SEC Consult

ADVISOR FOR YOUR INFORMATION SECURITY

COBOL versus Cyber Security

WHITEPAPER

prepared by SEC Consult

ABSTRACT

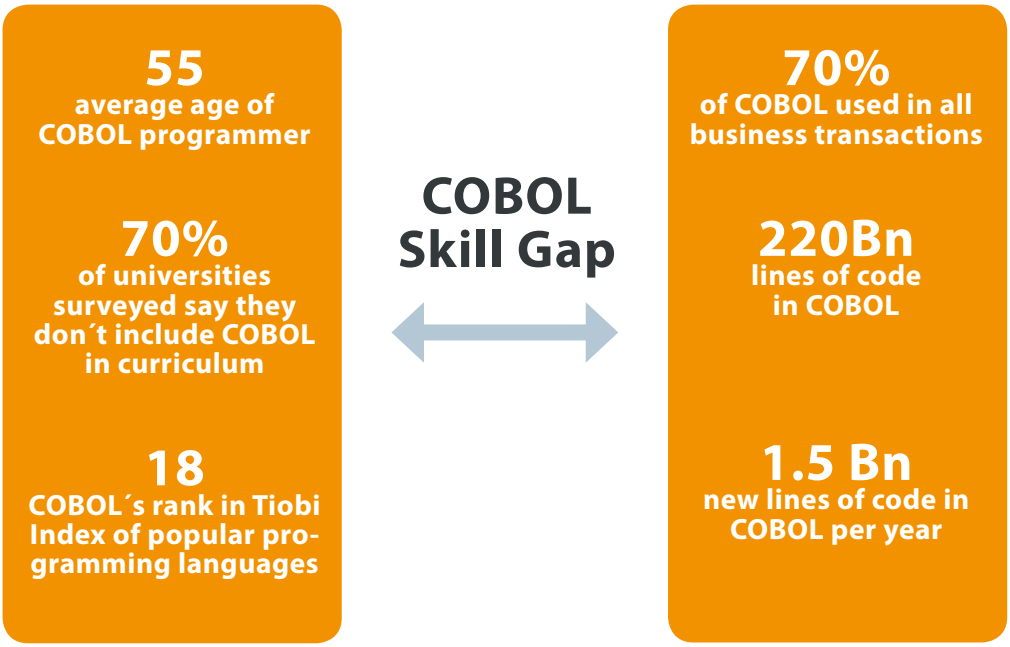


Figure 1: COBOL related numbers (source: Microfocus, Gartner and laserfiche)

COBOL the „common business-oriented language" is a compiled English-like computer programming language designed for business use. It was in 1959 as COBOL60 and is now available in the Version COBOL2014. It runs and has been ported for most common operating systems such as z/OS, VME, Unix, OpenVMS and Windows.

Despite many rumors, COBOL is still one of the most used programming languages in the world and 70% of all financial transactions are executed with the help of COBOL programs.

60 million
patients are cared for daily

95 %
ATM transactions daily

96%
vacations booked daily

60 million
Lines of code at the Social Security Admin

80 %
Point of sale transactions daily

50 million
lines of code at the IRS

COBOL AND CYBERSECURITY

During the last couple of years, there has been a paradigm shift in how network infrastructure is seen. The walls between the internet and the so called „local area network" are vanishing.

Hundreds of different communication channels exist between the internet and a company's typical network infrastructure. In addition to this, targeted attacks are known to bypass any types of firewalls or AV (Anti Virus) systems on a daily basis.

Beside to this, it is a known fact that a certain percentage of world-wide computers have been infected with a virus, which might be a RAT (remote access tool) and can be remote controlled from some C&C (Command and control center) from the internet.

Category	Worldwide	United States	China	Brazil	Russia	India	Turkey	France	Mexico	U.K.	Germany
Trojans	11.3 %	5.1 %	13.5 %	21.9 %	19.2 %	26.6 %	31.6 %	6.0 %	16.0 %	4.7 %	5.3 %
Browser Modifiers	4.1 %	2.2 %	6.8 %	8.4 %	7.0 %	7.6 %	5.5 %	4.0 %	4.6 %	1.7 %	3.1 %
Software Bundlers	3.9 %	1.9 %	0.2 %	6.0 %	12.1 %	8.8 %	5.3 %	3.8 %	3.0 %	2.6 %	4.6 %
Worms	3.8 %	0.5 %	2.9 %	4.6 %	1.9 %	21.0 %	8.1 %	1.0 %	9.6 %	0.6 %	0.4 %
Other Malware	1.6 %	1.0 %	1.5 %	3.3 %	2.2 %	2.5 %	3.0 %	1.0 %	1.8 %	0.8 %	0.8 %
Downloaders & Droppers	1.6 %	1.0 %	1.6 %	5.1 %	1.4 %	2.9 %	1.1 %	1.7 %	2.0 %	1.2 %	0.9 %
Exploits	1.5 %	1.0 %	0.7 %	0.9 %	0.4 %	1.3 %	1.1 %	1.9 %	0.7 %	2.0 %	1.5 %
Viruses	1.3 %	0.2 %	4.5 %	1.1 %	0.6 %	3.5 %	2.7 %	0.2 %	0.6 %	0.2 %	0.1%
Obfuscators & Injectors	1.1 %	0.3 %	1.3 %	1.5 %	2.3 %	3.0 %	2.4 %	0.6 %	1.1 %	0.4 %	0.4 %
Adware	1.0 %	1.0 %	0.0 %	1.0 %	1.3 %	1.1 %	1.0 %	1.7 %	0.9 %	1.4 %	1.5 %
Backdoors	0.4 %	0.2 %	0.6 %	0.8 %	0.4 %	1.1 %	1.0 %	0.3 %	0.3 %	0.2 %	0.2 %
Ransomware	0.3 %	0.4 %	0.0 %	0.1 %	0.3 %	0.2 %	0.4 %	0.2 %	0.2 %	0.2 %	0.2 %
Password Stealers & Monitoring Tool	0.2 %	0.1 %	0.2 %	0.2 %	0.2 %	0.3 %	0.3 %	0.1 %	0.2 %	0.1 %	0.1 %

Figure 3: Microsoft Security Intelligence Report 2016 on Malware

Since many Core-Banking, -Insurance and other critical systems are running on COBOL, security must be seen as a serious issue.

COBOL also played a very important role in the 2015 data breach where 4 million user accounts were stolen from the office of personal management in the US.

COBOL AND CYBER-THREATS

Contrary to a common misconception COBOL, RPG and other typical legacy programming languages are prone to similar security vulnerability classes „modern“ technologies are:

- DB2/SQL injection
- CMD injection
- JCL injection
- Column truncation
- Logical errors
- Bypassing audit trails
- Input validation issues
- Privilege escalation
- Insecure cryptographic algorithms
- Ignored error conditions
- and others

Figures 4: FedTech Post (source: www.fedtechmagazine.com/article/2015/06/cobol-and-outdated-technology-cited-factors-opm-hack)

SEC CONSULT COBOL CODESCAN

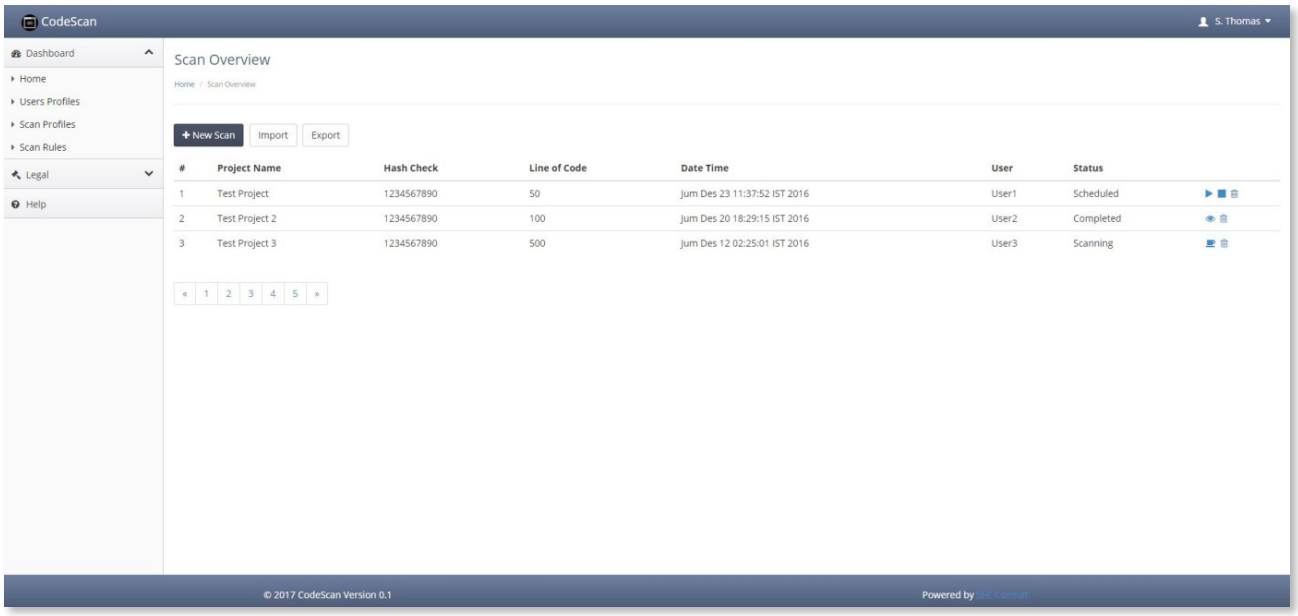
Due to the strong need for security testing of legacy systems SEC Consult developed a methodology and corresponding toolset for auditing COBOL applications.

The SEC Consult methodology for security code reviews has been developed for a multitude of technologies over the last decades and has been proven to be extremely effective and mature. SEC Consult has conducted thousands of code reviews for „modern" technologies like C/C++, Java, PHP, Python and many other technologies.

Reviewing COBOL, applications needed a completely new approach and a new toolset as well.
Therefore, SECobol, which is a true SaaS solution, was developed.

SECobol is a tool, which supports security exports conducting comprehensive security reviews for COBOL applications.

It currently supports 15 different COBOL specific security vulnerability classes and is extendable via programmable modules/plugins.



Figures 5: SECobol CodeScan main view (source: by Sec Consult)

CASE STUDY

Auditing a legacy system for an international insurance company.

CHALLENGE

The insurance company operates a core insurance system, which is based on COBOL on AS400. This legacy application has been developed and extended over the past 25 years and is still actively maintained and extended today. Over the years, the total codebase has grown to more than 20 million lines of COBOL code.

Being a business-critical application, the insurance was concerned regarding the risk of the application being vulnerable to cyber-attacks. In addition to stringent access control (both physical and on a network layer), the insurance was looking for an effective but economical way to inspect the application itself for security deficiencies and means to prioritize fixes based on the risk imposed by respective vulnerabilities.

Figures 6: Grace Hopper working on UNIVAC (source: www.quotabelle.com/author/grace-hopper)

CASE STUDY

APPROACH

To resolve this task in an economical way, a full manual source code review was not feasible, as the effort for this task was estimated at 100 man-years. Therefore, SEC Consult proposed a hybrid approach of a full automated static source code analysis paired with manual verification of findings and manual source code review of selected critical components. Threat modeling and dynamic testing methods were used to assess the risk of the respective vulnerabilities, propose solutions and prioritize the deficiencies for fixing.

To accomplish the full automated static source code scan, SEC Consult found that existing solutions offered on the market were not able to meet SEC Consult's requirements in terms of coverage of vulnerability classes and capability to deal with large codebases of several million lines of code. Tapping into the expertise, SEC Consult collected over the past decade source code reviews of COBOL applications. SEC Consult decided to pool this knowledge into a true SaaS solution.

FINDINGS

SEC Consult identified thousands of instances of vulnerabilities. The root cause for the vulnerabilities were improper input validation, bad coding practices and lack of authorization checks.

The application was found to be vulnerable to SQL injection. Threat modeling and dynamic verification proved that data passed to the application by an online portal was not sanitized properly during batch processing and allowed an attacker to execute arbitrary SQL commands on the AS400 system. Further investigation showed that this vulnerability could not only be used to manipulate arbitrary records of the database (e.g. premiums or insurance coverage) but also to access arbitrary records of the database and exfiltrate the data by embedding it into policy statements and using out-of-bands mail communication. Furthermore, misconfiguration of the DB2 database allowed an attacker to take full control of the AS400 system and run arbitrary commands on the operating system.

The application was found to be vulnerable to privilege escalation. An attacker with a low-privileged user to the application is able to load arbitrary libraries and change the execution flow of the application. Abusing this vulnerability, an attacker is able to bypass logging and audit measures as well as dual-control measures built into the application.

CONCLUSION

SEC Consult was able to identify thousands of vulnerabilities in the application. The provided risk assessment and demonstration of the impact aided the insurance company to prioritize the fixes of the vulnerabilities accordingly, thus addressing high-risk vulnerabilities first.

Finally, SEC Consult demonstrated that a source code audit of a COBOL legacy system can be done in an economic way by reducing the required effort from 100 man-years to a few 100 person days.

ABOUT SEC CONSULT

SEC Consult is an international leader in application security services and information security consultancy. SEC Consult's competence in improving the application security of enterprise applications supports major international banks, government organizations and global software vendors. We provide consultancy and specific, high-end services such as security quality gates or Managed Vulnerability Information Services (MVIS) which help to protect our clients from 'toxic' (i.e. heavily insecure) enterprise software. Our many years of experience with the remediation of application security problems in software and systems allow us to help software vendors and other customers to reduce their risk of application security vulnerabilities.

VERSION HISTORY

Version	Date	Status	Created by	Responsible
1.0	2017-03-06	Initial document	M. Eiszner	M. Eiszner