https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-336

Conception of a Secure Remote Maintenance Procedure Using Dedicated Hardware

Franziska Schwarz, Klaus Schwarz, Reiner Creutzburg

Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany

Email: franziska.schwarz@th-brandenburg.de, klaus.schwarz@th-brandenburg.de, creutzburg@th-brandenburg.de

Abstract

Remote control and remote servicing are often very problematic due to restrictive policies in health care and other critical environments. This paper describes our new design of a Secure Remote Service Box, which is a tiny box that offers restricted access and robust security policies for critical environments and institutions. It allows secure remote access (for example, Team Viewer, ...) for remote control and remote servicing and blocks all other Internet traffic and connections. All devices connected to the LAN port are secured by NAT and complex filters that are natively detected and imported by Windows Network Management. The Secure Remote Service Box fulfills Cybersecurity policies for critical environments and institutions and is, of course very reliable and secure by design.

Keywords

secure remote service, secure remote control, firewall, critical infrastructure maintenance, cybersecurity, secure remote desktop, healthcare security, security.

Introduction and Motivation

Many manufacturers and service providers want to offer their customers convenient monitoring and remote maintenance services and support for their equipment or IT systems. The same applies to the customer side. Many customers use several remote maintenance services and have to enable external service providers to access a company's internal network. These main requirements are important in both cases: The remote maintenance service should ensure reliable IT security, audit-proof recording of all service activities, flexible integration in different environments, and simple operation with the highest possible security. Another important requirement is the openness of the system for different remote desktop software. Different vendors use different software solutions to perform maintenance work (fig. 1). The Secure Remote Service Box must allow the secure integration of different remote service solutions. The goal of this work is the conception of a Secure Remote Service Box, with which an extremely secure remote maintenance access can be realized almost everywhere in the world. The robust device should be able to be installed e.g., on the diesel engines of seagoing vessels, on industrial robots or wind turbines or directly in server rooms or in hospitals. After all, these are the very places where manufacturers or service providers need to monitor and support remotely. The Secure Remote Service Box to be designed in this work is intended to provide security in the event of maintenance and to establish an encrypted connection for data transfer. Besides, its firewall function restricts external access exclusively to the system to be maintained. This means that other sensitive networks owned by the customer are not accessible via the maintenance access.

Figure 1. *Most Popular Free Remote Desktop Solutions 2019*

Different applications have different security policies and regulations. By restricting access to the device requiring maintenance, neither the selection of remote desktop software nor the setting of security policies may be restricted. In this way, customers can also cover all possible requirements for remote maintenance service activities in different environments, such as military applications or medical environments. With the Secure Remote Service Box, any kind of machines and IT systems should be able to be conveniently monitored and maintained remotely, without external access endangering IT security or requiring special types of connection.

The requirements for the Secure Remote Service Box, in brief, are as follows:

- Reliable protection of the remote maintenance access,
- Physical and logical separation of the maintenance object from the surrounding network,
- Connections via a standard RJ45 interface and thus particularly low requirements on the characteristics of the interfaces of the maintenance object,
- Comfortable operation with any remote desktop software,
- Mobile remote access also via Smartphone and Tablet-PC,
- Separate maintenance area due to the firewall function,
- Freely definable regulations according to company policy,
- Easy integration into existing networks,
- High availability and permanent operability,

- Maintenance-free industrial hardware.

For many small and medium-sized companies, this list of requirements simply cannot be met with their resources. Since hardware and software of such a Secure Remote Service Box has to be designed mainly by IT experts who are familiar with all relevant IT security and compliance regulations and have received extensive training.

Definition of the term remote maintenance

Remote maintenance can be defined as all activities that are carried out without the need for a technician to be physically present on-site at the system to be maintained. Remote maintenance can be realized ”online” or ”offline”. The remote maintenance of a system, which is realized by means of a CD, for example, which contains a self-executing update program, corresponds to ”offline remote maintenance”. Remote maintenance via the local or global network corresponds to access by a partner external to the LAN, who connects to the system to be maintained via the Internet and an access system and carries out the maintenance work. This paper deals with securing remote maintenance via a network.

Application possibilities for remote maintenance

Especially in the age of globalization, many companies are expanding into widely distributed locations. Products with maintenance contracts or maintenance requirements are sold worldwide. It is precisely this global activity of companies and the worldwide sale of products requiring maintenance that results in the fact that for administrative purposes, these systems can only be accessed at their respective locations for ”direct” configuration at significant expense. Especially manufacturers who offer their customers regular updates and maintenance, as well as service and maintenance work, need a way to administer and control the decentralized systems centrally. Remote maintenance serves this purpose. The following advantages result from remote maintenance access:

- Enables administrators and manufacturers to have central access to decentralized systems
- Target systems are accessible 24/7, around the clock
- Relevant and important data can be loaded from and onto the system
- No physical access to the system necessary

Realization possibilities of remote maintenance

As already described in the definition of the term remote maintenance, remote maintenance access is usually realized via the Internet, because the Internet offers the advantage of a worldwide network, which is available free of charge except for the dial-up costs of the provider. A procedure specified by the manufacturer usually provides access to the systems to be maintained. These procedures usually involve so-called remote desktop software such as TeamViewer. A logical interface for administrative access on the system is used for this purpose. The respective network operator must then activate access to this interface for maintenance purposes. Such accesses are, due to the access path via the Internet, mostly encrypted procedures, such as HTTPS, SSH, or VPN accesses, which have to be secured by extended firewall rules. These procedures protect the data sent in the connection, and the interfaces enabled for maintenance from being viewed and accessed by third parties.

Remote Desktop Software

Remote Desktop refers to the remote access to the user interface of a computer. Application programs are executed on one computer in the form of a server and are displayed and operated on another computer in the form of a client. In contrast to screen sharing, no user needs to log on to the server locally. A remote desktop session runs independently of any other session that may be running.

Risks associated with remote maintenance procedures

If a secured interface does not provide a remote maintenance access and with the possibility of encrypting the data, a multitude of attack possibilities arise, such as man-in-the-middle attacks or sniffer attacks, in which security-relevant data, such as passwords or processes, can be read and exploited by third parties on the Internet, but also in the LAN. The figure 3 shows the unsecured access to a system. Although encrypted, remote maintenance access prevents third parties in the network from reading the connection, encrypted access also restricts the local administrator from checking which the encrypted connection performs connections or actions. Remote maintenance access thus opens a door into the network of the respective company and thus represents a security risk. Since systems to be maintained are often located in an existing computer network, there is a risk that computer viruses from a system to be maintained will continue to be transferred to other systems in the local network or that further information about the internal network topology of the company network will become known through espionage measures, which can be exploited for further attack measures. The possibilities of maliciously exploiting open access to a system are significant. It is, therefore, essential to make access as secure as possible, but also as transparent as possible. Figure 4 shows encrypted, remote maintenance access, and still existing dangers.

General concept description

The concept of secure remote maintenance consists of logically separating the system to be maintained from the LAN. When accessing the system, it is therefore not possible to spread computer viruses in the local network or sniff other existing connections. Furthermore, the present concept does not allow connections directly from the Internet to the LAN, i.e., to the system to be maintained. Also, the system to be maintained should only be connected to the Internet via the ports that are necessary for maintenance and should only be allowed to communicate on these ports via specified protocols. Figure 2 shows a possible appearance of a Secure Remote Service Box. This concept makes it possible to provide an encrypted connection via the Internet, but to limit the connections to the most necessary and thus make them transparent and testable (e.g., for viruses or known attack methods). Furthermore, no direct access to the system in the LAN is possible, since the system is not visible from outside due to the logical separation. In order for remote maintenance access to take

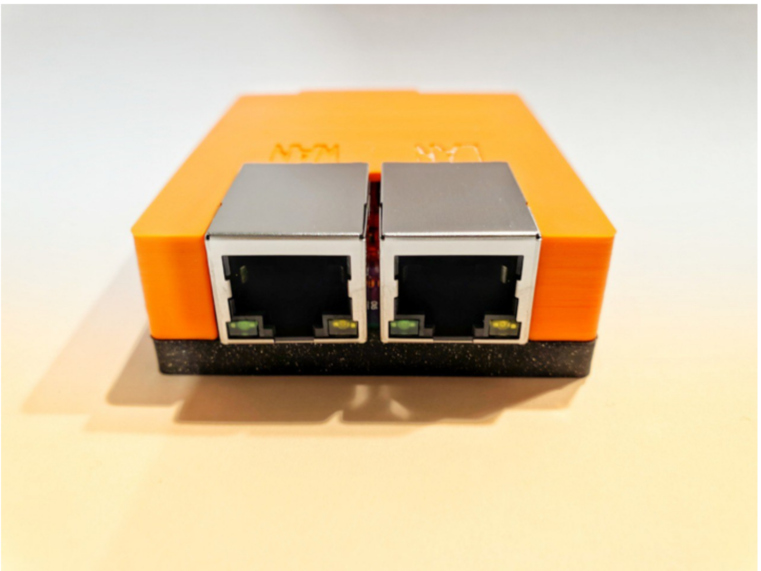


Figure 2. *Possible appearance of a Secure Remote Service Box*

place, it must comply with the previously defined rules of the respective remote desktop software. Figure 5 shows a schematic diagram of the Secure Remote Service Box in a hospital-like environment.

Technical backgrounds

The Secure Remote Service Box is a shielding, as shown in figure 5. The connected system is thus physically and logically separated from the external network. The LAN interface of the Secure Remote Service Box provides direct access to the system to be serviced. The external partner connects to the server to be serviced via previously configured Remote Desktop Software. The connection via the Internet corresponds to the specifications and the security level of the software used in each case and can thus be freely adapted to the intended purpose and location. The Secure Remote Service Box can identify the remote terminal using proper authentication and authorization, preferably utilizing certificates — all connections from and to the system to be maintained run via the Secure Remote Service Box. The Secure Remote Service Box can identify the nature of incoming and outgoing connections and whether they comply with the predefined rules. By assigning a system requiring maintenance to exactly one Secure Remote Service Box, different types of Remote Desktop Software can be used for each device. It is also possible to allow connections to the system to be maintained only from a particular well-known host. When the Secure Remote Service Box receives the signal for a connection request, it checks the sender data. There is no direct connection from the remote host to the system to be maintained. If the sent parameters match the internal policy of the Secure Remote Service Box, a connection may be established. At the same time, the system is logically separated from the surrounding network by the Secure Remote Service Box by being assigned to a specially generated VLAN and integrated into a separate zone. If all predefined rules are followed when establishing a connection, the Secure Remote Service Box connects the connection establishing client and the server requiring maintenance with each other. The external technician can now access a system requiring maintenance via the Internet and through the LAN of the respective customer following the predefined policy. The logical environment is designed as if the system to be maintained is located in its maintenance network and thus isolated.

Advantages of the access method

This solution eliminates all the risks mentioned and offers the following advantages:

- The influence of remote maintenance and all associated hazards is limited to the smallest possible area around the maintenance object.
- Remote maintenance access is impossible without the cooperation or approval of the customer network administrator.
- Except for the maintenance object, access by outsiders is impossible.
- The external connection to the Secure Remote Service Box is logically and physically separated from the internal connection.
- The internal part of the network and thus the maintenance object cannot be seen from outside.
- The filter function of the Secure Remote Service Box prevents the remote maintainer from accessing other customer systems from the maintenance object that is not located in the area of the maintenance object.
- This remote maintenance solution is independent of the type of the customer's existing firewall and can be used agnostically against different types of remote desktop software.

Summary and Conclusion

Especially in the age of globalization, many companies are expanding into widely distributed locations. Products with maintenance contracts or maintenance requirements are sold worldwide. Many manufacturers and service providers want to offer their customers convenient monitoring and remote maintenance services and support for their equipment or IT systems. The same

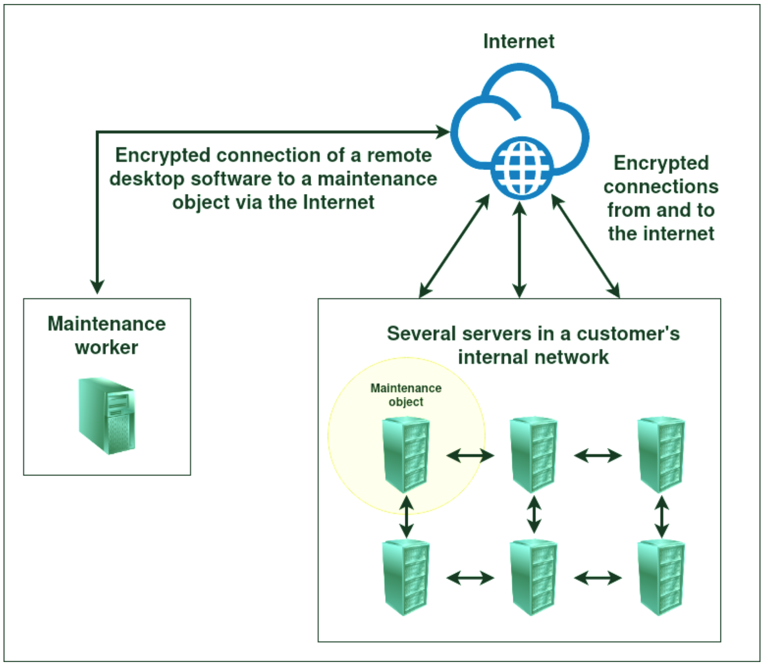

Internet
Encrypted connection of a remote desktop software to a maintenance object via the Internet
Encrypted connections from and to the internet
Maintenance worker
Several servers in a customer's internal network
Maintenance object

Figure 3. *Unsecured but encrypted access to a maintenance object*

applies to the customer side. For many small and medium-sized companies, this list of requirements simply cannot be met with their resources. Since hardware and software of such a Secure Remote Service Box has to be designed mainly by IT experts who are familiar with all relevant IT security and compliance regulations and have received extensive training. With the Secure Remote Service Box, the described problems could be solved. The concept described in this work allows the free choice of the remote desktop software as well as the free adaptation to different security policies for different application areas. At the same time, it offers a physical as well as the logical separation of the maintenance object from the surrounding network with low demands on the nature of the interfaces of the device to be maintained.

Future Work

In future work, besides the actual prototypical implementation of the Secure Remote Service Box, an evaluation could also be carried out on potential customers of this box.

Author Biography

Klaus Schwarz received his B. Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017. He is finishing his Master Thesis in 2020, and his research interests include IoT and Smart Home Security, Embedded Systems, Artificial Intelligence, and Cloud Security.

Franziska Schwarz received her B.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2019. Since 2019 she is working as a scientific assistant in Technische Hochschule Brandenburg. Her research work is focused on IoT and Smart Home Security.

Reiner Creutzburg is a retired professor for Applied Informatics at the Technische Hochschule Brandenburg in Brandenburg, Germany. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence, Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

References

[1] Holtbrügge, Dirk, Hartmut Holzmüller, and Florian von Wangenheim, eds. Remote services. Springer, 2007.

[2] Knafo, Jenny. - ”[UPDATED] 2019 Most Popular Free Remote Desktop Solutions”. The Devolutions Blog, 2019, `https://blog.devolutions.net/2019/01/updated-2019-most-popular-free-remote-desktop-solution`. Accessed Jan 2019.

[3] Biehl, Markus, Edmund Prater, and John R. McIntyre. ”Remote repair, diagnostics, and maintenance.” Communications of the ACM 47.11 (2004): 100-106.

[4] Mori, M., et al. ”Development of remote monitoring and maintenance system for machine tools.” CIRP annals 57.1 (2008): 433-436.

[5] Masoni, Riccardo, et al. ”Supporting remote maintenance in industry 4.0 through augmented reality.” Procedia manufacturing 11 (2017): 1296-1302.

[6] Herndon, J. N., et al. State-of-the-art model M-2 maintenance system. No. CONF-840413-6. Oak Ridge National Lab., TN (USA); Sargent Industries, Inc., Red Wing, MN (USA). Central Research Labs. Div., 1984.

[7] Neely, Andy, et al. ”Customer expectations of remote maintenance services in the medical equipment industry.” Journal of Service Management (2014).

[8] Draper, John V., et al. ”Remote Maintenance Design Guide for Compact Processing Units.” ORNL/TM-

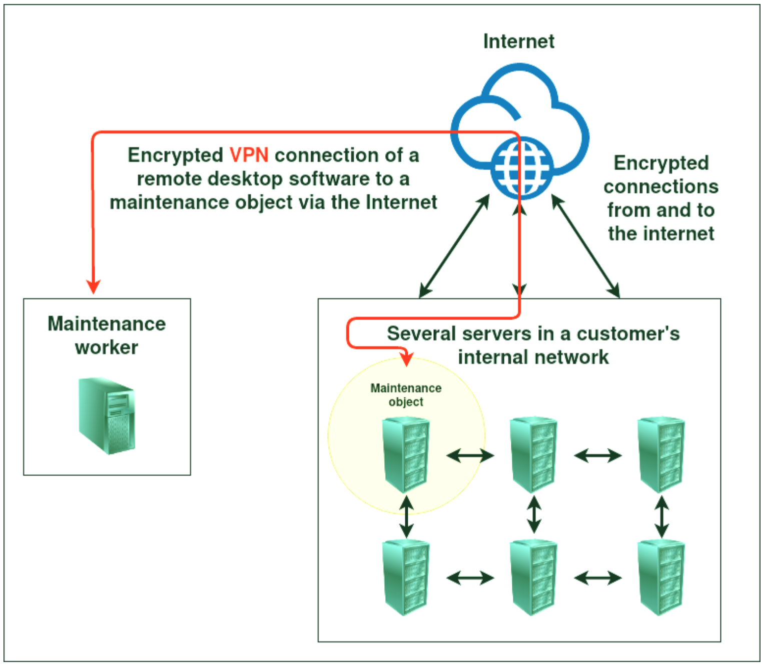

Internet
Encrypted VPN connection of a remote desktop software to a maintenance object via the Internet
Encrypted connections from and to the internet
Maintenance worker
Several servers in a customer's internal network
Maintenance object

Figure 4. *Encrypted, remote maintenance access, with still existing dangers*

2000/124 (2000).

[9] Muller, Alexandre, Adolfo Crespo Marquez, and Benoit Iung. ”On the concept of e-maintenance: Review and current research.” Reliability Engineering & System Safety 93.8 (2008): 1165-1187.

[10] Luo, R. C., et al. ”An intelligent remote maintenance and diagnostic system on mobile robot.” IEEE 2002 28th Annual Conference of the Industrial Electronics Society. IECON 02. Vol. 4. IEEE, 2002.

[11] GAO, Xiang, et al. ”A Digital Communication Network Based Remote Maintenance System for Intelligent Electronic Device of Substation [J].” Power System Technology 23 (2005).

[12] Hang, Jianjin, W. U. Xiangyang, and Chaoqun Zhang. ”Remote Maintenance and Its Application in Medical Equipment.” Chinese Medical Equipment Journal 10 (2003).

[13] LI, Jie, et al. ”Design of Medical Equipment Remote Repair System and Maintenance [J].” Chinese Medical Equipment Journal 10 (2008).

[14] Wikipedia - Comparison of remote desktop software. `https://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software`, Last Acces: February 25, 2020

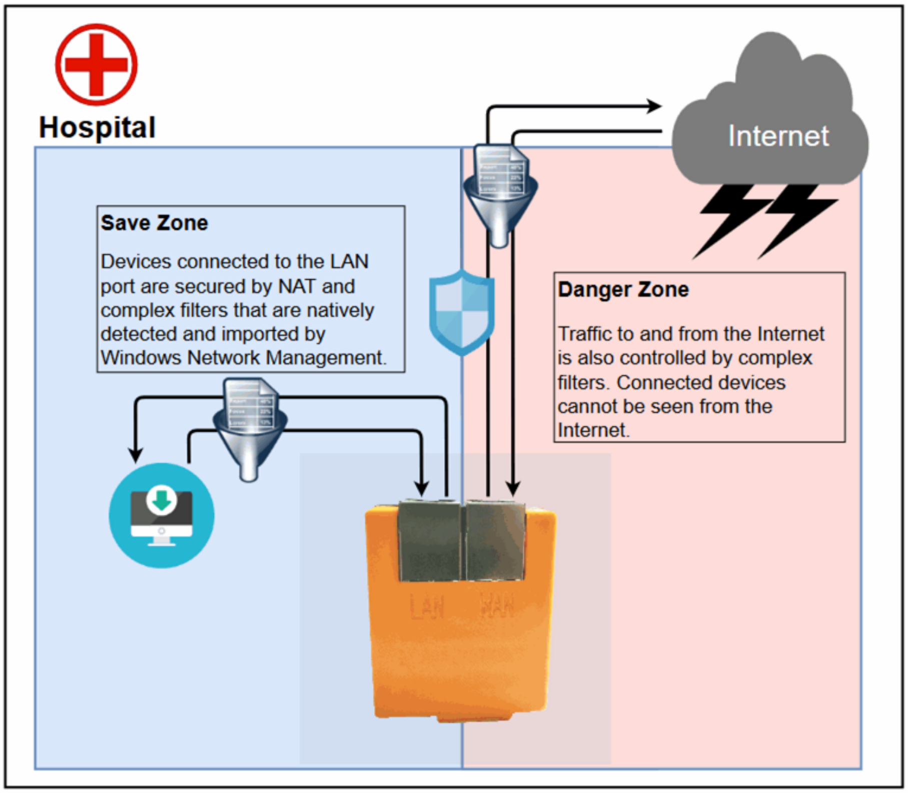
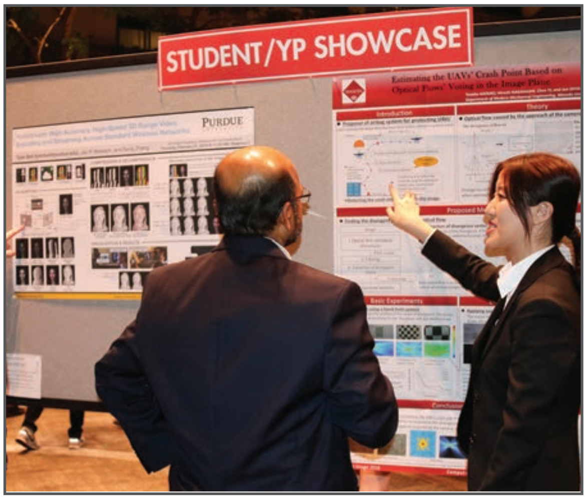
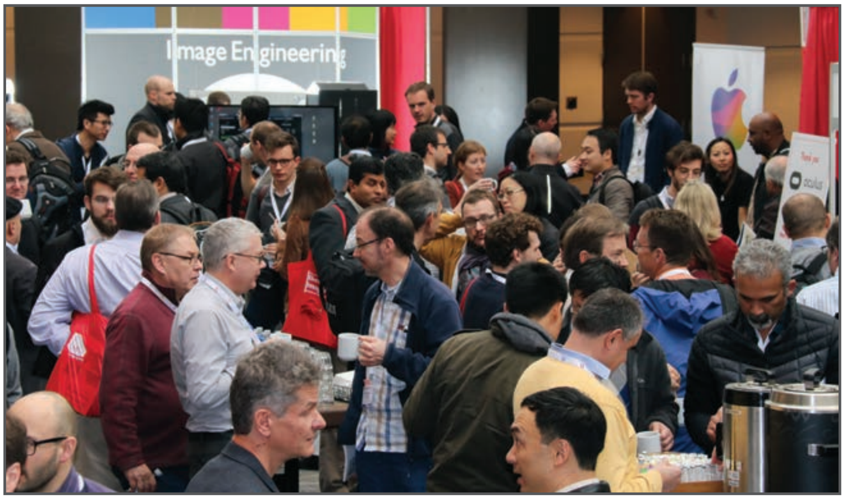

Hospital
Internet
Save Zone
Devices connected to the LAN port are secured by NAT and complex filters that are natively detected and imported by Windows Network Management.
Danger Zone
Traffic to and from the Internet is also controlled by complex filters. Connected devices cannot be seen from the Internet.
LAN
WAN

Figure 5. *Schematic representation of the Secure Remote Service Box in a hospital-like environment*





AR is a fundamental and transformative interface and platform.

20+ years from my initial working demo to today's AR displays

Optimistic that it won't take another 20 to reach ubiquitous consumer AR!