyboard scan code data.
 - **Kernel-Mode Development:** Extensive experience in developing and debugging drivers at the highest privilege level.
 - **Networking & Protocols:**
 - Custom TCP/IP Stack implementation.
 - Developed proprietary secure network protocols.
 - Expert in Server-Client Architecture using Windows Sockets I/O (Nonblocking I/O, Overlapped I/O with completion indication).
 - **Windows System Internals & API Hooking:**
 - **API Hooking:** Implemented techniques to hide processes from Task Manager, hide files/folders from File Explorer, capture text rendered by User32/DirectWrite, intercept/block CTRL-ALT-DEL, and prevent application execution.
 - **COM Hooking:** Captured and altered data passing via COM interfaces, such as SQL commands.
 - **Clipboard/OLE Interception:** Hooked `IDataObject` interface to intercept and modify clipboard data.
 - **System Initialization:** Created native applications designed to run before the Win32 subsystem starts.
 - **Screen Capture & Recording:** Developed robust solutions for real-time screen capturing and recording.
 - **Authentication & Security Systems:**
 - **GINA/Winlogon Customization:** Developed custom GINA (for Windows 2000/XP) and Winlogon modules for enhanced authentication flows.
 - **Biometric Integration:** Integrated fingerprint devices (e.g., Siemens ID mouse) into Windows login interfaces.
 - **Custom Authentication:** Hooked native credential providers to enable custom USB authentication methods.
 - **Cryptography:** Designed and implemented custom encryption algorithms.
- **Web & Cloud Technologies:**
 - **Web Development (Full-Stack):** Developed 10+ full-stack web applications using jQuery, Angular, React, and ASP.NET Core.
 - **Real-Time Communication:** Implemented high-performance data synchronization using WebSocket and gRPC.
 - **Frontend Optimization:** Experience with Virtual Scroll for improving large data scrolling performance.
 - **Cloud Platforms:**

- **AWS:** Developed Alexa custom skills using AWS Lambda, experience with EC2, S3, IoT, DynamoDB.
- **Azure:** Experience with Azure web hosting, CI/CD pipelines with Azure and Team Foundation Server.
- **Google Cloud:** Experience with Firebase Hosting, Cloud Run, Storage, Firestore, and developed custom skills for Google Home.
- **Cloudflare:** Experience with Cloudflare Workflows and Zero Trust concepts.
- **Mobile Application Development:**
 - Developed native Android applications with Android SDK.
 - Experience with Universal Windows Platform (UWP) and Progressive Web Apps (PWA).
 - **Game Console Development:** Experience with Nintendo DS SDK and Homebrew for custom game console development.

Other Experience

- **Reverse Engineering & Digital Rights Management (DRM):** Successfully disassembled and reverse-engineered commercial e-book reader applications to read data from SQLite, generate keys and salts, then call hidden functions within the application's DLLs to retrieve the true keys for unlocking the DRM of each e-book set, demonstrating deep binary analysis and vulnerability assessment skills.
- **Thai Character Rendering Solution:** Developed a specific solution to correct incorrect Thai character (ตัวอักษร) positioning for certain fonts in PDF files, showcasing sharp attention to detail and advanced problem-solving in character rendering.
- **Document Manipulation (XML):** Gained experience in manipulating OpenOffice documents using XML syntax, highlighting proficiency in document structure and data transformation.
- **Game Console Development:** Possess extensive experience with Nintendo DS SDK and Homebrew (non-official SDK), demonstrating strong low-level programming capabilities for embedded gaming platforms.
- **Microcontroller & Embedded Systems Development:** Hands-on experience with a wide range of microcontrollers and embedded systems, including Arduino, ESP32, PIC, ARM, 80cxx, Atmel, AVR, and 68000.
- **Mobile & Wireless Innovations:** Developed "BTJoypad" using Nokia Symbian SDK to transform a Symbian phone into a Bluetooth wireless joypad, showcasing innovation in mobile and embedded wireless communication.
- **Telephony & API Integration:** Possess experience with TOT Telephone Directory Server SDK (OSA API) and Telephony API for interfacing with Nortel telephony devices, highlighting strong integration skills with complex communication systems.

