Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Instituut voor Informatica en Informatiekunde

Kamer 19.29
Erasmusgebouw
Erasmusplein 1
6525 HT Nijmegen

Telefoon 024 36 53133

www.cs.ru.nl

David van Weel, Minister van Justitie en Veiligheid
Teun Struycken, Staatssecretaris Rechtsbescherming
Zsolt Szabó, Staatssecretaris Digitalisering en Koninkrijksrelaties
Judith Uitermark, Minister van Binnenlandse Zaken en Koninkrijksrelaties
Dirk Beljaarts, Minister van Economische Zaken
Caspar Veldkamp, Minister van Buitenlandse Zaken

Ons kenmerk	Uw kenmerk	Doorkiesnummer	Datum
		06 20619554	11 september 2024

Betreft
Over de risico's van client-side scanning

E-mail
jhh@cs.ru.nl

Hooggeachte bewindslieden,

De Europese Commissie wil serieus werk maken van de bestrijding van online kindermisbruik. Vanwege de gevoeligheid van het onderwerp, en de grote impact die het oorspronkelijke voorstel voor een Verordening zou hebben op zowel de bedrijfsvoering van online dienstverleners als de fundamentele rechten van Europese burgers, is hierover nog steeds geen overeenstemming bereikt.

Gezien de ernst van kindermisbruik is de voortvarendheid van de Commissie volledig te begrijpen. Maar ook aan het meest recente compromisvoorstel, dat in concept is opgesteld onder het Hongaarse voorzitterschap, kleven fundamentele bezwaren. Het totale pakket aan voorgestelde maatregelen is breed, maar ik wil me hier beperken tot het zogenaamde detectiebevel.

Het detectiebevel *verplicht* aanbieders van *end-to-end* versleutelde communicatiediensten (zoals WhatsApp, iMessage, en Signal) maatregelen te nemen om de verspreiding van kinderpornografie tegen te gaan. Het voorstel laat open *hoe* ze hieraan gevolg moeten geven. Maar als aan de bescherming van end-to-end encryptie zelf niet getornd mag worden (zoals het kabinet, de Kamer en ook de Commissie steeds in niet mis te verstane woorden hebben aangegeven), dan zal het scannen van kinderpornografisch materiaal op de telefoons van de burgers zelf moeten plaatsvinden, voordat de berichten versleuteld worden. Iedere te verzenden afbeelding wordt dan vergeleken met bekend kinderpornografisch materiaal, opgeslagen in een (gecodeerde) database. Bij een match wordt het materiaal en de eigenaar van de telefoon aan een nader onderzoek onderworpen. Hiertoe stuurt de telefoon een melding aan een nog op te richten EU Center (onderdeel van Europol), die na nadere beoordeling de melding doorstuurt naar de nationale politie. Dit heet '*client-side scanning*'.

In het laatste compromisvoorstel is deze verplichting vooralsnog beperkt tot enkel het detecteren van *bekende* afbeeldingen van kindermisbruik. Waarbij opgemerkt moet worden dat de verplichte detectie van onbekend materiaal en grooming in tekstberichten (met behulp van kunstmatige intelligentie) zeker niet definitief van tafel is: volgens het voorstel kan de Commissie deze na een nadere beoordeling alsnog verplicht stellen, en is er grote druk op dienstaanbieders om dit ook 'vrijwillig' te implementeren.

Maar zelfs aan deze beperkte verplichting tot client side scanning van bekend materiaal kleven

fundamentele bezwaren. Laat mij deze kort toelichten. In de bijgevoegde 'open letter' van een groot aantal wetenschappers op het gebied van informatiebeveiliging en privacybescherming worden deze bezwaren in meer detail besproken.[1]

Ten eerste is ook de technologie voor het detecteren van bekend kinderpornografie inherent onbetrouwbaar. Weliswaar is de kans op *toevallige* fouten minimaal, maar dat geldt niet voor *moedwillige* acties. Kinderpornografisch beeldmateriaal is eenvoudig zo aan te passen dat het niet als zodanig herkend wordt. Ook is het makkelijk om ogenschijnlijk onschuldige foto's zo te manipuleren dat ze als kinderpornografisch worden gezien, en de nietsvermoedende en onschuldige ontvanger of doorstuurder op een lijst van verdachten voor verder onderzoek te plaatsen.[2] Dit maakt de maatregel zowel ineffectief als riskant.

Ten tweede is end-to-end encryptie een middel om het grondrecht op vertrouwelijke communicatie in technische zin te waarborgen, en geen doel op zich. Client side scanning (dat ongericht is, daarover later meer) omzeilt die waarborg. Het briefgeheim is betekenisloos als de overheid over je schouder kan meekijken met iedere brief die je schrijft, voordat je hem in een envelop stopt. En dat is in feite wat client side scanning doet: op je eigen telefoon meekijken bij ieder bericht dat je verstuurt, om te controleren of je niet stiekem een afbeelding van kindermisbruik meestuurt, voordat het bericht versleuteld wordt. In tegenstelling tot wat de Minister van Veiligheid in Justitie tot nu heeft gesteld ("op dit moment lijkt client side scanning de enige manier waarop de maatregelen in de Verordening kunnen worden uitgevoerd zonder end-to-end encryptie aan te tasten"[3]) wordt de essentie van end-to-end encryptie dus wel degelijk ondermijnd als client side scanning wordt ingevoerd. En daarmee ook de toegevoegde waarde van end-to-end versleutelde communicatiediensten. Bepaalde aanbieders van end-to-end versleutelde communicatiediensten hebben daarom al gedreigd de Engelse markt te verlaten als vergelijkbare voorstellen aldaar worden aangenomen.[4]

Onze telefoon is zeer persoonlijk: we hebben hem altijd bij ons en zetten alles wat we doen, zien of denken in onze telefoon. Je zou je telefoon kunnen zien als je digitale huis.[5] Het voorstel introduceert een fundamenteel nieuwe opsporingsmethode waarbij de opsporingsdiensten in feite toegang krijgen tot je digitale huis en daar een "verklikker" mogen laten installeren, die een melding naar de autoriteiten kan sturen bij iedere match met de database. Het wetsvoorstel komt er dus op neer dat opsporingsinstanties technisch de mogelijkheid krijgen mee te kijken in ons privéleven. Dat dit middel volgens het voorstel alleen maar ingezet wordt voor het detecteren van bekend kinderpornografisch materiaal maakt hierbij niet uit: er wordt een fundamentele grens overschreden. Alle Europese burgers worden zo onderworpen aan een panopticon: "Als alles wat je doet zichtbaar is, maar je nooit zeker weet wanneer je wordt bespied, gedraag je je uiteindelijk alsof je altijd wordt bekeken"[6].

---

[1] Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation: 4 July 2023. https://edri.org/wp-content/uploads/2023/07/Open-Letter-CSA-Scientific-community.pdf

[2] Prokos, J. et al. "Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning". In: 32nd USENIX Security Symposium (Aug. 9–11, 2023). Anaheim, CA, USA, 2023, pp. 211–228. https://www.usenix.org/conference/usenixsecurity23/presentation/prokos

[3] Beslisnota inzake Motie Van Ginneken c.s. over client side scanning, 20 april 2023.

[4] Signal would 'walk' from UK if Online Safety Bill undermined encryption, BBC News, 2023. https://www.bbc.com/news/technology-64584001

[5] Hoepman, J.-H. & Koops, B.-J. Offering 'home' protection to private digital storage spaces, 15 Aug 2020, In: SCRIPTed. 17, 2, p. 359-388.

[6] Kobus Versteegh, Door de toevoeging van cameraschermen bij zelfscankassa's wordt boodschappen doen een stuk dystopischer, De Volkskrant, 11 september 2024. https://digitalekrant.volkskrant.nl/volkskrant/2279/article/2116131/24/3/render/?token=ffea79384ddc9c62da3ab826e69a26b1

Ten vierde is zo'n detectiebevel *ongericht*. Stel (even als voorbeeld) dat WhatsApp een detectiebevel opgelegd zou krijgen. Dan zou dat betekenen dat WhatsApp client side scanning moet inbouwen in de eerstvolgende versie van WhatsApp voor de Europese markt. Dat zou dus betekenen dat bij *alle* Europese WhatsApp gebruikers een verklikker meekijkt met welke afbeeldingen ze versturen. Nou zou in theorie die verklikker na installatie eerst nog uit kunnen staan en later op afstand geactiveerd kunnen worden. Echter, het voorstel vereist dit niet, en het zou in de praktijk ook onwerkbaar zijn omdat op voorhand niet altijd duidelijk is wie eventueel kinderporno verspreidt. Dit is fundamenteel anders dan andere opsporings- en handhavingsmethoden die in essentie *gericht* (horen) te zijn.

Als laatste bepaalt de inhoud van de database wat door de verklikker als verdacht materiaal wordt gezien. Daarmee is de scope van wat verdacht is dus eenvoudig uit te breiden: dat is een simpele update van de database. Op die manier kan het systeem ook gebruikt worden om ander ongewenst materiaal te detecteren, zoals terroristisch promotiemateriaal, of haatzaaiende afbeeldingen. Omdat de database gecodeerd is en dus ook de inhoud hiervan voor de dienstaanbieders zelf (logischerwijs) niet zichtbaar is, is onafhankelijk toezicht op dergelijk misbruik moeilijk. Dat enkel een procedurele maatregel hierbij in de weg staat, is niet erg geruststellend gezien de vele voorbeelden van misbruik van een dergelijke mogelijkheid tot 'function creep'. Zie bijvoorbeeld de ophef over het misbruik van spyware door opsporingsdiensten in Europese landen.[7] Dit maakt burgers, maar ook ambtenaren, politici, journalisten, CEOs – die allemaal wel gebruik maken van een end-to-end versleutelde communicatiedienst – potentieel kwetsbaar.

Het bestrijden van kindermisbruik is ontegenzeggelijk van groot belang. Maar ik hoop dat deze brief duidelijk heeft gemaakt dat ook het afgezwakte voorstel van de Commissie een gevaarlijk precedent schept ten aanzien van de mogelijkheid tot verregaande inmenging van een (Europese) overheid in het privéleven van Europese burgers.

Mochten er nog vragen leven naar aanleiding van deze brief dan ben ik natuurlijk van harte bereid de brief in een nader gesprek toe te lichten.

Met vriendelijke groet,

Prof. dr. J.-H. Hoepman

Bijlage(n): Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation.

[7] Sophie in 't Veld: 'Europa is een soort eldorado voor de spyware-industrie', NRC, 6 oktober 2023. https://www.nrc.nl/nieuws/2023/10/06/sophie-in-t-veld-europa-is-een-soort-el-dorado-voor-de-spyware-industrie-a4176390

Dear Members of the European Parliament,
Dear Member States of the Council of the European Union,

Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation: 4 July 2023

The signatories of this statement are scientists and researchers from across the globe.

First and foremost, we acknowledge that child sexual abuse and exploitation is a very serious crime which can cause lifelong harm to survivors. It is the responsibility of government authorities, with the support of companies and communities, to undertake effective interventions which prevent this crime and react to it quickly when it does happen.

The European Commission has proposed a law with the stated aim of stopping the spread of child sexual abuse material online and of grooming of children online. To do so, the law allows authorities to compel providers of any apps or other online services to scan the messages, pictures, emails, voice mails and other activities of their users. In the case of end-to-end encrypted apps, the claim is that this scanning can be done on users' devices – so-called 'Client-Side Scanning' (CSS).

The effectiveness of the law (at its stated aims) relies on the existence of effective scanning technologies. Unfortunately, the scanning technologies that currently exist and that are on the horizon are deeply flawed. These flaws, which we describe in detail below, means that scanning is doomed to be ineffective. Moreover, integrating scanning at large scale on apps running in user devices, and particularly in a global context, creates side-effects that can be extremely harmful for everyone online, and which could make the Internet and the digital society less safe for everybody.

As the problems we describe speak to measures that are at the core of the EU's legislative proposal, it is our professional recommendation as scientists that such a proposal be not taken forward. It is not feasible or tenable to require private companies to use technologies in ways that we already know cannot be done safely – or even at all. Given the horrific nature of child sexual abuse, it is understandable, and indeed tempting, to hope that there is a technological intervention that can eradicate it. Yet, looking at the issue holistically, we cannot escape the conclusion that the current proposal is not such an intervention.

Passing this legislation undermines the thoughtful and incisive work that European researchers have provided in cybersecurity and privacy, including contributions to the development of global encryption standards. Such undermining will weaken the environment for security and privacy work in Europe, lowering our ability to build a secure digital society.

The proposed regulation would also set a global precedent for filtering the Internet, controlling who can access it, and taking away some of the few tools available for people to protect their right to a private life in the digital space. This will have a chilling effect on society and is likely to negatively affect democracies across the globe.

We therefore strongly warn against pursuing these or similar measures as their success is not possible given current and foreseeable technology, while their potential for harm is substantial.

1. Detection technologies are deeply flawed and vulnerable to attacks

Tools used for scanning for **known Child Sexual Abuse Material (CSAM)** must not contain CSAM material itself as this would bring major risks. Thus, the only scalable technology to address this problem is by transforming the known content with a so-called perceptual hash function and by using a list of the resulting hash values to compare to potential CSAM material. A perceptual hash function needs to achieve two goals: (i) it should be easy to compute yet hard to invert and (ii) small changes to an image should result in small changes to the hash output, which means that even after image manipulation the known image can still be detected. While this sounds easy, after more than two decades of research there has been no substantial progress in designing functions that meet these properties.

Research has shown that for all known perceptual hash functions, it is virtually always possible to make small changes to an image that result in a large change of the hash value which allows evasion of detection (false negative). Moreover, it is also possible to create a legitimate picture that will be falsely detected as illegal material as it has the same hash as a picture that is in the database (false positive). This can be achieved even without knowing the hash database. Such an attack could be used to frame innocent users and to flood Law Enforcement Agencies with false positives – diverting resources away from real investigations into child sexual abuse.

These attacks are not theoretical: for concrete designs such as Photo DNA, Facebook's PDQ hash function and Apple's NeuralHash function, efficient attacks have been described in the literature. The only way to avoid such attacks for the time being is by keeping the description of the perceptual hash function secret. This "security by obscurity" not only goes against basic security engineering principles but, in practice, is only feasible if the perceptual hash function is known only to the service provider. In the case of end-to-end encryption, the hashing operation needs to take place on the client device. Thus, keeping the design secret is an illusion.

As scientists, we do not expect that it will be feasible in the next 10-20 years to develop a scalable solution that can run on users' devices without leaking illegal information and that can detect known content (or content derived from or related to known content) in a reliable way, that is, with an acceptable number of false positives and negatives.

The proposal of the European Commission goes beyond the detection of known content. It also requires that **newly generated images or videos** with CSAM need to be detected based on "artificial intelligence" tools. In addition, the proposal requires that **grooming in communication services** including both text and audio should be detected using similar techniques. While some commercial players claim that they have made progress, the designs remain secret and no open and objective evaluation has taken place that demonstrates their effectiveness. Moreover, the state of the art in machine learning suggests that this is way beyond what is feasible today. In fact, any time that client-side designs have been evaluated (as in the case of prototypes funded by the UK Home office) they have been found to be neither effective nor compliant with privacy and human-rights law.

AI tools can be trained to identify certain patterns with high levels of precision. However, they routinely make errors, including mistakes that to a human seem very basic. That is because AI systems lack context and common sense. There are some tasks to which AI systems are

well-suited, but searching for a very nuanced, sensitive crime — which is what grooming behaviour is — is not one of these tasks.

At the scale at which private communications are exchanged online, even scanning the messages exchanged in the EU on just one app provider would mean generating millions of errors every day. That means that when scanning billions of images, videos, texts and audio messages per day, the number of false positives will be in the hundreds of millions. It further seems likely that many of these false positives will themselves be deeply private, likely intimate, and entirely legal imagery sent between consenting adults.

This cannot be improved through innovation: 'false positives' (content that is wrongly flagged as being unlawful material) are a statistical certainty when it comes to AI. False positives are also an inevitability when it comes to the use of detection technologies -- even for known CSAM material. The only way to reduce this to an acceptable margin of error would be to only scan in narrow and *genuinely* targeted circumstances where there is prior suspicion, as well as sufficient human resources to deal with the false positives -- otherwise cost may be prohibitive given the large number of people who will be needed to review millions of texts and images. This is not what is envisioned by the European Commission's proposal.

The reporting system put forward in the draft CSAM proposal is likely to encourage novel attacks on detection technologies. This is because right now, providers have the discretion to sift out obvious false alerts. Under the new system, however, they would be required to report even content that seems unlikely to be CSAM. Besides the attacks we mention, many more are starting to appear in specialized academic venues, and we expect many more are being prepared by those motivated to share illicit material.

Finally, it has been claimed that detecting CSAM should be feasible as scanning for computer viruses is a widely deployed technology. While superficially both seem similar, there are essential differences. First, when a computer virus is detected, the user is warned and the virus can be removed. Second, a virus can be recognized based on a small unique substring, which is not the case for a picture or video: it would be very easy to modify or remove a unique substring with small changes that do not change the appearance; doing this for a virus would make the code inoperable. Finally, machine learning techniques can sometimes identify viral behaviour, but only when such behaviour can be precisely defined (e.g. code that copies itself) and thus detected. This is in opposition to defining CSAM for which clear boundaries cannot easily be established.

2. Technical Implications of weakening End-to-End Encryption

End-to-end encryption is designed so that only the sender and recipient can view the content of a message or other communication. Encryption is the only tool we have to protect our data in the digital realm; all other tools have been proven to be compromised. The use of link encryption (from user to service provider and from service provider to user) with decryption in the middle as used in the mobile telephone system is not an acceptable solution in the current threat environment. It is obvious that end-to-end encryption makes it impossible to implement scanning for known or new content and detection of grooming at the service provider.

In order to remedy this, a set of techniques called “Client-Side Scanning” (CSS) has been suggested as a way to access encrypted communications without breaking the encryption. Such tools would reportedly work by scanning content on the user’s device before it has been encrypted or after it has been decrypted, then reporting whenever illicit material is found. One may equate this to adding video cameras in our homes to listen to every conversation and send reports when we talk about illicit topics.

The only deployment of CSS in the free world was by Apple in 2021, which they claimed was state-of-the-art technology. This effort was withdrawn after less than two weeks due to privacy concerns and the fact that the system had already been hijacked and manipulated.

When deployed on a person’s device, CSS acts like spyware, allowing adversaries to gain easy access to that device. Any law which would mandate CSS, or any other technology designed to access, analyse or share the content of communications will, without a doubt, undermine encryption, and make everyone’s communications less safe as a result. The laudable aim of protecting children does not change this technical reality.

Even if such a CSS system could be conceived, there is an extremely high risk that it will be abused. We expect that there will be substantial pressure on policymakers to extend the scope, first to detect terrorist recruitment, then other criminal activity, then dissident speech. For instance, it would be sufficient for less democratic governments to extend the database of hash values that typically correspond to known CSAM content (as explained above) with hash values of content critical of the regime. As the hash values give no information on the content itself, it would be impossible for outsiders to detect this abuse. The CSS infrastructure could then be used to report all users with this content immediately to these governments.

If such a mechanism would be implemented, it would need to be in part through security by obscurity as otherwise it would be easy for users to bypass the detection mechanisms, for example by emptying the database of hash values or bypassing some verifications. This means that transparency of the application will be harmed, which may be used by some actors as a veil to collect more personal user data.

3. Effectiveness

We have serious reservations whether the technologies imposed by the regulation would be effective: perpetrators would be aware of such technologies and would move to new techniques, services and platforms to exchange CSAM information while evading detection.

The proposed regulation will harm the freedom of children to express themselves as their conversations could also be triggering alarms. National criminal law enforcement on-the-ground typically deals in a nuanced way with intimate messages between teenagers both around the age of consent. These technologies change the relationship between individuals and their devices, and it will be difficult to reintroduce such nuance. For other users, we have major concerns of the chilling effects created by the presence of these detection mechanisms.

Finally, the huge number of false positives that can be expected will require a substantial amount of resources while creating serious risks for all users to be identified incorrectly. These resources would be better spent on other approaches to protect children from sexual abuse. While most child protection work must be local, one way in which community legislation might help is by using existing powers (DMA/DSA) to require social network services to make it easier for users to complain about abuse, as it is user complaints rather than AI that in practice lead to the detection of new abuse material.

Signed,

Australia

Dr. Shaanan Cohney	University of Melbourne	
Prof. Vanessa Teague	Australian National University & Thinking Cybersecurity Pty Ltd	

Austria

Prof. Dr. Elena Andreeva	TU Wien	
Univ.-Prof. Dr. Rainer Böhme	Universität Innsbruck	
Prof. Maria Eichlseder	TU Graz	
Prof. Daniel Gruss	TU Graz	
Prof. Dr. Martina Lindorfer	TU Wien	
Univ.-Prof. Dr. Matteo Maffei	TU Wien	
Prof. Stefan Mangard	TU Graz	
Univ.-Prof. Dr. René Mayrhofer	Johannes Kepler University Linz	
Prof. Elisabeth Oswald	University of Klagenfurt	
Univ.-Prof. Dr. Christian Rechberger	TU Graz	
Dr. Michael Roland	Johannes Kepler University Linz	
Univ.-Prof. Edgar Weippl	University of Vienna, SBA Research	

Belgium

Prof. Dr. Rosamunde van Brakel	Vrije Universiteit Brussel	
Prof. Claudia Diaz	KU Leuven	
Prof. Dr. Gloria González Fuster	Vrije Universiteit Brussel	
Prof. Dr. Joris van Hoboken	University of Amsterdam and Vrije Universiteit Brussel	
Prof. Olivier Pereira	UCLouvain	
Prof. Thomas Peters	UCLouvain	
Prof. Bart Preneel	KU Leuven	Fellow IACR
Prof. François-Xavier Standaert	UCLouvain	
Prof. Florentin Rochet	University of Namur	
Prof. Nigel Smart	KU Leuven	Fellow IACR
Prof. Mathy Vanhoef	KU Leuven	
Prof. Ingrid Verbauwhede	KU Leuven	Fellow IACR, IEEE

Brazil

Prof. Ian Brown	Centre for Technology & Society, Fundaçao Getulio Vargas	
Prof. Alexandre Augusto Giron	Federal University of Technology - Parana	
Dr. Jean Martina	Universidade Federal de Santa Catarina	
Prof. Dr. Marcos Antonio Simplicio Jr	Universidade de Sao Paulo	

Canada

Prof. Ian Goldberg	University of Waterloo	
Prof. Florian Kerschbaum	University of Waterloo	
Prof. David Lie	University of Toronto	Canada Research Chair
Prof. Nicolas Papernot	University of Toronto and Vector Institute	Fellow Sloan

Czechia

Dr. Vit Bukac	Masaryk University	

Prof. Vashek Matyas	Masaryk University	
Prof. Kamil Malinka	Brno University of Technology	
Dr. Petr Svenda	Masaryk University	
Dr. Martin Ukrop	Masaryk University	

Denmark

Prof. Diego F. Aranha	Aarhus University	
Prof. Carsten Baum	Technical University of Denmark	
Prof. Joan Boyar	University of Southern Denmark	
Prof. Ivan Damgård	Aarhus University	Fellow IACR
Dr. Christian Majenz	Technical University of Denmark	
Prof. Claudio Orlandi	Aarhus University	
Prof. Luisa Siniscalchi	Technical University Denmark	
Prof. Tyge Tiessen	Technical University Denmark	
Prof. Dr. Emmanouil Vasilomanolakis	Technical University Denmark	

Estonia

Dr. Dan Bogdanov	Personal capacity	Estonian Academy of Sciences

Finland

Prof. Kimmo Halunen	University of Oulu

France

Dr. Daniele Antonioli	EURECOM
Dr. Gustavo Banegas	Independent Researcher
Mr. Karthikeyan Bhargavan	Cryspen
Dr. Bruno Blanchet	Inria
Prof. Olivier Blazy	École Polytechnique
Prof. Christina Boura	University of Versailles
Dr. Anne Canteaut	Inria
Dr. Veronique Cortier	CNRS
Dr. Jannik Dreier	Université de Lorraine
Prof. Antonio Faonio	EURECOM
Dr. Caroline Fontaine	CNRS
Dr. Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Dr. Pierrick Gaudry	CNRS
Prof. Elham Kashefi	CNRS and University of Edimburgh
Dr. Steve Kremer	Inria
Dr. Gaëtan Leurent	Inria
Dr. Pierre Laperdrix	CNRS
Dr. P. G. Macioti	Medicines du Monde
Prof. Melek Önen	EURECOM
Dr. Maria Naya Plasencia	Inria
Dir. Research Catuscia Palamidessi	Inria
Dr. Léo Perrin	Inria
Dr. Yann Rote	Université Paris-Saclay
Dr. Emmanuel Thomé	Inria

Germany

Dr. Ali Abassi	CISPA Helmholtz Center for Information Security
Prof. Patricia Arias Cabarcos	Paderborn University
Dr. Gilles Barthe	Max Planck Institute for Security and Privacy
Dr. Sebastian Berndt	University of Lübeck
Dr. Asia Biega	Max Planck Institute for Security and Privacy
Prof. Dr. Kevin Borgolte	Ruhr University Bochum
Dr. Sven Bugiel	CISPA Helmholtz Center for Information Security
Dr. Rebekka Burkholz	CISPA Helmholtz Center for Information Security
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security

Prof. Thomas Eisenbarth	University of Lübeck
Prof. Thorsten Holz	CISPA Helmholtz Center for Information Security
Prof. Tibor Jager	University of Wuppertal
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Dietmar Kammerer	Weizenbaum Institute for the Networked Society
Dr. Franziskus Kiefer	Cryspen
Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Prof. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Dr. Christian Mainka	Ruhr University Bochum
Prof. Dr. Esfandiar Mohammadi	University of Lübeck
Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Dr. Andreas Peter	University of Oldenburg
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Prof. Joachim Posegga	University of Passau
Dr. Elissa Redmiles	Max Planck Institute for Software Systems
Dipl. Ir. Rainer Rehak	Weizenbaum Institute for the Networked Society
Prof. Konrad Rieck	Technische Universität Berlin
Prof. Paul Rösler	FAU Erlangen-Nürnberg
Prof. Dr. Christian Rossow	CISPA Helmholtz Center for Information Security
Prof. Dr. Sebastian Schinzel	Münster University of Applied Sciences
Prof. Thomas Schneider	Technische Universität Darmstadt
Prof. Dr. Dominique Schröder	Friedrich-Alexander Universität Erlangen-Nürnberg
Dr. Peter Schwabe	Max Planck Institute for Security and Privacy
Prof. Juraj Somorovsky	Paderborn University
Dr. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Thorsten Strufe	KASTEL/Karlsruhe & Centre for Tactile Internet with Human-in-the-Loop, Dresden
Prof. Florian Tschorsch	TU Berlin and HU Berlin
Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Prof. Christian Wressnegger	Karlsruhe Institute of Technology
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Xiao Zhang	CISPA Helmholtz Center for Information Security
Dr. Yixin Zou	Max Planck Institute for Security and Privacy

Greece

Prof. Vasiliki Diamantopoulou	University of the Aegean
Prof. Christos Kalloniatis	University of the Aegean
Prof. Georgios Kambourakis	University of the Aegean
Prof. Costas Lambrinoudakis	University of Piraeus
Prof. Emmanouil Magkos	Ionian University
Prof. Stefanos Gritzalis	University of Piraeus and Hellenic Authority for Communication Security and Privacy

Ireland

Dr. TJ McIntyre	University College Dublin Sutherland School of Law & Digital Rights Ireland
Dr. Stephen Farrell	Trinity College Dublin

Israel

Prof. Orr Dunlekman	University of Haifa
Dr. Yossi Oren	Ben-Gurion University
Dr. Eyal Ronen	Tel Aviv University
Dr. Mahmood Sharif	Tel Aviv University

Italy

Prof. Stefano Calzavara	Università Ca' Foscari Venezia
Prof. Mauro Conti	University of Padua
Prof. Bruno Crispo	University of Trento
Prof. Paolo Falcarin	University of Venice

Prof. Fabio Massaci	University of Trento/Vrije Universiteit Amsterdam
Prof. Giuseppe Persiano	Università di Salerno
Prof. Daniele Venturi	Sapienza University of Rome
Prof. Stefano Zanero	Politecnico di Milano

Liechtenstein

Prof. Giovanni Apruzzese	University of Liechtenstein

Luxembourg

Prof. Dr. Gabriele Lenzini	University of Luxembourg
Prof. Peter Y A Ryan	University of Luxembourg

The Netherlands

Dr. Gunes Acar	Radboud University Nijmegen
Prof. Dr. Lejla Batina	Radboud University Nijmegen
Prof. Dr. ir. Herbert Bos	Vrije Universiteit Amsterdam
Dr. Corinne Cath	Delft University of Technology
Dr. Andrea Continella	University of Twente
Prof. Joan Daemen	Radboud University Nijmegen
Dr. Zekeriya Erkin	Delft University of Technology
Prof. Cristiano Giuffrida	Vrije Universiteit Amsterdam
Dr. Seda Gürses	Delft University of Technology
Prof. Jaap-Henk Hoepman	Radboud University Nijmegen
Prof. Andreas Hülsing	Eindhoven University of Technology
Prof. Bart Jacobs	Radboud University Nijmegen
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Prof. Ot van Daalen	University of Amsterdam
Prof. Michel van Eeten	Delft University of Technology
Dr. Heloise Vieira	Eindhoven University of Technology
Prof. Ben Wagner	Delft University of Technology

New Zealand

Prof. Steven Galbraith	University of Auckland

Norway

Prof. Helger Lipmaa	Simula UiB

Poland

Prof. Stefan Dziembowski	University of Warsaw
Dr. Anna Ratecka	Jagiellonian University in Krakow

Portugal

Ms. Sofia Celi	Brave
Prof. Manuel Eduardo Correia	University of Porto
Prof. Manuel Barbosa	University of Porto and INESC TEC
Prof. Hugo Pacheco	University of Porto
Prof. Bernardo Portela	University of Porto
Prof. Henrique Santos	Universidade do Minho
Prof. Nuno Santos	INESC-ID and University of Lisbon

Taiwan

Dr. Lorenz Panny	Academia Sinisa

Turkey

Prof. Cihangir Tezcan	Middle East Technical University

United Arab Emirates

Prof. Michail Maniatakos	New York University Abu Dhabi
Prof. Chirstina Pöpper	New York University Abu Dhabi

United Kingdom

Dr. Ruba Abu-Salma	King's College London	
Prof. Martin Albrecht	King's College London	
Prof. Ross Anderson	Universities of Cambridge and Edinburgh	
Prof. Reuben Binns	University of Oxford	
Prof. Ioana Boureanu	University of Surrey	
Dr. Jaya Klara Brekke	Nym Technologies	
Prof. Lorenzo Cavallaro	University College London	
Dr. Michele Ciampi	University of Edinburgh	
Prof. Liqun Chen	University of Surrey	
Dr. Richard Clayton	University of Cambridge	
Prof. Angela Daly	University of Dundee	
Dr. Partha Das Chowdhury	University of Bristol	
Dr. Benjamin Dowling	University of Sheffield	
Dr. François Dupressoir	University of Bristol	
Dr. Tariq Elahi	University of Edinburgh	
Prof. Hamed Haddadi	Imperial College London	
Prof. Julio Hernandez-Castro	University of Kent	
Dr. Alice Hutchings	University of Cambridge	
Dr. Dennis Jackson	Mozilla	
Dr. Rikke Jensen	Royal Holloway, University of London	
Prof. Adam Joinson	University of Bath	
Dr. Philipp Jovanovic	University College London	
Prof. Vasilis Katos	Bournemouth University	
Prof. Aggelos Kiayias	University of Edinburgh	
Dr. Bernardo Magri	University of Manchester	
Prof. Corinne May-Chahal	University of Lancaster	
Prof. Keith Martin	Royal Holloway, University of London	
Dr. Maryam Mehrnezhad	Royal Holloway, University of London	
Prof. Sarah Meiklejohn	University College London	
Prof. Steven Murdoch	University College London	
Prof. Douwe Korff	London Metropolitan University	
Dr. Daniel Page	University of Bristol	
Dr. Claudia Peersman	University of Bristol	
Dr. Fabio Pierazzi	King's College London	
Prof. Awais Rachid	University of Bristol	
Dr. Luc Rocher	University of Oxford	
Dr. Kaspar Rosager Ludvigsen	University of Edinburgh	
Dr. Christos Sagredos	King's College London	
Dr. Siamak Shahandashti	University of York	
Dr. Jose Tomas Llanos	University College London	
Dr. Michael Veale	University College London	
Dr. Niovi Vavoula	Queen Mary University of London	
Dr. Christian Weinert	Royal Holloway, University of London	
Prof. Alan Woodward	University of Surrey	

United States of America

Prof. Giuseppe Ateniese	George Mason University	
Prof. Adam J. Aviv	George Washington University	
Prof. Steven Bellovin	Columbia University	
Prof. Matt Blaze	Georgetown University	McDevitt Chair of CS and Law
Prof. Álvaro Cárdenas	University of California, Santa Cruz	
Prof. Chandrasekaran	University Illinois Urbana-Champaign	
Prof. Nicolas Christin	Carnegie Mellon University	
Mr. Roger Dingledine	The Tor Project	
Prof. Zakir Durumeric	Stanford University	
Dr. Kelsey Fulton	Colorado School of Mines	
Dr. Simson L. Garfinkel	Digital Corpora Project	Fellow AAAS, ACM, IEEE
Prof. Christina Garman	Purdue University	
Prof. Matthew D. Green	Johns Hopkins University	

Prof. Daniel Genkin	Georgia Tech	
Prof. Paul Grubbs	University of Michigan	
Dr. Joseph Lorenzo Hall	Internet Society	
Dr. Britta Hale	Independent researcher	
Prof. Emeritus Martin Hellman	Stanford University	Turing Award
Prof. Nadia Heninger	University of California, San Diego	
Prof. Nicholas Hopper	University of Minnesota	
Prof. Gabriel Kaptchuk	Boston University	
Prof. Vasileios Kemerlis	Brown University	
Dr. Jennifer King	Stanford University	
Prof. Engin Kirda	Northeastern University	
Prof. Susan Landau	Tufts University	Fellow AAAS, ACM
Prof. Anna Lysyanskaya	Brown University	
Prof. Abigail Marsh	Macalester College	
Prof. Michelle Mazurek	University of Maryland	
Prof. Ian Miers	University of Maryland	
Prof. Prateek Mittal	Princeton University	
Ms. Riana Pfefferkorn	Stanford University	
Prof. Michalis Polychronakis	Stony Brook University	
Dr. Niels Provos	Independent researcher	
Prof. Aanjhan Ranganathan	Northeastern University	
Prof. Amir Rahmati	Stony Brook University	
Prof. Franziska Roesner	University of Washington	
Prof. Ronald L. Rivest	MIT	Turing Award
Dr. Sarah Scheffler	Princeton University	
Prof. Barbara van Schewick	Stanford University	
Prof. Bruce Schneier	Harvard Kennedy School	
Prof. Adam Shostack	University of Washington	
Nick Sullivan	Independent	
Dr. Santiago Torres-Arias	Purdue University	
Prof. Daniel Votipka	Tufts University	
Prof. David Wagner	UC Berkeley	
Prof. Daniel J. Weitzner	MIT	
Dr. Lian Wang	Princeton University	
Prof. Christo Wilson	Northeastern University	Sloan Fellow
Prof. Matthew Wright	Rochester Institute of Technology	

Singapore

Prof. Thomas Peyrin	Nanyang Technological University	

South Korea

Prof. Sang Kil Cha	KAIST	

Spain

Dr. Jorge Blasco Alis	Universidad Politécnica de Madrid	
Prof. Pino Caballero-Gil	University of La Laguna	
Dr. Ignacio Cascudo	IMDEA Software Institute	
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili	Fellow IEEE
Dr. Dario Fiore	IMDEA Software Institute	
Dr. Gemma Galdon Clavell	Eticas Tech	
Prof. Maribel González Vasco	Universidad Carlos III de Madrid	
Dr. Marco Guarnieri	IMDEA Software Institute	
Dr. Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona	
Prof. Llorenç Huguet	Balearic Island University	
Dr. Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona	
Prof. Fernando Pérez-González	University of Vigo	Fellow IEEE
Dr. Cristina Perez-Sola	Universitat Autònoma de Barcelona	
Prof. Jose Such	Universitat Politecnica de Valencia	
Dr. Carla Ràfols	Universitat Pompeu Fabra	
Prof. Josep Rifà	Universitat Autònoma de Barcelona	

Prof. Juan Tapiador	Universidad Carlos III de Madrid	
Dr. Narseo Vallina-Rodriguez	IMDEA Networks Institute	

Sweden

Prof. Simone Fischer-Hübner	Karlstad University & Chalmers University of Technology	
Prof. Dr.-Ing.Meiko Jensen	Karlstad University	
Prof. Panos Papadimitratos	KTH Royal Institute of Technology	Fellow IEEE
Dr. Tobias Pulls	Karlstad University	
Prof. Vicenç Torra	Umeå University	Fellow IEEE

Switzerland

Prof. Srdjan Capkun	ETH Zurich	Fellow IEEE
Prof. Bryan Ford	EPFL	
Dr. Julia Hesse	IBM Zurich	
Prof. Kenneth Paterson	ETH Zurich	Fellow IACR
Prof. Mathias Payer	EPFL	
Dr. Apostolos Pyrgelis	EPFL	
Dr. Raphael M. Reischuk	National Test Institute for Cybersecurity NTC	
Prof. Shweta Shinde	ETH Zurich	
Prof. Carmela Troncoso	EPFL	