Meet the seven people who hold the keys to worldwide internet security

It sounds like the stuff of science fiction: seven keys, held by individuals from all over the world, that together control security at the core of the web. The reality is rather closer to The Office than The Matrix

James Ball

Friday 28 February 2014
13.00 GMT

In a nondescript industrial estate in El Segundo, a boxy suburb in south-west Los Angeles just a mile or two from LAX international airport, 20 people wait in a windowless canteen for a ceremony to begin. Outside, the sun is shining on an unseasonably warm February day; inside, the only light comes from the glare of halogen bulbs.

There is a strange mix of accents - predominantly American, but smatterings of Swedish, Russian, Spanish and Portuguese can be heard around the room, as men and women (but mostly men) chat over pepperoni pizza and 75-cent vending machine soda. In the corner, an Asteroids arcade machine blares out tinny music and flashing lights.

It might be a fairly typical office scene, were it not for the extraordinary security procedures that everyone in this room has had to complete just to get here, the sort of measures normally reserved for nuclear launch codes or presidential visits. The reason we are all here sounds like the stuff of science fiction, or the plot of a new Tom Cruise franchise: the ceremony we are about to witness sees the coming together of a group of people, from all over the world, who each hold a key to the internet. Together, their keys create a master key, which in turn controls one of the central security measures at the core of the web. Rumours about the power of these keyholders abound: could their key switch off the internet? Or, if someone somehow managed to bring the whole system down, could they turn it on again?

The keyholders have been meeting four times a year, twice on the east coast of the US and twice here on the west, since 2010. Gaining access to their inner sanctum isn't easy, but last month I was invited along to watch the ceremony and meet some of the keyholders - a select group of security experts from around the world. All have long backgrounds in internet security and work for various international institutions. They were chosen for their geographical spread as well as their experience - no one country is allowed to have too many keyholders. They travel to the ceremony at their own, or their employer's, expense.

What these men and women control is the system at the heart of the web: the domain name system, or DNS. This is the internet's version of a telephone directory - a series of registers linking web addresses to a series of numbers, called IP addresses. Without these addresses, you would need to know a long sequence of numbers for every site you wanted to visit. To get to the Guardian, for instance, you'd have to enter "77.91.251.10" instead of theguardian.com.

The master key is part of a new global effort to make the whole domain name system secure and the internet safer: every time the keyholders meet, they are verifying that each entry in these online "phone books" is authentic. This prevents a proliferation of fake web addresses which could lead people to malicious sites, used to hack computers or steal credit card details.

The east and west coast ceremonies each have seven keyholders, with a further seven people around the world who could access a last-resort measure to reconstruct the system if something calamitous were to happen. Each of the 14 primary keyholders owns a traditional metal key to a safety deposit box, which in turn contains a smartcard, which in turn activates a machine that creates a new master key. The backup keyholders have something a bit different: smartcards that contain a fragment of code needed to build a replacement key-generating machine. Once a year, these shadow holders send the organisation that runs the system - the Internet Corporation for Assigned Names and Numbers (Icann) - a photograph of themselves with that day's newspaper and their key, to verify that all is well.

The fact that the US-based, not-for-profit organisation Icann - rather than a government or an international body - has one of the biggest jobs in maintaining global internet security has inevitably come in for criticism. Today's occasionally over-the-top ceremony (streamed live on Icann's website) is intended to prove how seriously they are taking this responsibility. It's one part The Matrix (the tech and security stuff) to two parts The Office (pretty much everything else).

For starters: to get to the canteen, you have to walk through a door that requires a pin code, a smartcard and a biometric hand scan. This takes you into a "mantrap", a small room in which only one door at a time can ever be open. Another sequence of smartcards, handprints and codes opens the exit. Now you're in the break room.

Already, not everything has gone entirely to plan. Leaning next to the Atari arcade machine, ex-state department official Rick Lamb, smartly suited and wearing black-rimmed glasses (he admits he's dressed up for the occasion), is telling someone that one of the on-site guards had asked him out loud, "And your security pin is 9925, yes?" "Well, it was..." he says, with an eye-roll. Looking in our direction, he says it's already been changed.

Lamb is now a senior programme manager for Icann, helping to roll out the new, secure system for verifying the web. This is happening fast, but it is not yet fully in play. If the master key were lost or stolen today, the consequences might not be calamitous: some users would receive security warnings, some networks would have problems, but not much more. But once everyone has moved to the new, more secure system (this is expected in the next three to five years), the effects of losing or damaging the key would be far graver. While every server would still be there, nothing would connect: it would all register as untrustworthy. The whole system, the backbone of the internet, would need to be rebuilt over weeks or months. What would happen if an intelligence agency or hacker - the NSA or Syrian Electronic Army, say - got hold of a copy of the master key? It's possible they could redirect specific targets to fake websites designed to exploit their computers - although Icann and the keyholders say this is unlikely.

Standing in the break room next to Lamb is Dmitry Burkov, one of the keyholders, a brusque and heavy-set Russian security expert on the boards of several internet NGOs, who has flown in from Moscow for the ceremony. "The key issue with internet governance is always trust," he says. "No matter what the forum, it always comes down to trust." Given the tensions between Russia and the US, and Russia's calls for new organisations to be put in charge of the internet, does he have faith in this current system? He gestures to the room at large: "They're the best part of Icann." I take it he means he likes these people, and not the wider organisation, but he won't be drawn further.

It's time to move to the ceremony room itself, which has been cleared for the most sensitive classified information. No electrical signals can come in or out. Building security guards are barred, as are cleaners. To make sure the room looks decent for visitors, an east coast keyholder, Anne-Marie Eklund Löwinder of Sweden, has been in the day before to vacuum with a $20 dustbuster.

We're about to begin a detailed, tightly scripted series of more than 100 actions, all recorded to the minute using the GMT time zone for consistency. These steps are a strange mix of high-security measures lifted straight from a thriller (keycards, safe combinations, secure cages), coupled with more mundane technical details - a bit of trouble setting up a printer - and occasional bouts of farce. In short, much like the internet itself.

As we step into the ceremony room, 16 men and four women, it is just after lunchtime in LA and 21.14 GMT. As well as the keyholders, there are several witnesses here to make sure no one can find some sneaky back door into the internet. Some are security experts, others are laypeople, two are auditors from PricewaterhouseCoopers (with global online trade currently well in excess of $1tn, the key has a serious role to play in business security). Lamb uses an advanced iris scanner to let us all in.

"Please centre your eyes," the tinny automated voice tells him. "Please come a little closer to the camera... Sorry, we cannot confirm your identity."

Lamb sighs and tries again.

"Thank you, your identity has been verified."

We file into a space that resembles a doctor's waiting room: two rows of bolted-down metal seats facing a desk. Less like a doctor's waiting room are the networks of cameras live-streaming to Icann's website. At one side of the room is a cage containing two high-security safes.

Francisco Arias, Icann's director of technical services, acts as today's administrator. It is his first time, and his eyes regularly flick to the script. To start with, things go according to plan. Arias and the four keyholders (the ceremony requires a minimum of three, not all seven) enter the secure cage to retrieve their smartcards, held in tamper-evident bags. Middle-aged men wearing checked shirts and jeans, they are Portuguese keyholder João Damas, based in Spain; American Edward Lewis, who works for an internet and security analytics firm; and Uruguayan Carlos Martinez, who works for Lacnic, the internet registry for Latin America and the Caribbean.

All but one of the 21 keyholders has been with the organisation since the very first ceremony. The initial selection process was surprisingly low-key: there was an advertisement on Icann's site, which generated just 40 applications for 21 positions. Since then, only one keyholder has resigned: Vint Cerf, one of the fathers of the internet, now in his 70s and employed as "chief internet evangelist" by Google. At the very first key ceremony, in Culpeper, Virginia, Cerf told the room that the principle of one master key lying at the core of networks was a major milestone. "More has happened here today than meets the eye," he said then. "I would predict that... in the long run this hierarchical structure of trust will be applied to a number of other functions that require strong authentication." But Cerf struggled with the travel commitment and dropped his keyholder duties.

At 21.29, things go awry. A security controller slams the door of the safe shut, triggering a seismic sensor, which in turn triggers automatic door locks. The ceremony administrator and the keyholders are all locked in an 8ft square cage. Six minutes of quiet panic go by before they hit on a solution: trigger an alarm and an evacuation. Sirens blare and everyone piles out to mill around in the corridor until we can get back to the 100-point script. Every deviation has to be noted on an official record, which everyone present must read and sign off at a later point. Meanwhile, we use the downtime to snack: people rip open a few bags of Oreo biscuits and Cheez-Its.

Both the US commerce department and the Department of Homeland Security take a close interest, to differing degrees, in Icann's operations. In the wake of the ongoing revelations of NSA spying, and of undermined internet security, this does not sit well with many of Icann's overseas partners. Some, including Russia and Brazil - whose president has made such demands very public - are calling for a complete overhaul of how the internet is run, suggesting it should be put under UN auspices.

The question of who put Icann in charge is hotly contested. Lamb argues that "it's the online community; it's the people who've put Icann in charge". Eklund Löwinder, the Swedish keyholder who vacuumed the day before, puts it more bluntly. "Well, mainly, it was the US Department of Commerce," she says. The European Commission wants changes to this system, though it still expresses its faith in Icann; the EU recently called for a "clear timeline for the globalisation of Icann".

Eklund Löwinder explains that while the security might occasionally seem ridiculous, every step is very important when it comes to maintaining trust. "It's a system based on backups of backups, layers and layers of security," she says, her dangly cat earrings swinging. "Of course it is a bit romantic and thrilling to be a part of this, because I am a romantic by heart. I have to admit I love the internet. It's a piece of engineering art you have to admire. And to be able to contribute to make this a safer place makes me feel good."

Where does she keep her key? She admits she has two copies, in case she loses one; one of them never leaves a bank deposit box. The other, which she uses twice a year in the ceremonies on the east coast, is attached to a long metal chain. Most of the time it sits in a wooden puzzle box, with a hidden lock, created by her furniture designer son.

By 22.09 (we are all sticking to GMT) the ceremony is back on and everyone's returning to the script. The high-security machine that will generate the master key is set up. Once activated by the smartcards, this will produce a lengthy cryptographic code. If dropped, or even knocked too hard, the machine will self-destruct.

Now that everything has been removed from the safes, we move to act two of the ceremony: the key signing. The first step would be familiar to anyone - getting the laptop plugged in and booting it up - but some witnesses watch like hawks, logging and initialising each step. Others are beginning to flag, checking their watches or having whispered conversations with their neighbours.

At 22.40, a series of USB drives is set up, one of which will be used to load the signed key on to the live internet at the end of the ceremony: this is when the code is uploaded to the servers that dictate who controls .com, .net, .co.uk and more.

The output of the previous ceremony is checked, to make sure people are working off the same key - a process that requires Arias to read aloud a 64-character code. Everyone nods as they verify it against their sheets.

At 22.48 the high-security machine - a small, plain grey box with a keypad and card slot in front - is wired up. Each keyholder hands over his individual smartcard. Then, at 22.59, nearly two hours after the ceremony began, it's show time. Alejandro Bolivar, an American expert from Verisign, the security company that administers the "root zone" of the domain name system, steps forward to read out a nonsense sequence of words generated by the previous key. He begins: "Flatfoot warranty brickyard Camelot..." and continues for nearly a minute before concluding, "blackjack vagabond." The sequence corresponds with the witnesses' notes, so they nod and sign their script. A short line of code is typed into the laptop at 23.02, and seconds later the new key is signed, to a smattering of applause.

After a 20-minute sequence of disconnecting secure machines and powering down the laptop, a USB stick is handed to Tomofumi Okubo, another Icann staffer. Deliberately or otherwise, Okubo makes a slight bow as he is passed the stick holding the "signed" digital key. Later Okubo will transmit the key on a secure channel to Verisign and this signed key will be made live across the internet. It will take effect for three months, from 1 April (yes, really). After that, the key will expire and error messages will start to appear across the internet.

Given how high the stakes are, and the number of possible targets, does Okubo think the system is trustworthy? "I think so," he says. "You'd have to compromise a lot of people..." He trails off.

Does this often slightly bizarre ceremony work? Are the security precautions integral, or just for show? Bruce Schneier, an American cryptologist and security expert who worked with Glenn Greenwald and the Guardian to analyse some of the files leaked by Edward Snowden, suggests it's a little of both. "A lot of it is necessary, and some of it is necessary theatre," he concedes. "This process is both technical and political, which makes it extra complicated... I think the system is well designed." As to whether the system will survive in the aftermath of the NSA revelations, Schneier thinks the jury is still out: "That, we don't know."

Back in the ceremony room, the four keyholders are once again locked in a cage with the safes holding their smartcards, this time returning them for future use. It is 23.32 on the clock and each is solemnly holding up their keycard, in a new tamper-evident bag, for the cameras to witness before returning it to the safe. Not everyone present is entirely gripped. "It's like a combination of church and a baseball game and I don't know what else," says Icann PR Lynn Lipinski. "I'm getting sleepy."

At 00.06, five hours after we all arrived, it's time to shut off the live-streaming cameras. Lamb checks in to see how many people have been following the ceremony.

The system admin calls back: "We peaked at 12."

We file out, job done.

"Wait," Okubo says. "One question before we go... Can I ask who's coming for dinner?"

There's a show of hands and, with the web secure for another three months, the keyholders to the internet file out into the LA sunshine.

- Watch a film about the Icann keyholder ceremony at theguardian.com/video

- This article was edited on 28 February 2014. The original said El Segundo was in northern Los Angeles, rather than the south-west of the city. This has been corrected.

Topics

Internet Internet safety Cybercrime