CENSUS
Cybersecurity Engineering

CYBERSECURITY SERVICES FOR THE BANKING AND FINTECH INDUSTRIES

Banking was one of the first industries to adopt electronic transactions and since then, it has been building security architectures to facilitate delivery of trusted financial services. Companies in the FinTech space share a similar journey, as the technological means that have enabled them to provide innovative financial services come with cybersecurity risks that require their constant attention.

CENSUS has a long history of supporting organizations in the Banking and FinTech fields with security assessment and consulting services that span across a wide range of topics, including device assessments for customer facing devices, configuration audits for infrastructure elements, application assessments for online and internal services, design reviews for new software features / protocols / infrastructure architectures, threat modeling and security documentation for financial products, penetration testing (through different adversarial scenarios) for organization infrastructure and processes, social engineering and physical attacks to financial organization headquarters and branch offices, but also consulting on secure development practices for the development and continuous deployment of trustworthy systems.

This whitepaper sheds light to some of these projects and describes the unique benefits of CENSUS services in the Banking and FinTech space.

DESIGN LEVEL REVIEW

Through Design Level Reviews CENSUS identifies security vulnerabilities in the specification of software features, protocols and/or infrastructure architectures. This **early assessment** process enables development teams to reap the benefits of the **Security by Design** paradigm. Examples of past projects include the review of planned integrations with third-party systems, such as card clearing and fraud detection systems, the review of cryptographic protocols, the review of authentication & authorization processes that would need to comply with certain standards & regulations (e.g. PSD2, 3DS etc.), the review of the simultaneous deployment

of multiple versions of a banking API, the review of API calls used for mobile device & user registration, but also the review of candidate network architectures for hosting e-banking services in a private cloud environment.

SOURCE CODE AUDITING

Source Code Auditing services offer a **manual line-by-line security review** of a product's (or component's) source code, coupled with functional security testing, third-party library checks and build process inspection. This is **the best way to identify software vulnerabilities** and prepare for a high-quality release. CENSUS has provided Source Code Auditing services to organizations that create software for the Banking and FinTech organizations, such as international banking software vendors, development branches of banks & virtual banks, POS solution integrators and FinTech startups. Related projects include e-banking and mobile banking software, wallets and micro/peer-to-peer payments, customer loyalty platforms, POS and virtual POS integrations, advertisement and telemetry app integrations, payment gateways, open banking APIs, as well as core banking components of mainframe systems.

APPLICATION SECURITY TESTING

Application Security Testing offers "black box", "gray box" or "white box" security testing for any type of application, including desktop applications, mobile apps and web applications. It is a form of "best effort" functional security testing where the terms "black / gray / white box" refer to the various degrees of knowledge shared with the CENSUS team (i.e. no information, limited information or detailed specifications and/or source code). **Testing examines all product functionalities and user roles / privileges**, as designated by the client or identified through the team's **reverse engineering** efforts.

Application Security Testing would be the assessment service of choice when access to the source code would not be made available to CENSUS engineers, or when the assessment project would need to be carried out within a limited timeframe. In the past, CENSUS has conducted Application Security Testing projects in a wide variety of software in the financial space, such as e-banking and mobile banking software, web and mobile payment solutions, virtual POS apps, stock exchange systems, "Know Your Customer" solutions, wealth management platforms, anti-money laundering and fraud detection systems, HSM platforms and PKCS handling libraries, multi-factor authentication integrations, MDM and binary protection suites, as well as custom-built tools for internal use, such as a bank's ticket tracking system.

Web Application Security Testing is a specialized service for web applications, providing remote testing for the complete stack of deployed web applications.

Mobile App Security Testing is a specialized service for the in-depth testing of iOS and Android apps; it also covers related web APIs and other types of communication with device peripherals and third-party services.

DEVICE SECURITY TESTING

CENSUS provides comprehensive Device Security Testing services covering the complete technology stack of modern electronic devices. Through **hardware**, **enclosure**, **firmware, and communications inspection,** CENSUS identifies important security issues in product prototypes and product releases. Past projects include the assessment of POS devices, ATMs, mobile payment features of mobile phones, Kiosk systems, and internally used devices, such as VoIP phones and video conference solutions. For these projects, CENSUS carried out extensive testing on the hardware of these systems (emulating physical attacker threats) and their software and communications (such as GSM, NFC and Bluetooth communications, where applicable).

NETWORK & CLOUD INFRASTRUCTURE TESTING

Either as part of a Product Assessment or as part of the assessment of an organization's infrastructure,

Network & Cloud Infrastructure Testing allows to **identify misconfigurations and other security vulnerabilities in networking and cloud computing components**. Vulnerabilities in such components may jeopardize the security of transactions and have a serious impact on business operations. Past projects in this space have examined the cloud infrastructure of virtual banks, data centers of international banks, network segments with SWIFT or ATM systems, network segments with VoIP devices, as well as enterprise Wi-Fi networks.

TIGER TEAM, RED TEAMING & PENETRATION TESTING

These services provide for systematic testing of an organization's security, taking into consideration the technology, the processes, and the human resources of the client organization.

Penetration Testing offers a fully controlled assessment of a predefined set of organization assets or infrastructure components. Such projects in the past have looked at ATM operations, remote access systems & processes, the security perimeter of financial institutions, as well as their reliance on Wi-Fi networks.

One type of technology that requires a special mention is **Mainframe Systems**, commonly used as Online Transaction Processing (OLTP) systems in the Banking industry. CENSUS has performed extensive penetration testing to z/OS mainframe facilities, including CICS which is used as a middleware that sits between the z/OS IBM mainframe operating system & business applications and supports commercial electronic transactions, such as withdrawing money from an ATM, paying with a credit or debit card etc. CENSUS has also performed Penetration Testing on iSeries (AS400) components which are used to administrate, control, and audit ATMs and POSs, as well as carry out credit and debit card transactions.

Red Teaming enables CENSUS to carry out different adversarial scenarios in an agreed scope within the client organization. Through Red Teaming, CENSUS has evaluated the security of the SWIFT network operations while under attack from different access levels (malicious insider, access to other corporate network, external threat actor etc.). Furthermore, CENSUS has emulated several workstation theft scenarios that have led to corporate workstation hardening measures.

Tiger Team extends beyond the scope of a Red Teaming Assessment, bringing into scope every aspect of the organization's core business. The team is free to conduct any type of attack (e.g., physical attack, social engineering, cyber-attack to applications & systems etc.) at any time, while making every effort to stay undetected. Through Tiger Team Testing, CENSUS has evaluated the security of large international financial institutions in both the Banking and Investment sectors.

In Tiger Team, Red Teaming or Penetration Testing assessments, it is often useful to test whether a certain piece of enterprise software that has been adopted in the organization processes could be used in a harmful way against the organization itself. CENSUS has in the past conducted such tests on mobile apps, web applications, and desktop software. Examples of such software include e-banking (and related back-office) software and online collaboration suites.

THREAT MODELING & OTHER PRODUCT SECURITY DOCUMENTATION

Security Documentation comes in various forms and helps teams understand and build upon a project's security foundations. A **Threat Model** is perhaps the most important part of a project's Security Documentation, as it **maps out significant threats and allows the prioritization of work on countermeasures**. Other forms of Security Documentation are the **Product Security Plan**, the **Product Security Architecture document**, the **Data Classification document,** and the **Product Disposal Plan**. CENSUS has provided such documentation in the past for vendors developing e-banking solutions within the context of a Secure Systems Development Lifecycle. This documentation then served as a plan for developers to prioritize on the development of crucial security controls, as a

blueprint for customers regarding the security actions carried out for each product release, as well as the basis for marketing material describing the security architecture of the product.

TRAINING & CONSULTING

CENSUS offers Security Training courses that aim to **raise the security awareness of personnel** regarding cybersecurity threats. CENSUS also offers courses to enable **developers** and **management** to efficiently address security defects within an existing systems development lifecycle (SDLC). This allows for the earliest possible treatment of security errors and the development of better, more robust software.

The courses span from introductory material on cybersecurity hygiene and software security, to highly technical vulnerability studies of issues commonly found when developing in particular programming languages (e.g., Java) or particular types of software (e.g., web applications). Through training and consulting, CENSUS also guides development teams into forming a Secure Systems Development Lifecycle that suits their security requirements and business goals. Finally, CENSUS experts also deliver custom training on topics selected by clients.

In the past, CENSUS has delivered Cybersecurity Awareness Training to banking staff, and Secure Development courses to software development teams working in the financial sector.

Furthermore, CENSUS has provided **consulting services** to help **guide development teams** in their work towards **cybersecurity resilience**, on subjects ranging from software architecture to vulnerability handling and security tooling.

SECURE SDLC

The Secure SDLC service allows integrating CENSUS security expertise into an organization's systems development pipeline. International banks have used this service to augment their security teams and handle higher loads (and a broader scope) of security assessment work. On the other hand, software vendors have in the past used this service to gradually build their own Secure Systems Development Lifecycle.

The Secure SDLC offering **combines security training**, **assessment**, **consulting and documentation services** to support the timely delivery of high-quality product releases.

Through this service, CENSUS has shaped the product lifecycle of major players in the financial services space, enabling development teams to gain visibility in previously unexamined parts of the codebase, design and build upon previously audited components, as well as enabling management to better handle cybersecurity risk throughout a project's lifetime.

For more detailed information about CENSUS services, please visit: ***www.census-labs.com***

CENSUS
Cybersecurity Engineering

www.census-labs.com

USA
607 Boylston Street, Suite 165L, Boston, MA 02116
T. +1 8882 029 846
E. usa@census-labs.com

UK
Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
128 A. Siggrou Ave.,
Athens 117 45, Greece
T. +30 2102 208 989
T. +30 2102 208 990
E. eu@ census-labs.com

ABU DHABI
Office 110 - First Floor
Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

DUBAI
Unit GA-00-SZ-L1-RT-201,
Level 1, Gate Avenue - South
Zone, Dubai International
Financial Centre, Dubai
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com