Non-Boolean Authentication

Alec Yasinsac

Florida State University, Computer Science Department
Tallahassee, Florida 32306-4530 USA

Abstract. Traditional authentication is two valued. Unfortunately, authentication mechanisms cannot perfectly establish electronic participant's identity. Despite years of research and its manifestations such as digital signatures, zero knowledge proofs, public key infrastructures, certificates, biometric tools, etc. the best authentication evidence is a combination of multiple factors. All authentication systems are imprecise, but there are no existing systems that capture or that facilitate reasoning about this property. This paper introduces many fundamental issues in multi-tiered authentication systems.

1 Introduction and Motivation

In theory, authentication is Boolean; either someone is who they say they are, or they are not. Unfortunately, as any good practioner will tell you: "In theory, theory and practice are the same, but in practice, they are not". Unfortunately for information security, this "practicality axiom" holds true with authentication; that is, in general it is practically impossible to establish absolute authentication. Sophisticated intruders can guess, mine, or acquire passwords through social engineering. Private keys can be stolen or (more likely) mishandled. Adversaries can electronically capture biometric information or compromise underlying biometric security protocols.

Still, most trust systems treat authentication as though it were Boolean. Even in systems that partition trust into levels [1] there are few approaches (if any) that can cope with varying *authentication confidence* levels.

We introduce a model, architecture, and mechanisms that accommodate the reality that authentication is rarely Boolean. We rely on abstract notions of limited transitive trust with time-sensitive, information maturity and growth in a multi-level authentication model. Our architecture is a two-tiered structure that allows action categories that active responses offset as additional authentication information emerges. Our mechanisms focus on independent, cooperating identity sensors and state reversion.

1.1 Multi-State Authentication

Security systems canonically have two authentication states, roughly corresponding to (1) Identity Authenticated and (2) Identity Not Authenticated. Until we properly enter our account identifier and password, we are "not authenticated", so we receive no access privileges. We are so accustomed to this paradigm that it may be hard to imagine how an n-tiered authentication confidence scheme may work. Let us illustrate.

Most of us have experienced account suspense as a result of failing to correctly enter our password in three attempts. Account suspense after three failed authentication tries is one common practice that recognizes a third authentication class, call it *Identity Claim Disproven* (ICD). Essentially, the ICD authentication category reflects a negated identity claim or that a mechanism verified that a false identity claim occurred. Thus, we identify the following authentication classes within this *three state paradigm*: (1) Identity Unknown, (2) Identity Authenticated, and (3) Identity Claim Disproven.

The three state authentication paradigm leads to numerous research questions, e.g.:

1. Can we systematically categorize authentication confidence states?
2. What are legitimate actions/responses for a given n-state authentication system and how can this state/action relationship be best represented?
3. Can we characterize the optimum, minimum, and maximum number of authentication states for a given protection system?
4. Can we capture the essential authentication properties to allow continuous, incremental re-authentication?

Earlier work [2] investigates possible responses to incomplete authentication based on *vanilla* services. This notion leverages traditional access control and information flow models [3, 4], particularly that different objects have different protection requirements. Intuitively, objects with minimal sensitivity need the minimum or vanilla protection.

A complementary issue relates to proactive responses to incremental authentication and re-authentication. For example, we consider whether or not it is reasonable to reverse actions taken by a partially authenticated party if their identity claim is later refuted or its confidence level downgraded. We offer a general approach that we call *Rollback*.

A fundamental component of this research is to determine if rollback is essential for incremental authentication confidence systems. This idea appears intuitive, i.e. an act made while masquerading should be reversed when the masquerade is discovered. There is little in the literature on systematic approaches to backing-out to a previous secure state, though there is related work concerning disaster recovery that we address in the next section.

1.2 Theoretic Foundations

In their seminal paper, Harrison, Ruzzo, and Ullman introduce mathematical security models for managing computer access control [4]. There are many similar models [1], evaluations [5], and refinements [3] in the literature and research continues [6, 2] with significant interest in access control models for ubiquitous computing [7, 8]. Different environments demand different security models, and computing continues to change at breakneck pace. Access control models are not keeping pace with this change.

The literature is also rich with works targeting authentication definition [9,10] and properties [11] with an early, extended bibliography in [12]. Most recent work focuses on cryptographic authentication techniques triggered by [13], with seminal works by Burrows, et al.[14], Lampson et al. [15], Diffie, et al. [16], and Bird et al. [17] with a litany of variations [18, 19, and many others].

A common thread of this work is that it distinguishes only two authentication states. Work in threshold cryptography [20] offers an environment that has inherent opportunity for multi-state authentication and response, but we have seen no such work in the literature. We examine the opportunity in this area in this paper.

2 Multi-tiered Authentication Confidence States

2.1 Foundations in the Three State Model

We begin this description by adopting the three-tiered *three state model*, as described earlier, as our foundation. We fix the endpoints at "perfect confidence" with the

Identity Authenticated state on one flank and *Identity Claim Disproven* (ICD) on the other. ICD users are denied all access while access for fully identity authenticated users are controlled by the normal access control system. Our primary interest lies in the middle state: *Identity Unknown*.

We consider the three level model foundational because here we prove and exercise the concept of vanilla access that is granted to *Identity Unknown* subjects. The term "vanilla" seems particularly applicable as an intentional double-entendre. First, it reflects a plainness that characterizes the least protection afforded objects in a protection system. Vanilla objects require no special access control because they are not sensitive, either for confidentiality, integrity, or availability. Since they require [essentially] no protection, unknown subjects may access them. Depending on the environment, there may be a rich set of vanilla services, or there may not be any.

2.2 Vanilla Users

The vanilla user notion is evident in a variety of open laboratory environments. For example, many university libraries do not require user authentication on library computers. In some cases, the only applications available on accessible terminals provide library search capabilities. In general, such library search applications are not sensitive; in fact library patrons are encouraged to utilize these systems to locate resources without engaging reference personnel. We might call this system, vanilla-only access or a single state model.

A mild adjustment to the library illustration of requiring authentication for system administrators using library computers reflects the earlier described two-state model. In this scenario, an authentication system partitions users into the *identity unknown* and *identity authenticated* classes. Once authenticated, administrators have special access privileges not available to vanilla (unknown) users. A central theme of our paper is that access states may be monotonic, e.g. administrators are inherently vanilla users and need not be authenticated to receive vanilla access.

To extend the library illustration to a three state model, we require weak authentication for all users. For example, the authentication may be so simple as swiping a student identification card or entering a library issued group key, reflecting the likely status of the user being a university student. The classes in the illustration are:

(1)	[Specific] Identity Unknown:	Vanilla university students
(2)	Identity Authenticated:	System administrators
(3)	Identity Claim Disproven:	Users failing student authentication

In this simple illustration, system responses for vanilla users seem reasonably clear. They may access any provided library applications as often as they like, for as long as they like. If the applications allow file writing, the user may write to the files through applications. Of course, some libraries may set more liberal or more restrictive access policies for vanilla users, but these seem to reflect vanilla access for this illustration.

The more interesting question relates to limitations on vanilla users. Clearly, they are not allowed to perform system administration functions, such as installing programs or editing existing program or system configuration. Possibly not so clear is whether other general, non-sensitive functions (such as web browsing, Internet chat, even simple file editing, say through Notepad) are available. In the three state model, the system owner must decide if any of these applications should be available on the library nodes, and if they should be available only to system administrators or to all vanilla users.

2.3 The N-State Model

The core of this paper is to partition the vanilla state to form an n-state model, where n is greater than three, e.g. Figure 1. We begin by describing a state split to form a four state model, and then give a theory regarding further partitioning and refinement. Central to this process is how we identify vanilla session classes that correspond to vanilla object classe, and reasonable respective responses.

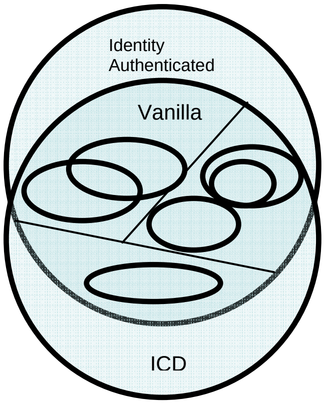

Figure 1

2.3.1 Incremental Session Re-authentication

Many security models (e.g. [1]) are founded on the notion of tranquility, that is, that subjects and objects' security posture does not change. Conversely, a foundation of this paradigm is that while objects are tranquil, the authentication posture of each subject in every session may continuously change. For most cases, we expect to gain authentication confidence with time, eventually reaching the *identity authenticated* state and remaining in that state with access controlled by the normal protection system.

Conversely, we contend that re-authentication should be continuous as, e.g.:

(1) An authentic user is unable to successfully complete the authentication process
(2) An intruder advances into a vanilla authentication state
(3) A session involving an authenticated, or partially authenticated, user is hijacked by an intruder

While these are three distinct situations, each can be resolved by invoking a continuous authentication process along with a dynamic access control mechanism. Many identity indicators support continuous inspection and incremental reevaluation.

1. Personal Entropy. Beyond biometric mechanisms that may comprise normal authentication systems, humans have characteristic, involuntary behavior that can uniquely identify them. Keystroke pattern (made famous during Carnivore [21] discussions) is one such behavior.

2. Functional behavior. Humans are creatures of habit, thus form behavior patterns that identify them as distinctly as physical and biological characteristics. Intrusion detection systems adopted behavioral profiling as early as 1986 [22].

3. Password hamming Distance. One of the most common authentication errors is the mis-typed password. Present password protection approaches are designed to prevent, rather than leverage, password similarity analysis. We examine mathematical metrics to password protection measure password accuracy.

4. Stored semi-private information. A common authentication approach is to store semi-private user information. Items such as birthday, mother's maiden name, etc. are public information, thus are not strong authentication. In combination with other mechanisms, they provide corroboration that is the essence of vanilla access control.

5. Peer confirmation. Though not fool-proof, personal identification is one of the most reliable authentication mechanisms.

6. Threshold schemes. Threshold schemes [20] partition a secret (e.g. that proves identity) and distribute the shares to several different share-holders. In this paper, we investigate threshold mechanisms that recognize the number of accumulated signatures.

Incremental identification allows vanilla user partitioning so that object access can receive appropriate protection in an unsure world. We make a simple extension, this time of the three state model, to generate a four state model. For example, we may categorize a session as *strong vanilla* if the user entered (1) A correct account identifier (2) An entry that differed from the correct password by a hamming distance of one, or (3) Both of these entries were accomplished on the first try.

The authentication classes in this *four state model* are:

(1) Vanilla	Access objects in the lowest protection level
(2) Strong Vanilla	Users surpassed some, but not all, authentication
(3) Identity Authenticated	Authentication process completed
(4) Identity Claim Disproven	Users whose identity claim is refuted

Classes (1), (3), and (4) are exclusive in the sense that they share no members. Class (2) is a subset of (1). We illustrate these relationships in Figure 2, part a. We then add a fifth class we call *pure vanilla*. We show this class as a subset of strong vanilla in Figure 2 b, but it need not be so. Multiple vanilla classes may form that are proper subsets (as shown in Figure 2), others that are exclusive to one another, and others that overlap, possibly combining all of these architectures within a single protection system.

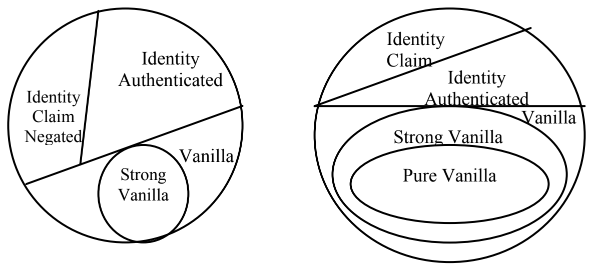

Figure 2. Vanilla Session Access Classes

2.3.2 Classifying Services for Multi-tiered Authentication

We consider how to answer the question of what objects are accessible for a subject-initiated vanilla session. In the three state model, sensitivity is the deciding factor (non-sensitive objects are available to vanilla users). In the four state model, there are two flavors of vanilla sessions, pure vanilla and strong vanilla. We may form corresponding object classes that we may call (1) vanilla and (2) [integrity] sensitive, but recoverable.

The intuition behind this partitioning is that all users whose identity is unsure may access all non-sensitive vanilla data, while users that achieve a threshold of identity confidence may be granted access to sensitive processes as along as the results of those processes are easily reversible (can be rolled back). For example, strong vanilla users may be allowed to add an entry onto the personal calendar associated with its account. These *vanilla* calendar entries are easily removed if the authentication is later refuted.

Notice, we intentionally did not suggest that existing calendar events be revealed to strong vanilla users. The difference is that once revealed information is difficult or impossible to rollback. This does not preclude protection systems from partitioning the vanilla states to allow sensitive information to be revealed to vanilla users, but it is likely that criteria other than rollback potential would guide that permission.

2.3.3 A Mild Formalization

In order to use incremental authentication, we need an implementation structure that supports its semantics. Notionally, we want to be able to add granularity to the access decision. While classification partitions access into sensitivities

Consider a mandatory access control security system consisting of subjects (S), objects (O), classification (C), privileges, and an identity confidence level (ICL), a variation of [1], where classification is a small, ordered, discrete set while the ICL is a continuous vector between zero and one. Subjects and objects are labeled with their classification, which is tranquil. Objects are also labeled with a set of pairs containing a privilege and an ICL, which are also tranquil. When a subject enters the system, they are associated with a dynamic ICL. The security system manages this attribute through mechanisms such as the ones we mention above.

An access request is a triple of the form: AR = {s, o, p}. The access algorithm contains two steps: (1) Decide if the subject and object classifications support granting the desired permission and (2) Ensure that the subject’s ICL is high enough to allow the requested action. The former generally follows the Bell-LaPadula structure. We give a simple algorithm for the later in Figure 3. The object icl is extracted from the [classically] static security system object identification file. The subject icl comes from a dynamic record that continuously monitors the subjects’ actions and adjusts the icl (again, based on the approaches we mentioned earlier). Security system policy dictates complete mediation, or requires re-authentication when an access durations surpasses some time or volume threshold, this algorithm fully supports the non-tranquility of continuous authentication.

2.3.4 Service Recoverability and Rollback

Previous results [2] identify two situations that allow access privileges to be granted to users that are not fully authenticated. The first is that the information sensitivity does not demand the strongest protection that the security mechanisms provide. The second is whether vanilla privileges actions are reversible, or as we term, can be rolled back.

```
boolean id_confident (s,o,p)
    icl := get_sub_icl(s);
    icl’ := get_obj_icl(o,p);
    if icl ≥ icl’ return true;
    else return false;
```

Figure 3. ICL Algorithm

The former is mostly a matter of information categorization, similar to that in a multi-level security model such as Bell and LaPadula [1]. An important distinction between Bell and LaPadula and our approach is rollback. Bell-LaPadula-based models assume tranquility because they cannot seamlessly handle down-graded [subject] clearances or upgraded [object] classification. Rollback is one vehicle to offset this dilemma.

Many computer systems and applications require Rollback-type capabilities. Consider file backup systems included in business continuity plans. When important files are lost, properly administered backup systems can return lost files in good working order. File backup issues include currency, immediacy, granularity, history, backup volume capability, and responsiveness, among others. Database recovery systems face similar, though more tightly granular, challenges.

Rollback for security faces many challenges. It is naturally difficult to identify rollback-capable transactions. Clearly, once information is divulged, "forced forgetfulness" is not an option. However, some data items can be easily changed if changed to respond to a dynamic security state. Others cannot be "retracted".

Similar to other multi-level security models, we must correlate vanilla session state and object vanilla access class. The starting point here is access control matrices and lattice structures, as we illustrate earlier. The novelty lies in the ability to handle dynamic authentication status. Rollback is an essential element. We can also partition confidentiality, integrity [23, 24], and conflict of interest [25] sensitivities where such partitioning facilitates vanilla access capabilities.

3 Conclusion

Authentication has a rich bibliography in theoretical and applied researchfrom some of the top information security researchers in the world. We recognize a reality that is not addressed in previous work, that authentication is not Boolean in practice and that Boolean mechanisms cannot properly characterize security properties in the dynamic Internet and mobile computing environments. This work is particularly relevant to wireless computing environments where peer-to-peer authentication has yet to overcome sophisticated attacks such as Sybil [26] and the invisible node attack [27].

Where absolute authentication is impossible, there must be mechanisms that deal with the uncertain identities. Non-Boolean Authentication enables such mechanisms and offers dynamic multi-level access control designed to leverage (where classical and present operational models prohibit) dynamic privilege assignment and privilege reassignment including classification upgrade and clearance downgrade.

We additionally offer a novel approach to security recovery based on Rollback. Again, we rely on existing work in business continuity planning and database recovery as the foundation for our work. We extend these notions to fit the security perspective and the dynamic authentication environment of worst case attack and Byzantine adversaries.

We base our work on advances that are well-documented in the literature. We leverage lessons learned in security models for confidentiality, integrity, conflict of interest, threshold cryptography, business continuity planning, and many other known technologies to form a comprehensive approach to handle dynamic [re] authentication, classification, and access control.

4 REFERENCES

[1] D. E. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model, M74-244, MITRE Corp. Bedford, MA, 1973

[2] Mike Burmester, Breno DeMederios, and Alec Yasinsac, "Community-centric vanilla-rollback access…", 13th International Workshop on Security Protocols, April 20-22, 2005

[3] D. Denning, "A Lattice Model of Secure Information Flow," *Communications of the ACM* 19 (5), pp. 236-243 (May 1976)

[4] M. A. Harrison, W. L. Ruzzo and J. D. Ullman. Protection in Operating Systems, *Communications of ACM*, Volume 19. No. 8. August 1976.

[5] Anita Jones, "Protection Mechanism Models: Their Usefulness", In *Foundations of Secure Computation*, 1978, pp. 237-252

[6] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank, "Role-Based Access Control Models", *IEEE Computer*, Volume 29, Number 2, February 1996, pp. 38-47

[7] *International Workshop on Ubiquitous Access Control*, July 17-21, 2006 - San Jose, California, USA, http://www.mobiquitous.org/

[8] The Second International Workshop on Security in Ubiquitous Computing Systems (SecUbiq-06), August 1-4, 2006, Seoul, Korea

[9] Dieter Gollman, "What do we mean by Entity Authentication?", In Proceedings of the *IEEE 1996 Symposium on Research in Security and Privacy*, pages 46--54. IEEE, 1996

[10] R. R. Jueneman, S. M. Matyas, and C.H. Meyer, "Message Authentication", *IEEE Communications Magazing*, Vol. 23, No. 9, September 1985

[11] Martin Abadi, Cedric Fournet, Georges Gonthier, "Authentication Primitives and their Compilation", *Proc. of the 27th ACM Symp. on Prin. of Prog. Lang.* (Jan. 2000), 302-315.

[12] Armin Liebl, "Authentication in Distributed Systems: A Bibliography", Operating Systems Review, 27(4):31--41, October 1993

[13] Roger M. Needham, Michael D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Comm. of the ACM, Dec, 1978, Vol. 21, N0. 12, pp. 993-999

[14] Burrows, M., Abadi, M., and Needham, R. M. "A Logic of Authentication", In *Proceedings of the Royal Society of London*, A 426:233-271, 1989

[15] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in Distributed Systems: Theory and Practice", ASM OS Review, Vol 25, No. 5, pp. 165-182

[16] W. Diffie, P. C. van Oorshot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges", *Designs, Codes and Cryptography*, 2(2):107-125, June 1992

[17] Ray Bird, Inder Gopal, et al. "Systematic Design of a Family of Attack Resistant Authentication Protocols", *IEEE Journal on Selected Areas in Comm.*, Vol. 11, No. 5, June 1993

[18] Wm. A. Wulf, Alec Yasinsac, Katie S. Oliver, and Ramesh Peri, "Remote Authentication Without Prior Shared Knowledge", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, February 2-4, 1994, San Diego, Ca., pp. 159-164

[19] Gavin Lowe, "Casper: A Compiler for the Analysis of Security Protocols", Journal of Computer Security, Volume 6, pp 53-84, 1998.

[20] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," In Crypto 89, Springer-Verlag Lecture Notes in Computer Science (Vol. 435), pp. 307-15, 1990

[21] Independent Review of the Carnivore System, Final Report, Contract No. 00-C-0328, IITRI CR-030-216, IIT Research Institute, 8 December, 2000

[22] Dorothy E. Denning, "An Intrusion-Detection Model," Proceedings of the 1986 *IEEE Symposium on Security and Privacy*, p. 118

[23] K. Biba, "Integrity Considerations for Secure Computer Systems," Technical Report MTR-3153, MITRE Corporation, Bedford, MA (Apr. 1977)

[24] D. Clark and D. Wilson, "A Comparison of Commercial and Military security Policies, "*Proceedings of the 1987 Symposium on Security and Privacy,* pp. 184-194, (Apr. 1987)

[25] D. Brewer and M. Nash, "The Chinese Wall Security Policy," *Proceedings of the 1989 Symposium on Security and Privacy,* pp. 206-214 (May 1989)

[26] J. Douceur. "The Sybil Attack," In *Proceedings of the 1stInternational Workshop on Peer-to-Peer Systems,* (IPTPS), 2002

[27] J. Marshall, V. Thakur, and A. Yasinsac, "Identifying Flaws in the Secure Routing Protocol", Proc. of 22nd Intl. Perf., Comp., and Comm. Conf., Apr. 9-11, 2003, pp. 167-174