Hackers Steal Data on up to 80 Million US Insurance Customers

Attackers breached the network of US insurance giant Anthem Inc. and stole sensitive personal data—including names, birth dates, Social Security numbers, street and email addresses, and employment and income information—for up to 80 million current and past customers.

So far, said Joseph R. Swedish, president and CEO of Anthem—the US’s second-biggest health insurance provider—there has been no sign that the hackers obtained credit-card or personal medical data. The company also hasn’t indicated that any passwords were stolen.

Initially, security experts looking into the breach said the servers and tools the attackers used are like those that a Chinese government-sponsored hacker group has employed in the past. However, US law-enforcement agencies, including the FBI, that are investigating the incident say it’s too early to tell who is responsible.

Anthem has hired security firm Mandiant to look into the breach and determine how many and which accounts were compromised.

According to researchers, the intruders may have first broken into the company’s website in April 2014.

Without providing details, Anthem said the hackers used a sophisticated cyberattack to breach its network. The company’s IT staff detected the intrusion after observing suspicious network activity. The firm has since started a website (http://anthemfacts.com) to provide information about the incident.

Anthem has begun contacting people whose data was stolen and says it will provide them with free credit-monitoring and identity-protection services. However, 10 US states have written the company contending it was too slow to notify consumers of the cyberattack.

When data is stolen in cases like this, said Purdue University professor and cybersecurity expert Eugene Spafford, “[It] can be used for identity theft [and] extortion, and to gain people’s trust. So, it really is a big problem, even if medical or credit card information is not given out. The company providing a year or two of credit monitoring won’t fix that.”

Anthem becomes the latest major company to experience a data breach during the last year, joining businesses such as eBay, information-service provider Experian, banking giant JPMorgan Chase, and the Neiman Marcus and Target department store chains.

Systems Begin Using Advanced Technologies to Improve Cellular Telephony

As popular as mobile telephony has become, customers still see room for improvement.

For example, many users are frustrated with poor sound quality, dead zones in which they can’t receive cellular signals, and areas with expensive mobile rates.

With this in mind, phone makers and service providers are increasingly adopting three technologies: Wi-Fi Calling, Voice over LTE, and HD Voice.

To help people when they can’t find cellular signals, numerous smartphone makers and mobile service providers worldwide are turning to Wi-Fi Calling, which utilizes Wi-Fi for voice communications.

The technology uses Kineto Wireless’ Smart Wi-Fi Application, which manufacturers such as Apple, HTC, LG, Motorola, Nokia, Orange, and Samsung preload onto their smartphones. The application—which runs automatically when users enable Wi-Fi on their devices—works with the Android, iOS, and Windows Phone mobile operating systems. Service providers enabling Wi-Fi Calling include Canada’s Rogers Wireless, Orange UK, and T-Mobile US.

The technology transfers voice packets over the Internet via Wi-Fi from a smartphone to the service provider, which then transmits them on the cellular network.

Wi-Fi Calling lets people utilize their own telephone numbers, rather than a separate identifier as is the case with Skype. And unlike Skype, users can dial calls directly from their phones rather than having to work with an Internet interface. Another advantage
A new technique would increase supercomputers’ performance by changing the way they conduct checkpointing, a process that periodically stores information about their state to help them recover from system crashes.

for customers is that Wi-Fi calls aren’t charged against their cellular minutes. Some experts say that handoffs from the cellular system to the Wi-Fi network might not always be seamless and that the technology thus needs more work.

Voice over LTE allows the transmission of high-quality audio as IP packets over high-speed, 4G long-term evolution networks previously used only for data. This not only enables better audio- and video-call quality but also lets carriers operate just one network for all of their services, rather than one for data and one for voice.

The technology is based on the IP Multimedia Subsystem architectural framework, which allows the use of IP packet switching, rather than traditional circuit switching, for voice communications. Voice over LTE uses the adaptive multirate codec employed in many other cellular systems, which lets it interoperate with those systems.

HD Voice, also known as wideband audio, enables high-definition audio for mobile telephony.

Traditional telephony samples an audio stream 8,000 times per second and limits the sound reproduction to between 200 Hz and 3.3 KHz. HD Voice improves audio quality by using any of several wideband codecs to double the sampling rate and reproduce the sound over a wider range, between 50 Hz and 7 KHz.

---

**Bug Could Let Hackers Eavesdrop on Cell Calls**

German researchers have discovered security flaws in a long-used mobile-communications technology that could let hackers listen to cellular phone calls and intercept text messages, even on wireless networks using today’s most advanced encryption.

In addition, hackers could exploit the bugs to record encrypted calls or texts for decryption later and also determine callers’ locations.

Two researchers—Tobias Engel, founder of privacy-technology vendor Sternnauke, and Security Research Labs chief scientist Karsten Nohl—separately found the vulnerabilities in the SS7 (Signaling System 7) global network. SS7 lets cellular providers route calls, texts, and other services between one another’s networks. In recent years, security experts have found other problems with SS7.

The recently discovered flaws could be exploited by anyone with access to SS7 and the technical skills required to send the proper queries, even though cellular providers have spent time and money securing their networks. That’s because carriers still must send calls and texts that travel between their networks over the vulnerable SS7.

The researchers found two ways to exploit the system to eavesdrop on calls.

In the first, hackers could send commands over the network and take over a mobile phone’s forwarding function.

They could then redirect calls through their own system—where they could listen to or record them—and then on to the intended recipient. In the process, they create an open channel for future use.

Attackers could also use antennas to collect calls and texts transmitted via SS7. If the communications are encrypted, as is usually the case with 3G systems, the hackers could use the network to ask the carrier for a temporary decryption key.

Engel and Nohl found that hackers could also send SS7 queries that acquire the temporary identification numbers cell phones use during calls and identify the corresponding phone numbers. The attackers could then track callers.

Because of such security problems, many industry observers say it’s time to replace SS7, which was first standardized in 1980.

---

**Researchers: Less Checkpointing, More Supercomputing**

Scientists have developed a way to make high-performance computing systems more efficient and powerful by adjusting the way they perform checkpointing.

Applications running on supercomputers conduct checkpointing periodically to store information about their state. If the system crashes, it can then restart applications from the last stored state.

However, the more checkpointing a supercomputer does, the fewer resources it can devote to solving problems.

Researchers Devesh Tiwari and Saurabh Gupta of the Oak Ridge Leadership Computing Facility (OLCF) at the US Department of Defense’s Oak Ridge National Laboratory have developed a new checkpointing approach.

They said that users typically schedule checkpointing based on the idea that the mean time between failures (MTBF) is 10 to 20 hours. The
researchers studied supercomputers at the OLCF and at other facilities and determined that the time between failures isn't regular, so scheduling checkpoints based on an MTBF is not optimal. Also, they said, additional problems occur as a result of failures.

Tiwari and Gupta said a new lazy checkpointing approach based on these patterns is needed. Thus, they explained, after a failure, applications should increase their checkpoint frequency to cope with the clustered problems that could follow. As the amount of time following the last in a series of problems increases, the time between checkpoints could also grow. Overall, this would reduce checkpoint frequency.

The approach would not only help supercomputers deal better with failures but would also reduce checkpointing’s impact on the systems by 20 to 30 percent, according to the researchers.

Ultimately, the scientists say, they want to develop a tool to help high-performance computer users better handle checkpointing, based on factors such as the nature of their system and the jobs it performs.

Researchers Develop Poker-Winning Application
Teaching computers to win at games is nothing new.

However, computers generally excel only at perfect information games, in which all players know all information relevant to making decisions. For example, in checkers and chess, both players can see where all the pieces are.

Computers have not been very successful in most card games, however, as players typically don't know all of the other participants’ cards.

Now, though, University of Alberta researchers led by professor Michael Bowling have developed the Cepheus application designed to beat humans at Texas hold 'em poker, saying it represents an artificial-intelligence and game-theory breakthrough.

University of Alberta researchers have developed the Cepheus application designed to beat humans at Texas hold 'em poker, saying it represents an artificial-intelligence and game-theory breakthrough.

US Requires Faster Speeds for Broadband Services over ISPs’ Objections
Many people have just lost their broadband Internet access without making a single change to their service.

That’s because a divided US Federal Communications Commission (FCC) has raised the minimum speed that ISPs must offer for their services to be considered broadband.

The commissioners voted 3–2 to raise the minimum broadband speeds from 4 to 25 Mbits per second for downloads and from 1 to 3 Mbps for uploads.

Supporters, including consumer groups and the three FCC members who belong to the Democratic Party, say this is important because it would guarantee that broadband is significantly faster than other types of service, which isn't the case now. They also contend the new ruling will encourage the faster service that the US needs to be competitive.

Opponents, including large ISPs and the two Republican Party commissioners, say the FCC majority is making a power grab and has selected arbitrary standards without considering the Internet-access speeds that consumers actually need. They say that most US customers who have the option to pay for 25 Mbps Internet service don’t do so.

Because of the FCC’s actions, the service provided to millions of customers in the US—where the average Internet access speed is 10 Mbps—will no longer be considered broadband.

In a report, the commission said that 55 million people, which represents 17 percent of the US population, don’t have Internet service with at least 25 Mbps download rates. Most of them are in rural areas, where 53 percent of residents don’t have access to such speeds, compared to 8 percent in urban areas. In fact, 20 percent of rural residents don’t have service of even 4 Mbps.

Consumer groups—such as the Public Knowledge advocacy organization—support the new broadband standards. They argue that the old standard is too slow and not in keeping with today’s technology.

The Communications Workers of America union also backed the recent ruling, saying that new broadband standards will encourage carriers to do work that will create new jobs and is also necessary to keep the US strong and competitive.
LIST OF 2014’S “WORST” PASSWORDS HAS A FAMILIAR LOOK

Security vendor SplashData has released its annual bad-password list for 2014, and it includes some familiar “names,” most of which violate security experts’ advice for choosing good passwords.

Atop the rankings, as it has been since the first list in 2011, was “123456.” In fact, 9 of the top 25 bad passwords consist of numbers, with “12345” in third, “12345678” in fourth, “123456789” in sixth, and “1234” in seventh.

“Any password using numbers alone should be avoided, especially sequences,” noted SplashData CEO Morgan Slain.

In second place, as it has been since 2011, was the classic “password.” Other oldies—but-not-goodies include “qwerty”—the first six letters from the left on a keyboard’s top row of letters—in fifth place.

“Passwords based on simple patterns on your keyboard remain popular despite how weak they are,” said Slain. “Longer keyboard patterns are becoming common passwords, and they are still not secure.”

For sports fans, “baseball” was in eighth place and “football” was in tenth.

And for comic-book and fantasy enthusiasts, “dragon” was in ninth place; “superman” was in 21st, and “batman” was in 24th.

“iloveyou” was one of nine passwords from 2013 to not appear on the 2014 list.

SplashData generated its rankings by analyzing 3.3 million passwords leaked in various ways during 2014 and determining which were most commonly used and thus, presumably, the easiest to guess.

Independent security consultant Mark Burnett, who helped SplashData with its study, agreed that strong passwords are important but said that the study’s results must be taken in context.

For example, he wrote in his blog, while “123456” is the most common password, only 0.6 percent of the users involved actually employed it.

Also, Burnett noted, all of 2014’s top 25 bad passwords combined represented only about 2.2 percent of passwords exposed, the lowest in recent years. He said this indicates that users may be increasingly moving away from easy-to-guess passwords.
game's *heads-up limit* variant, in which there are just two players, who can make only a set number of bets, all of a fixed amount.

To develop Cepheus, the team used a game-theory approach called Nash equilibrium. This equilibrium exists at the point at which players gain no benefit by changing their strategy, as long as other players don't alter their approaches. The technique predicts what will happen when people make decisions that affect the outcome of an undertaking and thus can help identify the best strategies to take under various circumstances, such as poker games.

The researchers also employed the counterfactual regret minimization approach, in which a system plays many games and identifies which strategies win and lose, thereby determining which are most effective in different situations.

These complex, time-consuming processes require a computer system to store and then work with a lot of information. In response, the researchers applied computation- and storage-optimization techniques that decreased the amount of data they had to keep on hand from 260 to 17 terabytes.

Nonetheless, running on a cluster of 200 2.1-GHz cores with 32 gigabytes of RAM each, Cepheus still had to play billions of simulated hands of Texas hold 'em per second for two months to become proficient at the game.

The University of Alberta team says their application could have uses outside of games, such as in designing energy and national-security strategies.

---

**New Head-Mounted Display Projects Images onto Users’ Eyes**

Head-mounted displays have been in the news recently, with the promised upcoming release of virtual-reality-related headsets such as Oculus VR's Oculus Rift and Sony Computer Entertainment's Project Morpheus.

Now, a new product is taking a different and innovative approach to display technology.

Avegant Inc. plans to release its Glyph headset late this year. The company generated $1,509,506 in pledges via Kickstarter, much more than its $250,000 goal. It also raised $9.37 million from venture capitalists.

The Glyph looks like a large set of headphones. Audio comes from the earphones, and video comes from a system in the crosspiece.

The headset uses a pair of small digital-light-processing (DLP) devices—rather than the common organic LED displays—to generate bright, clear images that are projected directly onto part of the wearers' retinas, leaving the rest of the field of vision clear.

The 16-ounce headset connects via an HDMI cable to a smartphone or other device that provides the images or video shown to wearers.

The company hasn't yet developed a production version of its product but says it's close to doing so. Avegant plans to ship the production versions to its Kickstarter supporters later this year and to other customers shortly thereafter.

Company officials say they originally planned to market the Glyph to the military but changed their focus to consumers when devices such as the Oculus Rift began generating public interest.

---

**19,000 French Websites Suffer Cybervandalism in Wake of Terrorist Attacks**

In what French cybersecurity officials call an unprecedented incident, hackers have attacked 19,000 of the country's governmental and nongovernmental websites.

The hackers placed pro-Islamic text and images on the website homepages of French businesses, religious groups, city governments, and universities, according to the French Defense Ministry and the Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), the national information-system-security agency.

Hackers also briefly shut down the Defense Ministry's website with a denial-of-service attack that officials quickly resolved.

These incidents followed the recent Islamic terrorist attack in France against Charlie Hebdo magazine—a longtime target of some Muslims.
Terrorist groups have threatened organizations in the future. To make their attacks more dangerous, they affect governmental operations. Nonetheless, hackers execute malicious code on the types of servers currently used for important applications such as email and webpage hosting.

The so-called Ghost vulnerability also affects most Linux-based software that performs domain-name resolutions. Security experts say Ghost is a critical Internet threat along the lines of the Heartbleed and Shellshock bugs that received so much attention last year.

The vulnerability is in the GNU C Library (glibc), Linux’s most common code library, which contains functions that C and C++ programs use to carry out common tasks. Ghost also affects Linux programs written in Python, Ruby, and most other languages that also use glibc.

Thus, security experts say, organizations should assume most of their Linux systems are vulnerable unless they either don’t run glibc or use a glibc version that contains a patch that the GNU Project issued in May 2013. Most users of Linux-based production systems haven’t downloaded the fix, in part because when such systems are patched, they must be taken offline for partial or total rebooting.

Security experts say there could be major problems if anyone ever publishes Ghost-related exploit code on the Internet.

Nonetheless, Qualys researchers say they plan to publish via Metasploit a proof-of-concept exploit they wrote that implemented a remote code-execution attack on a fully protected Exim mail server.

Hackers who exploit Ghost could cause buffer overflows and subsequently execute arbitrary code on target machines.

Numerous Linux vendors say they are aware of the bug and have been working on fixes, which reportedly are already available for Red Hat and Ubuntu distributions.

A new fast, durable, energy-efficient type of resistive RAM consists of silicon oxide (SiOₓ) that has pores filled with metals such as platinum (Pt) or gold (Au). SiOₓ doesn’t typically conduct electricity. However, applying a high voltage opens conductive paths—consisting of nanocrystalline silicon (Si–NC) or amorphous silicon (a-Si)—through the material. The presence or absence of these paths represents binary ones and zeros, thereby enabling data storage and retrieval.

for running satirical cartoons about Mohammed—in which 10 employees and two police officers were shot to death. Security officials subsequently killed the two assailants.

Two days later, an Islamic terrorist murdered four people in a Paris kosher supermarket before police killed him.

The Al Qaeda in the Arabian Peninsula terrorist group claimed responsibility for both attacks.

French officials say organized hacker groups, including several that claim links to the terrorist Islamic State of Iraq and Syria (ISIS), were responsible for the French website vandalism.

According to French military officials, the recent cyberattacks were not particularly complex and did not affect governmental operations.

Terrorist groups have threatened to make their attacks more dangerous and target more sensitive French organizations in the future.

**Linux Bug Represents Major Internet Threat**

Security vendor Qualys says it has recently discovered that most Linux releases contain a major flaw that would let hackers execute malicious code on the types of servers currently used for important applications such as email and webpage hosting.

The so-called Ghost vulnerability also affects most Linux-based software that performs domain-name resolutions.

Security experts say Ghost is a critical Internet threat along the lines of the Heartbleed and Shellshock bugs that received so much attention last year.

The vulnerability is in the GNU C Library (glibc), Linux’s most common code library, which contains functions that C and C++ programs use to carry out common tasks. Ghost also affects Linux programs written in Python, Ruby, and most other languages that also use glibc.

Thus, security experts say, organizations should assume most of their Linux systems are vulnerable unless they either don’t run glibc or use a glibc version that contains a patch that the GNU Project issued in May 2013. Most users of Linux-based production systems haven’t downloaded the fix, in part because when such systems are patched, they must be taken offline for partial or total rebooting.

Security experts say there could be major problems if anyone ever publishes Ghost-related exploit code on the Internet.

Nonetheless, Qualys researchers say they plan to publish via Metasploit a proof-of-concept exploit they wrote that implemented a remote code-execution attack on a fully protected Exim mail server.

Hackers who exploit Ghost could cause buffer overflows and subsequently execute arbitrary code on target machines.

Numerous Linux vendors say they are aware of the bug and have been working on fixes, which reportedly are already available for Red Hat and Ubuntu distributions.

**New RAM Approach Could Enable Terabyte Smartphones**

People are using smartphones for an increasing number and variety of tasks. However, the devices’ storage capacities haven’t kept pace with their growing capabilities.

This has limited the ability of many users to store apps, as well as data, photos, videos, audio, and other types of material, on their phones.

Now, though, a Rice University research team has developed a new type of storage that could solve this problem.

Their RRAM (resistive random-access memory) technology uses silicon oxide, a very common, well-known material—found in microprocessors and substances such as glass—that could enable the affordable building of high-density memory devices using current production approaches.

“Because our devices use silicon oxide—the most studied material on Earth—the underlying physics are both well understood and easy to implement in existing fabrication facilities,” research team leader James Tour noted.

The scientists say their approach could eventually enable smartphones with a terabyte of memory, much more than the 64-gigabyte maximum that today’s flash-memory-based devices currently offer.

The Rice team uses silicon oxide—containing pores filled with metals such as platinum or gold—to offer denser storage, more read and write cycles, and greater energy efficiency than previous RRAM approaches. Using porous, rather than solid, silicon oxide greatly reduces the power the resulting device consumes.

The researchers are working with an as-yet-unnamed manufacturer to commercialize their technology.

RRAM is nonvolatile like flash memory but is considerably faster and more versatile. For example, it could be used to manufacture powerful 3D chips that are built vertically as well as horizontally.

The technology has thus become a focus of memory researchers, many of
whom are using materials more exotic, more expensive, and less well understood than silicon oxide.

Resistive memory works by placing a dielectric material—one that typically doesn’t conduct electricity, such as silicon oxide—between two wires. Applying a high voltage creates a narrow conduction path through the dielectric material. The presence or absence of these paths represents digital data’s binary ones and zeros.

Big Tech Firms Settle Lawsuit over Accusations They Conspired to Limit Workers’ Wages
Adobe Systems, Apple, Google, and Intel have agreed to a $415 million settlement in a suit filed by 64,000 current and former employees who claim the companies conspired to not actively recruit one another’s workers, reducing competition for their services and thereby holding down their wages.

The four defendant firms were accused of conducting these practices from 2005 through 2009. The plaintiffs were employees who worked in the companies’ technical, creative, and R&D units.

In 2010, the US Justice Department accused Adobe, Apple, Google, Intel, Intuit, and Pixar Animation Studios of anticompetitive hiring-related policies. The companies—which said they were just trying to be fair to and work well with one another—subsequently agreed to stop such activity but weren’t penalized financially.

Claiming $3 billion in lost wages, the affected employees then joined forces to file a class-action lawsuit against the six companies, as well as Lucasfilm. Early in the process, Intuit, Lucasfilm, and Pixar settled for $20 million.

Last April, the plaintiffs’ and remaining defendants’ lawyers agreed to a $324.5 million settlement. However, at least one plaintiff complained about the settlement. Freelance programmer Michael Devine is on record as having written to presiding US District Court Judge Lucy Koh that the settlement “is grossly inadequate and fails to achieve justice.”

Koh agreed and rejected the offer. The new settlement of $415 million—reached after ongoing bargaining—will net each plaintiff only about $6,500, much less than they originally sought. The agreement also stipulates that, in addition to these payments, the defendants will pay the plaintiffs’ legal fees up to $81.125 million.

Devine’s lawyers say they intend to negotiate further.

ACM - IEEE CS ECKERT-MAUCHLY AWARD
Call for Award Nominations • Deadline: 30 March 2015 • www.computer.org/awards

ACM and the IEEE Computer Society co-sponsor the Eckert-Mauchly Award, which was initiated in 1979. The award is known as the computer architecture community’s most prestigious award.

The award recognizes outstanding contributions to computer and digital systems architecture. It comes with a certificate and a $5,000 prize.

The award was named for John Presper Eckert and John William Mauchly, who collaborated on the design and construction of the Electronic Numerical Integrator and Computer (ENIAC), the first large-scale electronic computing machine, which was completed in 1947.

Questions? Write to IEEE Computer Society Awards Administrator at awards@computer.org or the ACM Awards Committee Liaison at acm-awards@acm.org