AN INTERVIEW WITH GUIDO RONCHETTI
CTO, XTN COGNITIVE SECURITY

STOPPING ONLINE FRAUD

STOPPING FRAUD is a mature issue in online payment applications and services, and is based on well-conceived concepts such as profile-based analytics. But extending these techniques to web-based eCommerce has not been as straightforward, simply because attribution, network protocols, application credentials, and account management are so different from legacy approaches. Cyber security solutions for addressing web fraud have thus required creative algorithms and novel methods for detection, mitigation, and response.

XTN Cognitive Security is an Italian firm that specializes in addressing fraud-related issues. Their platform is well-known in local Italian markets because of its integrated approach to fraud protection, smart authentication, and behavioral monitoring. We spent time with Guido Ronchetti of XTN Cognitive Security to learn more about their plans to extend their solution to an international market and how he sees the web-based fraud ecosystem evolving.

EA How do traditional fraud methods translate to online services? What is the goal of the fraudster?

GR Online services suffer from a wide variety of frauds. One of the more common patterns is related to account or sensitive information takeover. Takeovers range from taking control of the bank account of the victim, to stealing their credit card information. The result is that, most of the time, an undesired transfer to a temporary account is accomplished by the fraudster. There are also more technologically-advanced fraud scenarios, where the attacker takes control of the application used to perform fraudulent transactions directly. With the rising of online onboarding procedures in next-generation payment services, there is also a rising trend related to rogue identities and BOT driven account creation. The fraudster's goal is to monetize the attack as quickly as possible, and to find an easy to scale and maintain fraud flow (cost reduction is an issue for everybody).

EA How does the XTN Cognitive Security Platform work? What problems are you solving?

GR XTN Cognitive Security Platform is a comprehensive fraud prevention platform. Our vision is to correlate different layers of analysis to obtain a holistic approach to detect fraudulent events. The platform considers the posture of the endpoint used to access a critical service, the digital identity of the user, and the risk profiling related to business content of events. Our unique technology relies on cutting edge artificial intelligence to provide for accuracy. Our technology combines different needs that are mandatory in the fraud analysis space: Behavioral perspective, the intelligibility of the risk causes, flexibility, and real-time response. We address the challenge of providing visibility about fraud attempts coming from consumer-facing or internal critical services. The banking sector is one of our reference markets, where limiting payment related fraud is especially important. But other markets also need this kind of protection. We are working, for example, in the automotive environment to protect connected vehicles' services.

EA You've had great success in the Italian market. What is your strategy for extending your offer globally?

GR We are excited to be approaching the global market, knowing full well that our technology offers a unique set of features and differentiators. From a go-to-market point of view, we are selecting some strategic partners with specific skills in fraud and logical security fields. Moreover, we are engaging in marketing initiatives (online channels, exhibitions, market events) in order to spread the know-how about our solutions. Finally, we activate partnerships with other synergistic vendors or partners.

EA How does your solution enhance authentication for mobile and web applications?

GR Authentication to us implies use of multiple proof factors. In the XTN Cognitive Security Platform, digital identity validation relies on different layers: Behavioral biometrics features, endpoint trust, and cryptographic quantities. These layers let us modulate the authentication factors considering the endpoint trust or risk, and including continuous behavioral analysis to recognize anomalies. Our goal is to provide the smoothest user experience possible, while keeping the highest security level. To do that, we consider the endpoint, and in particular, mobile devices, as the central actor in identity proofing.

EA Any near- or long-term predictions about online fraud or about mobile and web application security in general?

GR We see high pressure globally on mobile online services. Security awareness is increasing, and users demand secure services, both considering privacy and money. On the other hand, service providers are struggling to address growing security threats, while also maintaining ease of use in their apps. We are now very focused on getting everyone to understand the importance of In-App Protection. We strongly believe that protecting the app goes beyond the app assets in the end-point. We think that modern protection requires implementing a probe-evaluate-react pattern, including the app's technological threats detection together with behavioral and identity-related features. Our technology is taking all relevant information from the app to our clients without any user experience impact, and building risk-driven reaction flows that originate at server-side, where the trust should be.

Our vision is to correlate different layers of analysis to obtain a holistic approach to detect fraudulent events.