HACKING AS ARTISTIC PRACTICE

Theory/Practice Seminar by
Johannes Büttner and Grayson Earle

For two semesters we gathered as a temporary collective of artists, designers, and theorists. Not to master disciplines, but to dissolve them. We believe that the most interesting ideas emerge where categories collapse and borders become interfaces.

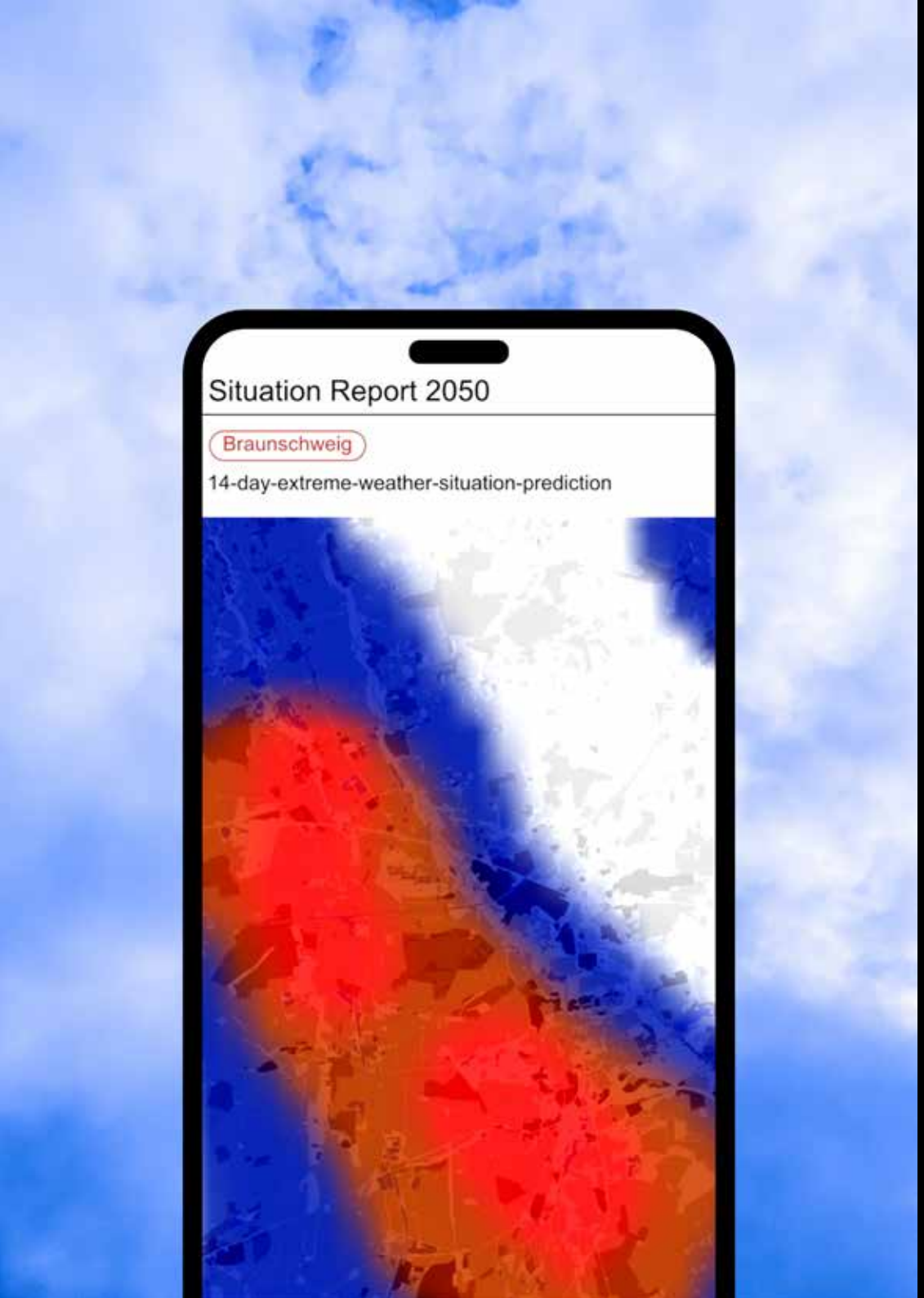
Winter was dedicated to reading systems. Summer to rewriting them.

We understood hacking not as a technical skill but as an artistic method: questioning the status quo, imagining alternative realities, misusing objects, challenging infrastructures, exposing hidden protocols and building prototypes of other futures. Every object is unfinished. Every institution editable. Every failure a new version.

Our projects were acts of self-empowerment, solidarity, speculation and joyful sabotage. They did not seek efficient solutions but productive disturbances. Temporary glitches in reality. Moments in which another world briefly booted.

The future will not be delivered. It has to be hacked.

The projects are scattered across the HBK, treating the Rundgang itself as material. They infiltrate its routes, interrupt its routines and turn the exhibition's own infrastructure into something that can be rewritten.

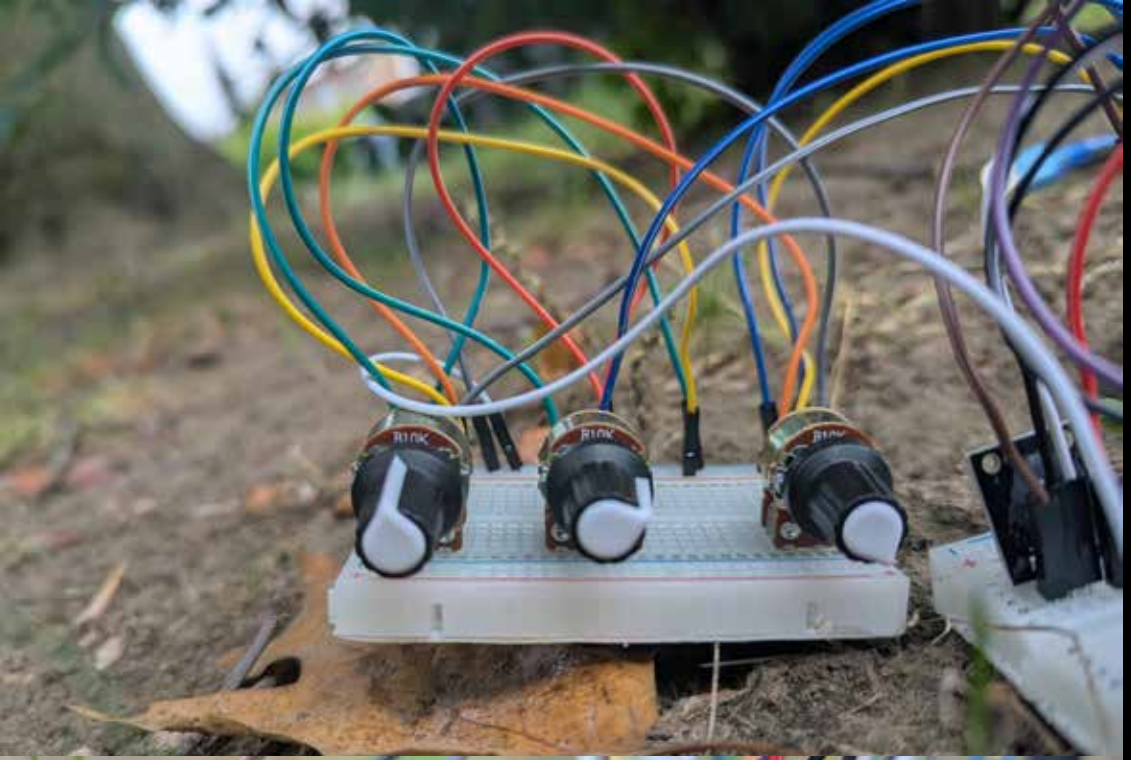


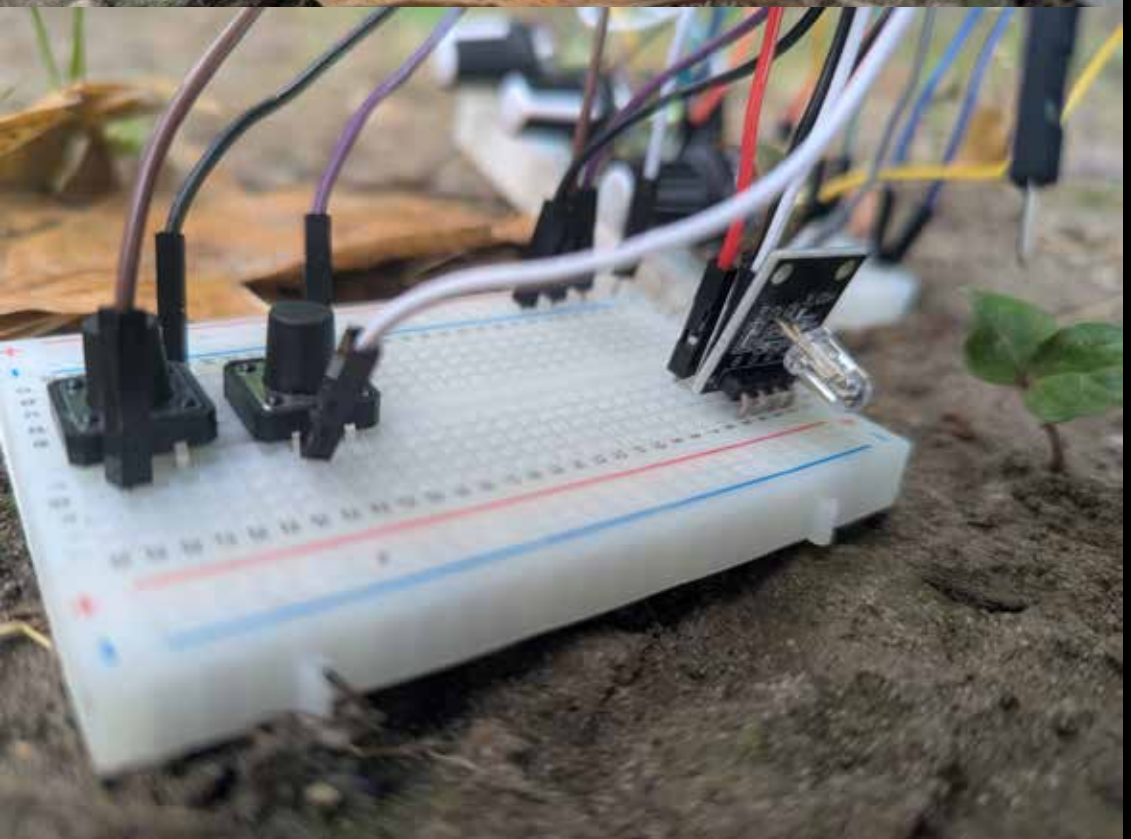
Situation Report 2050

Anton Rusch

In the face of more frequent extreme weather events, one could ask if the usual weather app still has all the necessary information needed to manage daily life. Once extreme conditions become more common, we may stop looking at the weather and start looking at the situation. The situation report 2050 is a speculative web interface that references different data and information about the weather, the city, the landscape, satellites, etc. and presents it in a way that challenges our interaction with the situation through the data we gather.

Location: Birkenhof





Synthesizer aus Naturgeraeuschen // synthesizer from nature sounds

Luna Möbius

Ein Arduino-basierter Synthesizer, der mithilfe einer SD-Karte funktioniert.
Der Ton wird über die Kopfhörer wiedergegeben, und kann durch die Drehregler in den Tiefen, Mitten und Hóehen geformt werden.
Die Knöpfe auf der anderen Seite ermoeglichen eine weitere Modifizierung des Sounds durch Downsampling oder Aenderung der Tonhoehe.
Basis des Synthesizers sind atmosphaerische Klaenge aus dem Alltag, die in der Natur aufgenommen wurden.

//

an arduino based synth using an sd card.
the sound is played via the headphone jack and you may influece bass, mids and treble by tweaking the knobs.
the buttons on the other side can further influence the sound through downsampling and pitch-shifting.
backbone of the synthesizer are sounds recorded from nature, demonstrating the possibilities of everyday-life ambiences in music.

Location: an dem Baum beim Aussenbereich nach der Eingangshalle der HBK

// DEUTSCHE VERSION.
// RUNDGANG '26: HACKEN ALS PRAXIS.
// LUKAS HEMEIER.

THEMA: SMARTPHONES - JEDE FUNKTION HAT IHRE SCHWACHSTELLE.

Das Smartphone, ein Alltagsgerät, das man fast stündlich berührt, überall mit hinnimmt und die wahrgenommene Tageszeit verkürzt. Das Smartphone von heute ist nicht mehr das Smartphone von gestern. Jede Komponente wird stets verfeinert und für einen definierten, meist legitimen Zweck entworfen. Fast jede Komponente trägt aber auch ein zweites Potenzial in sich - denn das Smartphone ist zugleich ein vielseitig hackbares Objekt. Diese Arbeit dient als Versuch, diese beiden Parallelen selektiv und prägnant offenzulegen.

// Biometrische Erkennungsfunktion.

Ein Handy mit Fingerabdruckscanner wurde bereits im Jahr 2000 durch das Sagem MC 959 auf den Markt gebracht. Durch das iPhone 5s, welches die Technologie als Touch ID massentauglich machte, ist es nun zur Normalität geworden, dass Smartphones die Biometrie ihrer Nutzenden abspeichern und zur sicheren Entsperrung des Geräts nutzen.

Mitglied des Chaos Computer Clubs (CCC) Jan Krissler aka Starbug gab lediglich 48 Stunden nach der Veröffentlichung des iPhone 5s an, den Fingerabdruck von Ursula von der Leyen - damals noch Bundesministerin für Arbeit und Soziales - rekonstruiert zu haben. Diese Ankündigung machte er auf einer Konvention des CCC, die selbsternannt Europas größte Hackervereinigung sei, um auf die Gefahr biometrischer Erkennungsmerkmale aufmerksam zu machen. Im Anschluss daran gab er einen nützlichen Ratschlag: „wear gloves“ (dt.: trag Handschuhe).

Schritt-für-Schritt Anleitung:

1. Wähle eine Person aus, dessen Fingerabdruck du erhalten möchtest.
2. Recherchiere nach hochauflösenden Videoaufnahmen der ausgewählten Person.

Tipp: besonders geeignete Suchanfrage: „Pressevideo/bilder [Personname]“

3. Speichere diverse Aufnahmen des Personenfingers aus verschiedenen Blickwinkeln.
4. Nutze die Software [REDIGIERT], um aus den Aufnahmen eine Fingerabdruck-Fälschung zu erstellen.
5. Fertig!

// Mikrofon.

Groß erläutern muss man die Funktion des Mikrofons bei einem Smartphone nicht.

Viele Menschen sind sich darüber unsicher, ob sie von ihrem Alltagsbegleiter abgehört werden. Diese Angst ist nicht unbegründet. Bereits im Bundestag wurde vermerkt, dass durch die Spionagesoftware Pegasus „unbemerkt die komplette Kommunikation auf dem Mobiltelefon einer Zielperson überwacht werden“ könne. Hier ein inhaltlicher Auszug der Bundestagswebsite hinsichtlich einer kleinen Anfrage der Fraktion Die Linke:

„Wissen wollen die Abgeordneten, ob nach Kenntnis der Bundesregierung deutsche Sicherheitsbehörden Produkte der Firma NSO Group erworben haben. Auch fragen sie unter anderem, ob die Bundesregierung und deutsche Sicherheitsbehörden „Kenntnis über die Ausspähung in der Bundesrepublik lebender Journalistinnen und Journalisten, Politikerinnen und Politikern oder Menschenrechtsaktivistinnen und -aktivisten mithilfe der Spionagesoftware ‚Pegasus‘“ haben.“

Schritt-für-Schritt Anleitung:

[Aus aktivistischem Interesse sowie zugunsten der Meinungs- und Pressefreiheit redigiert.]

Präventionsmaßnahmen:

Pegasus-Spyware ist schwer erkennbar. Folgende Maßnahmen können helfen:

1. Meide das Öffnen dubioser Hyperlinks via SMS oder Messenger-Dienste.
2. Installiere das Mobile Verification Toolkit (MVT) der Menschenrechtsorganisation Amnesty International zur Erkennung von Pegasus-Spyware. Mehr Details: https://docs.mvt.re/
3. Sofern im Rahmen von Schritt 2. Probleme auftreten, installiere nutzerfreundlichere und open-source Softwarealternativen, wie iMazing.

// Wi-Fi

WLAN-Kompatibilität ist der Standard jedes neuen Smartphones. Zugang zum Internet ist für viele Menschen heutzutage unabdingbar.

Viele öffentliche Plätze und Einrichtungen bieten ihren Nutzenden kostenfreie WLAN-Netzwerke an. Dies ist nicht nur für Surfende praktisch, sondern auch aus Sicht eines Hackenden lukrativ, da Netz-Aktivität ausspähbar ist. Zugriff ermöglichen Hackende, indem sie das öffentliche WLAN-Netzwerk imitieren. So ein Netzwerk nennt man auch Evil-Twin-Netzwerk.

Schritt-für-Schritt Anleitung:

1. Suche ein stark besuchtes, offenes und kostenfreies WLAN-Netzwerk auf.
2. Richte z.B. mithilfe von WiFi Pineapple ein WLAN-Netzwerk mit identischem Namen (Service Set Identifier) ein. Nun kann schwer zwischen dem echten und falschen Netzwerk unterschieden werden.
3. Wenn das Netzwerk deiner Wahl eine Login-Page hat, dann fertige eine exakte Kopie dieser Seite an und hinterlege sie. Tipp: Kostenfreie LLMs wie ChatGPT und Gemini können bei der Erstellung identischer Website-Interfaces helfen.
4. Nähere dich deinen Cyberopfern physisch, sodass das Signal zu deinem Netzwerk erhöht ist.
5. Trenne mithilfe eines DDoS-Angriffs auf das authentische Netzwerk die Verbindung zu allen angemeldeten Nutzenden, sodass sich diese neu anmelden müssen.
6. Greife relevante Daten ab, sobald sich Nutzende in deinem Netzwerk anmelden.
7. Fertig!

// Quellen.

https://www.bbc.com/news/technology-30623611
https://www.tagesspiegel.de/gesellschaft/panorama/hacker-kopieren-fingerabdruck-von-ursula-von-der-leyen-6900634.html
https://www.okta.com/identity-101/evil-twin-attack/
https://www.bundestag.de/presse/hib/853756-853756evil t
https://docs.mvt.re/
https://imazing.com/de

// ENGLISH VERSION.
// RUNDGANG '26: HACKEN ALS PRAXIS.
// LUKAS HEMEIER.

TOPIC: SMARTPHONES - EVERY FEATURE HAS ITS WEAKNESS.

The smartphone is an everyday device that people touch almost every hour, carry everywhere, and that seems to shorten the perceived length of the day. Today's smartphone is no longer what it once used to be. Every component is continuously refined and designed for a specific, usually legitimate purpose. Yet almost every component holds another kind of potential, because the smartphone is also a highly hackable object. This work aims to selectively and concisely reveal these two aspects.

// Biometric Authentication.

A mobile phone featuring a fingerprint scanner was introduced as early as 2000 with the Sagem MC 959. Since the iPhone 5s popularized the technology as Touch ID, it has become standard for smartphones to store users' biometric data and use it to securely unlock the device.

Chaos Computer Club (CCC) member Jan Krissler, also known as Starbug, claimed

just 48 hours after the release of the iPhone 5s that he had reconstructed the fingerprint of Ursula von der Leyen, then Germany's Federal Minister of Labour and Social Affairs. He announced this at a CCC convention to draw attention to the risks of biometric identifiers. He concluded with practical advice: „wear gloves".

Step-by-step guide:

1. Choose a person whose fingerprint you want to obtain.
2. Search for high-resolution video footage of the selected person.

Tip: A particularly useful search query is „press video/photos [person's name]".

3. Save several images of the person's finger from different angles.
4. Use the software [REDACTED] to create a forged fingerprint from the collected images.
5. Done!

// Microphone.

The purpose of a smartphone microphone hardly needs any explanation.

Many people are uncertain whether their everyday companion is wiretapping them. This fear is not unfounded. It has already been noted in the Bundestag that the „Pegasus" spyware can be used to „covertly monitor the entire communication on a target person's mobile phone." The following is an excerpt from the Bundestag website regarding a minor interpellation by the Left Party faction Die Linke:

„The Members of Parliament wish to know whether, to the Federal Government's knowledge, German security agencies have acquired products from the NSO Group. Among other things, they are also asking whether the Federal Government and German security agencies „have knowledge of the spying on journalists, politicians, or human rights activists living in the Federal Republic using the „Pegasus" spy software"."

Step-by-step guide:

[Redacted for activist reasons and in support of freedom of expression and press freedom.]

Preventive measures:

Pegasus spyware is difficult to detect. The following measures may help:

1. Avoid opening suspicious hyperlinks received via SMS or messaging services.
2. Install Amnesty International's Mobile Verification Toolkit (MVT) to detect Pegasus spyware. More details here: https://docs.mvt.re/
3. If you encounter problems with step 2, install more user-friendly open-source alternatives such as iMazing.

// Wi-Fi.

Wi-Fi compatibility has become the standard for every modern smartphone. Internet access also become essential for many people.

Many public places and institutions offer free Wi-Fi networks. While convenient for users, they can also be attractive to attackers because network activity may be intercepted. Attackers can do this by imitating a public Wi-Fi network, known as an Evil Twin network.

Step-by-step guide:

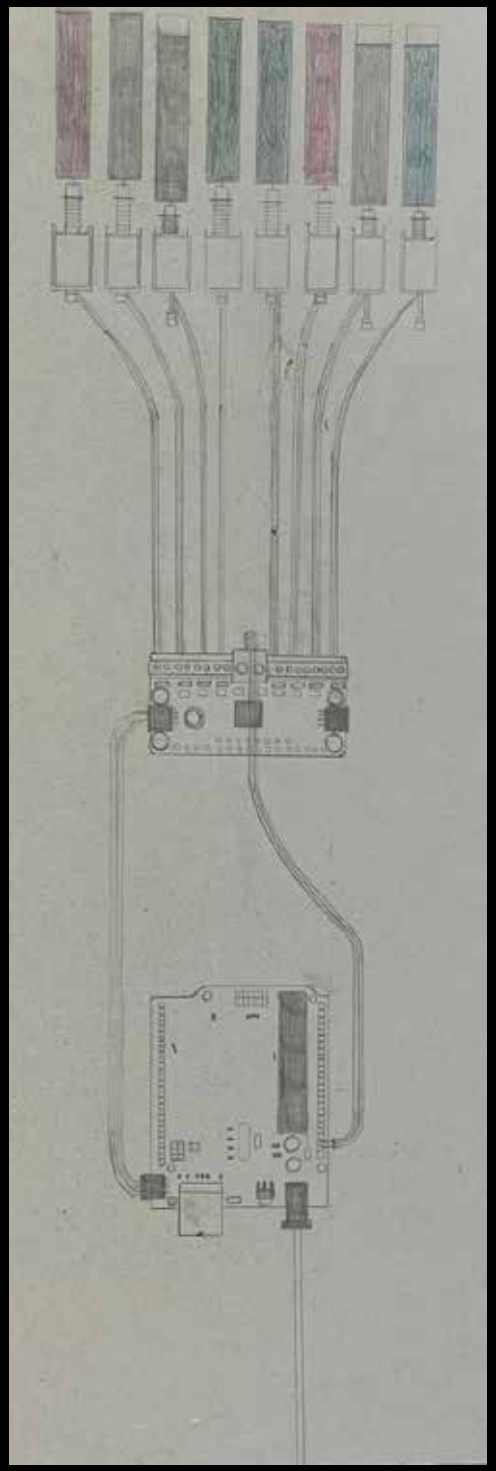
1. Find a free Wi-Fi network with plenty of users.
2. Set up a Wi-Fi network with the same Service Set Identifier (SSID), for example using WiFi Pineapple. Now, distinguishing between the genuine and fake network has become difficult.
3. If the target network uses a login page, create an exact copy of that page and host it.

Tip: Free LLMs such as ChatGPT and Gemini can generate identical websites using easy prompts.

4. Move physically closer to your cyber victims so that your network offers a stronger signal.
5. Disconnect all connected users from the legitimate network using a DDoS attack. This usually forces users to automatically reconnect.
6. Capture and collect all relevant data once users log into your network.
7. Done!

// Sources.

https://www.bbc.com/news/technology-30623611
https://www.tagesspiegel.de/gesellschaft/panorama/hacker-kopieren-fingerabdruck-von-ursula-von-der-leyen-6900634.html
https://www.okta.com/identity-101/evil-twin-attack/
https://www.bundestag.de/presse/hib/853756-853756evil t
https://docs.mvt.re/
https://imazing.com/

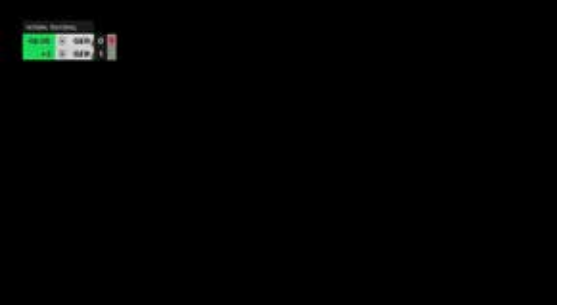


Anne-Mette Roemer

```
/ an array („list“) of 8 pins
// which will be connected to the solenoids
int myPins[] = { 2, 3, 4, 5, 6, 7, 8, 9 };

void setup() {
// put your setup code here, to run once:
Serial.begin(9600);

// ... set up the motion detector

// loop through all 8 pins and set them to output
for (int i = 0; i < 8; i++) {
pinMode(myPins[i], OUTPUT);
}
}

void loop() {
// randomly turn one on every 3 seconds

turnOnInSequence();

delay(1000);
//randomSequence();
}

void turnRandomOneOn() {
// randomly select a number from 0-7
int randomPin = random(8);

// print it in the monitor just to check it out
Serial.println(randomPin);

// turn the one lucky pin on
digitalWrite(myPins[randomPin], HIGH);
}

void turnAllOff() {
// loop through all 8 pins
for (int i = 0; i < 8; i++) {
digitalWrite(myPins[i], LOW);
}
}

void randomSequence() {
// this function first turns all the solenoids off
// then turns 3 randomly on for 300 milliseconds
// then turns them all off
// then waits a second
turnAllOff();

turnRandomOneOn();
turnRandomOneOn();
turnRandomOneOn();

// wait
delay(300);

turnAllOff();

delay(1000);
}

void turnOnInSequence() {
// turn them on in order
for (int i = 0; i < 8; i++) {
turnAllOff();
digitalWrite(myPins[i], HIGH);
delay(250);
}
}
```

Bodria Abivabuck

Location: Geb.40/110











Germany vs. Germany

Video Installation, 2026

Philip Rudzinski

Just because the World Cup is happening, and we quickly put on the same jersey—are we truly one?

Germany vs. Germany subtly shifts the rules of a familiar game. A football simulation stages the German national team against itself. What initially appears absurd gradually begins to feel

strangely familiar. Goals are celebrated, fouls are debated, sides are taken—even though no one can clearly say who „the others" actually are.

Who belongs to whom? Who is the opponent, who the ally? What happens when familiar images of national identification lose their certainty?

The public viewing invites visitors to watch together and engage in conversations about football, competition, and collective identification.

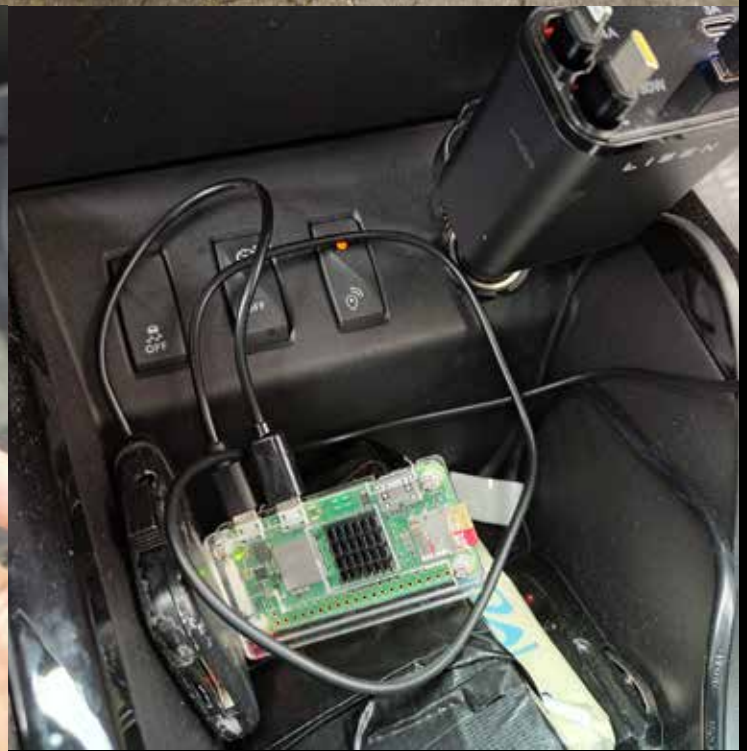
Public Viewing

Thu, 09 July ☐ 6-10 pm

Fri, 10 July ☐ 10 am-6 pm

Sat, 11 July ☐ 10 am-8 pm

Sun, 12 July ☐ 12-6 pm



Dacia Spring OBD2 Adapter

Max Präkelt

Die Elektrowende scheitert an einem einzigen Problem: Fahrzeugenthusiasten haben Gefühle. Und genau diese werden seit Jahren konsequent ignoriert. Denn Hand aufs Herz: Wie soll man ein Elektroauto lieben, wenn es klingt wie ein eingeschalteter Kühlschrank?

Damit ist jetzt Schluss. Das günstigste Elektroauto Deutschlands, der Dacia Spring, bekommt endlich den Motorsound, den es verdient. Im Motorraum lässt sich ein Modul nachrüsten, das mithilfe modernster technischer Magie die Fahrzeugdaten ausliest und daraus einen opulenten Klang erzeugt, der selbst gestandene Verbrennerfahrer kurz innehalten lässt.

Ob Tunnel, Unterführung oder die nächtliche Fahrt über den Bohlweg, endlich kann auch der Stromerfahrer das Gaspedal mit der nötigen Dramatik durchtreten. Die Nachbarschaft wird beeindruckt sein, Passanten drehen sich um und der Fahrer fühlt sich zum ersten Mal nicht mehr wie der Betreiber eines besonders leisen Haushaltsgeräts.

Die Zukunft fährt elektrisch. Sie darf dabei aber ruhig so klingen, als hätte sie acht Zylinder.

Link: https://github.com/Esol1337HaXor/dacia-spring

Location: Parkplatz