Journal of Cyber Forensics and Advanced Threat Investigations

CFATI

Volume 2(1), 63-68. https://doi.org/10.46386/ijcfati.v2i1.36

The Cybersecurity Aspects of New Entities Need a Cybernetic, Holistic Perspective

Rob van Kranenburg[1], Gaelle Le Gars[2]

Abstract

In our connected world security and proof (evidence constituted in Verifiable Credentials (VC, W3C)) is distributed over what an individual can attest, what my objects tell about me (that is why AI = inferences from that data, is so important), and my behavior: “apply shaving foam” is a number in coelition.org. It is clear that we can no longer isolate the notion of security as in securing devices or securing infrastructure. In this brief article which is the background to a number of workshops that the authors and the Journal will host together, we sketch what we believe to be the end of a paradigm of a government model that has outsourced capabilities to the market. It is in the process of privatizing its last public capability: identity management. This is causing tremendous stress in systems, services, organizational procedures, and individuals. We propose a holistic perspective, distributing security at two points: at the device level and a moral movement at a societal level. As a time out to create room to discuss this broadly, we propose a particular model of SSI and disposable identities.

Notes for Research

- This article mainly contributes to the concrete implementation of the disposable Identity framework in the self-sovereign identity model.
- This is a new research and innovation domain that focuses both on regulating device ecologies (including routers) and creating the moral and ethical guidelines for a governance model (cybernetics).
- This article draws on prior findings in workshops (Salons) of the EU project Next GenEration Internet Forward Strategy team. See https://www.disposableidentities.eu

Keywords

Cybersecurity, Devices, Morality, Societal Crisis, Internet of Things, Disposable Identities.

Submitted: 18/04/2021 — **Accepted: 19**/05/2021 — **Published: 23**/05/2021

Corresponding author 1 Email: kranenbu@xs4all.nl Address: IoT Council, Ghent, Belgium
[2] Email:gaellelegars@theinternetofthings.eu Address: IoT Council, Brussels, Belgium

1. Introduction

The Internet of Things (Kranenburg, 2017) is a combination of a technological push - an ecology of barcodes, QR codes, RFID, active sensors, ipv6 - and a human pull for more and ever-growing connectivity with anything happening in the immediate and further out environment, a logical extension of the computing power in a single machine to the environment; the environment as the interface (ubicomp, pervasive computing, and Mark Weiser’s text The Computer for the 21st Century 1991). This push-pull combination makes it very strong, unstoppable, fast and extremely disruptive. In our architectures we are used to dealing with three groups of actors:

- citizens/endusers
- industry/SME
- governance/legal

These all are characterized by certain qualities. In our current (Reference) Models and (Reference) Architectures we build from and with these actors as entities in mind. The data flow of IoT will engender new entities consisting of different qualities taken from the former three groups[1].

[1] For example: IOTA has fundamentally reengineered distributed ledger technology, enabling secure exchange of both value and data, without any fees. Cardano is a proof-of-stake blockchain platform: the first to be founded on peer- reviewed research and developed through

In this short article, we want to sketch three domains of research in a coordinated scope addressing anxiety and stress (whether in people or systems) in a structural way in the paradigm shift towards a 'talkative planet', 'ambient intelligence', cyber-physical systems, in short: a world in which every object is connected in an intranet or in an internet-enabled Cloud or to currently emerging 5G networks.

The first domain lies in what is currently called pathology. To us it is the ability to make changes at the system level and create building blocks that are so far out of the 'ordinary', that as they foreshadow a potential next normal, they cannot be immediately or ever implemented. Not being able to handle logical rejection has severe repercussions: creating and living in alternate realities (psychosis), iterating isolated actions in loops (OCD) (Pankanti et al., 2003), temporarily taking the edge of the horizontal and deep feelings of non-flow (blockades= addiction to substances, affected behavior). The structural element in the situation that has changed with the internet, web and internet of things is that the formative years of the humans endowed/afflicted have become data-driven (constant input) they lack the inner ability to reason with themselves. This ability – to create new foundations – has now been outsourced/taken over by scripted serendipity in the analytics of the content dashboards that inform current decision-making. It. Is therefore vital these individuals are found early and offered impulse-free education. The characterization of this intelligence is that they have immediate recognition of similarity (and difference).

The second domain lies in what is currently called reality. The lack of current attempts to distribute security through shared narratives with a core of beginning-middle-end has not simply lessened but become impossible. Not because of 'fake news' or conflicting visions on what is 'real' but because of the nature of the Internet of Things/Ambient Intelligence which until now has not foregrounded that it is successful only in so far as it 'disappears into the fabric of everyday life'(Weiser, 1999). The nature of this connectivity is that it is invisible and so it infuses what was once and analogue environment into connected objects, city furniture and infrastructures. Digital Twins (the data body of any person, object, AI, template/scenario) are not only separately collected and stored but are able to – in a very mundane way- act in real-time in and on the 'analogue' object in the way that for example, virtual implied car (taking into account information in the area, weather, surrounding cars...) can take over what was once the 'real car'. We are thus fully in Freud's Unheimliche, not just unable to encounter the Doppelgänger but growing up in a world in which it is no longer possible to differentiate between the two. This distribution of insecurity becomes the default. The world feels magical yet without the storyteller or the morphology of Propp. In fact, the narration itself is no longer conceivable as there is no more 'I' to conceive of.

The third domain lies in what is currently called the political[2] (GoNewsDesk, 2021). In the literature on schizophrenia, it is well documented how a disconnect between perceived particular sensorial reality (a slap to the face) and a simultaneous conflicting sensorial reality (hearing the utterance 'you are such a good boy/girl) can become the trigger for behavior that may seek replicates of these moments only in order to feel the resolve -temporarily- (release) of such moments. Life becomes a very short meaning-less (pure procedural) loop. Currently, this pattern is scaled to the level of an entire society (fake news, Q, alternative facts…).

These three actualizations have a similar shattering effect on all levels: ontological (false/true), real (analogue/virtual), and idiolect (the impossibility to connect to an 'I' in order to grow, heal, become 'whole'). So, what is needed is a full re-evaluation of pathology not as an illness but as a particular way of structurally not coping, of reality as a simple scripted set of iterated templates coming from the broad IoT industry (edge, cloud, 5G, AI) and of the political as a particular way and toolbox of designing friction. Concretely we must distribute security at two particular points, at the device level (Kranenburg & Kavassalis, 2021) and the moment it enters into operation and at the governance level of society itself. In between these two

evidence-based methods. Polkadot is a sharded protocol that enables blockchain networks to operate together seamlessly. OriginTrail is an ecosystem & open-source protocol contributing to a more transparent, fair & trusted global supply chain. The Internet Computer is formed by an advanced decentralized protocol called ICP (Internet Computer Protocol) that independent data centers around the world run. https://dfinity.org/faq

[2] A Morality of Movement, as the center will not hold: What then is the rationale behind this? What is the trade-off for the civil servants and politicians who are willingly carrying out these operations? Why would an actor coherently dismantle itself, and aim to hide each step from the participants in the model? The reason is that the next phase of a global underpinning of power has already begun to instantiate itself as CPS, Cyber Physical System outsourcing the security and stability of the assets acquired in the last thirty years fully to what is left of state actors – military and especially steadily militarizing police – and the operational capabilities to large private alliances of services (that are increasingly independent of specific brands and/or companies). This is the new program that we see carried out globally, as all 'systems' begin to look like each other. There may be some minor cultural sensibilities but that is all. The short emancipation of the individual in a democratic state has come to its (logical) end. From now on 'it' (yes it) will be approached at the level of capabilities just like any other good, machine, robot or script: an entity among entities

points which are both a space and a trajectory we can then distribute insecurity, that has a full flow of services, applications and innovation sheltered by the hardcoded values at the device level and the moral movement from the model.

2. Security at Device Level[3]

With so many diverse languages in the world, poor written and verbal communication can often be confused, with conversations devolving into utter nonsense. Before 2000, when the cloud was born and all else was just ideas or demos, we were used to having a "tribe" of easily recognizable devices, including desktop computers, terminals, laptops and the start of cell phones.

Since 2000 we have gone into a process where the ability to compute and interconnect became less immediately visible as the technology to connect moved into everyday things like lamps, cameras, fridges, TVs, cars, and city furniture like lampposts. We are thus in a world where a lot of connectivity and communications happen with no immediate transparency into who is talking to whom. We don't always know the who or what behind the data being collected, nor do we know where it is interpreted.

In some parts of the world, where the politicians are scientists and engineers, potential threats were countered early by building a strong cybernetic system harnessing infrastructure, hardware and services so that devices could control systems from the architecture. We need architectures that can frame the dispersion of IoT devices; otherwise, we increase cybersecurity risks.

Here in the West, with no uniform approach from industry, getting a grip on-device security and protocols has to be done with some forms of regulation. Thankfully, some U.S. politicians do see the need for this kind of protection and have signed into law H.R.1668, the IoT Cybersecurity Improvement Act of 2020. Yet this really is only the first step in that process. This bill will establish a minimum-security standard for all IoT devices purchased by government agencies and will ultimately result in a spillover into the commercial IoT ecosystem quickly.

In Europe, we have also lost control over infrastructure (privatized) and data platforms (GAFA), and are rapidly losing agency on AI, as it has no data lakes and worse, no broad vision on the digital transition. Of course, both the United States and Europe would do better if they were to build their own cybernetic systems, taking firm control over identity (of humans, goods, objects and robots). The EU has rapidly developed a multi-level cybersecurity policy and this policy should be one of the major references for problem-solving in the current IoT world.

This may mean that existing devices will need to be monitored by some form of agency. Ideally, security tests and the education of the market will take place at the moment the device is tested for the CE mark, which indicates conformity with requirements in the EU: "To place a CE Mark on electrical products to be legally sold on the European Market, a manufacturer has to be able to demonstrate compliance with the applicable EU regulations and directives including: the Low Voltage Directive (LVD) 2014/35/EU; Machinery Directive 2006/42/EC; Medical Devices Directive (MDD) 93/42/EEC; and In-vitro Diagnostic Medical Devices Directive (IVDD) 98/79/EC."

Similarly, we need to give any device in an IoT ecosystem a unique identity. This is a necessary step to create a layer of IoT security and control the risks, especially those associated with IoT deployment in home area networks and in public infrastructures. Such an identity can make these devices identifiable when they come online and improve the security of the use of the IoT devices within service chains, thus improving both cybersecurity and end-user's privacy. These identities do not need to be persistent, but on the contrary, must be designed as ephemeral or disposable to avoid systematic tracking of the device and of the owners of the device, but they should become regulated, accepted and widely used. They will obviously be based on the use of standardized digital certificates that will ensure proper authentication, transparency and authorization efficiency, and encryption.

A couple of good resources to ensure IoT devices conform and meet security requirements include:

- Eurofins E&E laboratories offer electrical safety testing for all of these directives and their respective regulations to enable you to place your products on the European market.
- IoT Security Foundation was established to respond to the myriad of challenges and concerns over security in a collaborative, vendor-neutral, international share knowledge, best practices and advice.
- NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a nonregulatory agency of the U.S. Department of Commerce.

[3] This section is published previously in the Guest section of Digicert: https://www.digicert.com/blog/guest-opinion-iot-devices-need-greater-conformity-and-security

ISSN 2753-9997 (online). The International Journal of Cyber Forensics and Advanced Threat Investigations under a Creative Commons License, Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

The world is at a critical crossroads in the battle to ensure strong security of IoT devices that protect user data and ensure integrity. Now is the time for industry and government bodies to work together for the better good of society and the growing IoT segment's future stability. The world is watching and wanting to trust that the right steps will be made.

It is becoming all the more urgent as the IoT — and what your objects are saying about you — is becoming as relevant to who you are as the wallet full of credentials that you will be showing. Device manufacturers, companies selling IoT devices and government regulators all have a role in ensuring device identity, authentication, integrity and data encryption using PKI certificates are adopted to protect users, without compromise.

3. Security at Society Level

In 2012, the first author of the present paper was invited to talk about the Internet of Things at an invitation-only event, run by the GFF and the Italian "Intelligence community", taking place in Rome that September. The session was entitled "Transformational Technologies #4: Implications for an Expanding Threat Environment". In the afternoon, participants - an impressive mix of senior intelligence, police and military, SOCA, CIA, MI6, Homeland Security - broke out in five groups, each tasked with identifying major threats with their unfolding scenarios spanning the coming decade. The groups came back with different scenarios with five topping the list: one was focused on a military conflict, two were about biological disasters produced by DIY Bio[4].To this author, the revelation came with the focus of the remaining two: a total breakdown of society triggered by the failure of existing institutions to manage the Digital Transformation.

Inside the room, Stuxnet (the name itself did not surface) was the talk of the day. Outside, most had no idea. Today, the possibility of the digitally triggered destruction of critical infrastructure is evoked in the mainstream news but it is hardly the full picture. Societal breakdown occurs when trust in core societal institutions abruptly evaporates following years of slow erosion. That final phase typically produced through a single action, a seemingly small action or unimportant move [5] in a long chain of similar moves but resulting in the final reveal. At this point, everyone sees that core institutions no longer operate to sustain a society's shared purpose – their purported raison d'etre has evaporated.

There are many occurrences of this scenario throughout human history, each with its own flavour. In our present instance, the long-running toxic agent eroding our shared purpose is the "digitalization" paradigm which went from a mean to better achieve the designated purpose of an institution to the sole aspirational end, deserving of ever greater sacrifices.

That process ran its course over the last 40 years. "Digitalization" eroded the trust in symbolic institutions through the subtle mean of dematerialization of money and the crude one of wealth dispossession, enabling that neo-feudal future some already predict (Klein, 2020) . One after the other, digitalization cannibalised the public mission of core governance institutions, first through their internal operations then as vectors of transmission, evangelizing for the cause of a cyber-physical system encompassing all life on earth through legislation and budgets. In just about all societal dimensions, from military to health, education or agriculture, the purposeless pursuit of digital efficiency finds concrete manifestations in projects aiming to predict, control and manage human exchanges as if mechanical systems.

The extra layer of insecurity that digitalization brings to those human exchanges is the glaring omission in each of these grand and small plans. When the issue of security finally arises, the merit of digitalization is no longer open for debate and the features expected to deliver "efficiency" are baked in the design. The matter of security is inevitably reduced in scope to securing the system or the process by treating every human as a threat until proven otherwise or, at best, as a more unpredictable component of the process, whose room for maneuver is reduced to the absolute minimum necessary. In other words, securing the system comes at the expense of those very human exchanges which its introduction was supposed to assist or enable.

Back to the scenario playing out at the societal level, the final trigger event, we argue, could well be the decision to deploy digital identity. But this is far from inevitable.

4. Time Out: Disposable Identities

The self-sovereign Framework renegotiates the power divisions between public institutions paid for by taxes, corporate actors paid for services, and citizens without whom both actors would not have a factual base for existence. Public institutions can and will move as much value over to more decentralized structures in Verifiable Credentials in which the legacy of administration and good governance lives on. Corporate actors will get much more granular insight into my behavior if I also get the analysis and feedback from their organizational capabilities to enrich the raw data. I will have much more personal

[4] A virus. That took me by surprise then.

[5] https://www.history.com/news/reasons-berlin-wall-fall provides an illustrative example

relationships with providers if I can decide what attributes of my existence is most relevant to share. I may end up being convinced that if I share more, I may also get better insights. I may outsource these decisions to a service provider. I could do that as part of a group, a local community, a family, a street.

Self-Sovereign Identity is a win-win-win for all actors. It creates a small time out in which we can renegotiate our rights and our duties as responsible individuals in the different contexts of our everyday lives, taking care of our streets, neighborhoods, regions, and the planet. We need the knowledge and praxis of the administrators, engineers, and domain knowledge experts.

The Object Management Group is exploring potential issues and opportunities for standardization across the world of distributed ledger (DLT) and Blockchain ecosystems (Kaili & Psarrakis, 2021). One area of interest is 'self-sovereign' identity (SSID), where we see the potential for standardization for a new kind of 'Disposable' SSID. These are context-specific or ephemeral identities, framed in terms of the existing W3C DID standard for SSIDs but with additional requirements for limited, context-specific usage.

The OMG believes that this requirement may benefit from the development of a standard and has released a 'Request for Information' (RFI) seeking information (Bennett, 2021) from industry and interested parties on the overall SSID space and the challenges of dealing with contextual and short-term identity requirements, privacy and data usage issues etc., in order to establish whether there is a potential need for a standard in this area. The RF has been extended to July 2021[6]

Disposable identities are the antidote to continuous and real-time tracking and tracing of identified users. Instead, they operate via multiples of composable' attribute-based relational identities. Generated for each single interaction between user and service (or object and service) disposable identities are to be disposed of immediately after an event transaction. With disposable identities, an enormous number of diverse applications can run on this ecosystem using a strict attribute-based solution, needing no full disclosure (of identity or social network ties) beyond the bare minimum: age, ability to pay for the service, legal compliance in terms of insurance and accountability. Digital services can be delivered to authenticated users without requiring the need for a single full set of identifying data on identity attributes to be shared.

5. Conclusion

We have shown how the stress caused by the combination of the end of an organizational paradigm in statecraft and incredible speed in internet-related technologies is renegotiating the power balance between industry, government. and citizens. We present the idea that security needs to be distributed at two moments: the moment a device enters the market and the organizational model that determines what is legal and fair in what constitutes that market. As the current stress is related to identity management and specifically to the proactive capabilities of either governmental and corporate actors to fully encapsulate individuals. We propose to break the core of that stress – the one person one number relationship – by implementing globally for both devices and persons multi-relational and contextual disposable identities which are limited in scope, domain and time, thus hardcoding GDPR to create a time out to debate with all stakeholders what kind of 'smart' society it is that we want.

Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article. Please insert relevant information here

Funding

The author(s) declared no financial support for the research, authorship, and/or publication of this article.

Acknowledgments

The research of this work on digital identity and trust was undertaken in the context of H2020 project NGI Forward, H2020 Grant Agreement number 825652.

References

Bennett, M. (2021). Disposable Self-sovereign Identity Request for Information. Retrieved from https://www.brighttalk.com/webcast/12231/461001

[6] Contact mbennett at hypercube.co.uk. (Mike Bennett).

GoNewsDesk. (2021). Rob Van Kranenburg: A Morality of Movement, as the center will not hold. Retrieved from https://www.gonewsindia.com/latest-news/news-and-politics/rob-van-kranenburg-a-morality-of-movement-as-the-center-will-not-hold-24412

Kaili, E., & Psarrakis, D. (2021). Disintermediation Economics : The Impact of Blockchain on Markets and Policies: Palgrave Macmillan.

Klein, A. (2020). Cédric Durand, Techno-féodalisme. Critique de l'économie numérique. Lectures. doi: 10.4000/lectures.44182

Kranenburg, R. v. (2017). Council: The Emergence of an IoT Think Tank. IEEE Pervasive Computing, 16(4), 22-24. doi:10.1109/MPRV.2017.3971130

Kranenburg, R. v., & Kavassalis, P. (2021). Guest Opinion: IoT Devices Need Greater Conformity and Security Built In. Retrieved from https://www.digicert.com/blog/guest-opinion-iot-devices-need-greater-conformity-and-security

Pankanti, S., Senior, A., Brown, L., Hampapur, A., Ying-Li, T., Bolle, R., . . . Kranenburg, R. v. (2003). Security, privacy, and health. IEEE Pervasive Computing, 2(1), 96-97. doi:10.1109/MPRV.2003.1186730

Weiser, M. (1999). The computer for the 21st century. SIGMOBILE Mob. Comput. Commun. Rev., 3(3), 3–11. doi:10.1145/329124.329126