Usable Survivability

Michael Atighetchi, Andrew Gronosky, Partha Pal, Joseph Loyall

Information and Knowledge Technologies, BBN Technologies, Cambridge, MA
matighet@bbn.com, agronosk@bbn.com, ppal@bbn.com, jloyall@bbn.com

Abstract: This position paper explores the interplay between usability and survivability. Survivability is the ability of a system to operate while under attack, while usability is a composite property indicating ease of use and user satisfaction. A survivable system necessarily incorporates multiple security mechanisms, and security and usability sometimes tend to be at odds with each other. The position of this paper is that usable survivability is fostered by a middleware-based integration of security mechanisms that a) hides the complexity of interoperating components and presents a simpler interface to the users and applications, and b) flexibly balances the security and usability requirements of various stakeholders.

1 Introduction

The evolution of cyber security research can be divided into three generations. The *first generation* focused on the prevention of intrusion through protection, e.g., via strong cryptographic algorithms, while the *second generation* aimed to detect intrusion that make it past prevention and contain their effects, e.g., through network intrusion detection systems and anti-virus tools. The current *third generation* of security research focuses on survivability, aiming to develop systems that can tolerate and recover from the impact of cyber attacks, regain lost capabilities, and improve defense over time.

Recent work in third generation security research has led to (1) survivability architectures that strategically combine redundancy, diversity, adaptive response, and containment [JC05], (2) byzantine fault tolerance techniques that degrade gracefully under attack and tolerate corrupted components [PP06], (3) automation of cyber defense reasoning and selection of defensive actions [PB08], and (4) service-oriented system design that tailors protection to specific operational needs and environmental constraints. Middleware, i.e., a specialized software layer, has played a critical role in each of these by providing integration glue that encapsulates the interaction and coordination complexities of multiple and diverse security mechanisms.

Usability has been studied extensively in the context of graphical user interface design and has focused on the elegance and clarity of the human-computer interface. Like security, usability is a non-functional property of a system that is important for the system's success and effectiveness, but is difficult to measure. Various definitions of usability exist, including work by Shneiderman, Nielson, and international standards [Is95].

This paper defines “usable survivability” based on the definition of “usable security” [St95]: Usable survivability is the ability of a system to continue to provide user satisfaction while at the same time tolerating and recovering from attacks. This definition encompasses both the quality of survivability mechanisms (how well attacks are tolerated) and the quality of the interactions between humans and the survivability mechanisms (how difficult it is for humans to maintain security).

It is generally observed that incorporation of stronger security mechanisms into a system negatively impacts the system's usability. For example, stronger passwords requiring a certain length, letter, digit and symbol combination, and avoidance of dictionary words make it harder for users to select passwords that can be easily remembered, affecting efficiency and memorability. Contrast that with an approach where a smart middleware layer derives the appropriate authentication token based on the user's identity. Similarly, ill-specified software or system configuration has often been argued to be the root cause of exploitable vulnerabilities. Recent approaches, such as the OASIS standards for Web Service Security (WSS), deliberately define multiple, overlapping standards attempting to provide a comprehensive specification with a lot of flexibility. But the proliferation of standards incurs usability costs for developers and administrators. Reconciliation of usability with security is a tradeoff that must be tailored to different stakeholders. Once again, the middleware layer provides an appropriate context for such customization.

2 Usability Issues in Survivability Research

This section describes five common challenges, together with candidate solutions, in designing systems that are survivable and usable at the same time.

Challenge 1: Supporting different stakeholder requirements. Security and usability only make sense if tied to stakeholder requirements in a specific context. This paper considers the following stakeholders:

- End users that participate in ongoing missions
- System/mission owners who have the overall responsibility of mission success
- System administrators who monitor and maintain IT infrastructure components

Each of these stakeholders has different requirements for usable survivability. End users require *transparent* security mechanisms with *minimal impact* on their behavior. Mission owners require a *clear operational picture* that captures information about key events and how these impact their ongoing missions. System administrators are often inundated by an enormous amount of low-level security alerts and struggle to separate important events from noise. They require *meaningful aggregation* with *drill down* functionality and tools to ensure that consistent security policies are enforced across multiple systems components and ISO layers.

Candidate Solutions: Analogous to frameworks available to create graphical user interfaces in the usability domain, an information assurance toolkit is needed that enables security engineers to select the right security mechanisms and cyber assurance functionality given a set of stakeholders and environmental conditions. The following

challenges call out individual stakeholder specific challenges and describe how embedding run-time decision logic in middleware helps increase both survivability and usability.

Challenge 2: Minimizing end user credential complexity. For end users, password-based authentication is the canonical example for showing an inverse relationship between usability and security for end users. Long and random passwords lead to good security, but poor usability since they are hard to remember. This often causes users to write down their passwords. In addition, availability is negatively impacted if users forget their passwords. To the same point, multi-factor authentication that requires physical possession of an authentication method, such as an ID card, and a secret, such as a password or PIN number, increases security over simple use of passwords, but requires "something you have" plus "something you know" – even more possibilities to lose one thing or forget the other.

Candidate Solutions: A potential solution to the password problem is autonomic identification of human subjects from observables. This includes identity management services that use commonly available video cameras to extract face features, microphones to establish voice profiles, and patterns generated by mouse/keyboard interactions to identity humans to move away from the proliferation of passwords found in today's world. Usability would increase by the nature of the simple non-intrusive interface and security could be maintained through multi-factor combination of different patterns (voice, face, etc). As the number of possible authentication factors increases, authentication protocols can be implemented in middleware to give developers the flexibility to combine factors in different ways for different contexts.

Challenge 3: Maintaining performance and availability. System administrators tend to be quite concerned with the impact of new security technologies on host and network resources. Although it is generally accepted that one has to pay a price for getting strong assurance guarantees, the overhead that security introduces needs to be carefully balanced with the timeliness requirements of applications, especially if security is added on to existing systems as an afterthought. For example, it is important to ensure the overhead introduced due to added security mechanisms protecting web traffic keeps the system's responsiveness within the normal variance, and certainly below pre-established critical response thresholds (e.g., ~1 s).

Candidate Solutions: For design time provisioning, composition techniques that bind the amount and type of security mechanisms to specific profiles, such as enterprise systems or mobile devices, can help ensure that appropriate security controls get deployed. For run-time management, emerging adaptive Quality of Service middleware technologies [LS09] can ensure gracefully degraded operation in cases of overloaded shared resources. Adaptations include automatic selection between different crypto protocols, key sizes, and layering depth in defense in depth architectures.

Challenge 4: Minimizing false positives. Another point affecting usable survivability is that false positives are worse than false negatives from a usability standpoint. Users are likely to simply overwrite or disable security controls altogether if normal interactions

are flagged as insecure (false positives), while the failure to detect attacks (false negatives) is often difficult to assess and therefore doesn't directly impact user experience.

Candidate Solutions: One common way for increasing detection accuracy and precision is to deploy a set of redundant and diverse sensors for monitoring the same attack. Middleware can coordinate and correlate output from those sensors and make the monitoring functionality available to a broader set of applications, increasing both security and usability. The redundancy must not introduce undue additional latency, or the solution risks simply trading one negative usability impact for another.

Challenge 5: Measurement and situational awareness. Measurement of security and survivability by itself is a difficult problem. A shortage of non-binary metrics makes it difficult to describe what is needed to adequately protect a system, let alone perform runtime assessments on whether the system is secure. Measurement of usability suffers similar difficulties due to the subjective nature of metrics. This primarily impacts usability for *system/mission owners* who need to make decisions based on the security of the overall system and who lack a direct way to link security events to mission requirements.

Candidate Solutions: Security assessments need to take input from various stakeholders and relate system events to predefined models of missions. A number of middleware research efforts are underway to enable integrated information assurance assessments involving different stakeholders [PH10]. Usability is a main driver in these efforts.

Managing the interplay between usability and survivability will be a key driver for the success of future distributed systems. Survivability architectures need to take human capabilities into account and lead to systems that are easy to use. Middleware-based approaches provide an elegant way to manage the complexity of integrating multiple security components and human interfaces to create systems that are both usable and survivable.

Bibliography

[Be08] Benjamin, P.: Using A Cognitive Architecture to Automate Cyberdefense Reasoning. BLISS 2008

[Ch05] Chong, J.: Survivability Architecture of a Mission Critical System: The DPASA Example. ACSAC, Tucson, Arizona, December 5−9, 2005, pp.495−504

[IS98] ISO 9241−11: Guidance on Usability (1998)

[Lo09] Loyall, J.: Quality of Service in US Air Force Information Management Systems. MILCOM, Boston, MA, October 18−21, 2009.

[Pa06] Pal, P.: An architecture for adaptive intrusion-tolerant applications. Software: Practice and Experience, Volume 36, Issue 11−12 (September – October 2006)

[PH10] Pal, P.; Hurley, P.: Managing Quality of Information Assurance. NATO IST Symposium on Cyber Defense and Information Assurance, 2010

[St95] Straub, T.: Usability Challenges of PKI, Dissertation Universität Darmstadt