

ATM_AND_FINANCIAL_SECURITY_SERVICES

Automated Teller Machine Security Services

Automated Teller Machines (ATMs) are an obvious target for criminals, with a successful compromise resulting in immediate monetary damages and loss of public trust. Once the domain of banking institutions, the growth of third-party ATM development has led to these machines popping up everywhere from public libraries to nightclubs. Along with this surge in demand, the need for improved usability and additional functionality has also increased. As ATMs have become more sophisticated, the attack surface has widened.

Building upon first hand research into this exciting market, IOActive is uniquely experienced in assessing the security of various types of ATMs, ranging from hole-in-the-wall banking machines to stand-alone retail models. IOActive combines its collective expertise in software, firmware, and hardware security assessment to provide a breadth and depth of skill ingenuity that few other services firms can offer. We employ custom-built tools and elite techniques that were developed specifically for performing audits and penetration tests on ATMs, enabling us to deliver accurate and stable results to our clients.

■ Beyond Physical Security - The New Software Threat

In general, securing ATMs has focused predominantly physical based attacks. The skimmer, ram-raids, and physical theft of the machines are the threats we hear about the most. Countermeasures such as increased surveillance and physical hardening of the ATM's construction have gone a long way toward better security. However, there is a new batch of threats to combat. IOActive Labs has led the way in discovering numerous software based attack vectors that cannot be mitigated by these typical countermeasures alone. Software based attacks require a whole new level of security solutions at the software level.

■ IOActive Labs ATM Research:

Barnaby Jack, Director of Security Research at IOActive Labs, is pioneering ATM security research and proactively working with financial institutions to strengthen the overall security posture of these machines. IOActive Labs has conducted research on multiple new models and manufacturers, uncovering previously unknown weaknesses that were unveiled

at Black Hat 2010 to demonstrate both local and remote attacks on ATMs that resulted in full compromise. IOActive Labs was then able to upload a root-kit specifically designed for ATMs that gave an attacker the ability to dispense cash from the machine, retrieve ATM passwords and settings, and capture and retrieve tracking data remotely.

■ Black-Box Penetration Testing:

During a black-box penetration test, IOActive assesses the security of the ATM firmware and software by simulating an attack without any source code access. Conducting a black-box penetration test enables IOActive to identify weaknesses, vulnerabilities, and different attack vectors that could be exploited if an attack occurred. IOActive performs both local penetration tests (walk-up attacks) and remote penetration tests (audit networks and dialup-based services). Additionally, IOActive performs penetration testing on the ATM management infrastructure.



■ **Malware Analysis/Detection:**

The recent disclosure of ATM-based malware in Eastern Europe highlights the seriousness and practicality of ATM malware infections. To help our clients mitigate and avoid future malware problems, IOActive offers malware analysis services with tools specifically designed to aid in both the detection and reversal of ATM-based malware. We can also ensure the integrity of ATMs and assert that ATMs are free from malware infection.

■ **Source Code Review**

IOActive consultants have years of code auditing experience and regularly assist organizations with highly complex and advanced security challenges. IOActive's expert consultants often conduct source code reviews of ATM firmware and ATM management software. Our experienced security auditors know how to identify and examine vulnerable points in design to uncover flaws that may result in a security compromise. We deliver detailed documentation of the location and nature of problems we find, and our consultants advise your developers on how to address each immediate problem so you can avoid similar problems in the future.

About IOActive

Passion and pride through quality work is rare, which is why IOActive has spent the last decade searching for the required blend of technical expertise and work ethic that comprise a world-class, international security team. We are committed to staying on the cutting edge of technologies and offering unrelenting value—something our customers have come to rely on over the years and can depend on in the future.

Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, application security and compliance. Boasting a well-rounded and diverse clientele, we not only provide unparalleled technical services, we also strive to become a trusted advisor to our clients, enabling us to fully understand and help them achieve their business and security goals.

As a home for highly skilled computer security professionals, IOActive attracts the likes of Barnaby Jack, Ilja van Sprundel, Mike Davis, Michael Milvich and Walter Pearce. We also boast key advisors like Steve Wozniak and Jason Larsen, luminaries who affect how security and technology shape our world. IOActive's vast industry experience consistently helps our clients stay ahead of tomorrow's threats.



Contact Information:

info@ioactive.com

206.784.4313

ATM_AND_FINANCIAL_SECURITY_SERVICES

www.ioactive.com