DIPL.ING.(FH)KLAUS ROCK

HTTP-QuSS

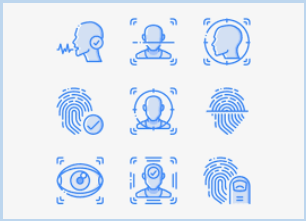
HTTP - QUANTUM SPEED AND SECURITY

February 14, 2022

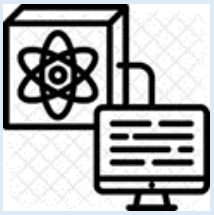
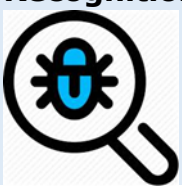
AI SUPPORTED CYBER SECURITY FACT SHEET

ROCK TECHNOLOGIES
Bonhoefferstr. 37 | 73432 Aalen | Germany | +49-7367-9222-958

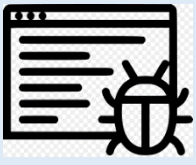
HTTP-QuSS – Active Cyber Defence compared to State of the Art

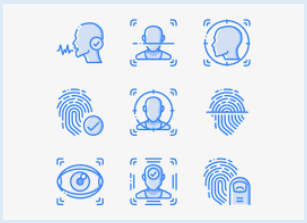
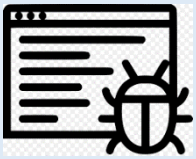
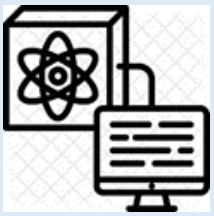
Threat	State of the Art Defence	HTTP-QuSS Defence
HTTP-QuSS Server Hack Backdoor Access Ransom Demand Data Theft	Securing all well-known Application Ports (**0 - 1023**) with strong Firewall. **Brute-Force secure Password** Strength for ssh Connections $H = \log_2 N^L = L \log_2 N = L \frac{\log N}{\log 2}$	Only UDP Port **80** for HTTP-QUSS Process Chains and secretly remapped **TCP Port XXXXX** for ssh Connection open and secured. **No unsecure Application** (WEB-, FTP Server etc.) behind these two Ports. **Uncrackable biometric Passwords** for System Administrators. 
Man in the Middle Attacks Malicious Software Injection Phishing	**Unsecure TSL/SSL Encryption** via exchanged Secrete Keys Hackable with available Tools and with Supercomputer On all existing WEB Servers must **manually installed SSL Certificates**.	**2 Level Keyless Quantum Secure Data Encryption** **Biometric Data** for 1 Level Encryption. **Delta Data Algorithm** for 2 Level Encryption. **No secret Key Exchange** **All the existing WEB Servers are automatically secured** **No** need of **SSL Certificates** **No time-consuming** manual Installations
(DDoS) Server Attack Server down Ransom Demand	**Securing all existing WEB-Servers** with strong Firewall Scripts against DDoS Attacks	Securing only a **few centralized HTTP-QUSS Supercomputer Server** with very strong AI based Firewall

		Can **handle Millions of Requests** per Second so **impossible to bring him down**
WEB Server Hack Backdoor Access Malware Flooding Data Theft	**Securing all existing WEB-Servers** against brute-force Attacks on well-known open Ports (**0 - 1023**) But **well-known Application Leaks** like WEB Server Directory Listings, FTP Downloads etc. **not possible to secure**. **Password Strength** must be managed by Billions of Users themselves.	**Secured** with **uncrackable biometric Passwords** **No Applications with well-known Security Leaks** are used Already **infected and hacked WEB Servers** are identified by **Sandbox Traps** The **rapid Spread of Malware** is **stopped immediately**
Cracking Passwords Identity Steeling Data Theft	**Password Strength** must be managed by Billions of Users themselves. Each **Internet User** must **manage many Passwords** which leads into **carelessness** in assigning Passwords **Easy to hack** by brute-force Attacks	**One-Time central secured** with **uncrackable biometric Passwords** **No countless Passwords** but clear **unique biometric Identification** for **all Internet Logins** and **Activities** • No Darknet • No Hacker Activities • No Identity Steeling
JavaScript Hacks Backdoor Access Malware Flooding Data Theft	**No Security Defence** against high professional JavaScript Hacks on Windows Devices **possible**.	**Supercomputer Sandbox Trap** With real-time Malicious JavaScript Injection **Recognition** and **Defence** 
Drive-by Attack Backdoor Access Malware Flooding	**No Security Defence** against high professional JavaScript Hacks on Windows Devices **possible**.	Dto.

SQL Injection Steeling Database Data	**No Security Defence** against high professional SQL Injection Attacks on WEB Servers **possible**	**Supercomputer Sandbox Trap** With real-time SQL Injection **Recognition** and **Defence** 
Cross-Site Scripting Attack Backdoor Access Ransom Demand Data Theft	**No Security Defence** against high professional Cross-Site Scripting Attacks on Windows Devices **possible**.	**Supercomputer Sandbox Trap** With real-time Cross-Site Scripting Attack **Recognition** and **Defence** 
Eavesdropping Attack Backdoor Access	SSL/TLS Encryption	**2 Level Keyless Quantum Secure Data Encryption** 
Macro Viruses Backdoor Access Ransomware	Microsoft Windows Defender On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
File Infectors Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 

Polymorphic Viruses Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Stealth Viruses Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Trojans Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Logic Bombs Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Worms Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 

Droppers Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Ransomware Ransom Demand	**No Security Defence** against high professional JavaScript Hacks on Windows Devices **possible**.	**Supercomputer Sandbox Trap** With real-time Malicious JavaScript Injection **Recognition** and **Defence** 
	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 
Adware Personal Tracking	Adware Cleaner On Billions of Windows/Android/iOS Devices	**Supercomputer Sandbox Trap** With real-time Adware Cleaner **Recognition** and **Defence** 
Spyware Personal Tracking Data Theft	**No Security Defence** against high professional JavaScript Hacks on Windows Devices **possible**.	**Supercomputer Sandbox Trap**  With real-time Malicious JavaScript Injection **Recognition** and **Defence**

AI-Powered Attacks Backdoor Access Data Theft	**No Security Defence** against AI supported malicious Software Injection Hacks on Windows Devices and WEB Servers **possible**.	**Uncrackable biometric Passwords** for System Administrators.  **Supercomputer Sandbox Trap** With real-time Malicious Software Injection **Recognition** and **Defence**  **2 Level Keyless Quantum Secure Data Encryption** 
Infected Email Attachment Backdoor Access Ransomware	Antivirus Scanner On Billions of Windows/Android/iOS Devices	**Central Supercomputer Virus Scanner Recognition** and **Defence** 

HTTP-QuSS - Major Advantages compared to State of the Art

- **Transparent Network Integration** and nothing to change on existing Infrastructure or Devices
- The latest Generation of Supercomputers can serve **Millions of Users Requests** in Real-Time
- All existing Devices and WEB Servers are **at once secured against Cyber Attacks**
- **No Need** and Installation of WEB Server **SSL Certificates** through 2 Level Keyless Quantum Secure Encryption
- **No Need** to install and continuously update **Antivirus Software** on Billions of User Devices
- **No Need** of managing many Internet **User Login Passwords** through unique biometric ID
- **No Need** of Purchasing and Installation of **VPN Software**
- **No Identity Steeling** by **Phishing**
- **Brute-force secure biometric Password** for using HTTP-QUSS Services
- **Cyber Criminals** and **Organisations** can be **identified** and **located**
- **Immediate Location** and **Classification** of **infected WEB Servers**
- **No Spy- and Adware for End Users**
- **Providing End User Privacy** when surfing the WEB
- **Closing** at once **Windows** and **JavaScript** Security **Leaks**
- **Protecting Economy**, **Government** and **Infrastructure** Organisations against **Cyber Attacks** and **related Financial Damages**