acsd applied cyber security darmstadt

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

fbi FACULTY OF COMPUTER SCIENCE

EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

UCS USER-CENTERED SECURITY

Towards Crypto-Agility Assessment and Cryptographic Migration

Introducing the Crypto-Agility Maturity Model (CAMM)
the PQC Migration Management Process (PMMP)
and the Crypto-Detection Tool (CDT)

Nouri Alnahawi - Johanna Henrich - Nicolai Schmitt - OpenRheinMain - 22.09.2023

Overview

Introduction

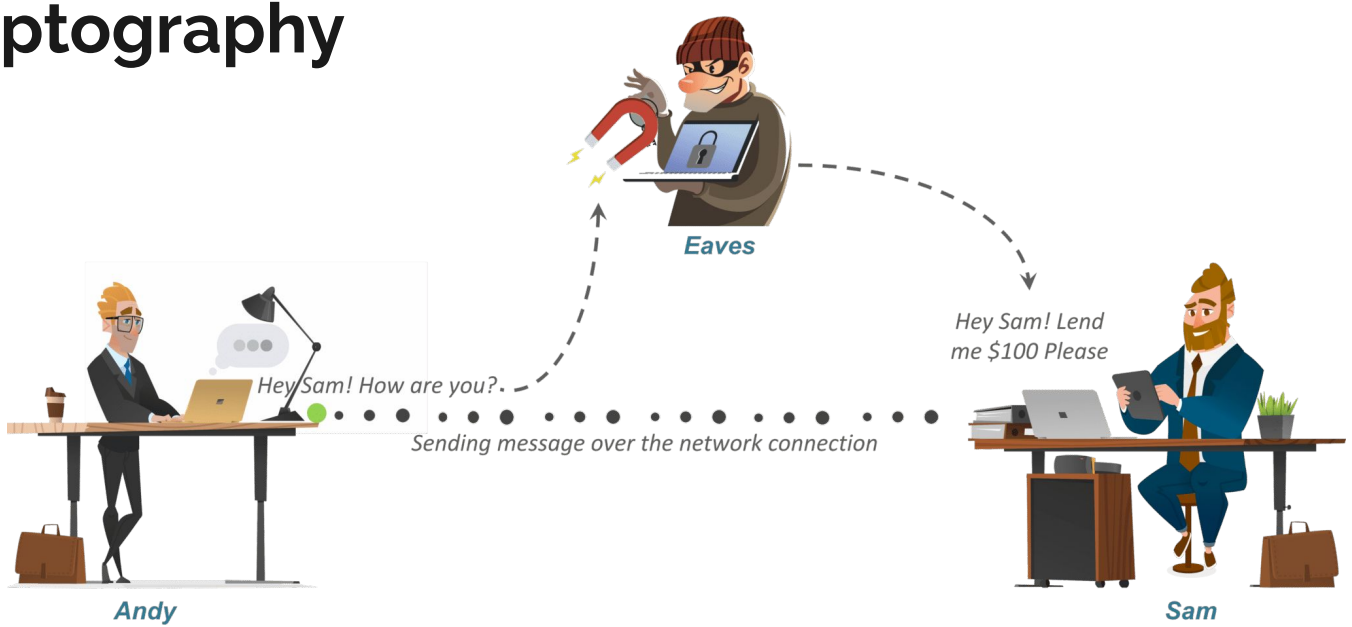
Problem (Migration to PQC)

Solution:

CAMM: Define different levels of crypto-agility (CA)
PMMP: Migration process that supports reaching different levels of CA
CDT: Set of tools to support compiling a cryptographic inventory

Conclusion & Outlook

Cryptography



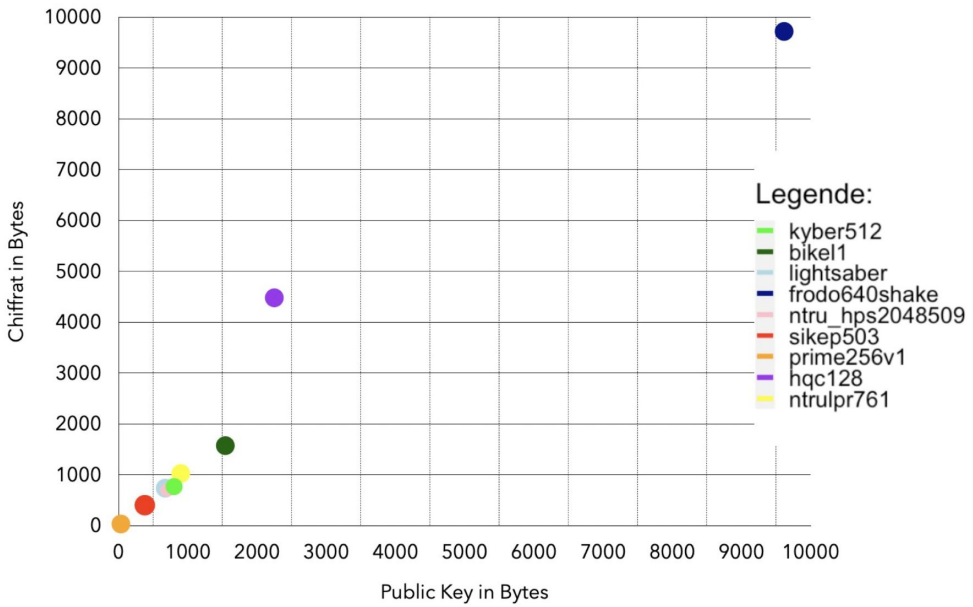
Source: https://www.edureka.co/blog/what-is-cryptography/ *(accessed 2023-09-01)*

Quantum Threat to Classical Crypto

Crypto alg.	Type	Usage	QC alg.	Effect
AES	Symmetric	Encryption	Grover	Larger keys needed
SHA-2, SHA-3	—----------	hash	Grover	Larger output needed
RSA	Asymmetric	Sign & KEX	Shor	Insecure
Elliptic curves (ECDSA, ECDH)	Asymmetric	Sign & KEX	Shor	Insecure
Finite Fields (DSA)	Asymmetric	Sign & KEX	Shor	Insecure

Adapted from Chen et al., 2016 [1]

Post-Quantum Cryptography as Replacement For Classical Crypto [5]

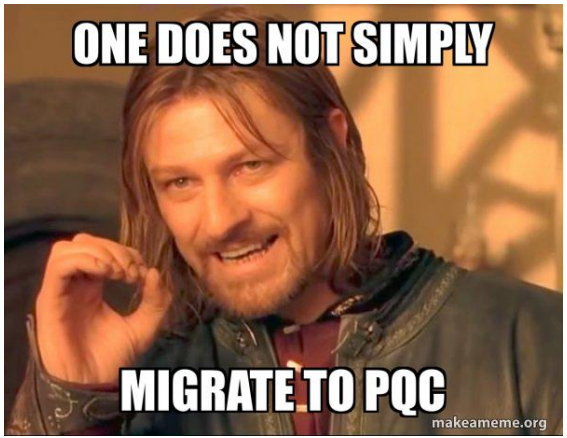


Migration to Post-Quantum Cryptography

- Drop-in replacement of algs. not always possible
- PQC algorithms pose new requirements
- PQC algorithms may differ in design and usage
- Certain systems cannot be upgraded
- Many systems are connected to other systems

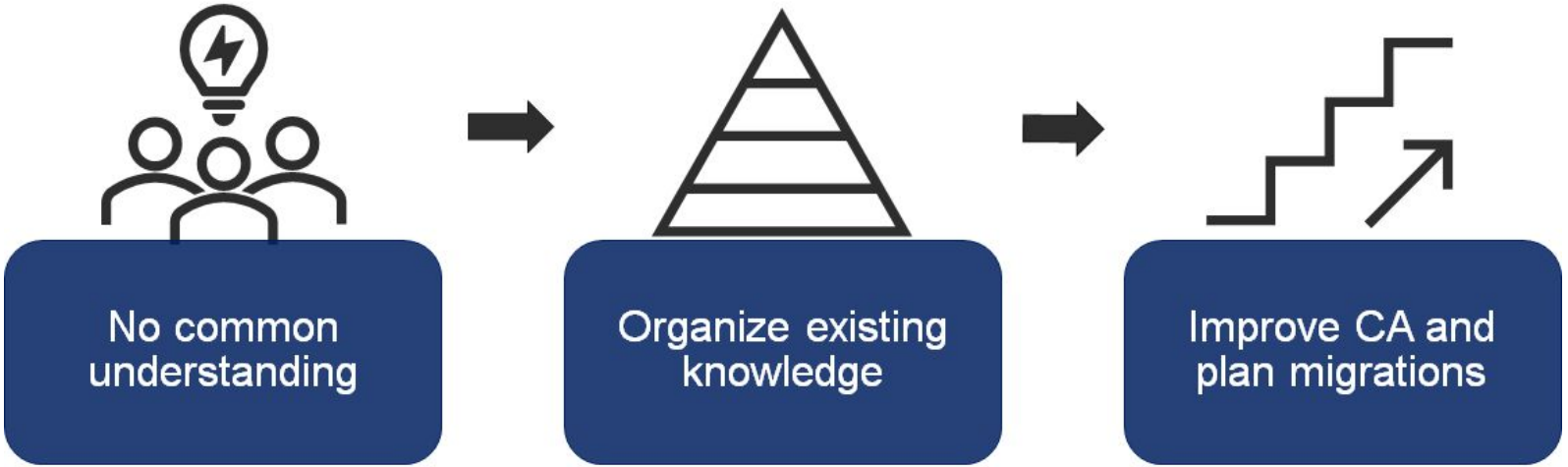
Where and How to start?

Problem cryptographic agility & planned migration



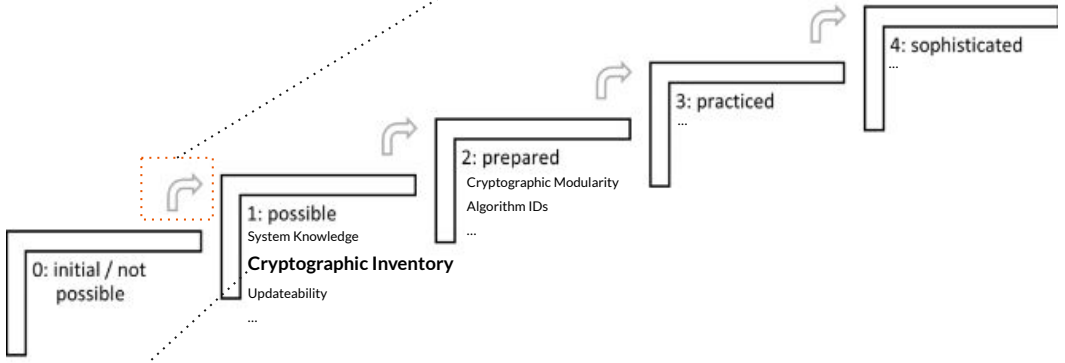
- **IT landscapes lack cryptographic agility**
- **No holistic understanding of deployed cryptography**
- **Cryptographic migrations are complex and take time**

Approach cryptographic agility & planned migration



Solution Overview

PMMP: Defines process to reach next level



CAMM: Defines multiple levels of Crypto-Agility

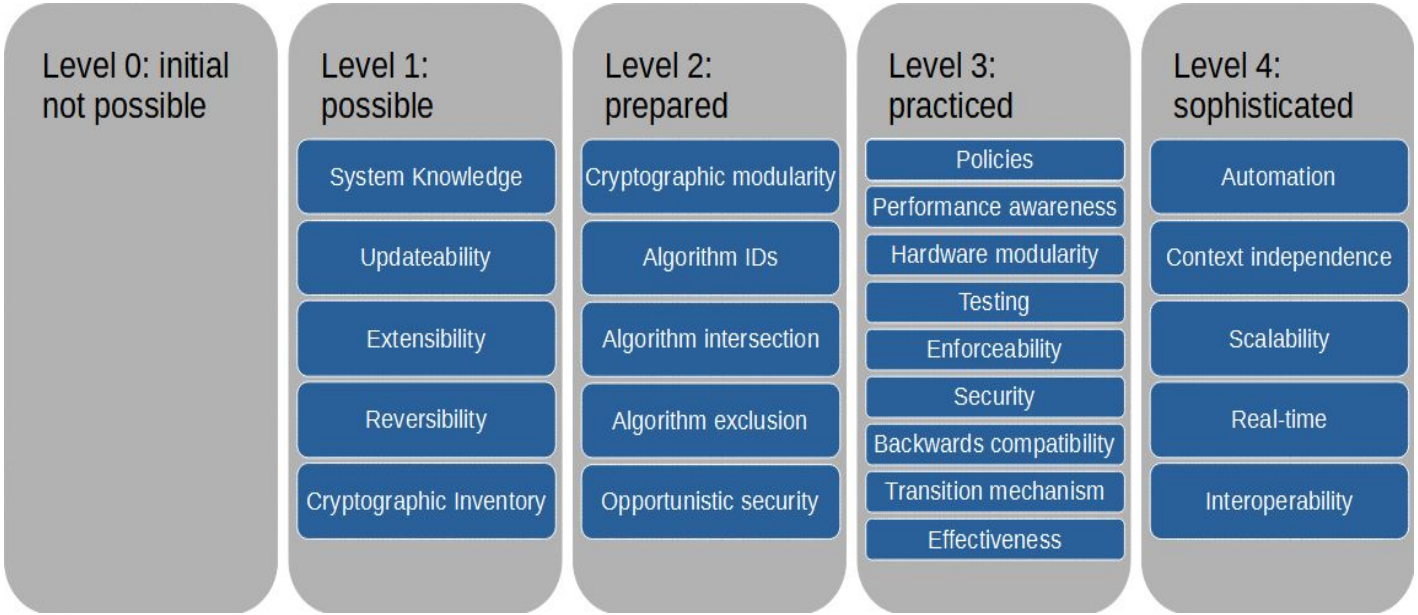
CDT: Approach to support compiling a Crypto-Inventory

Cryptographic Agility Maturity Model (CAMM)

J. Hohm, A. Heinemann & A. Wiesmaier [2]

- Map definitions, requirements & aspects onto maturity model
- First CA related model (to the best of our knowledge)
- Assessing the crypto-agility of a given software or IT landscape
- Five maturity levels and twenty-five requirements over the five levels

CAMM Levels and Requirements



CAMM Requirement Example

No 1.4

ID	1.4
Name	Cryptography inventory
Description	The cryptographic functions used are documented and their current security level is known.
Category	Knowledge
Problem	In order to assess whether the system is affected by known vulnerabilities in certain cryptography variants, there must be an overview of the cryptography implementations used.
Acceptance	A listing of the cryptographic methods used, their parameters and intended use is available, and current developments and recommendations for action on cyber security are observed.
Dependency	1.0
Source	Kreutzer et al. 2018 Horvath and Mahdi 2017
Example	Inventory as a table with table with the following information: cryptography methods, primitives used, key length, purpose of use, security level, date of deployment, date of deactivation. Trends and developments in cryptographic security are tracked at conferences and in related publications.

Bridging the Gap!

- CAMM measures CA in IT systems
- How to establish the desired level of CA?

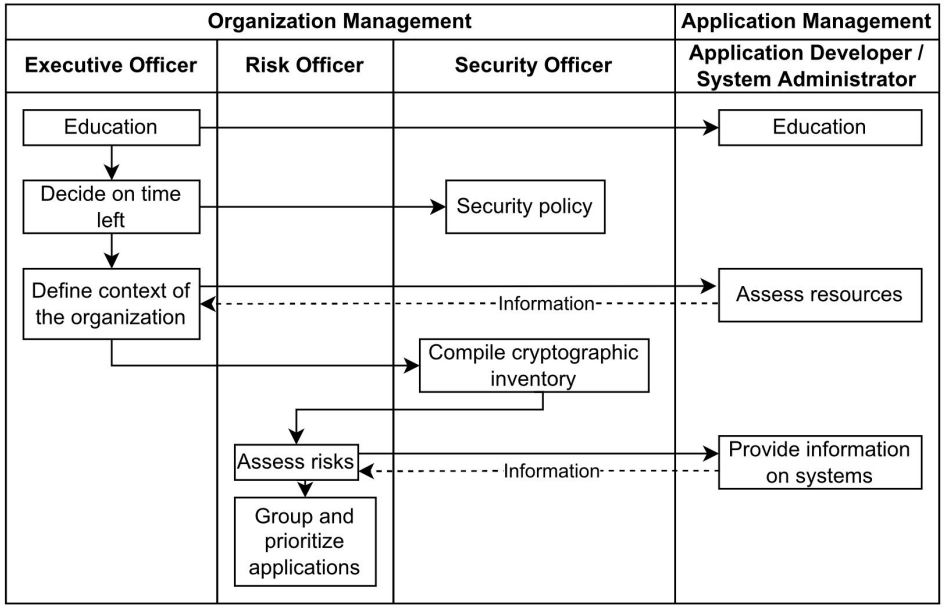
Manageable and implementable process ⟶ PMMP

PQC Migration Management Process (PMMP)

N. von Nethen, A. Wiesmaier, N. Alnahawi & J. Henrich [4]

- Inspired by previous migrations (Y2K-Bug)
- Risk-based approach
- Integrates into ISO 27001 ISMS
- Features interim incremental states
- Defines processes for reaching the different levels of CAMM organization-wide

PMMP Framework



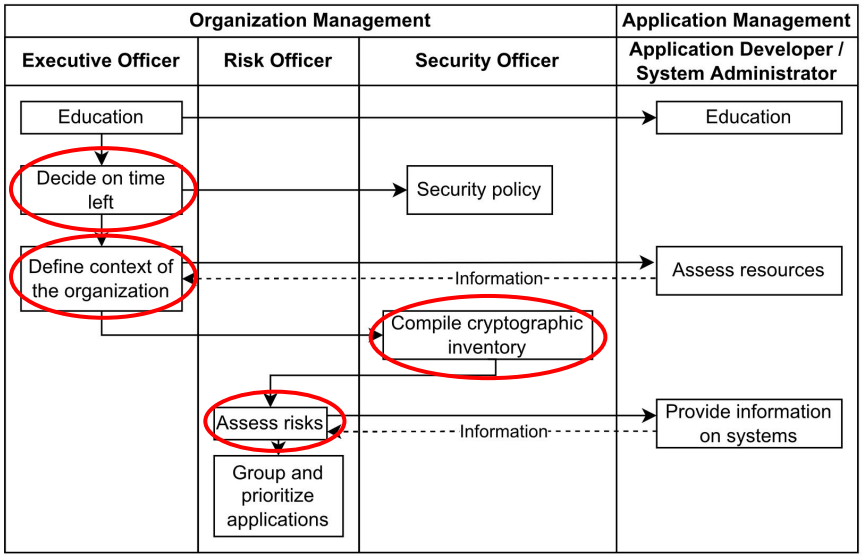
OK! Let's migrate, I guess...

PMMP Requirements

- **Timeline**
- **Completeness**
- **Context awareness**
- **Interoperability and availability**
- **Interim results (increments)**
- **Crypto-Inventory**

PMMP Step by Step

1. Educate decision makers
2. **Decide on timeline of quantum threat**
3. Define or change security policies
4. **Define context of the organization**
5. **Compile cryptographic inventory**
6. **Assess current cryptographic risks**
7. Group and prioritize systems
8. Ensure system compatibility and triage



Assess Cryptographic Risks

Precondition: Quantum computers are a real threat to assets of the organization.

Example: SSH access to Webserver only from inside the organization's network and under surveillance with session recording. Intruders would be instantly detected. Potential damage is high. Risk is medium.

Example 2: Loadbalancer connections to customers use EC 256-P certificate to establish TLS connection. Attacker could intercept connections and impersonate customers by reusing login-data. Attack would not necessarily be detected, potential damage is high. Risk is high.

→ How do I know which crypto I'm using anyway?

Compile Cryptographic Inventory

- Basis for identifying potential threats and assessing possible risks
- Use automatic detection tools where possible
- Complex (and distributed) dependencies need special attention (e.g. PKI, SSH keys etc.)

Compile Cryptographic Inventory (Example)

Application	Type of data	Used algorithm
Loadbalancer for Internet-facing webservers	Login data of customers	TLS 1.3 - AES-GCM 128bit, SHA256
Loadbalancer Certificate	Certificate	EC P-256
Webserver F2A1S	SSH key	RSA 2048bit
Root Certificate CA	Certificate	RSA 4096bit

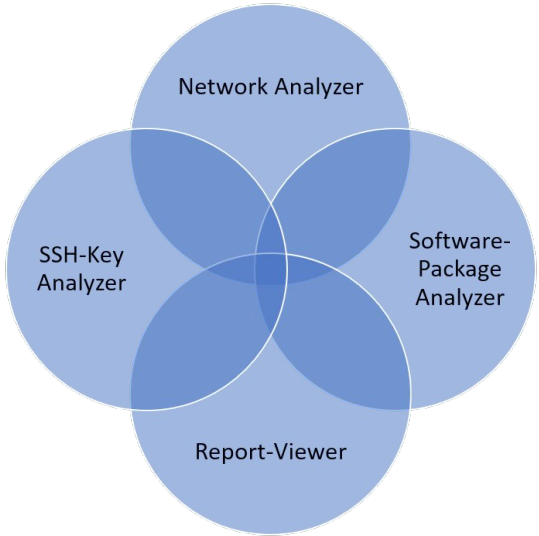
Crypto-Detection Tool (CDT)

N. Schmitt, D. Heinz, J. Henrich, N. Alnahawi & A. Wiesmaier

- An approach to help administrators compiling a crypto-inventory
- Prototype, work in progress
- Following the linux-philosophy, one tool per task: 4 individual task-specific tools
- Planned to go open-source this year

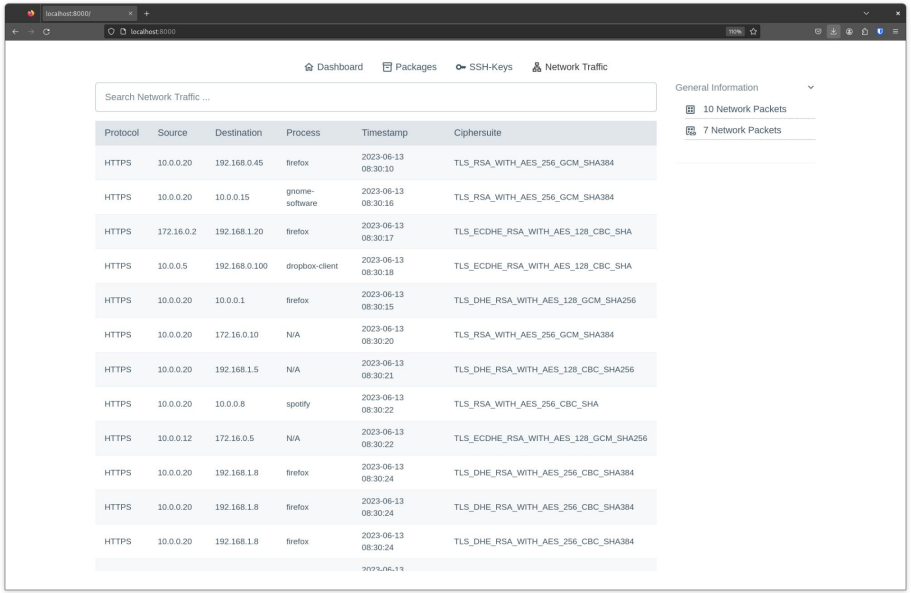
Crypto-Detection Tool (CDT) Strategies & Tools

- Analyzing network-traffic
  - Cryptography used in TLS handshakes
  - Local application owning a socket
- Analyzing installed software-packages on linux-systems
  - Supports apt[1]
  - Recursive evaluation
- Analyzing cryptographic key-material stored on disk
  - SSH-Keys
- Report-Viewer
  - Visualize reports

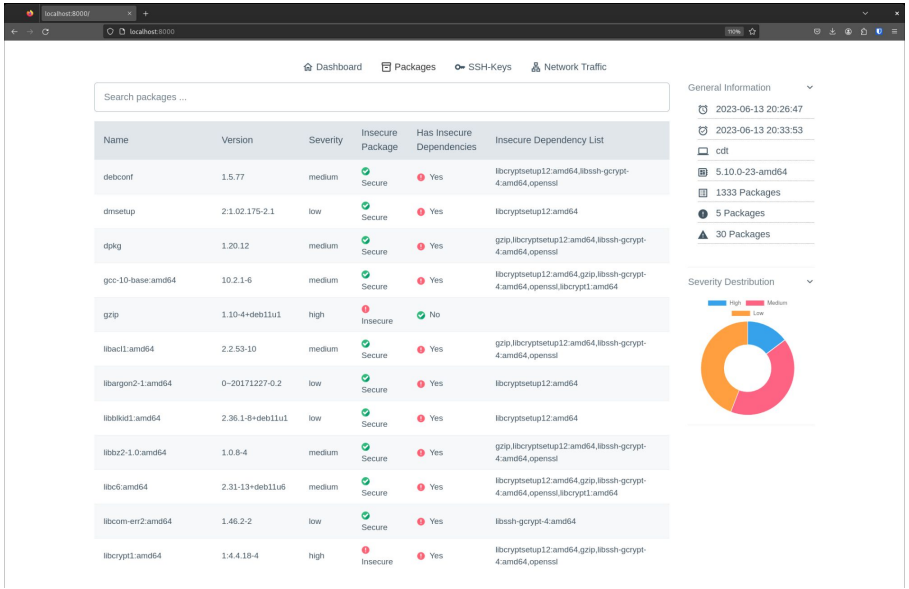


1: https://ubuntu.com/server/docs/package-management

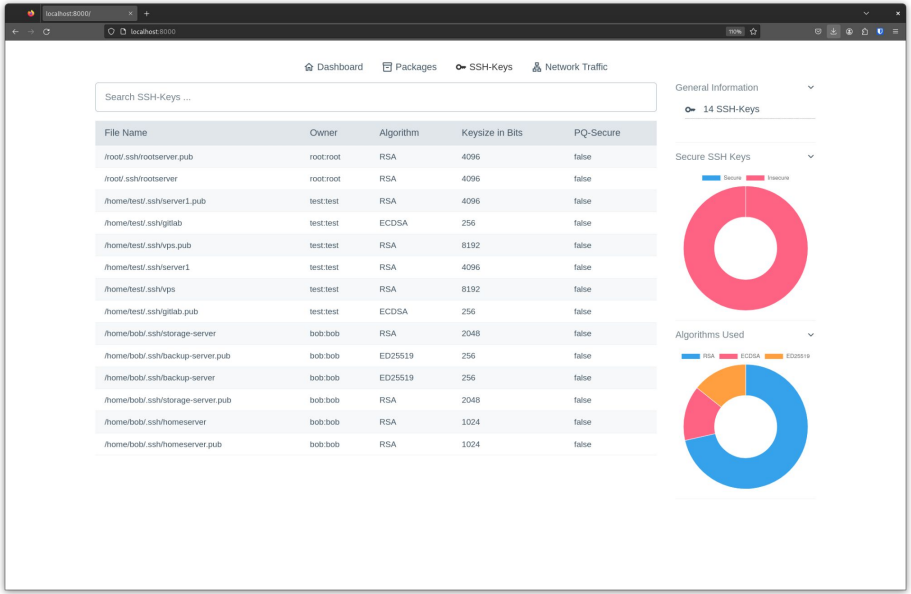
Crypto-Detection Tool (CDT) Report-Viewer



Crypto-Detection Tool (CDT) Report-Viewer



Crypto-Detection Tool (CDT) Report-Viewer



Conclusion & (Outlook)

- CA and managed migration come with some overhead
- CA provides ability to repetitively react to necessary cryptographic migrations
- CAMM and PMMP support establishing CA and migrating to PQC
  - Apply to existing IT systems and get feedback from organizations
  - Develop tools to support automated assessment
- Integrate PMMP into existing ISO standards
- Crypto-Inventory is prerequisite for CA and migration

Links

CAMM: https://camm.h-da.io/

PMMP: https://arxiv.org/abs/2301.04491

CDT: Publication in progress

Literature

1. L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner und D. Smith-Tone. *Report on post-quantum cryptography*. Bd. 12. US Department of Commerce, National Institute of Standards und Technology, 2016.
2. J. Hohm, A. Heinemann, and A. Wiesmaier. Towards a maturity model for crypto-agility assessment. 15th International Symposium on Foundations & Practice of Security (FPS). Springer, 2022.
3. J. Becker, R. Knackstedt and J. Pöppelbuß. Developing Maturity Models for IT Management. *Bus. Inf. Syst. Eng.* 1, 213–222. 2009. https://doi.org/10.1007/s12599-009-0044-5 (last accessed 21.09.2023).
4. N. von Nethen, A. Wiesmaier, O. Weissmann, and N. Alnahawi. Managing the Migration to Post-QuantumCryptography. Submitted to ACNS'23, 2023. Preprint: https://arxiv.org/abs/2301.04491.
5. J. Henrich. Performanz Evaluation von PQC in TLS 1.3 unter variierenden Netzwerkcharakteristiken. Preprint: https://arxiv.org/pdf/2303.15148.pdf (last accessed 21.09.2023).

Thank You for Your Attention!

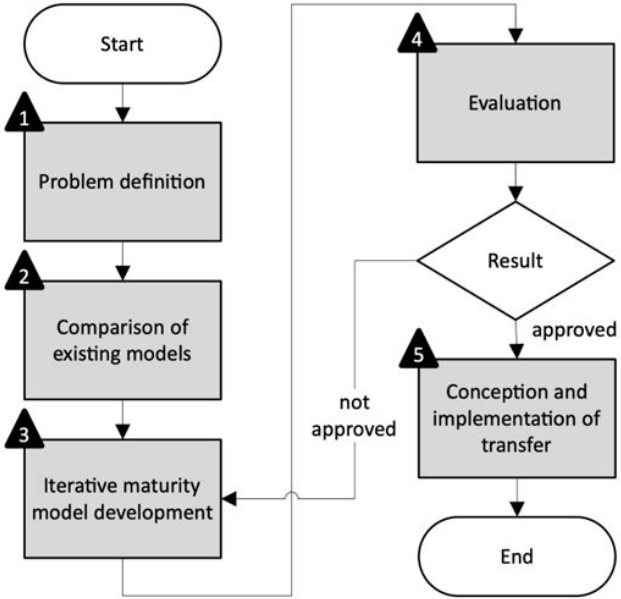
acsd applied cyber security darmstadt

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

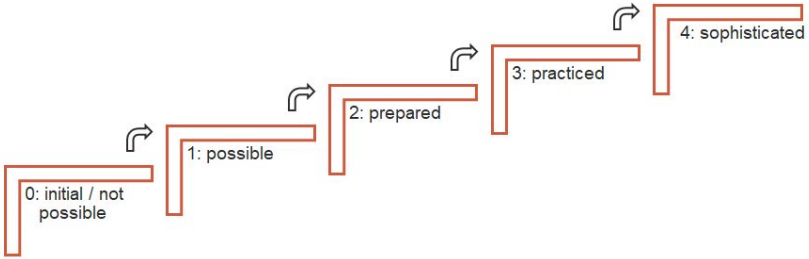
UCS
USER-CENTERED SECURITY

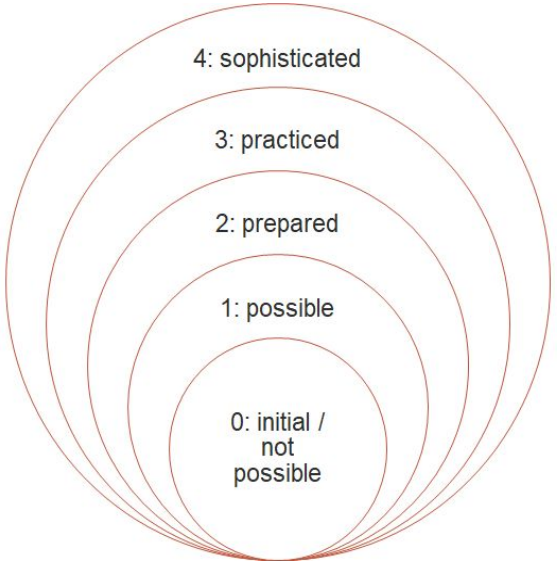
CAMM Development Approach



Adapted from Becker et al., 2009 [3]

CAMM Maturity Model





CAMM Outlook

- Apply to existing IT systems and get feedback from organizations
- Add weights to requirements
- Develop tools to support CA (automated) assessment

Define Context of the Organization

- Define the scope of the migration
- Stakeholders and partners
  - Who wants us to migrate?
  - Who do we want to migrate?
- Compile inventory of communication partners
  - With who do we communicate?
  - Where are our interfaces?
- Gather available resources in the organization and understand systems
  - Do we have enough knowledge and developers?
  - Are our systems powerful enough for PQC?

Agree on Timeline of Quantum Threat

- Unsure when quantum computers will become a threat
- Prioritize applications and business processes
- Consult estimates of authorities like BSI or NIST

“We think quantum computers will become a threat to our organization in 2030.”

PMMP Completeness

- All relevant systems have to be considered
- Detect relevant systems
- If a system is left behind, communication stops

PMMP Context Awareness

Stakeholders and communication partners

- One cannot migrate alone
- Understand context of the organization

Resources

- Acquire additional resources (education, hardware)
- Assess organization resources

PMMP Interoperability

- Ensure intended business processes functionalities
- Do not interrupt the business
- Forward/backward compatibilty