Enter the Mobile Financial Services experience

Experience a day-in-the-life of a full-scale mobile financial ecosystem, from mobile money and payment to mobile NFC – tailored to both developing and developed markets.

- **New York, 8am:** enjoy a hot beverage at your local Coffeebox and browse through dynamic coupons: there might be a special gift for you! Sit in the coffee lounge and do some online shopping, or get some account management done and start planning your next vacation. Buy the daily newspaper and you are now ready to head to work, just hop on the next tramway!

- **New Delhi, 2pm:** stop by your Hello Wireless agent to make a deposit and then reload your airline credit. You can then go for a walk around the market and buy some fruit and vegetables. Take a seat on the terrace, check your account balance and send money to your relatives overseas thanks to mobile international remittances.


---

China: digital superpower

In a country of 1.4 billion people, there’s everything to play for:

- A day in the life of NFC
- Safeguarding the videogame economy
- The phone of the future
- Locking down online banking security in the US
What would Alexander Graham Bell say if he could see a smartphone? Leaving aside the fact that they’re not only wireless but small enough to fit in our pockets, the phone has changed beyond all recognition. During the last decade, usage patterns shifted from pure voice communication to email, web browsing and GPS. Now, our phones are our wallets, our books and even our health monitors.

This is only a glimpse of what’s ahead. Mobile network operators are now the link between citizen consumers and organizations such as retailers, governments, banks and transportation authorities. And as personalized communication becomes more prevalent, we’re seeing the development of products and services that strike a balance between ease of use, security and privacy.

Gemalto’s wide range of cross-industry solutions offers innovations in mobile payment, full mobile IP connectivity (LTE), optimized roaming, one-to-one marketing and machine-to-machine (M2M) management. Our aim is to create a solid platform on which mobile operators and service providers can take full advantage of mobile’s potential.

In this issue of The Review, we look at the present and future of mobile. Journey through a day in the life of NFC, which is known primarily for its mobile finance capabilities but has the potential for so much more. We speak to Richard Armstrong of UK card provider Barclaycard, who gives his view on the future of contactless payment. And we glimpse the phone concepts of the (near) future, from flexible, borderless and foldable high-resolution screens to M2M capabilities.

We go beyond mobile, too, from the immersive world of online gaming to China’s rapidly expanding digital landscape. Elsewhere, we look at enterprise and the cloud, the security implications of M2M and whether the US banking system is finally ready to take the fight to the fraudsters.

Philippe Vallée
Executive Vice-President, Telecoms Business Unit, Gemalto
Three times a winner
In November 2011, for an unprecedented third year, The Review was named Best Business-to-Business Title at the APA International Customer Publishing Awards. The awards recognize excellence in customer publishing worldwide.

13 “The sharing aspect of NFC is really interesting and often overlooked”
Debbie Arnold, Director, NFC Forum

Contents

4 DIGITAL DIGEST
What’s new in digital security

8 BULLETIN
The US turns to eIDs; the rise of workplace tablets; why banks are embracing social networking

12 TRENDS
The magic touch
A day in the life of NFC – and why its potential is endless

16 TRENDS
The future of contactless
Barclaycard’s Richard Armstrong on what’s next

18 SOCIETY
Light speed
A look at China’s rapidly expanding digital landscape, from ePayment to the cloud

22 SOLUTIONS
Lofty goals
Enterprises are realizing the benefits of cloud computing, but what about security?

24 TRENDS
Smarter phone
Bendy, talkative and super-connected: the next smartphone

26 SOCIETY
Game over?
How online gaming providers are tackling cybercrime

30 GLOBAL SNAPSHOT
Statistics from the digital world

32 SOLUTIONS
Stars and swipes
Is the US banking system moving into fraud-fighting mode?

34 SOLUTIONS
Links in the chain
M2M is growing in popularity, but is it vulnerable to hacking?

36 IN BRIEF
The latest news from Gemalto

34 DIGITAL LIVES
Secret inventor
Hedy Lamarr, Hollywood inventor

Contributors

Tom Hancock
Tom is a freelance journalist based in Beijing. Fluent in Mandarin Chinese, he has contributed to a range of publications, focusing on green innovation and technology.

Adam Oxford
Adam has been writing about technology for more than 15 years. His work has been published in dozens of newspapers, specialist technology magazines and websites.

Wendy M. Grossman
The founder of UK magazine The Skeptic, Wendy has written about science and technology for titles including Wired, Scientific American and New Scientist.

The Review is produced for Gemalto by Wardour, Drury House, 34-43 Russell Street, London WC2B 5HA, UK
Telephone: +44 (0)20 7010 0999
Website: www.wardour.co.uk

COMMUNICATIONS MANAGER, GEMALTO
Laurence Manouelides
EDITOR
Molly Bennett
ART DIRECTOR
Steven Gibbon
DESIGN DIRECTOR
Ben Barrett
PICTURE RESEARCH
Johanna Ward
ACCOUNT DIRECTOR
Rob Strayer
SENIOR ACCOUNT DIRECTOR
Tim Turner
PRODUCTION
Jack Morgan
PRODUCTION DIRECTOR
John Faulkner
MANAGING DIRECTOR
Clare Oldfield
CEO
Martin MacConnol

www.gemalto.com
Within a decade, more than half of all Visa transactions in Europe will be conducted with mobile devices, according to projections by Visa. During 2012, Visa will launch mobile payment and digital wallet services, which are both part of its long-term Future of Payments strategy. And given that Visa Europe processed nearly a billion transactions each month in 2011, the potential for mobile payments is huge.

The company has already made headway into the electronic payments market by authorizing NFC-enabled smartphones from Samsung, LG and RIM for use with its payWave point-of-sale application.

Source: telecompaper.com

---

**EVENTS CALENDAR**

Gemalto regularly participates in trade shows, seminars and events around the world. Here’s a list of those taking place in the next few months.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Sector</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 Feb–1 Mar 2012</td>
<td>Mobile World Congress 2012</td>
<td>Telecom</td>
<td>Barcelona, Spain</td>
</tr>
<tr>
<td>6–7 Mar 2012</td>
<td>CEESCA Club Meeting</td>
<td>eBanking</td>
<td>Bled, Slovenia</td>
</tr>
<tr>
<td>13–14 Mar 2012</td>
<td>Retail Banking in Europe</td>
<td>eBanking</td>
<td>Brussels, Belgium</td>
</tr>
<tr>
<td>24–25 Apr 2012</td>
<td>EHI Kartenkongress 2012</td>
<td>Financial Services</td>
<td>Bonn, Germany</td>
</tr>
<tr>
<td>24–25 Apr 2012</td>
<td>Cards &amp; Payments 2012</td>
<td>Financial Services</td>
<td>Copenhagen, Denmark</td>
</tr>
<tr>
<td>25–26 Apr 2012</td>
<td>Cartes Afrique</td>
<td>Financial Services</td>
<td>Marrakech, Morocco</td>
</tr>
<tr>
<td>8–10 May 2012</td>
<td>European Banking Forum</td>
<td>eBanking</td>
<td>London, UK</td>
</tr>
<tr>
<td>15–16 May 2012</td>
<td>Cards &amp; Payments Middle East</td>
<td>Generalist</td>
<td>Abu Dhabi, UAE</td>
</tr>
</tbody>
</table>
BY THE NUMBERS

500 million
The number of consumers who will be using mobile banking services by 2013. According to a study by Juniper Research, consumers in the Far East and China will lead this growth, followed by Western Europe. It also predicts a surge in Latin America by 2016. SMS remains the channel most frequently used due to its accessibility, but tablets will become increasingly popular. The report predicts that online banking on home PCs will become “fairly limited.”
Source: juniperresearch.com

8%
The average mobile discount-coupon redemption rate expected by 2016 – more than eight times the rate of the most successful paper coupon campaigns. Once mainly available through SMS and MMS, coupons are increasingly available through mobile email, payments, apps and web. Juniper Research predicts that there will be 600 million regular mobile coupon users by 2016.
Source: juniperresearch.com

483 million
The number of Facebook users who access the social network from a mobile device – a significant chunk of its 845 million monthly active users globally. These numbers represent year-on-year growth of 48% and 39% respectively. Facebook revealed the numbers in February after it announced its plans to go public.
Source: Facebook

Cartography goes collaborative
A partnership between the World Bank and Google is harnessing citizen data to create interactive maps of social infrastructure. Under the agreement, the World Bank has access to Google Map Maker’s global mapping platform, which contains geoinformation about more than 150 countries. The aim of the initiative is to “crowdsource” information and feedback from volunteer cartographers equipped with GPS-enabled phones. This data can be compiled to build a more complete picture of, for example, water shortages in Tanzania. This sort of information is also crucial in the aftermath of natural disasters, when a lack of in-depth knowledge about local schools and hospitals can seriously hamper recovery efforts. The World Bank has so far mapped 2,500 projects in more than 30,000 locations.
Source: wbi.worldbank.org

How technology keeps us healthy
More than two million patients around the world now use a home monitoring service with integrated connectivity. People with common conditions such as cardiac arrhythmia, diabetes and sleep apnea can have regular medical reports sent to their clinic, saving time and money.
Analyst Berg Insight predicts that the number of these systems will grow by 18% between now and 2016, reaching nearly five million connections globally. With more than 200 million people in Europe and the US suffering from one or several chronic conditions, remote monitoring can help to relieve pressure on healthcare systems.
Elsewhere, the market for health and fitness apps, such as pedometers and calorie counters, is growing exponentially. API Research forecasts that the market will have grown from US$120 million in 2010 to US$400 million by 2016 – and that’s in the US alone.
Sources: berginsight.com, api.org
Industry update

Loyalty in a digital world

Customers in Ottawa, Canada, can now gain loyalty points in restaurants and cafés across the city by using NFC tags. With the Spoonity program, visitors to local establishments such as Grounded Kitchen & Coffeehouse and Luna Crêpes & Café can use their NFC-enabled smartphones to earn points and build “status” that can then be exchanged for rewards across the Spoonity group. It’s the latest in a growing number of NFC-based loyalty schemes. Since June 2010, Korean coffee shop chain Caffe Bene has been using the Olleh Stamp system, which was developed by Korean mobile operator KT. Customers tap their NFC phones against a terminal to receive a “stamp” and then exchange a full “book” for special offers. A similar program is in place at Swedish retail chain ICA To Go, and even McDonald’s is considering an NFC loyalty program in its UK outlets.

Source: nfcworld.com

Ultrabooks to feature NFC

The unveiling of new “ultrabooks” was the big news to come out of the Consumer Electronics Show (CES) 2012, held in January in Las Vegas. But more exciting for online shoppers is the fact that many of these super-slim, super-light notebooks will come fitted with NFC capability. Intel’s offering is a collaboration with MasterCard’s PayPass technology that will allow users to tap their NFC-enabled phone or contactless card on the ultrabook’s “wrist rest,” sending their billing and card details straight to the online shop. It is due to be released sometime in 2012.

Hewlett-Packard is also in the game; its Envy 14 Spectre ultrabook, which was released in February, will also be equipped with NFC capability that will allow users to transfer data such as the URL of a map or other information straight from their NFC handset to their ultrabook.

As NFC infrastructure becomes more commonplace, no doubt we will see many more gadgets come with NFC as standard.

Source: Intel, Hewlett-Packard
Pegasus: Open-gateway solution to integrate with your own business model using SYRUS GPS

Add the right tools and solutions to your business model and rapidly build and deploy GPS asset tracking applications

- Export data through a friendly web service platform.
- Add a wide range of distinctive applications to your business.
- Easily integrate accessories to your actual tracking platform.
- Total control and management of devices, SIM cards, data consumption, scripts and configurations.
- Include analytics and data mining to your existing platform.
- Guarantee data string integrity with SYRUS devices.
- Optimize SYRUS’s intelligent event engine and get the most accurate reports.

digitalcomtech.com
The US looks to smart cards for security

A recent Gemalto report sees eIDs as crucial to the government’s efforts to reduce identity fraud

**AUTHOR ANNA SAMBROOK**

Governments have been some of the most enthusiastic adopters of digital technology; countries such as Portugal, Oman and Belgium have introduced eIDs for their citizens. While the United States has adopted the technology for some aspects of its governmental administration, it has yet to fully embrace it.

But in a world of technological dependency and ever-increasing fraud statistics, safeguarding citizens’ identities has never been so important. A new report published by Gemalto examines the existing use of electronic IDs and smart card technology in US government-issued identity credentials and proposes applying this technology to other forms of identification.

Smart card technology is currently used in US passports, the Personal Identity Verification (PIV) cards of all federal employees and subcontractors, the Common Access Cards (CAC) of all Department of Defense personnel and first-responder authentication credentials. However, there have been calls to expand the use of smart card technology to remedy deficiencies in the current system.

Identity theft has been the most common consumer complaint to the Federal Trade Commission for 10 years in a row, and more than 535 million US personal data records have been breached since 2005. On the governmental side, the US Department of Justice estimates that fraud in Medicare, the national social health insurance program, accounts for a loss of US$60 billion a year — which is particularly unacceptable in times of economic austerity.

Identity theft and fraud cause havoc on a personal, commercial and federal scale and create huge financial losses, both directly and in terms of remediation costs.

The Gemalto report explores recommendations for solving these problems through the widespread implementation of smart card technology. One such suggestion is the development of eIDs: electronic versions of secure documents such as driver’s licenses and healthcare identification cards. The new document would contain a chip based on smart card technology, either embedded within the card or in a polycarbonate data page. To verify the eID, the physical document itself would have to be authenticated and the user would then have to provide a corresponding PIN, password or even a biometric identifier such as a fingerprint.

In 2011, US senators Mark Kirk and Ron Widen drew up the Medicare Common Access Card Act, which would apply the eID concept specifically to the Medicare system and be modeled on the Common Access Card scheme. Its supporters estimate that it would save US taxpayers about US$30 billion through preventing Medicare fraud, “phantom billing” and administrative errors. It would also protect the identities of the 48 million senior citizens on Medicare more effectively than the current system.

Tighter control of immigration is a further potential advantage of smart card technology. In April 2010, US senators Chuck Schumer and Lindsey Graham proposed that every US citizen and legal immigrant be given a biometric version of the existing Social Security card, arguing that this would not only decrease identity theft, but also provide employers with a way to verify the legality of hiring a potential employee.

With its benefits including a reduction in identity fraud and savings of tens of billions of dollars, it seems likely that the US will follow other countries’ lead and adopt smart cards for governmental services.

The Medicare Common Access Card Act could save taxpayers US$30 billion by preventing Medicare fraud
Some companies, such as Samsung and Gemalto, are taking the principle of easily managed security a stage further by embedding security functions on to the chips used in tablets, laptops and PCs. These encrypt data to prevent hacking and protect the employee as well as company secrets.

The simple fact remains that device management is an important discipline. Companies must have a defined process in place for dealing with lost devices, even if that means wiping them remotely. But, at the same time, being too overbearing could be counterproductive. A desire for security should not override usability, or all of a business’s productivity gains will be lost. In essence, to be secure should be to be free.

Companies must have a defined process for lost devices, even if that is wiping them remotely

straightforward — and somewhat safer — when it comes to iPads. The iPad app store is policed by Apple and hard-disk encryption comes as standard with iOS. While this means that a fleet of iPads is easier to harmonize, it is still vital to take steps to secure the tablets.

User-friendly tablets will improve productivity and widen IT coverage. But the security exposures need to be neutralized

AUTHOR NICK BOOTH

Lock down your tablets

■ Once the tool of the blue-collar worker, a handheld computer is now used at every point of the production cycle. Global sales of tablet computers are set to increase by 81% between 2010 and 2015, according to a recent IC Insights survey. And as these gadgets become ever more popular, concern is growing about how to keep them secure.

Corporate use is a major driver of this growth. The executive team of the London Stock Exchange, for example, uses iPads to keep pace with the world’s fastest-moving markets. And should anyone fall foul of financial regulations, they will find that the UK’s Crown Prosecution Service also issues tablets to its clerks and barristers (lawyers).

Though mobile data is not new, today’s plentiful supplies of processing power, mobile bandwidth and usability have ensured that tablets can be used anywhere. The sheer pace of change in business has made it an imperative for workers to have access to constantly updated information.

Willie Jow, Vice President of Mobility Solutions for Sybase, a US company that develops enterprise and mobile software, observes: “If you travel to see a customer with a paper binder full of information, by the time you’re off the plane it could be out of date.”

What is clearly of primary importance is keeping these devices, and any sensitive data stored on them, safe. While increasing numbers of companies are issuing employees with tablet devices, others have opted to reimburse employees after they have bought their own — a trend known as BYOD (Bring Your Own Device).

The latter approach can work both in the employee’s and the employer’s favor and have the side effect of improving security. Employees who use their own devices at work tend to look after them better because they have actually purchased them. This minimizes the risk of loss of both data and device. They may also be more motivated to learn how to use tablets properly if they have genuine ownership of them, Jow adds, which also helps lower training costs.

All of this benefits the human resources and finance departments, says Quentyn Taylor, Director of Infosecurity, Governance and Risk at Canon, as they play a crucial role in educating employees. But, he concedes, there are problems
Why the words ‘banking’ and ‘creative’ really can go together

Some banks are turning the industry’s boring image on its head with innovative social media applications

The rapid rise of tools such as Facebook and Twitter has left enterprises everywhere scrambling to come up with ways to take advantage of social media’s ability to reach millions of people instantly.

When thinking about companies that have embraced the power of social media, the banking giants may not immediately spring to mind—but that is changing. US bank Wells Fargo, for example, was one of the first to have a blog, it was the first to have a Second Life presence and it was the first with an avatar persona on MySpace. It now also has a presence on various business blogs and YouTube.

Following Wells Fargo’s lead, banks around the world are now using social media tools internally, and several large external initiatives are in the works. Deutsche Bank, which has been active on YouTube, Twitter (in both German and English) and Facebook for several years, is building on its experience in desktop video to introduce new social-computing tools. Citigroup, the third-largest US bank, is using Twitter, YouTube and its corporate blog in parallel with its traditional disclosure channels. And UK online bank First Direct has a “lab” on its website where users can test-drive new products and services, and suggest their own.

Yet, many banks’ Facebook pages still only feature a corporate blurb and the sort of statistics you would expect to find on their websites. To address this, global software company Serverside recently launched the first card customization application for Facebook. The aim is to help banks drive viral marketing: once the customer designs a card using the app and it is approved, the design is posted to their wall with a link that their friends can click to design their own.

“Banks have realized that they have to be on Facebook, because this is where their customers are engaging with their friends and spending more and more of their time,” says Connor Kinnear of Serverside. “Many banks have pretty unimaginative and unengaging Facebook pages. People do not want to have their banks as part of their social experience unless the banks have something interesting to offer.”

Kinnear cites Capital One and Citibank Malaysia as two of the most innovative banks currently on Facebook. What both have in common is the “un-bank-like” approach they have taken on their Facebook pages, both in terms of content and tone. The message to banks is that they have to do more than talk about their products and services. They must also engage with their customers in new, creative and interactive ways.
We hope you are enjoying this issue of The Review. To help us make it even better – and to tell us what you want to read about – please take a few minutes to fill in our reader survey, which you can find at review.gemalto.com.

You can also subscribe to the magazine at the same location. Subscriptions are free and we deliver the magazine directly to you. The first 75 people to subscribe using the online form will receive a YuuWaa – a digital storage solution from Gemalto, with 8GB of online storage and 2GB of flash drive storage, as well as a flash drive backup.

Don’t forget to select the relevant boxes on the survey if you would like to take out a free subscription to The Review and/or our regular eNewsletter. If you hurry, you could receive a free YuuWaa – the handy new digital storage solution from Gemalto.

review.gemalto.com
The past few years have seen the profile of near-field communication (NFC) grow exponentially. So far, mobile payment is the primary driver for NFC deployments, with high-profile services launched in Singapore; in the UK through Everything Everywhere and Barclaycard; and, most recently, the Isis joint venture of major US carriers T-Mobile, AT&T & Verizon. Around the world, NFC-enabled smartphones and contactless payment cards are already allowing consumers to buy small items with a single touch, while transportation systems such as the London Underground use NFC-enabled ticketing to keep passengers moving.

Much of the publicity surrounding NFC (including in previous editions of The Review) has rightly focused on payment offerings, especially with major players, such as mobile operators, banks, retailers and now Google, deploying services. While mobile payment will see a boom in 2012, the possibilities for its application in the real world are endless. At this year’s CES tradeshow, NFC is now integral to the mobile payment sector, but it can do much more and looks set to become a part of every aspect of our lives. Welcome to the future; just tap your phone to get on board.

A DAY IN THE LIFE…

6:00 am
You wake up and realize that you’re almost out of cereal. You tap your phone on the NFC chip on the box to add it to your shopping list. Milk and toothpaste go on there, too.

7:30 am
You run to the train station and use your phone to tap a reader on the turnstile, which lets you through. While you wait for the train, you tap your phone on the ATM to get some cash for a coffee from the kiosk on the platform.

8:30 am
On the walk to work, you notice the new John Grisham book is out. You tap your phone on the poster to find out how much it costs and read a more in-depth blurb. You decide to buy it and, with two taps on your touchscreen, order it from Amazon.
Intel announced an NFC-enabled ultrabook laptop that not only allows for contactless eCommerce payments, but also opens up a host of online authentication services. In the near future, instead of carrying a stack of business cards, loyalty cards, coupons, tickets and flight details, all you will need is one NFC-enabled device.

Debbie Arnold, Director at NFC Forum, says: “Think about digital interaction at your fingertips; this is the internet in the real world. When two NFC devices are brought close together, they can talk to each other — and it can be any device, as NFC allows a two-way conversation that is compatible with established technologies and is both flexible and useful.”

**Mobile to fingertips**
The beauty of NFC is that it can be applied to almost anything. It opens up a world where users can access anything from their car to their hotel room using a single NFC-enabled device. Early in 2011, BMW announced that it was working on an encrypted NFC key fob that, in conjunction with its ConnectedDrive system, could be used to buy and download train tickets, or book a hotel room and then use the fob to get into the room and pay for it on checkout.

BMW is not the only automotive company working on NFC applications. At the Frankfurt Motor Show in October 2011, Continental revealed the Simply Your Drive NFC key that allows for NFC-enabled phones to unlock and start cars. And Delphi unveiled a NFC-powered smart key fob at the IAA International Motor Show in September 2011 that remotely checks vehicle status, adjusts driver settings and even locates the car.

In the peer-to-peer (P2P) NFC arena, developments have gone from strength to strength. In November 2011, RIM added support for NFC P2P applications for the BlackBerry 7.1, such as tapping phones together to start a multiplayer game or to share files. And PayPal has released NFC-based P2P payments on its mobile app for Android, hot on the heels of the P2P security built into the Android Ice Cream Sandwich release.

**Touch and take**
“The sharing aspect of NFC is really interesting and often overlooked,” says Arnold. “This is the ability for a device to read a very simple RF tag that’s under NFC specs. In most cases, this is going to be a passive tag embedded in a smart poster in a mall or transit bus stop. It’s a tap and read situation — you reach out, touch and get the information you need.”

Singapore’s public transportation provider, SMRT, has already installed iMobSMRT spaces: smart posters in stations that deliver anything from the latest news to

---

**9:00 am**
Using your NFC-enabled fob, you gain secure entry to your office building and log into your computer.

**LUNCHTIME**
You visit Starbucks and use your phone to cash in your loyalty points for a free coffee and to add some new ones with your tuna melt. You also use the phone to find out what special offers are coming up and pay for your meal using your MasterCard.
service updates to consumers with NFC-enabled smartphones. In China, Starbucks worked with one of the country’s leading social media services providers, Jiepang, on a campaign during December 2011 that incorporated NFC technology, location-based services and social media, rewarding consumers who tapped their devices to the smart posters in its stores.

“Like NFC, the popularity of touch interfaces is exploding,” says Jared Bytheway, Research and Development Manager at Cirque. “From computers to tablets to smartphones, even household appliances, we are seeing touch become the interface of choice.”

While you’re busy driving around town with your NFC-enabled car, how about using your smartphone to download some coupons so your next coffee costs a fraction of the price? Applications such as the one developed by Gemalto and HighCo in 2011 make it possible for users to download mobile coupons over the air. The coupons are stored securely on the SIM card until they are redeemed at a contactless terminal at the point of sale.

“When consumers get all the additional benefits of being able to do things like redeem coupons or update loyalty points electronically, using their mobile phones to experience NFC-based transactions, it will become much more compelling,” says Arnold.

Secure and safe
But as with any new technology, security is on everyone’s minds. The media has latched on to the concept of “skimming,” whereby secure information is siphoned off NFC cards by malicious passersby, and a recent report by KPMG showed that more than 60% of consumers are concerned about the security of mobile payments.

The issue has to be addressed in two ways: by developing the technology and standards to counteract potential security flaws, and by building consumer trust in these safeguards.

Arnold believes NFC is extremely safe. “In the payment arena, there are several layers of security, and the NFC Forum has already issued about 16 specifications for our basic specs alone,” she says. “The real focus is going to be at the application level.
This is where the payment associations, the banks and the operators are going to say, “We need to download this application securely through a Trusted Service Manager [TSM].”

For example, Isis — an NFC consortium that includes Verizon, T-Mobile and AT&T — recently teamed up with Gemalto to implement a TSM that offers users an extra layer of security, laying the groundwork for widespread consumer take-up.

“On top of the TSM, it also looks at security over the interface itself when the connection is made. There may even be encryption going back and forth when the numbers are being sent,” Arnold adds. “In addition, consumers can turn off their NFC features and implement additional password protection. You’ve got multiple levels of security here that almost make it more secure than traditional forms.” The result is that mobile payments via NFC are as secure as those with a plastic card.

According to ABI Research, nearly half the NFC handsets shipped in 2016 will feature multiple secure elements, with both SWP (single wire protocol) and embedded solutions shipping as standard practice.

Paul Norbury, founder and CEO of Cardwave, says: “Security issues are being addressed by organizations such as the SD Association and Global Platform. When you’ve got Global Platform standards integrated into the SD card, for example, that’s going to be globally recognized as being safe and secure. And the buzz around the fact that Global Platform is addressing security standards is phenomenal.”

And in the future...
Many of the non-payment applications covered here are still being developed or are in their infancy, with early adopters using them to great advantage. Mass adoption is still over the horizon, however. Gartner predicted in July 2011 that worldwide mobile payment users would reach 141 million in 2011, but said this mass adoption would not happen until 2014.

“The biggest hurdle is the need to change user behavior by convincing consumers to pay with mobile phones instead of cash and cards,” said Sandy Shen, Research Director at Gartner.

Arnold sees the next few years as an exciting time for NFC. “We are working hard on interoperability platforms and I think we are going to see people putting marketing dollars behind the technology that needs to happen on the consumer side,” she says. “I often liken this to how, at the beginning of the internet, could anybody have predicted Facebook? We’re at that stage now where anything could happen.”

6:00 PM
Oh dear, you left your phone on the train! A quick call to the network operator from your landline disables your phone for all NFC activities and tracks it to the nearest station. Fortunately, an honest passenger gave it to the conductor. You can easily reactivate your services in the morning.

9:00 PM
Using your NFC-enabled tablet, you get a coupon from an ad for half-price movie tickets. Oops – you’re a bit late! Luckily, you can tap your tablet on the seat arm and have popcorn delivered to you.
Richard Armstrong of UK credit card provider Barclaycard is a firm believer in the power of contactless. He gives us his view on the state of the market globally, both now and in years to come.

Like many companies, Barclaycard has recognized the allure of contactless. To date, the UK card provider has distributed more than 15 million contactless cards and enabled more than 55,000 outlets across the UK to take contactless payments through its Quick Tap service, which it developed in partnership with telecom company Orange.

This and other initiatives are paying off: transactions through Barclaycard payment acceptance alone now total more than 300,000 a month. This number can only grow: while consumer awareness of contactless payments in the UK lags behind some markets, particularly in Asia, it is growing rapidly. When Barclaycard surveyed consumers’ recognition of the contactless symbol in 2010, 28% of respondents knew what it meant. Just a year later, in 2011, 44% recognized it.

We asked Richard Armstrong, Head of UK Payment Acceptance at Barclaycard, to give us his view on the contactless market in the UK – and beyond.

Q What markets do you see as particularly advanced in terms of contactless?
Some countries are very advanced...
from a contactless perspective, such as Japan, South Korea and Hong Kong. The Far East tends to be technologically advanced anyway, and they are certainly embracing the concept of contactless faster. I think some of this is driven by the fact that, in those countries, there is a higher limit on contactless transactions, which is something we would definitely support.

With the adoption of contactless on mobile phones, I can see the technology supporting higher-value transactions by requiring the consumer to enter a PIN on their phone to ensure the rigorous security standards are maintained.

Q Has Barclaycard been inspired by other banks’ or other companies’ initiatives?
The transport industry has been an important area for contactless transactions and has provided a good blueprint. With Oyster [London’s public transportation card], we saw a swift move from people buying paper tickets to the majority of people carrying an Oyster card. This is the sort of model that we would like to emulate with our own contactless transactions. We will soon be piloting contactless technology on the M6 toll road [a UK highway], allowing drivers to use a card at the tollbooths. I think that transit is an important sector for the use of contactless transactions.

Q What would you like to see in terms of new applications or technologies that are perhaps only in the “ideas” stage?
Consumers want to use contactless technology in areas where it is convenient for them, such as at sporting events and concerts. The contactless watches or wristbands are forward-thinking technological developments for this type of event transaction. Barclaycard has recently gone live at the UK’s busiest concert venue, the O2 Arena. On a typical night, about 75% of the transactions going through would be within the £15 limit, and, as there are a lot of people all trying to buy things at the same time [such as during an intermission], being able to get people through quickly, without having to get cash out, is important. A lot of the innovation that I would like to see is around mobile phones for higher-value transactions. This is a concept that is on the drawing board at the moment and it would be really good to see it take off. The evolution of this will be the acceptance of contactless, and I think we are reaching the tipping point now. We have seen a lot of merchants starting to accept contactless, and we are working with large retailers such as the Co-op [a UK food retail chain]. As contactless becomes more widely accepted, I think the adoption will spread from cards to mobile phones, and the evolution of this will hopefully be higher-value payments on mobiles.

Q What about security, which is a key concern for consumers?
A number of safeguards are in place to ensure the security of contactless payments. The first is the £15 limit, which reduces the amount that a fraudster could spend. Additionally, a card can only be used on multiple transactions using solely contactless payment a certain number of times before a customer is prompted for their PIN. In the unlikely event of fraud taking place, contactless debit and credit transactions also benefit from the same 100% fraud guarantee as standard transactions.

For these reasons alone, I can see the limit increasing on contactless transactions in the short term. In the longer term, some of the ways of facilitating higher-value contactless transactions will start to emerge in the marketplace.

From Barclaycard’s perspective, anything that makes the payment process easier and simpler for consumers, and more efficient for our retail merchants, is something we will support. It will make life easier for all users and we will hopefully see happier customers making more transactions.

We have also noticed that after a person has made three contactless transactions, he or she is increasingly likely to become a frequent user. The ease and convenience becomes obvious after repeated use, particularly when compared with the longer process of inserting a card into a card reader.

“The average contactless transaction takes 12 seconds, which is twice as fast as the average counter transaction”
Driven by government initiatives, China’s digital horizons are expanding rapidly. ePayment, smart meters and cloud computing are all technologies to watch in this emerging superpower.
At the age of 62, retired schoolteacher Tan Zhijing has two mobile phones — one smartphone and another older phone for staying in contact with her daughter, who works in a different province. She pays by debit card when shopping at a local department store and is hesitating about whether to apply for one of the credit cards offered by her bank. “At my age, I don’t think I need it,” she says.

With a population of 1.4 billion, staggering statistics on China’s growth in digital technology are easy to find. The country’s internet population now stands at 420 million, and more than a billion Chinese use mobile phones. More smartphones were sold in China in 2011 than any other country. The spread of digital technology is a result of China’s continued economic growth, averaging 10% over the past decade.

China’s rich coastal cities are home to most of the country’s middle class, the 100 million or so consumers who have come to depend on digital technology as part of their everyday lives. But uptake of digital technology is much lower in China’s countryside, where half the population still lives. In rural provinces, fewer people use the internet and cash remains by far the most popular method of payment.

Economists generally agree that Chinese growth will continue, although at a slower rate over the next decade, with consumer demand for technology continuing. Despite rising incomes, however, Chinese consumers are reluctant to spend relative to their developed-country counterparts. Consumer spending accounts for about 30% of GDP, half that of developed countries such as the US. That means government spending plays a more important role in China’s economy, accounting for almost 15% of GDP. The government’s purchasing of digital technologies is set to increase, covering everything from machine-to-machine (M2M) systems that will manage traffic in major cities to chip-enabled identity cards for every Chinese citizen.

China’s government sees strong strategic value in building a digital nation. Worried about falling into a “middle-income trap” — a period of economic stagnation following rapid growth — the government plans to push Chinese industry up the value chain from low-tech manufacturing to more hi-tech sectors. As part of the hi-tech drive, the government will provide subsidies for Chinese technology firms, creating new industry standards and leveraging the country’s internal demand to build capacity that it can later export to other countries.

China embraces chip technology
ePayment is one area where the government’s strategy is clearly visible. About a third of the population regularly uses debit cards, with 2.3 billion payment cards in circulation in 2010, according to ABI research. China’s digital payment market is dominated by UnionPay, a payment network established by a group of Chinese banks in 2003. More than 95% of UnionPay cards use magnetic stripe technology, but that’s set to change over the next five years. The Chinese government will require all debit cards to change to chip and PIN technology by 2015. It will be a major transformation.

The key reason for the switch is to prevent fraud, commonly committed through the use of cloned customer...
ATM cards. China’s new generation of chip and PIN cards will use a Chinese-designed standard called PBOC 2.0, which closely resembles the Europay, MasterCard, VISA (EMV) standard used in other countries and offers higher security for card users. As UnionPay is the only payment system that can be used with the PBOC 2.0 cards, the new standard will consolidate UnionPay’s dominance of China’s debit card market. PBOC 2.0 cards have already been piloted in the city of Ningbo, with the costs of transition paid for by China’s banks.

The transition to PBOC 2.0 will bring opportunities for firms across the supply chain, whether for ATM manufacturers or card manufacturers, which can sell to the banks. Opportunities abound for China to expand its digital payment infrastructure: it has 300,000 ATMs compared with 480,000 in the US, despite having four times the population.

Three of China’s state-owned telecom companies were awarded licenses in 2011 to set up mobile payment services. Peter Chen, head of new telecommunications product development at Gemalto China, says that if mobile payment is to gain mass adoption in China, creating an industry standard is vital, given that partners from various industries will have different interests. In Singapore, through the Infocomm Development Agency (IDA), a single, nationwide NFC mobile payment infrastructure is set to be launched in the middle of 2012. “The IDA can be a model for China,” Chen says, “whereby the Chinese government can step in and guide the industry.”

**Let the machines do the talking**

The Chinese government has announced its intention to foster the M2M industry, known in China as the Internet of Things. Chinese premier Wen Jiabao made a speech in 2009 stating that “the Internet of Things has a bright future” and calling for the rapid development of the industry. It has pledged 3,860 billion RMB to develop this industry by 2020, the China-based 21st-Century Business Herald reported.

Faced with a rapidly growing number of automobiles, Chinese cities are planning to use M2M technology for traffic management. One project in the city of Wuhan requires drivers to install a wireless card reader in their vehicles that automatically charges their bank accounts when they use certain tunnels in the city. Automated

China has 300,000 ATMs, compared with 480,000 in the US, despite having four times the population.
Mobile supermarket hits Chinese subways

Mobile payment is already taking off in China, thanks to the popularity of mobile phones. Chinese retailer Yihaodian launched several “virtual supermarkets” in 2011, posting pictures of its products on subway station platforms in major Chinese cities. After downloading Yihaodian’s smartphone application, users can purchase the items by tapping their phone on barcodes next to the pictures, and have the items delivered to their home within 48 hours. “The virtual supermarket targets young, tech-savvy consumers who don’t have time to shop the conventional way,” Yihaodian’s head of PR told local media.

Traffic management will be funded as part of China’s “Smart City” project, which will attract more than 40 billion RMB of government investment over the next five years. China’s largest power-grid company, the State Grid, has launched “smart meters” that send electricity-use figures back to the company along its power lines. Forty-five million homes have been fitted with smart meters and the State Grid plans to upgrade the rest by 2014.

In the cloud

Growing internet use is driving China’s cloud computing market, expected to grow by 30% this year, according to research firm IDC. The government has designated cloud computing as a “strategic industry” in its five-year plan. Although exact amounts have not been made public, it’s likely that cloud computing will receive a major slice of the two trillion RMB set aside for IT investment.

The first stage has been the establishment of “cloud computing bases” where cloud-computing firms are given rent-free space and tax breaks. The largest of these covers 646,000 square meters in northern Hebei province and was partly designed by IBM. Beijing plans to create 50,000 cloud-computing jobs in the city by 2015, establishing its own cloud-computing base, “Cloud Valley.”

There are serious obstacles to the development of cloud computing in China. Internet speeds in the country are less than half the global average, according to the China Internet Network Information Center. China also employs the “Great Firewall,” an internet censorship system, which further slows internet traffic.

For Tan Zhijing, the benefits of digital technology are “convenience and saving money.” The dynamic between Chinese consumers, who look to digital technology as a way of making life simpler, and the government, which views digital technology as a tool for social management and as a strategic element in China’s march up the global value chain, will be what drives the market for digital technology in the country over the next decade.
Lofty goals

Business are realizing the benefits of moving to cloud-based services, but challenges remain

Cloud computing is currently a hot topic, but it has existed in many forms for more than a decade. Software-as-a-service (SaaS) applications such as Salesforce.com were at the vanguard, opening our eyes to the cloud’s potential as a tool for productivity. There is now a move toward infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS), where companies are essentially leasing computing resources and development tools without capital expenditure.

On a practical level, the cloud can deliver a level of efficiency that many businesses have not yet been able to achieve. For one thing, they do not need to develop and maintain expensive local networks, as any internet-connected device can use the cloud. “The main advantage is that your business data is available from everywhere and anywhere, making a business more responsive and flexible,” says Graham Fern, Technical Director of Axon IT, a British corporate IT supplier. “There should certainly be cost-saving benefits from reduced hardware costs and an added benefit of a known, fixed IT cost per user.”

Skyrocketing numbers
The pace of wider corporate adoption of cloud computing is predicted to grow over the next decade from 10% to 70% of IT spend. In-Stat says that by 2014, the US alone will be spending US$13 billion on cloud-based systems, a 400% increase on today’s figure.

Global attitudes to cloud services vary significantly. In a June 2011 survey by chip maker AMD, 47% of respondents in Asia said the cloud represented a “strategic shift” in their companies’ IT policies, versus 33% in Europe. When asked whether the cloud was a cost-saving necessity or a strategic priority, 15% of Asian respondents said the former, compared with 31% of Europeans. And it seems chief information officers are behind much of Asia’s adoption of the cloud: 71% of Asian respondents said their CIOs were driving implementation, compared with 24% in Europe.

Whatever their reasons for doing so, companies that use the cloud must remain vigilant about how they are managing their IT overall. “Visibility of application performance is one of the biggest issues for companies using cloud services and virtualization,” says Dave Ball of US-based Visual Network Systems. “The corporate IT department is still very much responsible for delivering overall service quality to customers. They are not ‘off the hook’ because they have outsourced portions of their infrastructure or even the application.”

He adds that, if the enterprise is using a public-based cloud infrastructure, it will not have the same access or visibility as it does with its own data center. Virtualization of its own data center can also cause a lack of visibility if the enterprise is using legacy performance management tools, and performance problems can happen within the virtualized environment that legacy tools will not see.

For that reason, the idea of the cloud being the death of the IT department is premature. It will transform how IT is run and what its core competences will
be, but a level of control and oversight will always be needed, no matter how far the cloud is integrated into an enterprise’s operations.

Large businesses that are examining ways to rationalize their IT infrastructures to save money and improve services are also looking to partnerships within their sector. A good example is Everything Everywhere, the UK brand formed by the recent Orange and T-Mobile joint venture. The integration of the two IT platforms not only saved money, it enabled the new business to offer cloud-based services to its customer base. Everything Everywhere has publicly stated that it intends to place 40% of its IT in the cloud within three years. This will form the cloud-based backbone on which the company can build its future services through its service-oriented architecture.

Another factor driving the rapid expansion of the cloud has been the push to reduce carbon emissions. Adopting more cloud-based platforms could halve US firms’ carbon emissions, saving US$12 billion a year by 2020. But server farms are also under pressure to ensure that their own carbon emissions are within the targets of their host countries – a pressure that will continue as the cloud expands.

**Protecting data**

The benefits can be persuasive, but security remains the biggest barrier to more rapid corporate adoption. The main concern is the movement of sensitive data to and from the cloud and the fact that data owners no longer store this information in their own ringfenced data silos. Encryption is robust enough to ensure data transmission is secure, but access control and data-usage policies are also vitally important for enterprises that store sensitive data in the cloud.

Richard Thomas, head of the UK’s Information Commissioner’s Office (ICO), an independent authority, has been vocal for several years about the responsibilities that the government and private businesses alike have in relation to cloud-based services. After a spate of high-profile security breaches in 2007, he said: “The majority of organizations process personal information appropriately — but privacy must be given more priority in every UK boardroom. Organizations that fail to process personal information in line with the principles of the Data Protection Act not only risk enforcement action by the ICO, they also risk losing the trust of their customers.”

There are several ways to secure this data. Eitan Bremler, Virtualization Product Manager of Israeli IT security company Radware, says: “Cloud providers can implement security measures that can protect their data centers from DoS [denial of service] and DDoS [distributed denial of service] attacks by using an intrusion prevention system, and WAF [web application firewall] protection can prevent unlawful access into the hosted applications.”

Human error poses perhaps the greatest threat. Employees routinely misuse passwords, which is why many businesses are moving to two-factor or even multi-factor authentication. This can involve a physical token combined with a unique piece of data, typically a password, or it can be an application on a mobile phone, such as Gemalto’s Protiva Mobile OTP platform.

If companies can overcome both the practical and perceived barriers, the potential is huge. AMD’s figures are encouraging: on a global level, the majority of organizations (60%) are already seeing value from their cloud implementations, with that number jumping to 67% in Asia, while 28% of businesses stated it was too early to say.

Telecom companies may be showing the way, but businesses of all sizes will turn to the cloud at an ever-quickerening pace. Its versatility and cost savings will make the cloud an essential component of companies’ IT strategies over the next few years.
Smarter phone

The iPhone’s arrival in 2007 changed the way we think about our cellphones. No longer were we dealing with tiny screens and basic web and email. Now, our smartphones allow us to follow celebrities on Twitter, buy things without setting foot in a store, watch live TV and launch angry birds at green pigs — and all in glorious, high-definition color. But the potential of our favorite gadget doesn’t stop there...

AUTHORS RUTH GANTHONY & ANNA SAMBROOK
ILLUSTRATION RICHARD OSLEY/NB ILLUSTRATION

Look who’s talking
Machine-to-machine (M2M) mobile communication has been around for more than a decade in the form of GM’s OnStar vehicle communications system, but there’s more where that came from. Future applications include medical monitoring services that alert patients if there are changes to their vital signs and find them in an emergency, and a GPS-based taxi monitoring system that supplies real-time information on vehicle status and traffic congestion.

Doctor, doctor
In October 2011, NTT DOCOMO unveiled its Toshiba Regza smartphone and a range of prototype “jackets.” One jacket contained a radiation sensor; another a UV and breath-odor sensor; another a health management feature that allowed the user to check their body fat percentage and muscle ratio. It’s never been so easy to become — and stay — healthy.

Touch and go
NFC-enabled smartphones could soon replace your wallet, train and bus tickets and more. See our feature on page 12 for a look at how NFC is set to make your life even easier.

Goodbye, dead batteries
Apple has patented a technology that provides power to portable devices using energy from the sun. The patents also cover the development of a back-panel reflector that uses sunlight to illuminate laptop screens. And renewable energy company Go Solar USA has developed technology that uses solar power and wireless internet signals to charge smartphone batteries.

Get online and stay there
Social networking is becoming an increasingly important part of the smartphone experience. Reports suggest that HTC is producing a model — codename “Buffy” — designed entirely around Facebook and based on Android software. Android itself, meanwhile, is releasing a People App later in 2012 that will integrate all of the user’s social networking activity.
Breaking the mold
Both Samsung and Nokia have developed prototypes for bendy phones. Rather than pressing buttons or touching screens, the Nokia Kinetic operates entirely by flexing and twisting. While Nokia has said its flexible friend could appear on the market within three years, Samsung plans to introduce phones with bendable displays as early as the spring of 2012. The flexible AMOLED screen means it can be folded over or rolled up for easier storage.

Crystal-clear thinking
LG’s 2009 Arena phone came with a see-through keyboard, but a translucent screen is harder to achieve. The CTP002 concept phone from Aston Martin and Mobiado has a solid sapphire crystal capacitive touchscreen and is completely transparent. Researchers at Stanford University in the US have also created the first transparent phone battery. It’s made of a mesh of electrodes packed so tightly that they are invisible to the naked eye.

“What are you doing, Dave?”
The thought of a phone holding a conversation may be slightly unnerving, but voice recognition software promises to make users’ lives a lot easier. Android’s 4.0 operating system will feature a “continuous open microphone” function, allowing users to dictate for as long as they want, in any language. The Siri feature of the iPhone 4S allows users to schedule meetings, send messages and search the web without even touching the phone. In a few years’ time, keyboards could have become a thing of the past.

That’s a wrap
In November 2011, Nokia released its GEM concept phone, which has a wraparound touchscreen covering the entire surface of the phone. Depending on the function the user selects, the handset could take on the appearance of a camera, phone or map, with both sides being interactive and completely customizable. So, you could have the same map image on each side of the phone but at differing zoom factors, allowing you to flip between a detailed and large-scale view.

On cloud nine
The mobile cloud is the next big thing in cloud computing. Apple’s iCloud stores users’ music, photos, documents and apps in a “hard drive in the sky” so they can be accessed — without syncing — from any device. And Android’s 4.0 Ice Cream Sandwich release, set for later in 2012, will add browser and email functions to its cloud service.
Videogames are big business. Players devote hours – and real money – to online gaming, but recent security breaches have exposed the vulnerability of their personal data. When it comes to security, are manufacturers running out of lives?
The videogames industry had another successful year in 2011. Several landmark games broke sales records, underlining the industry’s position as a mainstream entertainment medium. For all the positive news, however, 2011 will probably be remembered as the year in which security threats to online gaming companies reached a critical point.

The good news is that the game market is growing again. Putting a figure on it is difficult; estimates vary wildly depending on whether they take into account console games, social gaming, PC hardware, smartphone games or handhelds. A report by Gartner in July 2011, however, estimated that the global games market was worth US$74 billion, up 10% on 2010.

The market’s scale becomes clear when it is compared with Hollywood’s output. Following its release in November 2011, Call of Duty: Modern Warfare 3, a cross-platform multiplayer game in which teams of players fight through rounds based on military scenarios, sold US$1 billion worth of copies in just 16 days. The fastest-grossing movie to date – James Cameron’s 2009 3D extravaganza Avatar – took 17 days to reach the same milestone.

Set against this success is the extraordinary number of attacks against servers owned by games companies in 2011, and gamers’ growing realization of just how much personal data these companies hold. The most significant incident involved electronics giant Sony and its PlayStation Network – a service that PlayStation 3 owners must sign up to if they want to join other players in online games. Account details belonging to millions of gamers were lost in an embarrassing series of attacks by hacktivist group LulzSec and subsequently posted to internet file-sharing sites.

Credit card information held in the compromised Sony database was, of course, encrypted. But what gamers lost was potentially more valuable to the console manufacturer: trust. The PlayStation Network was repeatedly taken offline, disabling access to online games that players rightly felt they had paid for. Worse, customers exposed to the risks of identity theft and credit-card fraud were forced to request new cards and change their banking details through no fault of their own.

While unfortunate for Sony, the incident – now resolved – underlines the complex relationship between interactive entertainment and security. The industry has been a prime target for hackers and criminals for years, and has an almost unique exposure to risk. Videogame companies routinely gather and store player details when players access online features of games, download new content and patches, and take part in community discussions and forums. In addition, newer and highly controversial forms of digital rights management (DRM) software require online authentication every time a game is started; as a result, player details are being logged and stored in several large, highly centralized databases every time they purchase or play a game.

Gaming binds together a player’s personal and financial information with their chosen hobby that PlayStation 3 owners must sign up to if they want to join other players in online games. Account details belonging to millions of gamers were lost in an embarrassing series of attacks by hacktivist group LulzSec and subsequently posted to internet file-sharing sites.

Credit card information held in the compromised Sony database was, of course, encrypted. But what
The number of PC games downloaded via digital distribution clients such as Steam or Direct2Drive have reached parity with traditional boxed copies.

New business models are also emerging, based on social gaming, micropayments and "freemium" online games in which access to a virtual world is free but players buy in-game items or upgrades for cash. These account for a market estimated at US$4 billion a year and require game companies to hold and store sensitive information.

Barely a single major game publisher or hardware vendor wasn’t affected by some kind of security breach in 2011. Valve Software, developer of the hugely successful Half-Life and Portal franchises and owner of the Steam digital download portal and digital rights-management platform for PC games, alerted users in November that its customer databases had been compromised. The year was rounded off with Square Enix, famous for the Final Fantasy and Deus Ex series, announcing that gamers’ personal information had been lost in an attack on its servers.

Nintendo, Sega, Microsoft, Codemasters, Epic, Bethesda and Bioware were all also subject to attacks that made news headlines around the world.

Companies are taking steps to address the threat. One of these is the publisher of the Call of Duty series, Activision Blizzard, which is arguably one of the most experienced when it comes to balancing customer service and account security. One of the company’s most lucrative titles, contributing about a quarter of its US$4.5 billion annual revenue, is the massively multiplayer online role-playing game (MMORPG) World of Warcraft (WoW). More than 10 million people pay up to £10 (US$15) a month to subscribe to WoW, making it between four and ten times more popular than its closest rivals (MMO companies are notoriously secretive about actual subscriber numbers).

The size and scale of WoW illustrates the problems faced by game companies operating in the online space. The virtual economy within WoW has a significant real-life value, with tradable items and characters exchanging hands for hundreds of dollars on sites such as eBay.

The value of the in-game economy is such that “gold farming” – in which criminal groups accumulate game-world currency and sell it for real money – has been cited in academic papers as a significant industry in developing nations. One estimate suggests as many as 400,000 people may be employed as gold farmers in an underground industry worth US$1.4 billion a year.

**Phishing: not just for banks**

While there have been no reports of credit card information going missing from Activision Blizzard’s servers in the seven years that WoW has been running, player accounts are hacked on a daily basis by groups looking for tradable items. Players are routinely subject to phishing scams and spam emails masquerading as communiqués from the game developers, and keylogging software that captures password data as it is typed is often distributed through sites targeted at WoW subscribers.
The effects of account breaches are often devastating to players and expensive for Activision Blizzard. To support the large player base, the company employs about 4,600 people globally, many in positions related to the management of player accounts. The company has been largely successful at maintaining its reputation among players, but it has come at a cost not many rivals can bear. Support staff must verify every report that items have been removed from an account illegitimately before restoring them. Attacks against individual accounts also affect the wider community, as gamers will often have access to resources that are shared with other players.

“These large MMO games stay popular for so long because the games are fun to play and they make it possible for people to build up a community,” says John Lineberger, Marketing Manager at Gemalto. “But then what keeps people coming back is that they’re accumulating virtual goods and they’ve invested their time and creative energy in their characters. So the last thing they want is to wake up one morning, log into their account and find that everything’s gone.

“It’s a terrible customer experience and, as a service provider, you really want to shield your customer from that kind of shock,” he adds. “It’s like buying a new car and then finding the engine has gone.”

**Battling the “boss”**

Activision Blizzard has responded to the problems in several ways. It has repeatedly made changes to the game’s architecture to devalue the real-world worth of items, and has introduced an optional two-factor security login in the form of the Blizzard Authenticator. Available as a hardware token or smartphone app, the authenticator generates a one-time passcode for entry every time players log in.

If World of Warcraft exists in the fascinating space between fantasy entertainment and real-world economics, it is also at the cutting edge of what customers will tolerate culturally in the name of security. When the company changed its forum rules to force players to post under their real names – partly to cut down on the number of abusive posts and partly to coincide with the extension of its security mechanism to other franchises – there was a backlash that forced the company to allow anonymity once more. When it tried to make game access more convenient by not requiring an Authenticator passcode under certain conditions — such as logging in from a recognized IP address — many players felt they were losing a level of security they relied on.

**Level up**

Having had such a successful 2011 in terms of sales, the creative and dynamic game industry is keen to keep 2012 free of bad-news headlines.

“Gamers are, for the most part, pretty tech savvy,” Lineberger concludes, “which means they have very high expectations. That’s one of the reasons there’s such a big backlash when there is a breach, because they know things can be done better, and they expect it.”

Successful security solutions for online gaming, then, must carefully balance a few conflicting needs: protecting a player’s emotional and creative investment and enjoyment; reducing piracy and maximizing the return for the publisher; and staying sensitive to the privacy of a game’s community while enabling social interaction and sharing. Combining those things may be harder than finishing the games themselves.
**Statistics from the digital world**

## Global snapshot

### 30,800

All of San Francisco’s 30,800 parking meters are being issued with NFC stickers during 2012. The stickers – which have been rolled out in the Castro district and will go citywide throughout 2012 – mean that drivers can use their handset to pay for parking, get a reminder of when their parking time runs out and add extra time remotely.

Source: sfmta.com

### US$10 billion

Ireland’s energy authority is considering moving to a system where a smart grid would monitor the country’s energy use. Other options under consideration include wind energy and electric vehicles. The Sustainable Energy Authority of Ireland estimates that measures such as these could save the country up to US$10 billion in fuel import alone by 2050, among other savings.

Source: seai.ie

### 37.5 million

Nearly 40 million US consumers aged 14 and older will make at least one purchase using their cellphone in 2012, according to eMarketer. This is up from 2011’s figure of 26.8 million.

Source: emarketer.com

### 60%

The mobile penetration rate in Sudan is now about 60%, according to mobile network operator Zain Sudan. South Sudan, which gained independence from Sudan in July 2011, has a penetration rate of just 20%. Mobile continues to be big in Africa: according to Informa, mobile subscriptions in the continent will pass the one billion mark by 2016 – a 60% increase from the current figure of 616 million.

Source: news.sudanvisiondaily.com, informa.com

Image: Andrew McConnell/Panos
The Danish island of Bornholm will get 77% of its power from renewable energy by 2025. The island, which aims to be 100% sustainable and CO₂ neutral, will function as a full-scale laboratory for future intelligent power systems that make use of M2M-powered smart grids.

Source: bornholm.dk

Barcelona and Madrid are throwing their weight behind contactless. Three major banks – La Caixa in Barcelona, and BBVA and Bankia in Madrid – are equipping thousands of points of sale (POS) with NFC and contactless card technology. In Barcelona, 17,000 La Caixa POS and a million cardholders will be moved to contactless and NFC by the end of 2012. In Madrid, BBVA and Bankia will equip millions of customers with contactless cards first, and then move to NFC once the technology becomes more commonplace.

Source: nfcworld.com

Mobile money service M-Pesa now has 14 million users in Kenya, providing mobile banking to more than 70% of the country’s adult population. In fact, M-Pesa currently facilitates more transactions locally than Western Union does globally, according to the International Monetary Fund.

Source: imf.org

By moving its paper-based national census online, Australia could save A$80 million. The Australian Bureau of Statistics (ABS) is aiming to collect 80% of the 2016 census electronically, which would cut down on the 29,000 staff needed to collect paper forms at a cost of A$160 million. For households with no internet access, the ABS is exploring the idea of deploying up to 10,000 tablet or smartphone devices.

Source: theaustralian.com.au

In Malaysia, 57% of mobile users primarily or exclusively access the web using their mobile devices, according to a study by mobile ad network InMobi. Mobile web users now spend 103 minutes a day using their mobile devices for activities other than calls or SMS, with those in small towns being the most enthusiastic adopters.

Source: inmobi.com

Ten percent of Koreans have NFC phones, with that number expected to quadruple by the end of 2012. This is due in part to the introduction of NFC-enabled transit ticketing and advertising. At the end of January 2012, an NFC shopping zone completed a three-month trial in Seoul’s busiest shopping district. Shoppers used their smartphones to make small purchases, order food from their tables, get bus timetables and collect loyalty stamps.

Source: kcc.go.kr
Stars and swipes

While the rest of the world adopts fraud-fighting technology such as chip-based cards, the US banking system has so far resisted change. But with fraud figures on the rise, how much longer can it hold out?

AUTHOR WENDY M. GROSSMAN

Why do you rob banks?”, a reporter once asked the legendary American bank robber Willie Sutton. His often-quoted but apocryphal reply: “That’s where the money is.”

Modern-day criminals still have their sights set on banks, but today the money is in cyberspace and, increasingly, the targets are not banks’ secure websites, but their customers. These cyber-attacks take many forms: computer malware; monitoring devices such as keyloggers; man-in-the-middle attacks; and phishing emails — those spam emails people get that look nearly identical to those from a bank, down to the logos and legal wording. Another is a new take on an age-old con: simply duping insiders or consumers into sharing confidential information, a practice now called social engineering.

Overseas solutions
Every country handles such problems differently. A trend among UK banks is to issue customers with handheld devices that generate one-time passcodes when they log into their bank’s website. Some of these devices, such as PINsentry from Barclays, create a code using the embedded chip when the user inserts his or her card. The result is two-factor authentication: something you have (the card) and something you know (the code).

In the US, however, most credit and debit cards still use magnetic stripes; chip and PIN is nearly unknown. One barrier is the US banking culture. Adam Dolby, eBanking Sales Manager, Gemalto Americas, says that, more than in Europe, US banks have tended to accept fraud as an inevitable cost of doing business. Conversely, security devices have been regarded as a cost with little benefit. But rising fraud and angry customers make this situation unsustainable.

Dolby explains that, in the US, online banking is roughly split in half: consumers do internet banking and corporates do direct deposit, tax payments and payroll. Like many countries, the US grants regulatory protection to consumers, protection that has been reinforced by efforts to encourage consumers to use the internet as a platform for eCommerce by teaching them that they are not liable for losses.

This approach presumes, however, that organizations have the staff and knowledge to look out for themselves. “Caught in the middle of that divide are municipalities, retailers, small businesses and non-profits, where often the services being used are similar to consumer online retail,” says Dolby. “However, they’re really considered a corporate banking client.”

Such operations do not have the manpower or expertise to protect themselves — and they

In the US, most credit and debit cards still use magnetic stripes; chip and PIN is nearly unknown
are increasingly the targets of online banking fraud.

According to the Nilson Report’s annual fraud figures for 2011, the US accounts for 47% of global card fraud even though it generates only 27% of the total volume of transactions. In August 2011, Dell SecureWorks estimated US banking fraud in 2010 at US$1 billion. The new Federal Financial Institutions Examination Council (FFIEC) guidelines announced in July 2011 do little to protect the customers on Dolby’s list, who are being stuck with the blame — and the losses.

Mounting losses

In 2010, the FBI said that 205 US businesses had reported incidents of corporate account takeover since 2004, with losses of US$40 million. By the end of 2011, those figures had mushroomed to 400 incidents and US$85 million and look set to continue growing. In one example, the Diocese of Des Moines, Iowa, lost US$600,000 in a single weekend through an organized attack that funneled funds through “money mules” — usually unsuspecting middlemen who transfer stolen money electronically from the victim account to the fraudster.

The reasons why this type of fraud is on the rise are simple: typically, organizations have larger balances than consumers and the fraud is harder to spot among numerous transactions.

Attacks are increasingly sophisticated. Phishing siphons victims’ money by targeting one or more individuals within an organization who have the authority to transfer funds. Man-in-the-middle attacks hijack browser sessions and direct internet users to a fake website. Alternatively, thieves gain access to vital information through implanted keylogging malware or social engineering.

Technology to prevent this type of fraud has long been available. eCommerce transactions, for example, are protected by the public key infrastructure (PKI) underlying the Secure Sockets Layer (SSL) protocol that ensures financial details are encrypted in transit. The one-time passcodes and PINs generated by the devices European banks deploy to their customers are another example.

While Americans are famous for enthusiastically adopting new technology, they are conservative when it comes to financial change: many families still pay their bills by personal check, and even smaller innovations like the $1 coin meet with near-total rejection. Any fraud protection device needs to be easy to use and offer clear benefits. The Ezio Plug&Sign is one recent development (see sidebar).

Dolby names two challenges for anyone operating in the online banking security space: continuing to evolve the design of any product to stay one step ahead of organized criminals, and addressing what he calls the “ultra mobile” space — smartphones, tablets and similar gadgets. “These are a challenge because often they don’t have a USB port or, in the case of the iPad, any ports at all,” he says, adding that such devices also run on a variety of operating systems. “How to make a device for one user that is potentially usable on multiple operating systems is a challenge. Fortunately, it’s not needed yet, but soon it will be.”

And the final challenge? Changing the culture so that banks, as well as their customers, accept that investing in technology to protect themselves is a necessity.

47%
The US share of global card fraud in 2011

Plugged in

Gemalto’s solution to the assault on account security is Ezio Plug&Sign, a USB stick that plugs into a spare port on a Windows PC or a Mac. The Linux version is due early in 2012. Plug&Sign installs no software, but launches an application from the stick’s read-only partition that offers a choice of functions, such as digitally signing a transfer of funds. To do this, the device opens a secure session within the bank’s site, the user chooses a transaction and types in a PIN, then has the opportunity to review the information she or he has sent. The device confirms the action by changing color and digitally signs the transaction to authenticate the user.

Adam Dolby argues that this design has several security benefits. First, it is “zero footprint” — it installs nothing on the user’s computer that could be intercepted or corrupted if the machine is infected by malware. The stick has two partitions: one read-only, one read-write. The secure session is opened in the browser software provided in the read-only partition and only loads legitimate, “white-listed” URLs. Also, the design builds on established standards that have been thoroughly tested by years of use, such as SSL for PKI and cryptography. Necessary updates — for example, if there are changes to certificate authorities or URLs, or if a browser update is necessary — are carried out remotely by the issuing bank and transmitted to the read-write partition without disrupting the user’s secure session.

Gemalto has also put effort into the usability of the Ezio system, knowing this is where many products fail. The color-change feedback on completion of a transaction aids the user, as does the gadget’s physical design that the company boasts requires just “a fully functional finger” to operate.

33 www.gemalto.com
Not long from now, billions of electronic devices will be linked together in the “Internet of Things.” Using machine-to-machine (M2M) technology, applications such as smart meters, security systems, point-of-sale systems and tracking devices can communicate autonomously with one another and with service platforms in the cloud, leading to huge savings in terms of energy, time and money.

But, as with any technology involving personal and corporate data, there are concerns about how secure the real-time data being transmitted between devices really is. Two researchers in Germany recently demonstrated that they could hack into a domestic smart meter, change the residents’ billing information and even find out what films they were watching. Using unencrypted data, the researchers simply correlated the power consumption of the TV with scheduled films to determine the owners’ viewing patterns.

Cellular devices are even vulnerable to attack by SMS text. This “war texting” is a multi-step process, says Holger Lenz, Director of Business Development at Cinterion, a Gemalto company. By “sniffing” the data link with the help of freely available tools, an attacker can learn a lot about the behavior of the M2M-enabled device. When SMS messages are sent to the device to trigger a specific action, the structure and syntax of the message can be used to reverse-engineer the internal protocol. Some implementations exchange server IP address information, user names and passwords within the SMS — all data that can help hackers plan their attack.

With interconnected devices already being installed in homes, vehicles and even devices such as pacemakers, keeping them secure is vital. Even if hacking attacks are not malicious, they can shut down or interfere with all kinds of connected equipment. This is why many M2M applications, such as the emergency-calling feature in BMW vehicles, now use Machine Identification Modules (MIMs). These specialized SIM platforms “lock down” the link through secure authentication and ciphering — meaning that only authorized service providers can communicate with the device.

The release of newly available “white space” frequencies (see box) is set to raise the profile of the security issue even further. This “digital dividend” from the shift from analogue to digital TV in Europe and the US is opening up new radio frequencies that will provide more capacity for M2M communications.

Even if hacking attacks are not malicious, they can interfere with all kinds of equipment.
Companies at the forefront of this new digital development see security as integral to their product and service offering. “Security is absolutely critical and not something we will compromise on at all,” says Professor William Webb, CTO of white-space startup Neul in Cambridge, UK. “We envisage a level of security [for M2M] better than cellular, including robust authentication of the network by the terminal and vice versa. For some applications, such as smart meters, security is paramount.”

While white space is a new, emerging technology, there are other well-established, mature technologies available for use by M2M applications. Traditional GPRS, EDGE (2G) and now HSPA+ and LTE (3G/4G) communication modules are used to connect M2M equipment through public mobile networks; there are already more than 100 million in use in global markets. And because this technology is already used in cellphones, it has built-in security with authentication using SIM cards, also known as UICC. But with Ericsson predicting that there will be more than 50 billion M2M-enabled devices by 2020, this method would be too costly to manage on this scale. That’s why companies are looking to standardize an embedded UICC that can be configured securely over the network, rather than needing to have a dedicated SIM card inserted.

So what are the proposed solutions that will keep our connected devices secure? According to Holger, careful engineering of end-to-end security architecture will use passive, reactive and active security measures. To safeguard elements in the M2M device and reduce the number of potential vulnerabilities, he says that the preferred choice for M2M device vendors is embedded Java-based cellular communication modules to set up an encrypted end-to-end connection with strong authentication, combined with an embedded MIM/UICC.

Beyond the trusted hardware and communication channel, it is important to have a secure way of updating the device’s OS and applications. This is increasingly necessary due to the long lifespan expected from M2M solutions and the speed at which security risks evolve.

Protecting the billions of connected devices in the Internet of Things is a significant but critical challenge. With attacks on M2M systems becoming more public and the connections between systems growing in scale, security must be built into their design and management from the start. With many different networks and protocols being used for M2M, and new ones emerging, the challenge now is to ensure that security is strong, whatever the technology.

What is white space?

The old analogue TV frequencies around 600MHz are lower than cellular phones (900MHz and 1800MHz) or wireless networks (2.4GHz), both of which are also used for M2M networks. This means signals can travel further, but they carry less information and are split into many different bands. While these frequencies could be used for things such as delivering rural broadband, M2M is seen as a good match for the technology.

The UK telecommunications regulator, Ofcom, is putting together an M2M strategy to be launched in the middle of 2012. Similarly, in the US, the Federal Communications Commission is still investigating how white-space spectrum can be used.

A key player in the field is a startup called Neul. It was formed in 2010 by the founders of Cambridge Silicon Radio, one of the largest wireless technology companies in Europe, to develop and build a network and devices to connect equipment using the white-space frequencies. It has developed a protocol, Weightless, which it wants to see as the basis of a standard, and has used it to develop the first white-space M2M equipment.

While there are still some regulatory and security issues, white-space systems are starting to emerge. A recent report by Cambridge Consultants said: “We should expect to see commercial volume product in a timeframe of around five years, but the first enterprise products in less than a year.”
In brief

The number of customers who use Gemalto smart cards when accessing FINO’s branchless banking program has swelled to 10 million across India. Financial transactions carried out through FINO, an electronic payment platform, are validated using biometric authentication, providing one of the highest levels of digital security. Transactions are approved once fingerprint information and card-embedded software has been verified.

Employees were asked to develop concepts related to fields such as communication, payment, transit, internet and M2M. Among the ideas put forward, business consultant BearingPoint was particularly impressed with wireless technology application eGo. Using human skin to conduct electricity, the small device transmits a signal that can, for example, unlock electronic devices such as car doors.

Cinterion wins TMC award

Cinterion, the global leader in cellular machine-to-machine (M2M) communication and a Gemalto company, has scooped an award for its innovative smart grid technology.

In January, Cinterion won the Smart Grid Excellence Award 2011 from TMCnet’s Smartgrid for its EU3 M2M module, a high-speed cellular communications system that enables smart grid deployment among global utility businesses. Equipped with Universal Mobile Telecommunications System (UMTS) capability on a 900MHz band, the system increases the coverage area for high-speed communications, even in remote locations, and enables communication on 2G and 3G wireless networks.

The EU3 system was designed for industrial automatic meter reading, smart grid applications and long-term deployments with simple integration and secure lines of communication.

At the forefront of NFC

Gemalto has already deployed 35 NFC projects around the world. In 2011, it was chosen by PTK Centertel, an Orange group affiliate, to help roll out Poland’s largest NFC program. In Singapore, it was chosen by Infocomm Development Authority as the trusted third party to deploy its NFC program for a commercial launch in 2012 involving the nation’s three mobile operators. It was also selected to secure the Isis mobile commerce platform in the US (see story, opposite, for more information).

Asia & Oceania

55%

The volume of India’s adults who are unsatisfied with the country’s finance sector, according to a Boston Consulting Group study. The majority of respondents to The Socio-Economic Impact of Mobile Financial Services said they were either underserved or not served at all by India’s financial institutions.

Gemalto then developed the best ideas.

Gemalto has won the BearingPoint Innovation Management Award after launching Business Innovation Garage (BIG), an initiative to encourage its 10,000 employees to develop and submit innovative ideas.

Employees were asked to develop concepts related to fields such as communication, payment, transit, internet and M2M.

The FINO system has proved popular in remote locations. Bandhus, a FINO partner company, deploys staff on motorbikes with portable card readers to villages where residents can carry out secure financial transactions.

Get smart

The number of customers who use Gemalto smart cards when accessing FINO’s branchless banking program has swelled to 10 million across India. Financial transactions carried out through FINO, an electronic payment platform, are validated using biometric authentication, providing one of the highest levels of digital security. Transactions are approved once fingerprint information and card-embedded software has been verified.

The FINO system has proved popular in remote locations. Bandhus, a FINO partner company, deploys staff on motorbikes with portable card readers to villages where residents can carry out secure financial transactions.

Cinterion, the global leader in cellular machine-to-machine (M2M) communication and a Gemalto company, has scooped an award for its innovative smart grid technology.

In January, Cinterion won the Smart Grid Excellence Award 2011 from TMCnet’s Smartgrid for its EU3 M2M module, a high-speed cellular communications system that enables smart grid deployment among global utility businesses. Equipped with Universal Mobile Telecommunications System (UMTS) capability on a 900MHz band, the system increases the coverage area for high-speed communications, even in remote locations, and enables communication on 2G and 3G wireless networks.

The EU3 system was designed for industrial automatic meter reading, smart grid applications and long-term deployments with simple integration and secure lines of communication.

Gemalto has already deployed 35 NFC projects around the world. In 2011, it was chosen by PTK Centertel, an Orange group affiliate, to help roll out Poland’s largest NFC program. In Singapore, it was chosen by Infocomm Development Authority as the trusted third party to deploy its NFC program for a commercial launch in 2012 involving the nation’s three mobile operators. It was also selected to secure the Isis mobile commerce platform in the US (see story, opposite, for more information).

Get smart

The number of customers who use Gemalto smart cards when accessing FINO’s branchless banking program has swelled to 10 million across India. Financial transactions carried out through FINO, an electronic payment platform, are validated using biometric authentication, providing one of the highest levels of digital security. Transactions are approved once fingerprint information and card-embedded software has been verified.

The FINO system has proved popular in remote locations. Bandhus, a FINO partner company, deploys staff on motorbikes with portable card readers to villages where residents can carry out secure financial transactions.

Asian & Oceania

55%

The volume of India’s adults who are unsatisfied with the country’s finance sector, according to a Boston Consulting Group study. The majority of respondents to The Socio-Economic Impact of Mobile Financial Services said they were either underserved or not served at all by India’s financial institutions.
Safe and secure

German bank Sparkasse Südholstein is increasing online banking security for its customers by distributing Gemalto’s Ezio strong authentication optical readers.

The Gemalto solution eliminates the need for one-time passwords, replacing them with more secure smart banking cards. It works by placing the authentication device in front of a PC monitor, tablet display or smartphone screen. Optical sensors then capture the transaction data, eradicating the need to enter passwords into reader keypads.

Sparkassen-Finanzgruppe, the leading banking group in Germany, will issue the credit card-sized optical authentication devices to all of its customers throughout 2012.

Student payments made easy

Banco Santander Brasil, one of the world’s largest financial institutions, turned to Gemalto when it needed to deploy Brazil’s first contactless EMV payment system.

The system has been introduced to provide students at Santander Universities with payment and digital ID cards for carrying out transactions, accessing campus facilities and using public transportation.

EMV cards will be distributed among students during 2012, a year when demand for advanced payment systems and NFC is expected to gather pace in Brazil.

“The card offers unmatched technology in our market and gives us a leading edge that adds great value to our brand, positioning and activities,” said Jamil Hannouche, Director of Santander Universities in Brazil. “We want to strengthen our ties with universities offering state-of-the-art technology, which improves the operation of the institutions.”

Secure mobile payments for US consumers

Isis, a joint venture company between AT&T Mobility, T-Mobile USA and Verizon Wireless, has chosen Gemalto to secure its mobile payment and NFC services platform in the US.

Gemalto’s Allynis Trusted Service Manager (TSM) technology will be incorporated into Isis’ platform, which was created to provide consumers and merchants with an open and secure mobile commerce system.

The platform enables consumers to make contactless payments using NFC technology at retail outlets such as restaurants, movie theaters and drug stores. By tapping their phones, they can make secure payments, present loyalty cards and redeem coupons.

Biometrics device boosts US security

A US government security publication has recognized Gemalto’s contribution to improving biometric data capture at US borders.

Government Security News (GSN) awarded Gemalto a Homeland Security accolade for the company’s Coesys Mobile Enrollment system, which was named best biometric identification device. Combining software and integration services, Coesys captures biometric data for secure identification documents such as ePassports, healthcare and identity cards and driver’s licenses. “Gemalto is honored to be acknowledged by GSN for our advancements in personal identity verification, specifically with regard to biometrics and identity management solutions,” said Neville Pattinson, Vice President of Government Affairs, Gemalto North America.
Digital lives _ Hedy Lamarr

Actress Hedy Lamarr was more than a pretty face. She also laid the foundations for Bluetooth technology.

Hedy Lamarr was always a pioneer. The beautiful star of the early cinema first soared to fame — and notoriety — in the 1933 German film *Ecstasy*, which shocked audiences by showing the actress in the nude. But few would have imagined that “the most beautiful woman in films” would also become the brains behind a patent that paved the way for modern-day Bluetooth technology.

Lamarr showed an aptitude for mathematics from an early age. Hedwig Eva Maria Keisler was born to Jewish parents in Vienna in 1913 and left when she was a teenager to pursue a film career in Berlin. But it was marriage to an arms manufacturer that set the 19-year-old Lamarr on the path that would lead to her later technological discovery.

Her husband was very possessive of his attractive young bride. Preferring to take her to his meetings with technicians rather than allow her to pursue her acting career, he told Lamarr about a problem plaguing the armaments industry at the time: how to guide a torpedo by radio while masking the signal from enemy interference.

The inquisitive Lamarr guessed that varying the frequencies at which radio signals were transmitted could protect wireless communication from jamming. But it was only after she had left her husband and established herself as a movie star in the US that Hedwig — now Hedy — met the man who would help her prove her “frequency hopping” theory.

George Antheil was an avant-garde musician who had also dreamed up several inventions, including an open-top pianola designed to teach basic keyboard technique. When Lamarr met him at a Hollywood party, she was one of the biggest pin-ups of the 1940s — but she was preoccupied by the war raging in her native Europe. On their first meeting, the star of Cecil B. DeMille’s *Samson and Delilah* scrawled her telephone number on Antheil’s windshield in lipstick. The pair soon set about developing Lamarr’s idea for a “secret communications system”.

Antheil saw a way of implementing Lamarr’s theory of shifting the radio signals of control devices to make it near impossible for the enemy to block the bands. He suggested coordinating the transmitter and receiver by using two identical piano rolls running at the same speed to control the switching between channels.

A patent was granted in 1942 to George Antheil and Hedy Kiesler Markey, her married name, but the technique was ignored and the patent expired after 17 years. The technology was belatedly acknowledged and implemented by the US government in 1962 during the Cuban missile crisis.

Now known as spread spectrum, Lamarr and Antheil’s innovation served as the basis for technology that allows for simultaneous multi-channel transmission of digital signals, the framework for cellular telephony. Transmission is efficient, with low-power transmitters working across considerable distances and multiple transmitters and receivers occupying the same frequency band, making wireless access to public networks inexpensive. Its best-known modern application is Bluetooth.

Hollywood may have secured Hedy Lamarr’s fame, but her pioneering work in radio technology — for which she received no payment — made a more lasting impact than any of her films. In 1997, three years before her death, Lamarr was finally acknowledged for her contribution to science with a special award from the Electronic Frontier Foundation.

Lamarr once said: “All creative people want to do the unexpected.” As a movie legend and radio communications innovator, Hedy Lamarr defied expectations to the last.

Her pioneering work in radio technology made a more lasting impact than any of her films.

The Review
Would you leave your house without locking the door?

- 75% of Americans don't use strongest kind of passwords for their most sensitive accounts
- Almost 20% used the same password for more than 5 accounts
- Usernames and passwords are no longer a secure way to protect any level of information within a company

What can happen when you are not secure.
- Epicor's hack exposed 2,200 global retail brands
- Sony Breach put 77m customers at risk

Why Strong Authentication?
- Provides protection from unauthorized access
- Provides audit trail of individual access activity
- Increases security while being easy to use for the employee
- Easy to deploy for the administrator

Are you at risk?
- Understand the Risks – ask yourself these questions:
  1. Is your security dependant on keeping passwords secret?
  2. Do you need stronger security for network access?
  3. Does your security depend on employees never failing for an attack?
- Examine How Strong Authentication Can Strengthen Layered Security
  - Something you know + something you have + something you are

What Can You Do?
- balance security with convenience

Get Started Quickly – Use Cloud Based Services or Channel Partners
- Choose Microsoft Infrastructure or Open Standards
- Secure Sensitive information with PKI Certificate-Based Identities

Listen Up Cloud Providers!
- By using strong authentication with OTP technology, your customers know that the right users are gaining access to online services and resources.
- Strong authentication makes it more likely for organizations working with extremely sensitive data to migrate to cloud based resources.

61% of organizations are either working on or have cloud services already have some approved

Strong Authentication is NOW an IT Security Best Practice

Learn more with Gemalto's Strong Authentication Implementation Guide

Resources:

follow us
- Gemalto Enterprise Blog
- Gemalto’s Strong Authentication Implementation Guide
- Gemalto Videos
- Gemalto’s Digital Security Group
Enter the Mobile Financial Services experience

Experience a day-in-the-life of a full-scale mobile financial ecosystem, from mobile money and payment to mobile NFC – tailored to both developing and developed markets.

> **New York, 8am:** Enjoy a hot beverage at your local Coffeebar and browse through dynamic coupons. There might be a special gift for you! Sit in the coffee lounge and do some online shopping, or get some account management done and start planning your next vacation. Buy the daily newspaper and you are now ready to head to work, just hop on the next tramway!

> **New Delhi, 2pm:** Stop by your Hello Wireless agent to make a deposit and then reload your airline credit. You can then go for a walk around the market and buy some fruit and vegetables. Take a seat on the terrace, check your account balance and send money to your relatives overseas thanks to mobile international remittances.