VOICE SECURITY ++

Executive Summary

Many systems claim to be secure, provide secure functionality, and may even be validated by an accredited security industry. However, what does it mean to be a good — or even usable — voice-based security system? What makes a secure voice platform exceptional?

In this paper, we present four characteristics that we believe are common among secure communication systems that surpass the competition: governance, resiliency, merger between UX and security, and interoperability.

Governance

If a company states that security is a primary tenant of its business model, then security must be embedded into the very fabric of the organization's operations. In some organizations, security is an afterthought. Engineers add the encryption library into their codebase, provide an overly simplistic configuration screen, and often ignore the end-user when it comes to workflows, configuration, or overall design. Where does this mentality start? It can generally be traced back to the leadership team, who rarely place much emphasis on security. Ideally, security should start at the C-Suite level.

There are two key issues regarding a company's board of directors and security: 1) boards often allocate very little time to discussing the topic of voice security and 2) few boards have directors with current technology or cybersecurity expertise, putting directors at a disadvantage when figuring if management is doing enough to address this area of significant risk.[6] Half of directors say their audit committee (which is typically overloaded) is responsible for cyber risk, and 16% give the responsibility to either a separate risk committee or a separate IT committee.[6]

Executive involvement sets the tone for cybersecurity in an organization. If the top executives are not involved directly, then the impression could be that cybersecurity is not the number one priority; employees can just add security measures tomorrow, or whenever they have time. When the board or CEO starts asking the management team about what measures the company has in place to avoid becoming a headline, then there is a much bigger chance of real change taking place.[3]

Resiliency

In 2017, Army Chief of Staff Gen. Mark Milley stated that the communications systems were "very, very fragile" and "probably vulnerable to sophisticated nation-state countermeasures" and that "the network we have today isn't the

network we need for that fight".[8] When the Army deployed its new communications systems in 2013, they proved that the system could push information around the way commanders envisioned, but that scenario was against an enemy with no ability to interfere with the operations. Now for any war in Europe, the Army is prioritizing speed and maneuverability, which would be hard to maintain with the current system.[8]

More recently, Lt. Gen. Bruce Crawford, the U.S. Army Chief Information Officer, stated in a December 12 C4ISRNET article, "My No. 1 concern when it comes to software optimization has to do with the resiliency of the applications developed by industry. A lot of the applications, they work great in the lab. But when you put them on a network, especially our tactical network, and then you must try and extend that to the disadvantaged user at the tip of the spear? A lot of the applications don't perform as well as they would in a sterile environment. Applications have got to be more resilient".[1]

Resiliency is an important topic today due to our dependence on cyber systems. **A corporation's — or even a nation's — critical infrastructures must be resilient against attackers to protect their citizens**.[7] Resiliency is defined as "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs".[7]

There are several key characteristics that make up a resilient system:

- **Attack Surface:** The attack surface of a software system is an indicator of the system's security in which the larger the attack surface, the more insecure the system. An attack surface represents the area from which adversaries can exploit or attack the system through the attack vectors.[7]

- **Integrity:** Integrity is defined as "the assurance of protection from unauthorized change".[7] An example of integrity is how well the code handles inputs, attempting to divide by zero or exceeding a limit of an array in memory.

- **Availability:** Availability is defined by NIST as "the timely and reliable access to and use of information" and resources by authorized entities. Availability may be expressed as the percentage of uptime over the total time of the system.[7]

- **Survivability:** Survivability is the ability of a system to continue to exist and operate at a level of acceptable performance in the face of attacks.[7]

- **Confidence:** Confidence is defined by NIST as "preserving authorized restrictions on information access and disclosure." There are several ways of protecting sensitive information from unauthorized entities, including the use of access control, passwords, and encryption.[7]

User experience

User experience (UX) is a person's perceptions and responses that result from the use and/or anticipated use of a product, system, or service.[10] This broad definition makes it difficult to exhaustively describe all facets of UX, but suffice it to say UX goes beyond good usability.[10] According to this definition of UX, attracting people to the topic of cybersecurity (before use) and motivating them to deal with it further (after use) is therefore a task of user experience design. We believe that the reluctance of users to be involved in security is mainly caused by the knowledge deficit of

nonexperts regarding cybersecurity systems. Moreover, a lack of motivation hinders people from looking critically at this vital topic. At the same time, human factors, including cyber interest and awareness, have been identified as the main element in cybersecurity to protect an organization from future cyber threats.[10]

It is assumed that computer security and computer usability are inversely proportional to each other. But with the advancement and contribution of UX in this area, this trend is starting to change. Usability affects security in systems that aspire to protect data confidentiality.[9] The security and usability are not fundamentally at odds with each other. A system which is more secure is more reliable, more controllable, and hence, more usable.[9] **Great UX reduces confusion regarding cybersecurity and is thus more likely to encourage a secure environment.** In the past, usability and security were treated as two different domains in computer systems because of their very different natures. Today, great UX and security work hand in hand in ensuring that the user can perform tasks that they want securely and efficiently.[9]

Defining the security strategies for software which is usable and strategies for a user interface design that is appropriate for that software is an indispensable concern. The design of usable, secure systems raises many considerable questions when it comes to properly balancing the properties of security and usability. Finding the right tradeoffs between these two quality attributes is not an easy task.[9] One method of accomplishing this balance is to incorporate security from early stages of software development by giving the high priority to security.[9] Working with customers is another method of accomplishing the merger between UX and security. Simply observing how customers use the software will provide the guidelines needed during the development process of the application.[9]

A well-designed security system provides several benefits that most system do not consider, such as reducing complexity and cognitive load on the user. Minimizing complexity helps the user avoid misconfigurations by proactively flagging inconsistencies, conflicts, and any potential blind spots.[4] A reduction in cognitive work load on the user allows for making quicker decisions, focusing on critical actions, and providing for quicker recommendations when a problem does occur.[4]

Interoperability

The best part of specifications is that everyone can interpret them differently, and not every company develops product that meets the same set of standards or requirements. **Ideally, companies that provide secure voice communication solutions should be validated against a common set of standards and against other validated solutions to guarantee a level of interoperability and security.**

One of the best interoperability and cybersecurity validations is DISA's Joint Interoperability Test Command, also known as JITC. Once products are approved, they appear on the DISA Approved Product List, known at APLITS.

Certification has two phases. In the first phase, cybersecurity testing validates that the system complies with the Security Technical Implementation Guides (STIGs), which contain guidance to "lock down" information systems/ software that might otherwise be vulnerable to a malicious computer attack.[12] In the second phase, interoperability testing ensures that the product meets the Unified Capabilities Requirements (UCR) and that the system can work with platforms from other vendors.

JITC supports the Warfighter in their efforts to manage information on and off the battlefield.[11] This support includes the following:

- Being an independent operational test and evaluation/assessor of DISA, and other DoD Command
- Providing Control, Communications, Computers, and Intelligence (C4I) acquisitions
- Identifying and solving C4I and Combat Support Systems interoperability deficiencies
- Providing C4I joint and combined interoperability testing, evaluation, and certification
- Bringing C4I interoperability support, operational field assessments, and technical assistance to the Combatant Commands, Services, and Agencies
- Providing training on C4I systems, as appropriate

In total, a product such as a VoIP call controller can expect to meet several thousand individual requirements for various parts of the solution.

REDCOM's Take

At REDCOM, the security of products is discussed at all levels of the company, from C-Suite to engineering. There is high priority on security coupled with an intuitive user experience which enables missions to be accomplished quickly and without error.

Since REDCOM is the call controller of choice for the tactical edge, resiliency and interoperability form the foundation our software platforms. The ability to be up and running within minutes, even after a power failure; the ability to work seamlessly with numerous other systems; and the ability to provide niche features that competitors do not is what keeps us at the forefront of the secure voice market.

Citations

[1] Gruss, Mike. "The Army's 'Triad of Opportunity'." C4ISRNET, C4ISRNET, 28 Dec. 2018, www.c4isrnet.com/it-networks/2018/12/28/the-armys-triad-of-opportunity/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB 12.31.18&utm_term=Editorial - Early Bird Brief.

[2] Pomerleau, Mark. "Here's Why the Army Needs Resilient Communications." C4ISRNET, C4ISRNET, 12 Nov. 2018, www.c4isrnet.com/c2-comms/2018/11/12/heres-why-the-army-needs-resilient-communications/.

[3] Review, CIO. "Why the C-Suite Must Embrace Cybersecurity." CIOReview, cybersecurity.cioreview.com/cxoinsight/why-the-csuite-must-embrace-cybersecurity-nid-24164-cid-145.html.

[4] Patwari, Rakesh. "4 Design Principles for Designing Enterprise Security Solutions." Medium.com, Medium, 12 Dec. 2017, medium.com/juniperux/designing-enterprise-security-product-experiences-4e4f833e3e51.

[5] "Security by Design: Embedding Privacy and Security Into the Enterprise Secure Architecture." NTT Security, 2017, https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_thought_leadership_esa_gdpr_uea_v1

[6] PWC, "How your board can be effective in overseeing cyber risk", 2018, pwc.com/us/governanceinsightscenter, https://www.pwc.dk/da/publikationer/2018/pwc-how-your-board-can-be-effective-in-overseeing-cyber-risk.pdf

[7] li, Danny Thebeau, et al. "Improving Cyber Resiliency of Cloud Application Services by Applying Software Behavior Encryption (SBE)." Procedia Computer Science, vol. 28, Mar. 2014, pp. 62–70., doi:10.1016/j.procs.2014.03.009.

[8] McLeary, Paul. "Army Looks To Replace $6 Billion Battlefield Network After Finding It Vulnerable." Foreign Policy, Foreign Policy, 21 Nov. 2017, foreignpolicy.com/2017/11/21/army-looks-to-replace-6-billion-battlefield-network-after-finding-it-vulnerable/.

[9] Sahar, F. "Tradeoffs between Usability and Security." International Journal of Engineering and Technology, Aug. 2013, pp. 434–437., doi:10.7763/ijet.2014.v5.591.

[10] Schufrin, Marija, et al. "Towards Bridging the Gap Between Visual Cybersecurity Analytics and Non-Experts by Means of User Experience Design." www.crisp-da.de/fileadmin/News___Veranstaltungen/PDF_fuer_news_events/Final_VizSec_Poster_Towards_Bridging_the_Gap_Between_Visual_Cybersecurit....pdf?_=1540985643.

[11] Federallabs. "DISA - Joint Interoperability Test Command (JITC)." Federal Labs, 9 Aug. 2017, www.federallabs.org/labs/disa-joint-interoperability-test-command-jitc.

[12] DoD Cloud Security Home, iase.disa.mil/stigs/Pages/index.aspx

©2019 REDCOM Laboratories, Inc. REDCOM and the REDCOM logo are registered trademarks of REDCOM Laboratories, Inc.
Subject to change without notice or obligation.

REDCOM®

www.redcom.com

20190314