



Sicherheit²

Das Zusammenspiel von Safety & Security im Fokus der Kryptoagilität

Karolin Varner & Wanja Zaeske
<https://rosenpass.eu>

Der Plan



1. **Wir stellen uns vor**
2. **Safety & Security: Kulturelle Aspekte**
3. **Kryptografie und Avionik im Dialog**
4. **Kryptoagilität als Prozess**



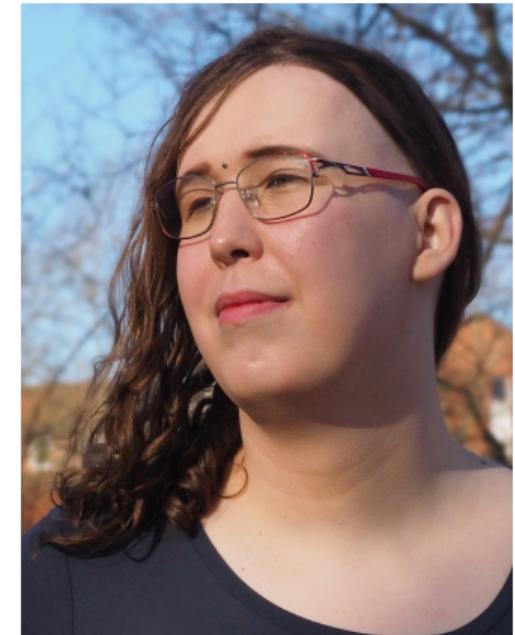
Zum mitschauen:

[github.com/rosenpass/slides/blob/main/ 2025-05-15-cast/slides.pdf](https://github.com/rosenpass/slides/blob/main/2025-05-15-cast/slides.pdf)

Karolin Varner



- Softwareentwicklerin & Kryptografin
- 11 Jahre in der Industrie bei Startups und Konzernen
- Seit 2024 am Max Planck Institut für Sicherheit und
Privatsphäre
- Initiatorin & Leiterin des Rosenpass e. V.
- Arbeit an weiteren Projekten wie zum Beispiel der X-Wing
KEM



Wanja Zaeske



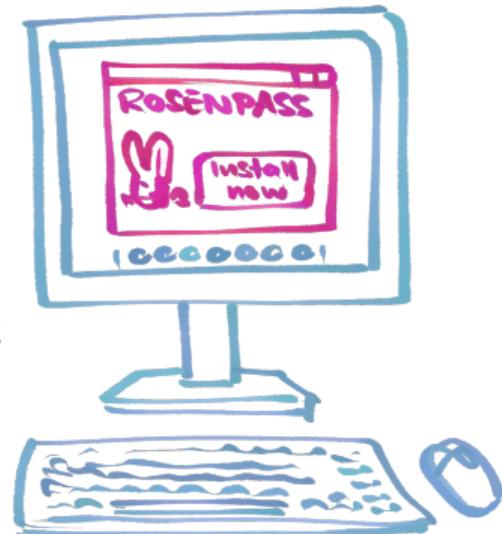
- Researcher & Softwareentwickler
- 4 Jahre Forschung in Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Schwerpunkte: Moderne Softwaretechnologien in die Avionik bringen
- Rosenpass Mitgründer

Rosenpass e.V.



- 2023 gegründet zur Betreuung des gleichnamigen Projekts
- Absicherung von WireGuard gegen Attacken durch Quantencomputern mittels Protokol-Level Hybridisierung
- Institution für Translationsforschung in der Kryptografie
- Schnittstelle zwischen Forschung, Industrie und Gesellschaft schaffen

rosenpass.eu



Safety & Security

Kulturelle Aspekte



Safety & Security: Unterschiede

Safety

- Zufällige Fehler
- Systemausfall kann tödlich sein
- Stabile Zieldefinition: Physik bleibt gleich
- Abgehängene Software -> Stabile Software!
- Rigitte Validierungsprozesse

Security

- Intelligente Angreifer
- Im Fehlerfall: Lieber das System stoppen
- Zieldefinition ist in Bewegung: Angreifer lernen auch dazu
- Abgehängene Software -> CVEs bekannt?
- Viele Freiheitsgrade in Validierung

Safety & Security: Gemeinsamkeiten



- Hohes Zuverlässigkeit nötig
- Analyse von Softwaresystemen in reeller Hardware
- Rigorose Validierungsprozesse
- -> Gesetzliche Anforderungen verpflichten zur Mittelmäßigkeit
- Dokumentation von Systemzielen ist sehr wertvoll

Akzeptanzkriterien

- Safety
 - Requirements-getriebenes Testen
 - "Proven in use"
 - Formale Verifikation
- Security
 - "Proven in use" reicht nicht, aber neuen Verfahren wird dennoch misstraut
 - Testen unzureichend, aufgrund gezielter Angriffe
 - Formale Verifikation ist der Goldweg
 - Security kann nicht so argumentiert werden, der goldene Weg ist die formale Verifizierung
- Redundanz um Ansprüche an Einzelkomponenten zu senken
- Unabhängiges Review

Safety- & Securitykultur



- Safety
 - Menschen Sterben bei Versagen
 - Probleme sind Verstanden und Stabil
 - => Konservative Ingenieurskultur
- Security
 - Versagen erzeugt eher Finanziellen Schaden
 - Problemtypen sind dynamisch und ändern sich dauernd
 - => Progressive Ingenieurskultur

Kryptografie und Avionik im Dialog

Die Vier Domänen der Sicherheit sind...



Luftfahrt

Automobile

Medizintechnik

Automatisierung

Zum erschrecken aller...



...wird in der Luftfahrt heutzutage keine sichere Kryptografie eingesetzt.

Zum erschrecken aller...



...wird in der Luftfahrt heutzutage keine sichere Kryptografie eingesetzt.

Der eine Ernstzunehmende Vorschlag den wir gefunden hatten – ein System zum kryptografischen absichern von LDACS – setzte auf post-quanten chiffren (SIKE), gegen die ein Jahr später Angriffe gefunden wurden.

TODO: Insert REFERENCE

Ansätze für Verbesserung in beiden Bereichen



Verifikationstechniken

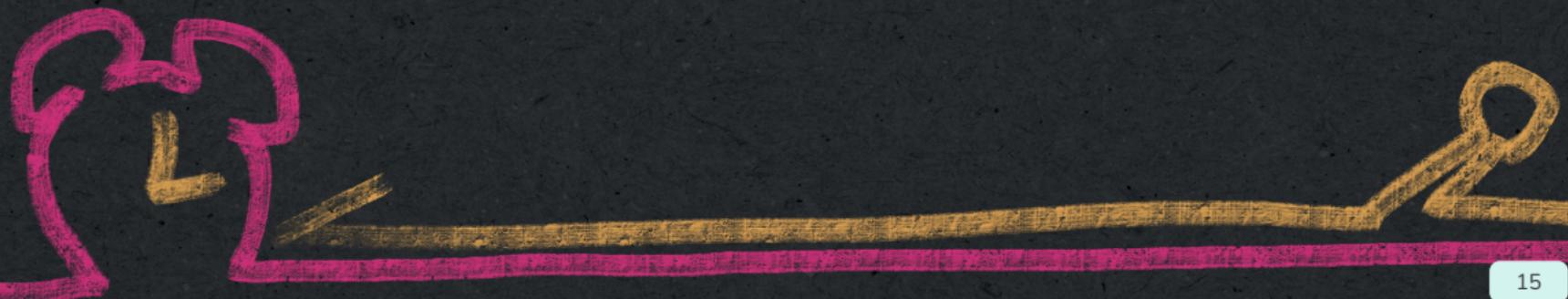
Zertifizierung <-> Sicherheitsbeweise

Kompartimentalisierung

Partitionierung <-> Brokerarchitekturen

=> Kryptoagilität

Kryptoagilität als Prozess



Modulare Systemdesigns

Möglichkeiten:

- Rapider Komponentenaustausch
- Vereinfachtes Systemdesign
- Validierung einzelner Komponenten

Herausforderungen:

- Abstraktionen sind häufig unvollständig
- Gute Modulgrenzen finden braucht Erfahrung
- Viele funktionelle & nicht-funktionelle Anforderungen
- Schlecht gewählte module bringen eine Illusion von Sicherheit
- Cargo Culting

Ein agiler Lebenszyklus für Module

- Laufende, agile Modulentwicklung
- Enge Zusammenarbeit zwischen Modul- und Systemdesignern
- Einsatz besonders Erfahrener Ingenieure
- Breite, industrieübergreifende Zusammenarbeit hilfreich

Korrekt von Anfang an

Reaktiv vs Proaktiv

- Externe Validierung essenziell (Sicherheitsbeweise, Zertifizierung)
- Ansätze können kombiniert werden
- Proaktive Methoden sind in Safety und Security weit verbreitet

Proaktives Vorgehen ist besonders schwer

- Avionik: Zertifizierung ist schwer
- Kryptografie: Formelle Beweise sind schwer
- Die Bürde der Verifikation erdrückt Innovation

Schritte für den Anfang

- Investition in Lehrmaterialien, Handbücher, Nutzerfreundliche Verifikationssysteme
- Benutzbare Beweistools, Menschenfreundliche Zertifizierungsbehörden
- Innovation für bessere, effektivere Verifikation müssen gefördert werden
- Kontinuierliche Verifikation in Aktiver Zusammenarbeit zwischen allen Akteuren

Konsequenzen & Chancen



- Sicherheit: Hochgradig formalisierte Prozesse
- Krypto: Strenge ethische, weniger formalisierte Prozesse
- => Shannons Prinzip
- => Verantwortungsvolle Offenlegung
- => Staatlich vorgeschriebene Berichterstattung über Schwachstellen
- => Es geht darum, eine Umgebung zu schaffen, in der man aus Fehlern lernen kann



Kryptoagilität

Eine Definition



Fortschritt benötigt fortschrittliche Prozesse:

- Abkehr von der technokratischen Perspektive auf Agilität: Es geht um Prozessgestaltung und soziale Realitäten
- Kontinuierliche Bereitstellung: Sie sind nicht fertig, nur weil das Produkt geliefert wurde
- Fehler akzeptieren – Ein Argument für Bescheidenheit
- Planen Sie für Fehlerszenarien, um auf Fehlerszenarien einfach und professionell reagieren zu können
- Keine Schuldzuweisungen für bestmögliche Reaktionen auf Vorfälle
- Scham und Bestrafung für absichtliches Verschweigen von Problemen
- Aufbau einer Infrastruktur zur Unterstützung von Einsatzkräften – Serviceorientierung statt Schuldzuweisungen