

# PIRACY - DISABLED AND DESTROYED

AN ASIA PACIFIC SUCCESS STORY

## THE CLIENT

Pay-TV operators across the globe face numerous threats, many of which are uniquely challenging to their particular market. Irdeto is committed to combating pirate activity and working with customers to break pirate business models -- ensuring revenues are protected. In each case, Irdeto analyzes pirate technology and practices, works with local law enforcement as appropriate, to provide a speedy and effective solution to the challenges of protecting content. There is no better way to demonstrate this than by a customer case study.

## THE SCENARIO

One of Irdeto's first and most prominent digital customers was a regional pay-TV operator based in Asia Pacific, serving more than 700,000 subscribers and offering over 100 TV channels.

The Operator found itself the victim of smart card emulation piracy. As a result of this piracy, the Operator's subscriber growth began to slow.

## THE STRATEGY

As the Operator's conditional access system (CAS) provider, Irdeto immediately stepped in, engaging its security team and dispatching a local Irdeto technical piracy expert to act as the on-the-ground liaison. The overall objective of the team was to focus not only on the technical aspects, but to find a way to break the pirate's business model.

Irdeto set about gaining a complete understanding of the model, since each client and pirate environment is slightly different. To start breaking the cycle of theft, Irdeto focused first on finding answers to questions such as:

- How does the pirate distribution model work?
- How do monetary transactions take place?
- How does the pirate sustain business?
- Is there paid support?
- What technical countermeasures are best suited to address this threat?
- How do the pirates respond to countermeasures?
- How is the pirated content monetized? At what point do they turn a profit?

After the answers to these questions were discovered, Irdeto focused on breaking down the business model at every point possible -- with the understanding that multiple, small countermeasures add up to unhappy pirate clients. This included:

- Discrediting pirates based on technical ability with repeated and carefully timed technical countermeasures
- Causing inconvenience to pirate clients with countermeasures
- Enabling evidence collection, investigation and legal actions against pirates

## WHY IRDETO?

While most first-generation conditional access (CA) vendors are forced to do a card swap, sometimes to the tune of millions of smart cards and millions of dollars, Irdeto's technology has the unique ability to renew the security of the deployed card base over the air. Irdeto had assisted another operator in successfully adding a layer of encryption keys and cycling the keys over the air, instantly securing the operator's entire smart card base and stopping the pirates in their tracks. It was a powerful proof point, and clearly a cost-effective solution. This immediate action stopped piracy without any customer outages or any influx in volume to the call center.

## THE SOLUTION

Irdeto worked with the Operator to apply the technical countermeasures, and in parallel fought piracy on the ground by working with local authorities and law enforcement agencies. In the spring of 2008, 50 Federal Police, Irdeto's security team, and Operator employees raided 14 properties across the country, apprehending the pirates and effectively destroying the sources of the volume distribution channels.

The operation was a real success. Pirate smart cards no longer worked, and the associated pirate customer base was frustrated -- their investment was made useless.

Following the eradication of smart card piracy, pirates turned to exploit a weakness in the DVB standard --- a form of piracy known as control word sharing (CWS) that affects all CA vendors in the industry. CWS is a major threat in the pay-TV industry, where a pirate steals the regularly changing control word, or scrambling key, that is passed between the smart card and the set-top box (STB) and re-transmits it over a network to other client devices to enable unauthorized viewing of the operator's content. With the mass penetration of the Internet and the advancement of pirate technology, a pirate can use a central server to transmit control words via the Internet to consumers all over the world, or a card splitter to share control words in a home, hotel or neighborhood network. To stop this type of piracy, Irdeto deployed a countermeasure over the air using the Irdeto FlexiFlash technology to establish an encrypted communication channel between the smart card and the set-top box for control word protection. It enforced the use of a legitimate smart card in an operator-controlled STB, preventing the STB from being used as a terminal in a control word sharing network. The system remains secure today.

## THE FUTURE

Currently, the Operator is secure from the piracy threats affecting its market -- including card emulation and control word sharing -- and its revenue stream has been restored. The Operator achieved this success with Irdeto -- without swapping out a single set-top-box or smart card! Pirates have now turned their attention to the next target: a competing CA system. Irdeto effectively eradicated piracy for this Operator, demonstrating the power and capability of its technology and the commitment of the Irdeto team to protecting and securing digital content for Irdeto customers.