KAZ
HACK
STAN

DHIS2

Building Security And Trust For An Open-Source Project

Michael Markevich

Michael Markevich

Who Am I

KAZ HACK STAN

> Security lead for the DHIS2 project, advisor, and academic lecturer

> Ex-CISO at Opera (Nasdaq:OPRA), Ulmart (now defunct), and GGA (an EPAM company)

> Sysadmin, penetration tester, IT auditor, security manager (ages ago)

What Are We Doing Here Today?

> Context: an overview of DHIS2 software and organization

> Public goods, core values, and security of open-source software

> Threat landscape and typical security design challenges

> Our security processes, practices and tools

DHIS2

An intro to the digital health world

KAZ HACK STAN

What Is DHIS2?

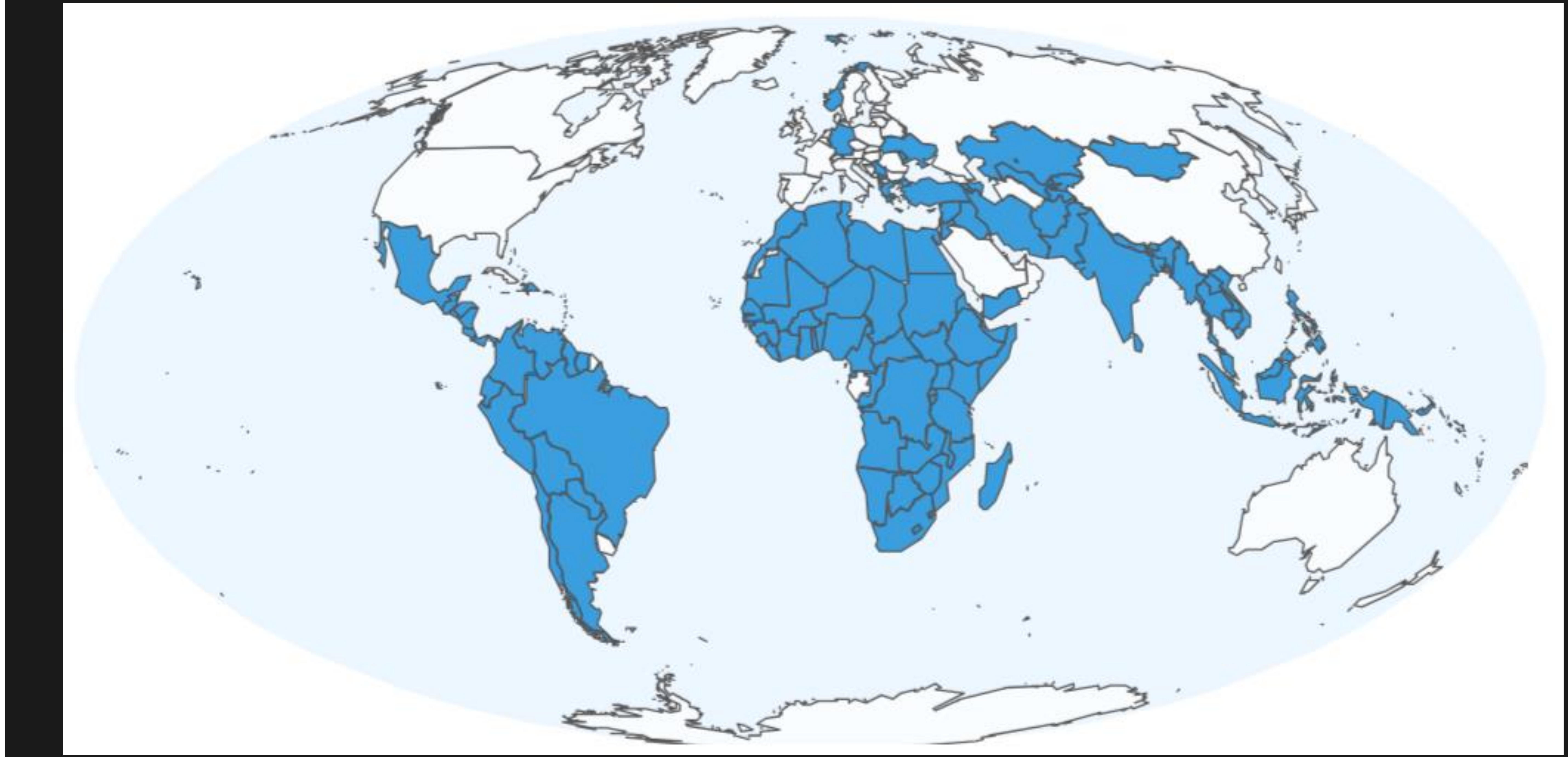
> DHIS2 (District Health Information System, version two) is an open-source software for capture, management, and analysis of data.

> The software is used for statistical and reporting purposes, scientific research, and collecting and managing personal data records.

> Supported data domains are health, education, logistics, and climate.

> DHIS2 has been developed at the University of Oslo since 2008.

The Scale



DHIS2 runs on thousands of instances in 129 countries with population of 3.2 billion people.

Tech Facts

> Written in Java (backend) and JavaScript (frontend)

> Runs on Tomcat with PostgreSQL as a database

> Has a companion Android application (Tracker, 100K+ downloads on Google Play)

> 585K lines of (Java) code

> 289 stars on GitHub (https://github.com/dhis2)

Our Team

> Headquartered in Oslo (but 100% remote)

> Has a board of sponsors (representatives of funding organizations)

> Has a board of project leads (strategic and operational management)

> Overall team size: more than 110 (~70 of them software engineers)

> Security team: 3 staff members and 5 security champions

Public Goods

What do they have to do with cyber?

KAZ HACK STAN

Public Goods

A public good is a commodity or service provided without profit to all members of a society (either by the government or by a private individual or organization).

A public good is always:
> Non-excludable
> Non-rivalrous

Cybersecurity is a public good in an information society.

Digital Public Goods

Digital public goods are generally free cultural works in the form of software, data sets, AI models, standards, or content.

Many open-source software projects (including DHIS2) are recognized as digital public goods.

Cybersecurity and ESG

Lack of cybersecurity (in digital public goods or any services using them) may have a critical social impact.

The ESG (Environmental, Social, and Governance) dimension adds social risks associated with security breaches or the unavailability of public goods.

Global Uncertainty

A deeper look at the DHIS2 security context

KAZ HACK STAN

Threat Landscape /1

Common for all open-source software:

> From the "vendor" perspective, we don't know (the majority of) our users

> Everyone can access and study (or hack) the code

Threat Landscape /2

Specific to DHIS2:

> Many deployments process high-risk data

> Most of the deployments are not at the bleeding edge of technology

Typical Design Topics

> How do we identify users who don't have government-issued IDs?

> How can privacy consent be obtained from customers with low literacy?

> How should we make a mobile application work in areas without data network coverage?

> How can data be securely kept (or destroyed) in case of civil unrest or revolution?

Ethical Software

Ethical considerations can impact security design decisions.

For example, should we implement biometric authentication in DHIS2 or defer it to third-party providers?

Security Architecture

×××

KAZ HACK STAN

Maintaining a broad context when planning security features for the product is extremely important in the open-source world.

For example, should we implement identity management (or mobile device management) functionality in DHIS2 or rely on external parties?

Privacy Design

How do we implement contradicting privacy requirements?

For example, how should cross-border personal data transfers work in case of tracking health of nomadic populations in sub-Saharan Africa?

Back To Security

Highlights of the
DHIS2 security program

KAZ
HACK
STAN

Security Principles

> Secure by default (ideally like OpenBSD)

> Adherence to open standards in software development (like OWASP)

> Reference deployment scenarios (standalone, LXC, Docker, Kubernetes)

> Capacity building (training for implementers) and community support

> Transparency and trust

Security Processes

Vulnerability management: avoid disclosure of security issues in public repositories and carefully coordinate disclosure timeline.

Incident response: we don't maintain any production systems, but we still have a moral responsibility to support implementers in trouble.

Security Tools

> Prefer open-source tools and utilities for internal use (OWASP ZAP, Semgrep OSS, Schemathesis, Sonarqube)

> Create security tools that can be used and enhanced by the community (dhis2-tools)

Transparency and Trust

> Website pages explaining security features and trust policies

> Public SAST dashboard

> Public security audits

> Vulnerability and feedback reporting channel

THANK YOU!

KAZ
HACK
STAN

ЦАРКА
ЦЕНТР АНАЛИЗА И РАССЛЕДОВАНИЯ КИБЕР АТАК

FREEDOM
HOLDING CORP.

Служба
Государственной
Охраны

Комитет
по информационной
безопасности
МЦРИАП РК