NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

SANDHIGUNA

IDNOG

CRYPTOGRAPHIC TOOLS IN WEB SECURITY

FREDERIC EZERMAN PH.D.,

Adjunct Assistant Professor,
Nanyang Technological University,
Singapore

Resident Cryptographer and CEO,
PT. Sandhiguna Widya Proteksi,
Indonesia

IDNOG 8th Conference 2023 | 27 July 2023 | Raffles Hotel Jakarta Ciputra World

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

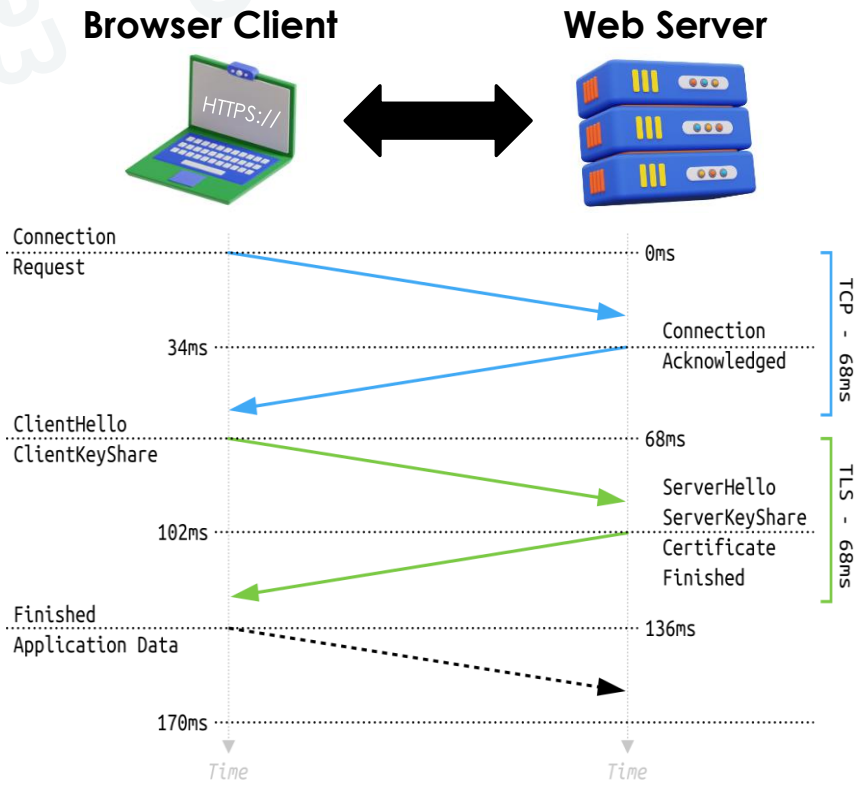
IDNOG

Securing Web Servers

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

SECURING WEB SERVER

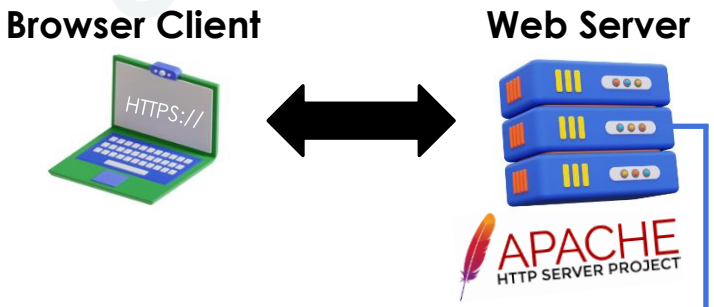
Transport Layer Security (TLS) as a protection layer for HTTP



Full TLS 1.3 Handshake
RFC8446 - The Transport Layer Security (TLS) Protocol Version 1.3

- Cryptography provides powerful algorithms and modules that protect our systems.
- Using **TLS as a protection layer for HTTP is a must**.
- Common practice: Keypairs for the TLS communication are stored and deployed based **solely on access control**.
  - ✓ A malicious administrator has **easy access** to the keypairs.
- Crucial to manage the keypairs in **all** states:
  in storage, in transit, and in use.
  - ✓ Best practice: manage the keypairs in a tamper-resistant Key Management System (KMS).
  - ✓ How? Through **integration** with Hardware Security Module (HSM), portable physical devices, or enterprise-grade KMS.

EXAMPLE: HTTPS CONNECTIONS BY APACHE HTTP SERVER



Apache HTTP Server Configuration for Private Key with .key or .pem format:

SSLCertificateFile /etc/pki/tls/certs/httpd.cr
SSLCertificateKeyFile /etc/pki/tls/private/httpd.key

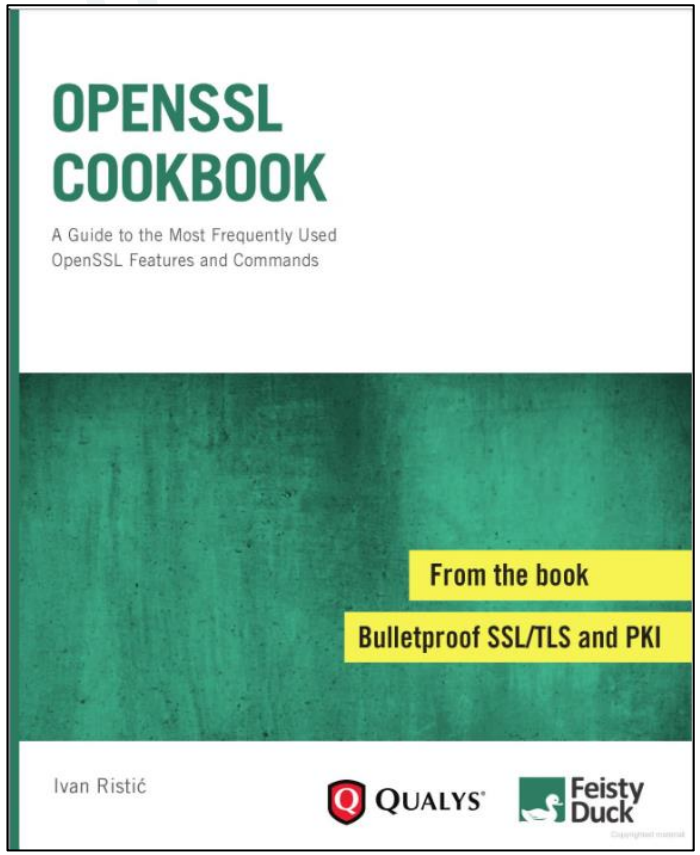
Apache HTTP Server Configuration File for Private Key with .PFX or .P12 format:

SSLCertificateFile /etc/pki/tls/certs/httpd.crt
SSLCertificateKeyFile /etc/pki/tls/private/httpd.key
SSLCertificatePassword cobatanyaadmin

- Apache HTTP Server uses the *apache mod_ssl* module to **secure web connections**.
- Must **prepare a keypair** and sign the certificate; by a CA (Certificate Authority) or self-sign (if browser trusts the self-signed cert).
- Private keys must be **secured but accessible** to the httpd service.
  - ✓ Usually kept in a folder **in the same server**, restricted by AC (Mandatory Access Control) and DAC (Discretionary Access Control).
  - ✓ In **.key or .pem format** configured in /etc/httpd/conf.d/ssl.conf.
- Optionally, private keys are stored **in .PFX or .P12 format** and password-protected.
  - ✓ How to ensure httpd can access the password? Write the **password in cleartext** in the same config file.
  - ✓ Even if the password is stored in a secret management (usually in cloud environment), the private key is used as a **cleartext in server memory**.

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

A COMMON PRACTICE ACKNOWLEDGED AS "NOT TOO SECURE".

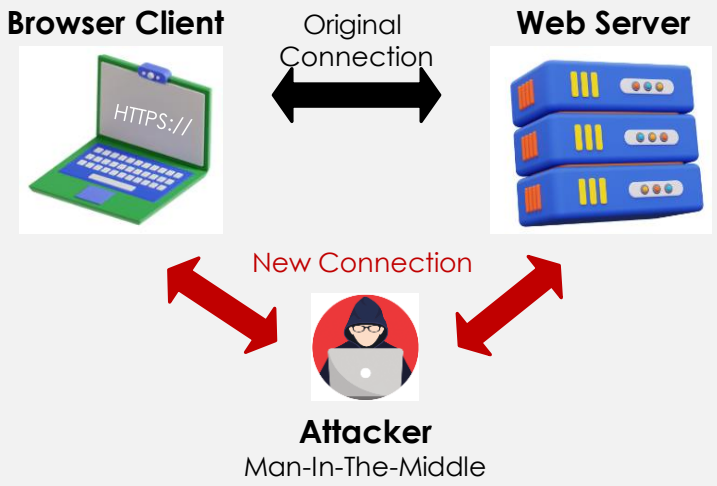


- Ivan Ristić in *OpenSSL Cookbook* (3rd Ed.): On protecting private key with a passphrase:
  "Using a passphrase with a key is optional, but strongly recommended. [...]. In other words, it's all right to keep passphrases on production systems, next to the keys. If you need better security in production, you should invest in a hardware solution."
- In the footnote of explaining about this "hardware solution":
  "A small number of organizations … have very strict security requirements that ***require the private keys to be protected at any cost****. The solution is to invest in a Hardware Security Module (HSM), which is … specifically designed to make key extraction impossible, even with physical access …. To make this work, HSMs not only generate and store keys, but also perform all necessary operations (e.g., signature generation). HSMs are typically very expensive."*
- Thus, storing private key along with the passphrase next to the key is an **insecure common practice**.

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

IMPACTS
WHEN PRIVATE KEY HAS BEEN COMPROMISED

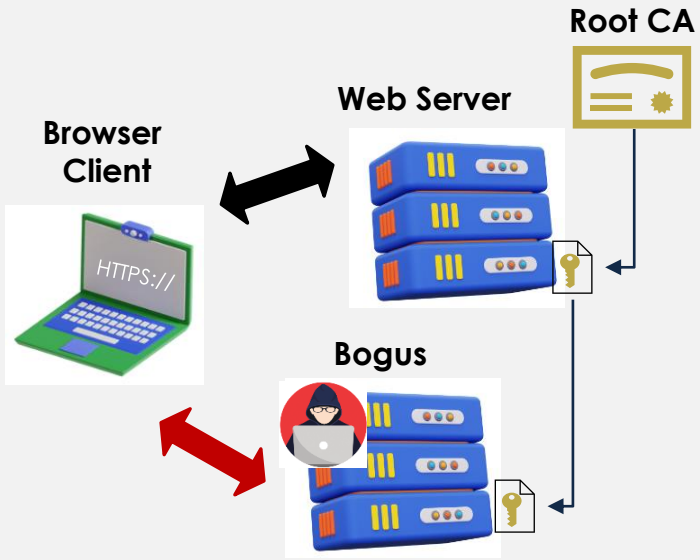
INTEGRITY ATTACK



- An anonymous proxy for man-in-the-middle attack to tamper the data.
- Impersonation attack: attackers pose as known or trusted web servers.

Demo Video

AUTHENTICITY ATTACK



- Create a fake website using compromised private key.
- Remember to trust the certificate to avoid browser showing some warning.

Demo Video

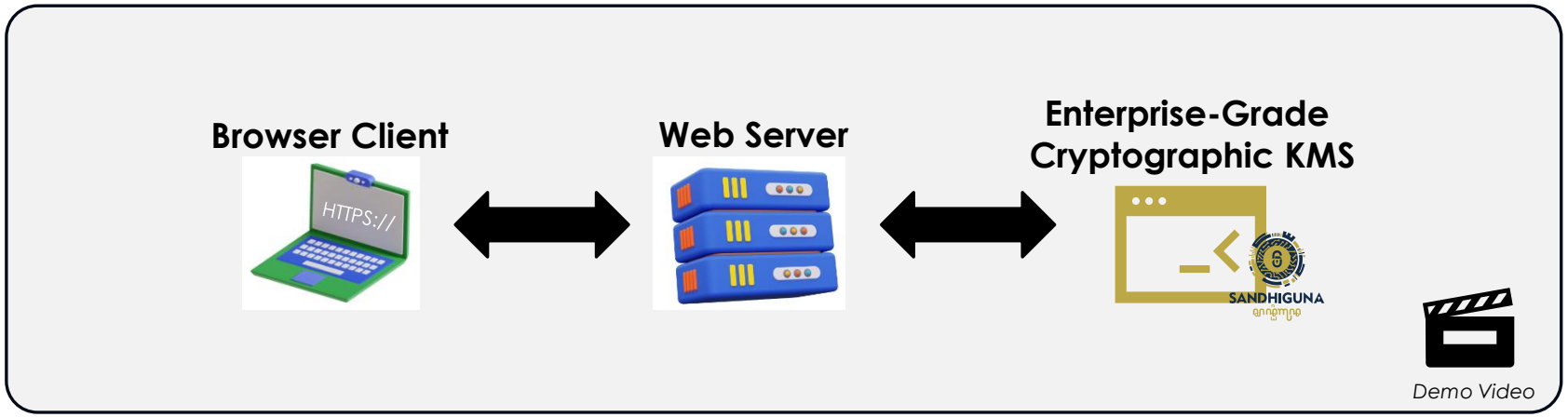
CONFIDENTIALITY ATTACK

- Using *sniffing* and *spoofing* tools, *e.g.*, wireshark, to intercept communication and reveal its content.
- Many web servers still use RSA-based cipher suites, *e.g.*, TLS 1.2, for backward compatibility on the browser or client side.

Demo Video

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

THE 'CURE' FOR ALL PROBLEMS WITH ENTERPRISE-GRADE CRYPTOGRAPHIC KMS



- We have seen that storing private keys in a password-protected PFX/P12 file does not improve security.
- We can **enhance the security by offloading the storage and usage of the private keys to an external cryptoki token**. Example: deploy Enterprise-Grade Cryptographic Key Management System (KMS), utilizing its PKCS#11 connector.
- Such a Cryptographic KMS can also secure application credentials to protect against DNS cache poisoning and to strengthen email servers.

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

IDNOG

Entering Post-Quantum Cryptographic (PQC) Era

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

YOUR ADVERSARY MAY HAVE POWERFUL QUANTUM COMPUTER, BUT YOU DON'T

Picture the following Scenario:

Soon enough, you may be in a situation, where

- **Your systems, *e.g.*, public key infrastructure (PKI), rely heavily on:**
  - ✓ **RSA**-based Cryptosystem and **Elliptic Curve** Cryptosystems for public key encryption and signing,
- **You have adversaries that can carry out large-scale quantum attacks on your security system.**

By Then

- **TLS handshaking and Diffie Hellman Key Exchange Protocols, for examples, are vulnerable**
- **The backbone of our internet communication is already exposed to the "HARVEST-AND-DECRYPT-LATER Attacks"**
- **Equipped with the right quantum tools, attackers, who may not be able to access webservers directly, can forge the signatures**
- **But you have NO ACCESS to quantum computer. You can only rely on digital computers to secure your assets.**

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

HOW LARGE-SCALE QUANTUM PROCESSORS AFFECT EXISTING CRYPTOGRAPHY

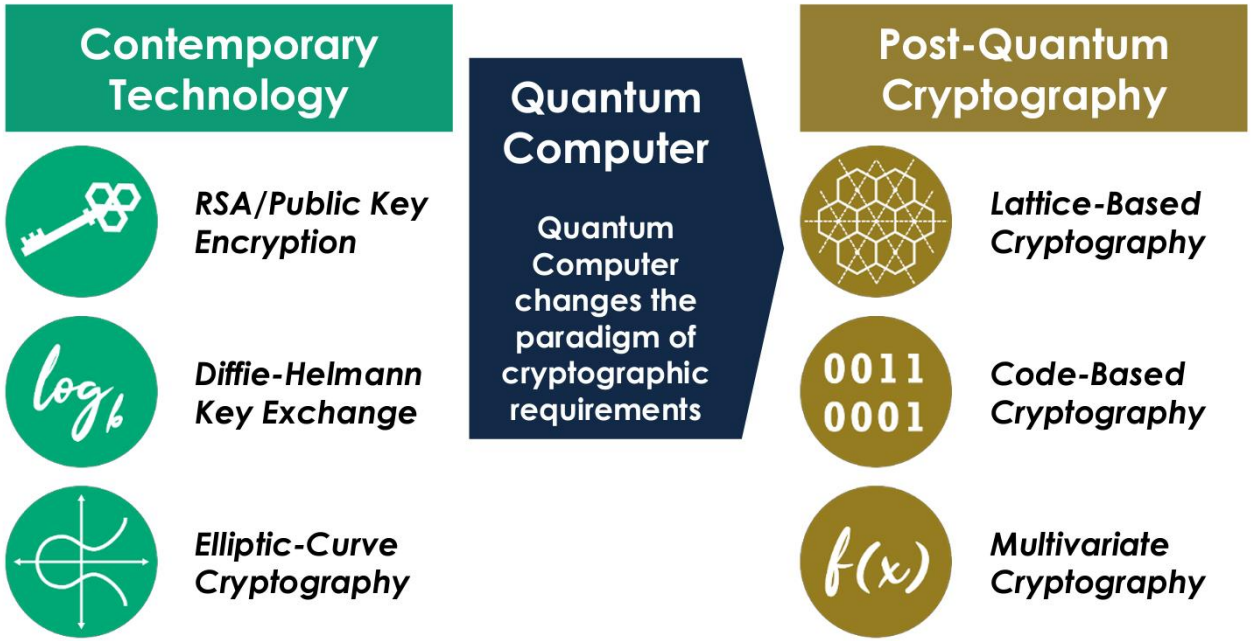
Table 1 | Examples of widely deployed cryptographic systems and their conjectured security levels

Name	Function	Pre-quantum security level	Post-quantum security level
Symmetric cryptography			
AES-128[8]	Symmetric encryption	128	64 (Grover)
AES-256[8]	Symmetric encryption	256	128 (Grover)
Salsa20[58]	Symmetric encryption	256	128 (Grover)
GMAC[59]	MAC	128	128 (no impact)
Poly1305[60]	MAC	128	128 (no impact)
SHA-256[61]	Hash function	256	128 (Grover)
SHA3-256[62]	Hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072[1]	Encryption	128	Broken (Shor)
RSA-3072[1]	Signature	128	Broken (Shor)
DH-3072[42]	Key exchange	128	Broken (Shor)
DSA-3072[63,64]	Signature	128	Broken (Shor)
256-bit ECDH[4–6]	Key exchange	128	Broken (Shor)
256-bit ECDSA[66,67]	Signature	128	Broken (Shor)

Security levels shown are against the best pre-quantum and post-quantum attacks known. Security level *b* means that the best attacks use approximately 2^b operations. This optimization ignores parallelization requirements; see text for discussion of the impact of such requirements. For hash functions, 'security' in this table refers to pre-image security.

Table reproduced from Nature volume 549, page 189, Sep 2017

How worldwide cryptographic community has been preparing to defeat quantum attacks

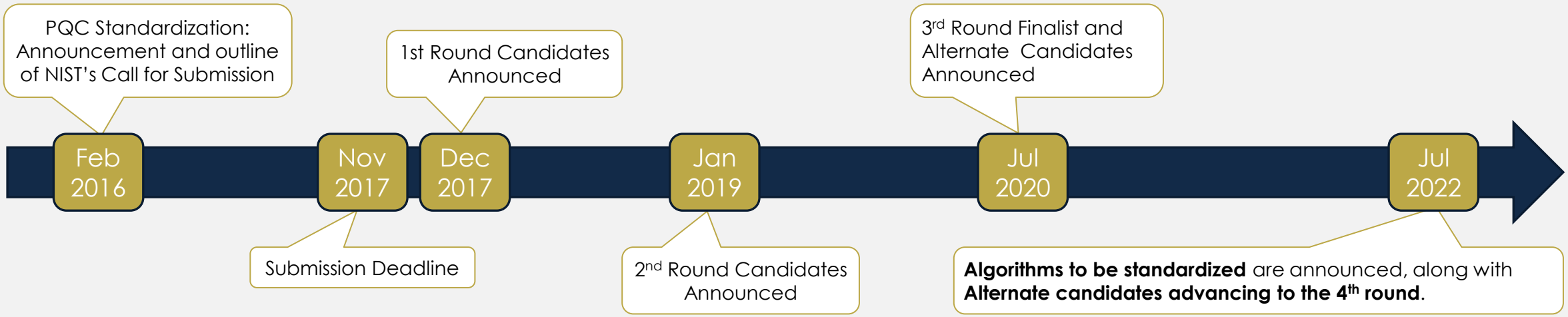


NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NIST POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION PROCESS

NIST Internal Report 8413 Update 1, 26 September 2022

Timeline of the NIST Post-Quantum Cryptography (PQC) Standardization Process



Algorithms to be Standardized	
Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS+

Candidate Advancing to The Fourth Round	
Public-Key Encryption/KEMs	**Digital Signatures**
BIKE	
Classic McEliece	
HQC	
~~SIKE~~	

August 2022
BROKEN ; Attack :
Complete Key Recovery

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

WHAT WE HAVE RIGHT NOW IN INDONESIA

- **We HAVE TO get ready: Large-Scale Quantum Computers can be ready anytime, if not already but kept secret.**

- **BSSN is including the new quantum-secure algorithms from the NIST PQC Standard in the list of approved algorithms for Indonesia, including for use in protecting Strategic Electronic Systems**

- **Sandhiguna Key Management System (SG-KMS) is incorporating quantum-secure modules:**
  1. **CRYSTALS-KYBER** to replace **RSA** and **ECDH**
  2. **CRYSTALS-Dilithium**, **SPHINCS+** and **FALCON** to replace **RSA Signing** and **ECDSA**

THANK YOU