(A SHORT SUMMARY OF OUR BACKGROUND)

Losing Ford £4.8M, with just four lines of code

Controlled cyber-physical security & safety research

In 2019, Atumcell conducted a research project with Ford Motor Company. The goals were to determine 1) if a cyber-physical attack could circumvent the company's defenses and 2) be untraceable by law enforcement, meaning the source of the attack could not be determined.

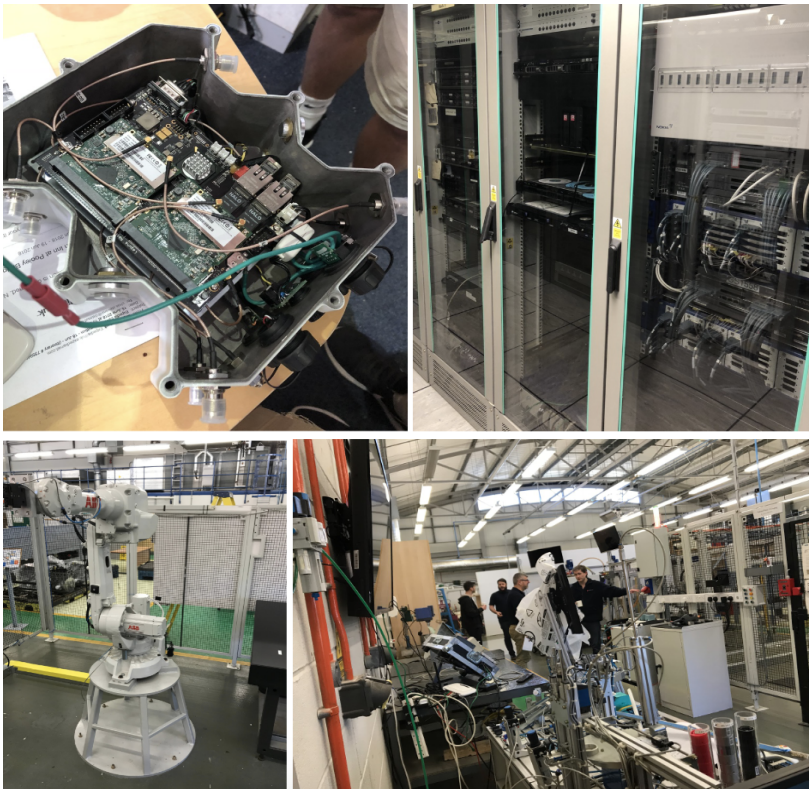
TLDR; it was possible.

The concept was simple: create a custom microcontroller that acted as a legitimate logic controller. The logic controller, once connected to the network, would seek out other devices and then send commands and exploits to them. In order to remain undetected, it was necessary to bypass CCTV, access controls, and IAM systems.

Initial reconnaissance revealed that the door took 4 seconds to close, just enough time to tailgate. Inside, cameras were positioned in many locations. However, one route to the factory floor had a blind spot. If a person entered the building through the side lobby door and kept close to the wall, they could evade CCTV detection.

The researchers carried forged gas inspector cards to present in case they attracted suspicion. No one challenged these credentials when they were presented.

Once inside, access controls were bypassed with traditional lock picks and custom RFID cloners concealed in clipboards. Forged ID badges were worn and the inspector pretext was used throughout without incident.



Once inside the factory, the researchers sought out key infrastructure components. They located the active switch that all traffic went through and within minutes a cold boot attack took full control of the switch and firewall.

They plugged in an out-of-band exfiltration tool to observe all network traffic. Once the network topology was mapped they could simply add the configuration to the weaponized logic controller. This whole process took less than 5 minutes. While they waited they linked out safety devices to prove that physical harm was possible too.

Once the device was ready, they plugged it into a free network port - if you look, you can often find these easily - unprotected. The ones that use port locks can be bypassed with crude tooling. Once the device was on the network, it sent the micro payload to all active controllers. Within 1 minute, the entire production line stopped.

The entire attack took less than 10 minutes and left people looking confused and bewildered as to why the lines stopped. In these environments, status check before operation is key; this process at Ford takes 60-120 minutes. Each line produces £10.000 of wholesale parts per minute. All four lines down for 120 minutes would cost Ford at least £4.8M in lost revenue.

When the attack was finished, Atumcell invited Ray Massie to investigate. He is a former Met Police Officer who ran the Met's E-Crime Unit until 2014 and successfully investigated the Anonymous hacking movement, and collaborated with major intelligence agencies to investigate cybercrime targeting the crown estate and British government.

The investigation found the following:

- No one was able to find the exact USB port the device was plugged into
- Cameras completely missed the adversaries entering the building
- Access controls, locks, and doors were bypassed without a trace
- The system did not recognize an issue with a completely new device issuing commands
- No one was able to trace the timeline of compromise
- No one was able to detect or find the cold-boot attack on core infrastructure
- No one detected the linked-out safety devices

Speaking at prestigious cyber security and industrial security events like Red Hat, B-Sides, Defcon, SteelCon & More.

The research attracted major press coverage and requests for solutions. Atumcell could not find the type of solution needed to truly defend a site from cyber-physical attacks. It was then that Atumcell's Flagship product, Gamayan, was born.

Gamayan is the first and last line of defense for simple to complex industrial systems.

Advisory roles and industry experience

The core team includes a number of specialists from all areas of cyber, physical, and industrial security and safety. The team comprises industry experts and world-renowned specialists. Our team, before joining Atumcell, have worked for the likes of Sony, Ikea, Secure Link, IBM, Erickson, Blackberry, BT, Ford, News Corporation, and many more. A number of our team have military and intelligence experience ranging from active service to consulting.

Atumcell is a company dedicated to providing AI-powered contextual cyber-safety for Industry X.

Our research into industrial cyber-physical threats has been featured in the likes of BBC One, The Telegraph & SVT (SE). The research was also presented at some of the world's largest cyber security conferences.

Atumcell chaired the secure data transfer committee for the Public Safety Technology Alliance (PSTA), which includes telecommunications, public safety, and technology leaders. It is a nonprofit coalition with a mission of adopting open, best-in-class, standards-based technology for AT&T FirstNet US emergency responder network.

Speaking and teaching at multiple Fortune 500 companies, universities, and conferences on matters of cyber/physical security.

Hosting popular webinars & meet-up groups