Establishing a digital emblem to protect humanitarian organizations in cyberspace

November 29 2023, by Samuel Schlaefli

In future, digital critical infrastructure should be labelled as worthy of protection by a digital emblem. Credit: ICRC

Ransomware attacks can paralyze organizations or entire countries by hacking into a network and encrypting critical data. The attackers then demand a ransom; if their demands aren't met, the data will not be decrypted and may be lost forever. Depending on the given situation, the financial and logistical damage can be enormous.

In January 2022, the International Committee of the Red Cross (ICRC) was the victim of a cyberattack. Data belonging to more than 500,000 people around the world was stored on the affected servers. This included data on people who needed special protection, such as missing persons, refugees from war zones and prisoners.

"The ICRC's digital infrastructure has grown considerably in recent years—and so has the number of cyberattacks on our systems," says Mauro Vignati, Adviser Digital Technologies of Warfare at the ICRC. Particularly during wars and armed conflicts, such cyberattacks could also have catastrophic humanitarian consequences, for example, if the digital infrastructure of a hospital is paralyzed by the enemy.

Trusted emblem for protection against attacks

For conflicts beyond cyberspace, the ICRC has employed protective emblems since the Geneva Conventions of 1949, the core of international humanitarian law. The red cross, red crescent and red crystal provide protection for hospitals, vehicles and employees of organizations in the International Red Cross and Red Crescent Movement network (including the ICRC).

Today, the network has more than 80 million members who are active in 192 countries. As a matter of principle, bearers of these emblems are protected by international humanitarian law, especially in conflicts. Warring parties are not allowed to attack them.

"That's why we've been wondering for some time whether we could also develop an emblem to protect our digital infrastructure," Vignati says. Such a system would have to fulfill a number of requirements. "It should be easy and cost-effective to integrate into existing digital systems worldwide and easy to maintain. It would also have to bridge linguistic, technological and cultural differences." What's more, the emblem ought to be as flexible as possible. In certain situations, it's important for ICRC staff to mask the emblem, Vignati says.

Three years ago, the ICRC contacted the Center for Cyber Trust, a research collaboration between ETH Zurich and the University of Bonn in the field of cybersecurity, with this idea of establishing a digital emblem. One of the people working on this since then is Felix Linker, who is currently writing his doctoral thesis in the group led by David Basin, Professor of Information Security at the Department of Computer Science at ETH Zurich.

"A digital emblem has a unique combination of security requirements, namely authenticity, accountability and a property that we call covert inspection," Linker says. The Authentic Digital EMblem (ADEM), which he has developed together with Basin, is based on the web PKI and CT ecosystem (Web PKI and CT stand for Web Public Key Infrastructure and Certificate Transparency).

"We rely on existing best practices on the internet. What makes our work innovative is how we've combined different solutions to meet the technical requirements," Linker says. In an article recently published in the *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, Linker and Basin describe in detail for the first time how ADEM works.

Machine-readable and decentralized

The emblem they have developed is cryptographically secured using a digital signature—a long sequence of bits that can be read by a program developed for this purpose. This makes it possible to retrieve information about the owner, the IP or domain worthy of protection, as well as the publisher of the emblem. "It's important that the emblem can be read by machines, because most cyberattacks today are automated," Linker says.

In other words, hacker software needs to automatically load and read the emblem, so it can recognize that it is accessing a system belonging to an organization that is protected by international humanitarian law. And that needs to happen during the software's first reconnaissance, before it does any damage to the system.

Another key requirement is for the digital emblem to be managed in a decentralized way rather than by a central authority. States that are committed to international humanitarian law should be able to verify that a certain digital infrastructure on their territory is entitled to protection and therefore bears an emblem. To this end, ADEM is based on an open standard, so governments can adapt the emblem's implementation as flexibly as possible to their own requirements.

Hackers remain undetected

Potential attacks on servers and networks can come from hacker groups, but also from states during a war. These want to remain undetected at all costs. "That's why attackers must be able to view the emblem without either the protected institution or the issuer of the digital signature being able to tell that the emblem has been looked at." Only then will potential attackers be prepared to have their systems run the scanner for detecting the emblem.

"Standard internet authentication protocols aren't suitable for this

because they require interaction between the two parties involved," Linker says. "That attracts attention, which means it won't work in a conflict." He managed to come up with a combination of suitable internet protocols (UDP, TLS and DNS) to mask the distribution of the emblem.

Linker has now evaluated the system in a security analysis under a comprehensive threat model. His evaluation shows that the digital emblem cannot be misused by attackers and acts as a security guarantee. He says that this provides proof of concept. He is now developing the first prototypes further, while colleagues from the Center for Cyber Trust in Bonn will conduct interviews with hackers to find out how willing people are to respect such an emblem.

After all, only then will they bother to run a program that can recognize emblems. But this is something Linker is confident about: in the past, hackers have been known to avoid humanitarian targets on occasion, "for ethical reasons or simply to avoid attracting too much attention."

Difficult legal implementation

Vignati from the ICRC is satisfied. "ADEM fulfills all our original requirements for a digital emblem." The main task now is to further optimize the emblem's visibility to potential attackers. However, it will probably be several years before the digital emblem actually starts helping to protect the ICRC's critical digital infrastructure and hospitals in war zones.

"The legal implementation is very challenging," Vignati says. Implementing the emblem in the legal framework calls for adjustments to the Geneva Conventions. "Either through a new additional protocol or through an addition to the existing protocols."

The ICRC plans to showcase ADEM, along with another system designed at John Hopkins University, at an international humanitarian law conference to be held in October 2024. It will also present legal pathways for bringing the digital emblem into operation. "That would be an important first step in strengthening humanitarian protection in cyberspace," Vignati says.

More information: Felix Linker et al, ADEM: An Authentic Digital EMblem, *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (2023). DOI: 10.1145/3576915.3616578

Provided by ETH Zurich