Non-Visible-Data Technologie - Daten werden nur für die bestimmungsgemäße Nutzung sichtbar

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Der Aufbau und Betrieb sicherer Anwendungen ist heute extrem aufwändig und komplex. Aufgrund der Komplexität werden Schwachstellen oft übersehen, Anwender nutzen die Lösungen nicht wie vorgesehen, oder der Sicherheits-Overhead ist zu groß, um jedes Gerät damit auszustatten. Werden Daten ausgetauscht, droht nahezu immer ein Kontrollverlust, da nur schwer sichergestellt werden kann, dass der Empfänger die Daten nur wie vereinbart nutzt (und z.B. nicht weitergibt).

Dies lässt sich aus technischer Sicht auf zwei konzeptuelle Schwachstellen zurückführen. Zum einem wird (A) der Schutz immer UM die Daten aufgebaut (z.B. mit physischer/logischer Segmentierung oder Verschlüsselung), zum anderen wird (B) der Zugriff auf die vermeintlich sicheren Segmente über eine Zugriffskontrolle durchgeführt, die auf der Evaluierung von Eingabewerten mit auf dem System gespeicherten Informationen basiert.

(A) Eine sichere Segmentierung ist in großen und verteilten Umgebungen nicht nur äußerst komplex, sondern auch extrem aufwändig. Worum baue ich die Mauer auf, wem kann ich vertrauen, wie kann ich Geräte/Anwendungen/Anwender wieder komplett aus einem Segment entfernen etc.?
Diese Anforderungen münden in sehr aufwändigen Lösungen, wobei insbesondere die Übergänge zwischen Segmenten und die Schlüsselverwaltung ideale Angriffsvektoren darstellen.
„Ende-zu-Ende Schutz“ hört sich zwar sicher an, bietet aber nur einen temporären Schutz über ein oder mehrere Segmente – ein durchgängiger Schutz der Daten von Erstellung bis zum Löschen fehlt.

(B) Die Authentifizierung und Autorisierung (Rechtezuweisung) der Zugriffskontrolle sind potentiell angreifbar, da sie darauf basieren, dass der gelieferte Input mit den gespeicherten Informationen vergleichen wird (z.B. stimmen Benutzername, Passwort, 2-Faktor etc. überein?). Selbst wenn hier eine Verkettung von Maßnahmen und eine Obfuskierung der Daten stattfindet, so findet immer eine Evaluierung mit einer Ja/Nein Antwort statt. Somit weiß ein Angreifer immer das gewünschte Ergebnis (ein „Ja) und kann versuchen die Prüfung entsprechend zu manipulieren, was mit ausreichenden Rechten auf dem System häufig erfolgreich ist.

Daher muss eine Lösung geschaffen werden, die hochgradig skaliert, einfach in Nutzung und Betrieb, sowie universell einsetzbar ist, und die den Kontrollverlust bei geteilten Daten ausschließt.

Beschreibung der Idee und wie sie das Problem lösen soll:

Die Grundidee der Non-Visible-Data (NVD) Technologie ist es, jegliche Daten für alle Parteien „unsichtbar“ zu machen. Nur die bestimmungsgemäßen Anwender bzw. Anwendungen können sie wieder sichtbar machen und verarbeiten. Damit können sie nicht mehr durch Dritte manipuliert, und jederzeit und an jedem Ort hochsicher übertragen und abgelegt werden. Der

Erzeuger der Daten behält dabei immer die Kontrolle über die Daten und kann einmal geteilte Daten bei Bedarf auch wieder nachträglich entziehen (unsichtbar machen). Wir erreichen dies durch drei Kern-Bausteine, A) Sofortiger, autonomer Schutz der Daten, wobei Informationen aus den Daten selbst für den Schutzaufbau genutzt werden, und auf jegliche sichtbaren Metadaten verzichtet wird, > Dies wandelt Daten in „Binärdaten-Müll“ um, der ohne Einschränkungen überall übertragen und gespeichert werden kann B) Ein neuartiges Referenzierungsmodell, dass die klassische Zugriffskontrolle (Authentifizierung und Autorisierung) durch einen Referenzwert ersetzt, > Damit wird ein hoch-granularer Zugriff möglich (z.B. abhängig von Lokation, Zeit, Applikation etc.) und eine Manipulation der Zugriffskontrolle wird unmöglich (selbst wenn ein Angreifer sämtliche Rechte auf einer Maschine besitzen sollte) C) Die Ersetzung aller übertragenen statischen durch ephemere Werte (zufällige Einmalwerte), wodurch ein aktiver Entzug geteilter Daten möglich wird. iese Grundidee wurde seit 2011 mit mehreren Patenten und Referenzimplementierungen in die Praxis umgesetzt, eine C-basierte API liegt für Windows 10 vor, wobei bei der Struktur auf eine entsprechende Portierbarkeit auf andere Software-Plattformen und sogar Hardware geachtet wurde. Der Kern der Technologie ist dabei mit ca. 30.000 Code-Zeilen sehr kompakt. ie Technologie kann als eine Art „Kernel-Treiber“ des Betriebssystems verstanden werden, der die Schreib-/Lese-Befehle der Applikationen so modifiziert, dass statt auswertbarer Daten nur geschützte NVD Blöcke erzeugt, abgelegt und übertragen werden. Je nach Anwendungsszenario wäre daher entweder bei Custom-Build Applikationen eine direkte Zusammenarbeit mit den Anwendungsentwicklern notwendig um die Schreib-/Leseoperationen anzupassen. Bei normalen, auf einem Betriebssystem basierenden Lösungen (z.B. ein hochsicherer, anonymer Arbeitsplatz) würde ein virtuelles Laufwerk in das Betriebssystem integriert werden, mit denen die Applikationen wie gewohnt zusammenarbeiten. Eine entsprechende Lösung ist für Windows 10 verfügbar, für andere Betriebssysteme müsste eine Portierung erfolgen.

Changing the game!

Non-Visible-Data Technology

Making data invisible to anybody other than the intended user

CODE 2019 - CfP Innovationstagung

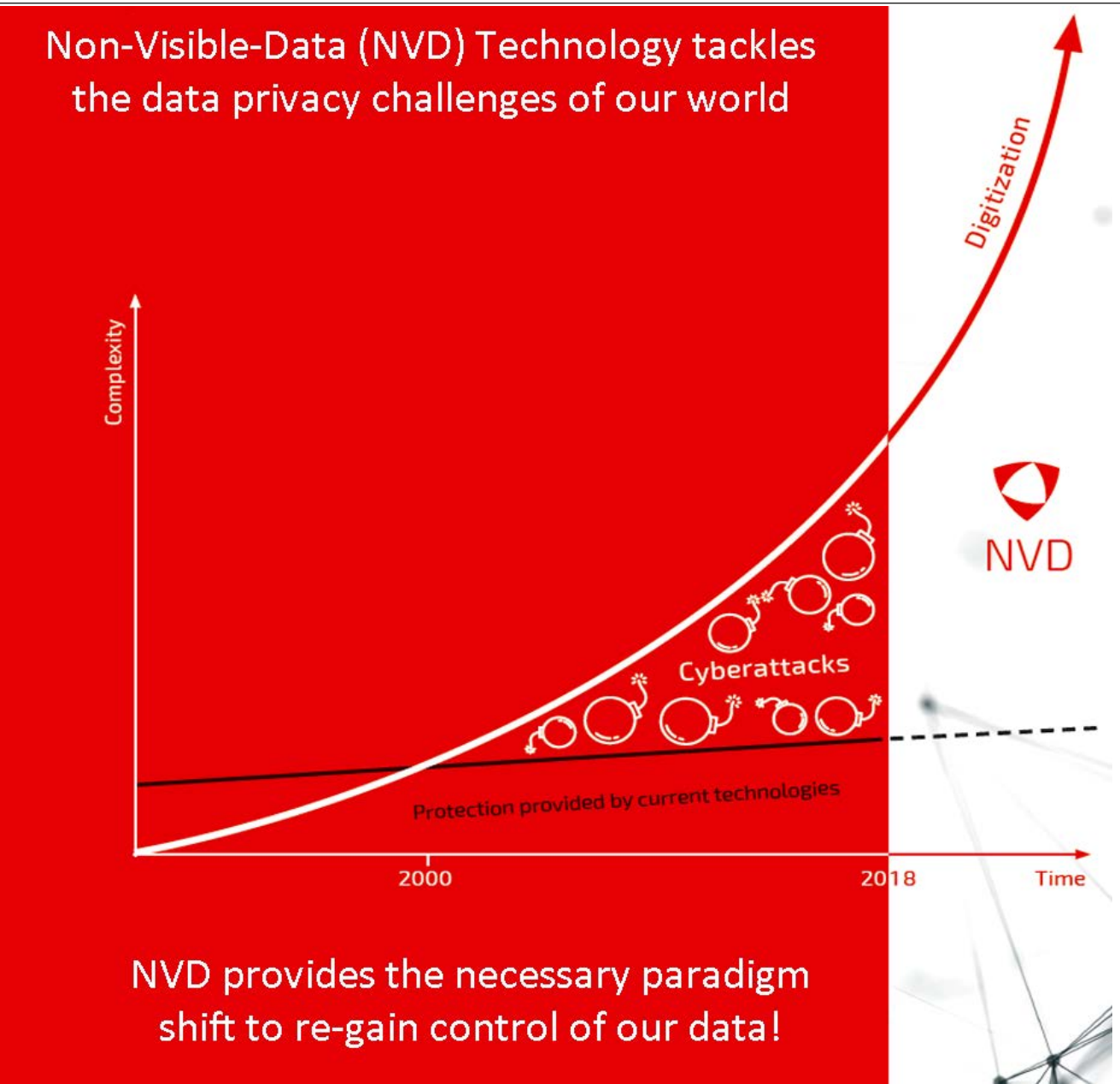
SECLOUS GmbH, Kai Rehnelt

May 2019

Agenda

1) Non-Visible-Data Technology (NVD) Introduction
2) Illustrative UseCases
3) The SECLOUS Team

It’s time to reach the next level in data protection – welcome to Non-Visible-Data Technology



Today’s data security and protection mechanisms and tools are following concepts developed decades ago. The incremental, evolutionary improvements are not sufficient to cope with the massive increased complexity driven by digitization and connectivity, as visible in the increasing number of data breaches.

Since 2011 our team has invented and developed a technology that both simplifies and protects data storage, exchange and usage, even in highly distributed and complex environments.

Our Non-Visible-Data (NVD) Technology makes any kind of data content invisible for anyone other than the intended users, so it doesn’t matter were even highly sensitive information is transferred or stored – without adding todays security overhead, complexity and cost.

Immediate and autonomous data protection, an unique tamper-free access control system and true data revocation capabilities build the main pillars of Non-Visible-Data.

Non-Visible-Data is a novel and unique data security and privacy technology that is easy to use, truly secure and highly scalable

Core components of Non-Visible-Data technology

1. Immediate, autonomous protection

- While data is generated, it is analyzed and, based on the results, converted into binary fragments without any visible information (distorted, encrypted, disjointed etc.) without any user interaction
- Data is thus immune to any attack or manipulation. It can now be transferred or stored at will, no further protection necessary

2. Dynamic referencing system

- Instead of verifying users and passwords based on existing information, as we do today, a number (address) is calculated based on various entry values that depend on the application, i.e. user credentials, timeframe, purpose
- Based on this address, the method can retrieve the data fragments generated in the first step and reconstruct the data

3. Ephemeral access algorithms

- The addresses generated in the second step are valid only one single time
- Each access involves calculating a new address, which is completely different from the previous one
- This makes any information that attackers may intercept utterly useless
- Virtual data referenced by ephemeral addresses allows true data revocation capabilities

Key differentiators of Non-Visible-Data technology

Easy to use ✓

- Data is protected autonomously from the instant of creation without the need for the user to focus on security
- Effortless key management without master keys or key storage – instead keys are calculated on demand as part of the referencing system
- Data can be stored and protected on arbitrary media, which helps to optimize both cost and user experience
- Easy GDPR compliance by true privacy by design (no personal / user related information available) as users have full control over their own data

Truly secure ✓

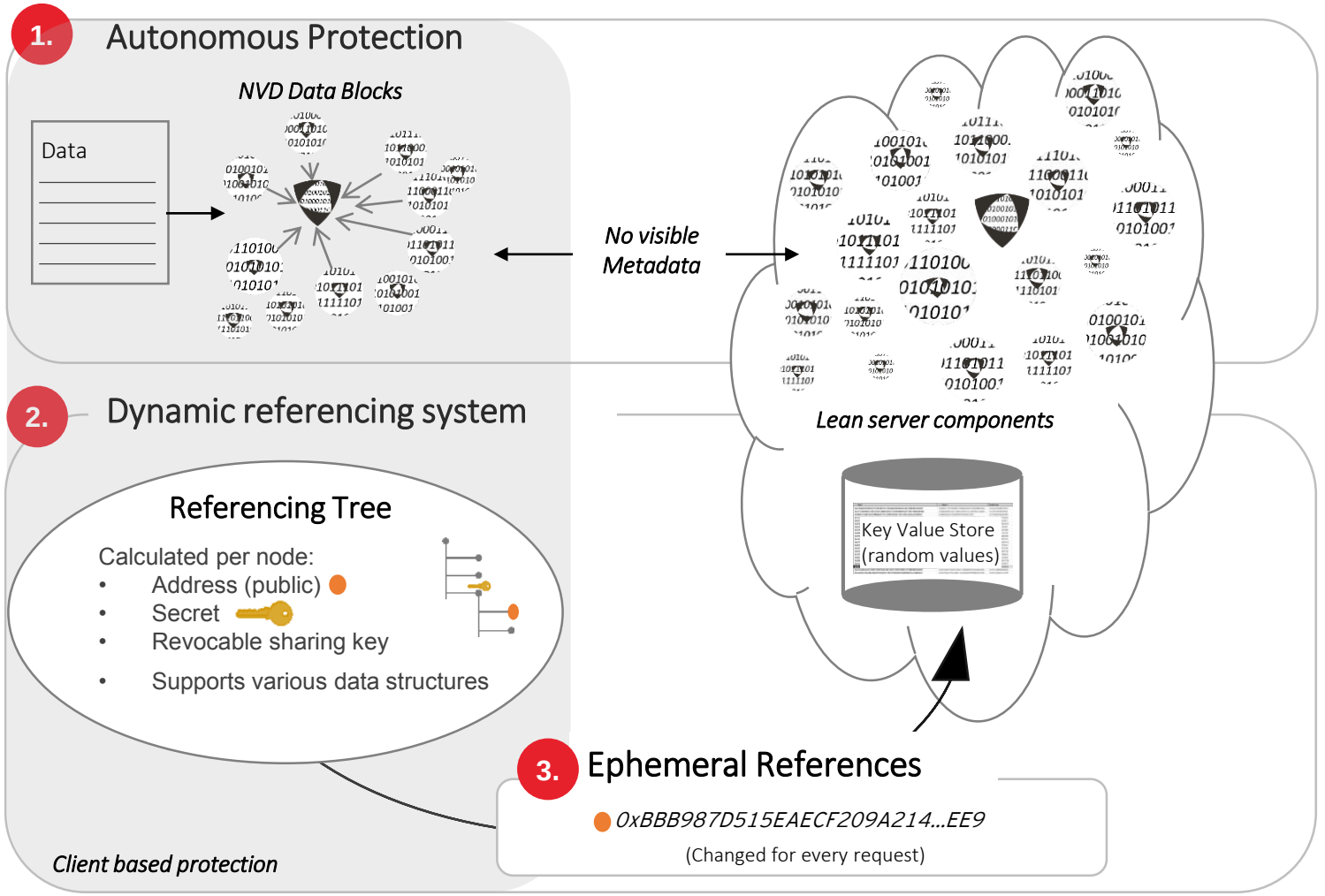
- Metadata free data transmission and storage of NVD fragments (indistinguishable from random data) eliminate the possibility of targeted attacks
- No matter where data is stored, the requirements regarding information security and data protection can be fulfilled
- True data revoke – no need to trust others as shared data can be revoked at any time
- Protection integrated into data across the complete data lifecycle (from creation till deletion)
- Quantum-computer resistant security

Highly scalable ✓

- Deduplication with encrypted data on client level – resulting in reduced data transmission and storage usage (up to 60 % less storage)
- Classical security layers are no longer required for data protection
- Performance-optimized data transfer and storage through efficient compression / transmission mechanisms
- Protection is distributed to data generating devices, resulting in extremely low server utilization
- Minimal computation power required, even on embedded devices

The NVD building blocks are tightly integrated

Data with integrated and autonomous protection, referenced by ephemeral addresses calculated on the fly by NVD's referencing system unique for every device



Facts and figures regarding NVD algorithms, source code and testing approach

Based on NVD referencing architecture

Algorithms

- Secure Hash Functions
  - BLAKE2 secure hash (>2x faster than SHA3)
- Fast Hashes
  - MURMUR3 high bit independence and entropy
- Maximum secure Hash Functions
  - PCKS#5 with BLAKE2
- Asynchronous crypto algorithms
  - ED25519 signature
  - Curve 25519 Key Exchange
  - Zhang-Kim blind signature
- Symmetric crypto algorithms
  - AES-IND
- Z-Standard Compression 1.3.4 (best compression /performance ratio)

API / Components

- Windows 10 API
- Core API developed in C (wrapping into C++, C#, JAVA JNI)
- Visual Studio 2017 (Windows 10)
- GUI C++/MFC used for pilot / show-case application: invisible-share
- MySQL 5.7 (server)
- SQLite3.23.1 embedded into source code (client)
- Data layer (UDP Enet 1.3.13 - transaction less protocol)
- # of Modules and Functions: 15
- # of Source-code lines: 30.000

Testing

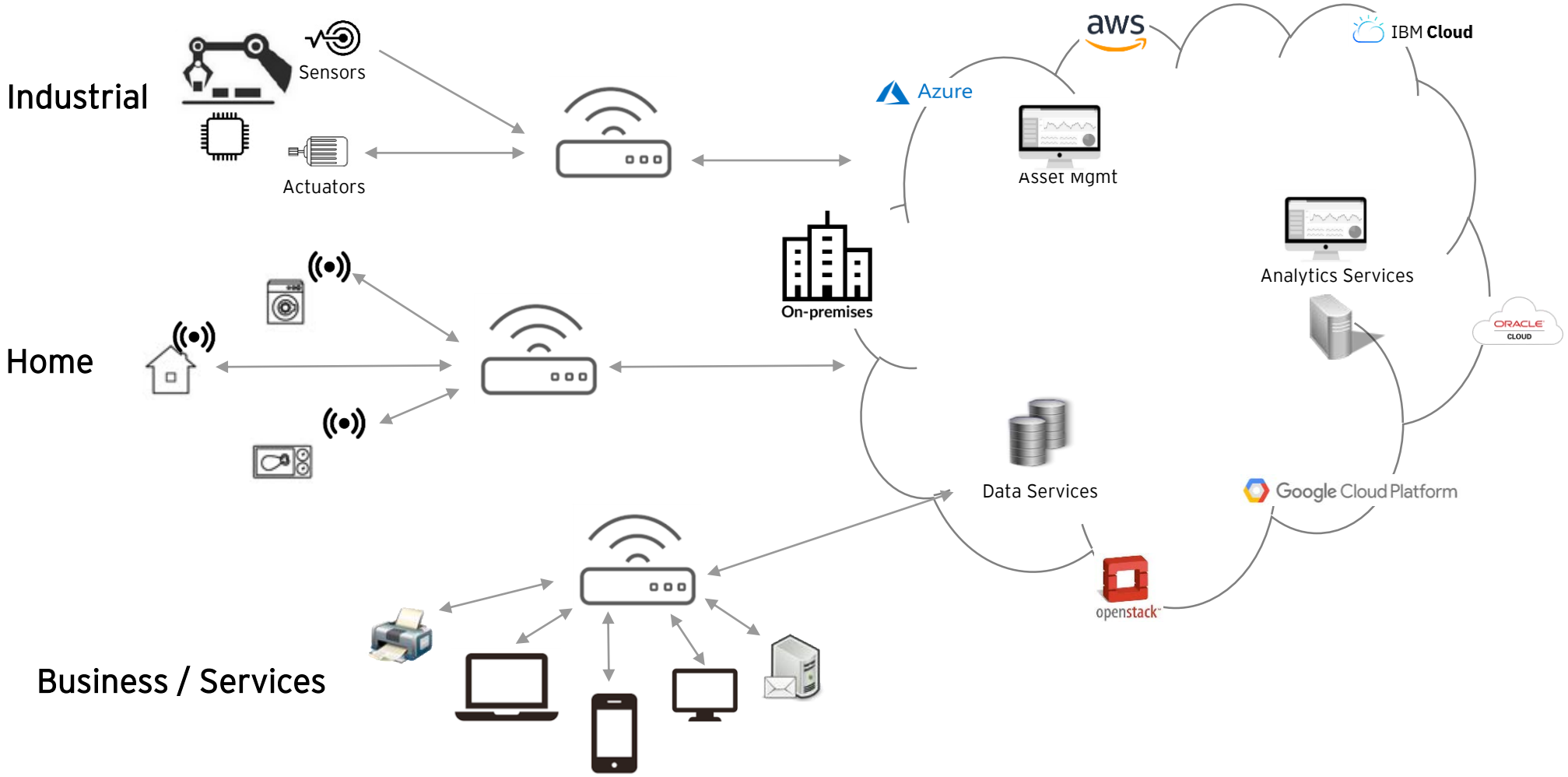
- 12 months of extensive testing (module-, integration-, user-acceptance and regression testing)
- Source Code Analyzer
  - Sonar QUBE with C/C++ Rule set
- Operating Systems
  - Windows 10
  - Mac OS via VM Ware
- Crypto Algorithm tests based on common known attack methods and mathematical evidence
- Expert Opinions from
  - Information Services Group
  - Alpha Strike Labs
  - SBA Research, Vienna
  - Chancellery Mayer-Steger-Schlauch, Munich

Agenda

1) Non-Visible-Data Technology (NVD) Introduction
2) **Illustrative UseCases**
3) The SECLOUS Team

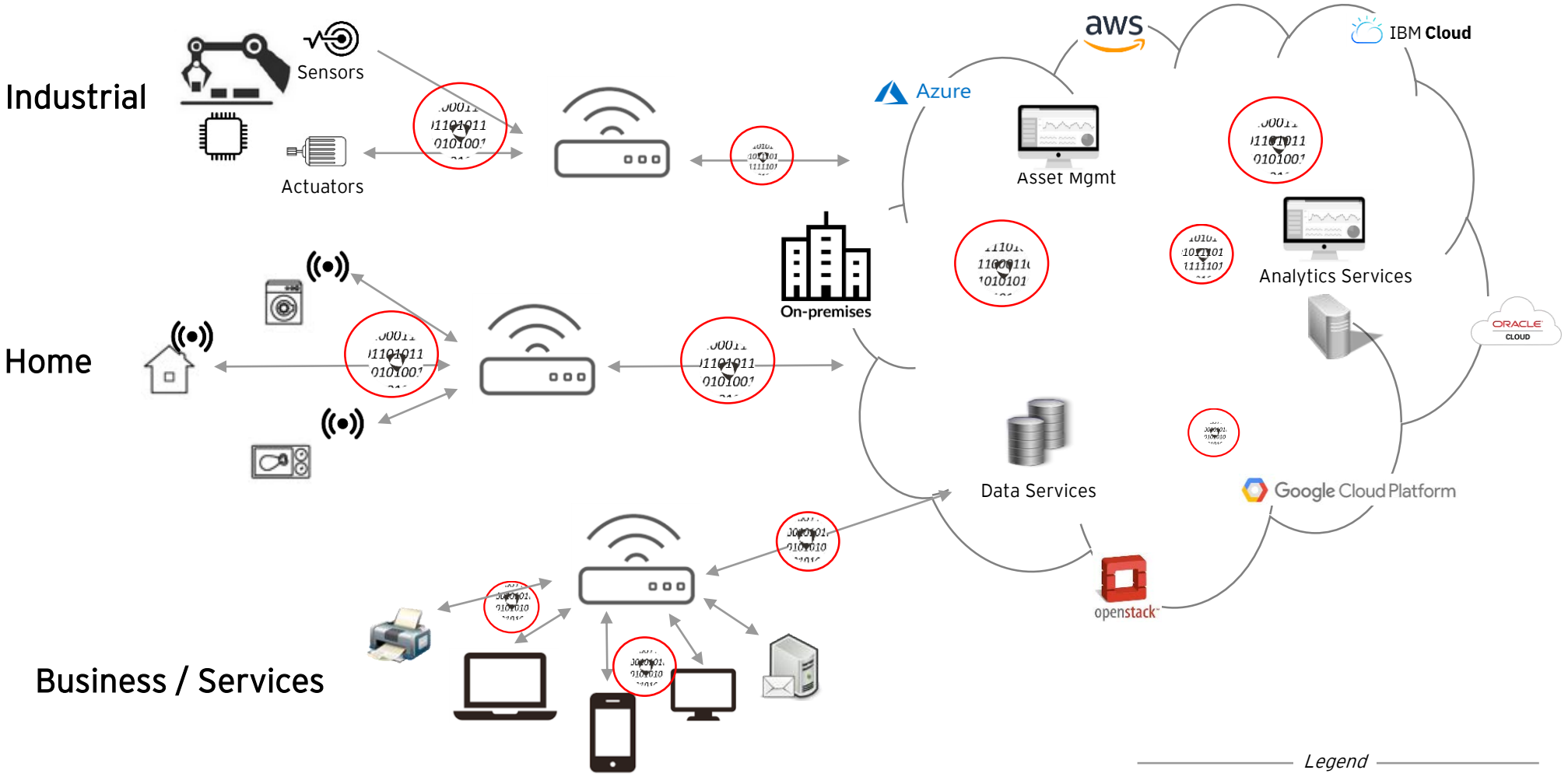
The (I)IoT / Cloud ecosystem is extremely diverse and involves all kinds of components, technologies and players

A consistent data protection approach is impossible with today's security and protection technologies

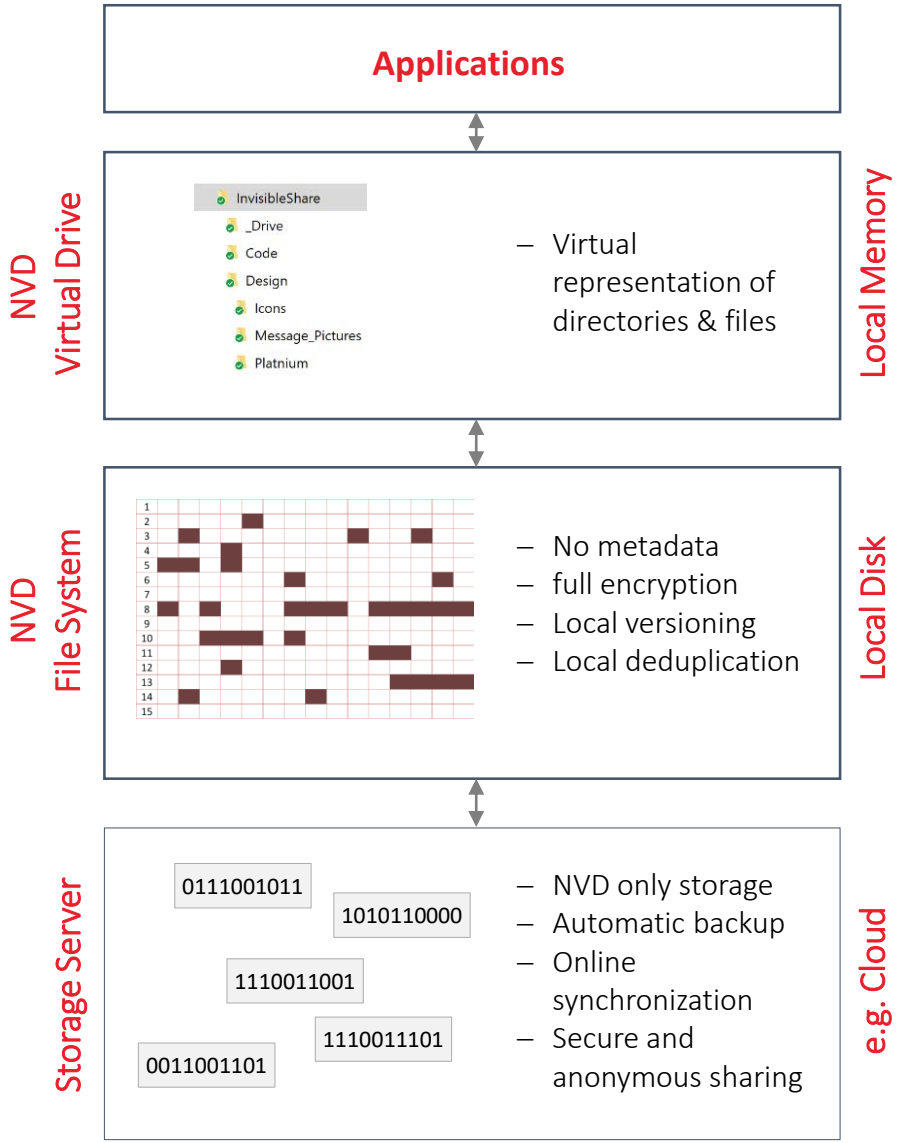


NVD technology provides highly scalable provider and device agnostic data protection, as data is only “visible” to the intended users, applications or services

(I)IoT and Cloud Ecosystem enriched by data security, privacy and integrity by design



NVD protected File Storage - data lifecycle protection for the WorkPlace



- **Applications can be re-used as is**, or new functionality like access control, file sharing, secure collaboration or versioning might be included

- The user works with the virtual drive as with any “normal” drive
- The virtual Drive is only visible when logged in
- Unencrypted information is **only temporarily available in memory**
- Could include **dynamic access information** like location, timeframe or company grant to make certain files “visible”

- On local disk, only NVD will be stored (**encrypted and locally obfuscated**)
- Due to **local deduplication**, redundant files will only be stored once in NVD, **lowering the local storage needs**
- This offers also **efficient file versioning capabilities**, as only the changes (delta) between files needs to be stored

- As only the protected and anonymous NVD blocks will be transferred and stored, **no additional protection mechanisms are needed** (OPEX reduction)
- The NVD conversion removes any personal related information, so NVD can be stored at any location (data center) **without compliance risk**
- The (Cloud) server provider or admins have no information what will be transferred or stored, **enabling further cloud usage**
- The NVD FS includes **autonomous backup** of all NVD blocks with the server
- Provides powerful **secure and anonymous file sharing capabilities**

Agenda

1) Non-Visible-Data Technology (NVD) Introduction
2) Illustrative UseCases
3) **The SECLOUS Team**

Deep expertise and intimacy in a variety of industries and competencies

Core Team

Kai Rehnelt (MD)

Our digitization expert and data privacy evangelist. 25 years in Business (Accenture, SMEs). Innovator, IT strategist and enterprise architect, bridging Technology and Business across industries.

Heinrich W. Pfluger (MD)

28 years in Business (Accenture, Capgemini, IBM). CIO Advisor and Business Development Executive in Manufacturing, Consumer Products / High-Tech Industries

Matthias Möstl

Our creative head and inventor of NVD. Matthias adds 20 years in-depth encryption, database and code optimization expertise SME in Cryptography, maths and gaming theory

Changing the game!

Alexander Schischek

Alexander adds more than 30 years of entrepreneurship and experience in innovative product development. He was one of the German internet business pioneers with an international sales network

Sven Schlotfeldt

Sven is an entrepreneur in marketing, communication and graphic design. He is in charge of marketing, communication and adds 25 years of subject matter expertise

Prof. Dr. Heinz Helmreich

Heinz adds more than 30 years expertise in finance-, tax- and legal advisory. He holds a professorship for law of taxation at the University of Hof

Thomas Andrew Zenner

Thomas adds more than 30 years in financial services and advisory and successfully manages a swiss family office.

Thank you for your attention

www.seclous.com