Surety Bond PKI *

Internet Security Research Lab Technical Report 2006-3

Jason E. Holt
Internet Security Research Lab
Brigham Young University

March 2006

Abstract

We propose Surety Bond PKI, an alternative to high assurance certificates which increases cost disparity between fake and legitimate web sites.

1 Introduction

The core technique of our contribution allows certificate authorities (CAs) to offer certification contingent upon the recipient posting a surety bond. Taken alone, this technique is not particularly startling. However, we also discuss ways in which our technique can be built with a modest investment from parties who stand to benefit directly from its adoption. We show a plausible path from concept to widespread adoption requiring only modest, incremental investments along the way. This can help alleviate the bootstrapping problems that hinder adoption of PKI technologies.

2 Definitions

- **Surety bond:** A *surety bond* is a contract in which a *principal* promises to perform to a certain standard. If the principal does not perform its obligations to the *obligee*, the *surety* promises to compensate the *obligee* by paying a *penal sum*.
- Certificate Authority (CA): The entity that certifies attributes about a Service Provider for the benefit of Relying Parties
- Service Provider (SP): Also referred to as a Subscriber, this is the entity about which the CA makes assertions
- Relying Party (RP): The entity which relies on the information asserted by a CA about a service provider

3 Overview

Meet Bob, a service provider who runs an online store at bob.com. When Bob contacts a CA to obtain a TLS certificate for his store, the CA gives him the option of purchasing a surety bond certificate attesting that he will not knowingly use his website to distribute malware, and that if his site is compromised and used for fraudulent activity, he will remove any malicious content as soon as possible, but no later than 72 hours after being notified. In addition, he can optionally grant the CA permission to automatically revoke his certificate if they discover his site to be compromised; this potentially helps him regain credibility in the case of a compromise (since it potentially reduces the window for attackers to abuse his certificate), and also reduces the price the CA needs to charge for the bond since it reduces the chances the bond will be broken. Bob opts for a bond with a penal sum of $1000 that costs him $800 if he is willing to verify his mailing address. If his site remains complaint-free for 2 years, the CA promises to refund $600 of his investment.

When Alice, a relying party, visits https://bob.com, her TrustBar informs her that the site is backed by a $1000 bond. (Initially, the bond terms will be uniform for all sites in order to minimize confusion for relying parties, but eventually

*This research was supported by funding from the National Science Foundation under grant no. CCR-0325951 and prime cooperative agreement no. IIS-0331707, and The Regents of the University of California.

Alice might need to click on an icon to see what the bond guarantees). Alice knows exactly how much incentive exists for Bob's site to remain secure, and exactly how "secure" is defined in this context.

Our story would not be complete without Mallory, a malicious phisher. Mallory usually uses machines from his botnet to execute phishing attacks, but when he wants extra credibility, he sometimes buys a TLS certificate for a domain before executing his attack [1]. Mallory could also buy a bond, but without address verification, the bond would cost the full sticker price of $1000. Since Mallory has no intention of leaving the site up long-term, rebates over time are also out of the question.

Mallory can target a site with an existing bonded certificate, but knows that site owners have a significant incentive to respond quickly as soon as his activities discovered. Since the CA also has a stake in the bond (having offered it to the site owner at less than face value, banking on its projections of the number of bonds that it will eventually have to pay out), they too have an incentive to help reduce fraud. Consequently, they have a reporting facility which allows users to report compromised sites, in addition to watching existing aggregators for incidents involving its bonded customers. If the CA notices an obvious compromise, they contact the certificate owner and immediately revoke the compromised certificate.

As this story illustrates, the parties able to prevent and repair compromise have a clearly defined incentive to do, and the relying parties know exactly what those parties have committed to.

4 Why Surety Bonds?

Perhaps the greatest benefit to RPs of Surety Bond PKI is that it makes very explicit guarantees and describes exactly how much money backs those guarantees.

It also has the potential to incur significantly greater costs for wrongdoers than for legitimate players. Our implementation is targeted at fraudulent SPs, and requires that SPs guarantee that they are who they claim to be and will make reasonable efforts to prevent malicious use of their sites. This presents virtually no risk for, say, IBM registering their ibm.com domain, even if they enter into a highly valued bond, since there is very little question as to who ibm.com represents, and due diligence ensures that their bond will remain secure even if a compromise happens, as long as they take the measures they committed to. Phishers trying to impersonate IBM on a separate site, on the other hand, must either incur the penal sum as soon as anyone reports their site, go without certification from a Surety Bond CA, or attempt to compromise another site with a Surety Bond certificate and exploit it before the site owner and CA can respond. Of course, phishers have been slow to adopt PKI in general, since one of its goals is to prevent fraud. However, lately phishers have found that proving ownership of a domain to a CA does not preclude them from executing a phishing attack. Even though CAs sometimes offer large sums of money as assurances that their certificates are secure, these assurances typically only apply to the security of the underlying cryptography. That makes the assurances irrelevant to a phisher who wants a perfectly valid certificate for his site; although he may be planning to impersonate paypal.com, he knows that many RPs will not be worried if his Paypal-esque site shows up with his site at, say, example.com, especially if the RP's browser displays a lock icon.

5 Surety Bond PKI

To establish a Surety Bond PKI, a CA performs these steps, described in the following subsections:

1. **Legal foundation:** The CA establishes a uniform surety bond contract to be the basis for the assertions it will make about certificate holders.
2. **Certification methodology:** The CA publishes the means by which it will assert the authenticity of service providers and by which RPs will be able to retrieve these assertions.
3. **Procedures for Default:** The CA publishes the means by which a surety bond's obligee may claim the penal sum incurred when a SP defaults on its obligations under the surety bond.
4. **Revocation methodology:** The CA publishes the means by which RPs can determine that assertions once made by a CA are no longer valid.
5. **Certification:** The CA begins certifying Service Providers.

5.1 Legal Foundation

When proposing the creation of potentially millions of surety bonds, CAs must obviously ensure that they do so on only the firmest legal footing.

Well-funded, well-established legitimate sites can easily present highly valued bonds, and since bond values can be made available to RPs as a metric for trustworthiness, a highly valued bond inspires trust in RPs (not to mention causing them to associate the SP with large amounts of money). Up-and-coming legitimate websites may have more difficulty finding a surety for a large bond, but have a higher incentive to gain the legitimacy it offers.

[1] http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html

One of the challenges in establishing a Surety Bond PKI is deciding who will be the obligee. RPs for any given SP may number in the millions, and each may have a vested interest in the validity of the assertions made by the CA. Most motivating to the RP would be a surety bond which paid damages to every RP affected by a default on the bond, but in many cases this makes the penal sum impractically large. However, even if RPs do not directly benefit from a broken bond, they can have confidence proportional to the penal sum that some party has an incentive to ensure that the CA's assertions about an SP are accurate. We propose two possible alternatives to the problem of designating an obligee:

- **Reporter obligee:** In this configuration, the first person to file a valid claim indicating that an SP has defaulted receives the penal sum. This has the advantage that it creates a potentially very large incentive for RPs to monitor and report compliance, but the high value of such a transaction could also lead to abuses and the potential for criminal activities such as money laundering.
- **Charitable obligee:** Rather than dealing with the risks and complexity involved with using reporter obligees, CAs may instead decide to designate charitable organizations as the obligees for its surety bonds. This eliminates potential controversy over who should be awarded penal fees, and even creates a "silver lining" for SPs who default, offsetting the negative aspects of a defaulting on a bond with the laudable act of donating to charity. CAs also benefit from this "good karma", and could advertise the (potentially extremely large) total amount of charitable donations that would occur if all bonds were to be broken. Such a value could easily reach many times the net worth of even a well funded CA, since surety bonds are typically issued under the assumption that they will never be paid out. CAs can allow RPs or SPs to vote or choose which charities should be named as obligees. Under certain circumstances, penal sums paid to charitable organizations could even be tax deductible.

In contrast to the vague correlation between website X.509 certificates and the businesses which hold them, and the varied implicit assertions made by the CA due to their differing approaches to validating ownership of a domain, Surety Bond PKI offers RPs both a precise legal definition of what the CA asserts, and a specific monetary guarantee that the assertion is correct.

The CA must ensure that the surety bond used for services offered to the general public (such as internet banking and e-commerce sites) embodies a narrow, specific guarantee easily understood by the RPs who are faced with the decision of whether a service is legitimate.

Our implementation aims primarily to combat phishing attacks. Consequently, our surety bonds simply guarantee that the SP will not knowingly use their site for fraudulent activities, and will respond quickly to reports of compromise. More demanding bonds could also be created; for example, SPs could guarantee that they will not store personal data about their customers, that they will keep payment data safe from attackers, or even that they will ship ordered products within a certain interval.

CAs will probably want to partner with agencies which already offer traditional surety bonds, such as insurance companies, in order to offer "one-stop shopping" for small SPs who may be deterred by the inconvenience of obtaining a surety bond separately. Such agencies have well established methods for assessing risk, and the financial resources to guarantee the large total of penal sums incurred by widespread adoption of a Surety Bond PKI. CAs will want to involve these agencies when establishing the terms of the bond, in order to negotiate a mutually acceptible agreement. Large, established SPs may instead prefer to bring their own surety bonds to the table, particularly for high-value bonds. CAs must establish clear requirements to ensure that any externally established bonds will be enforceable, so that RPs will be willing to trust any surety bond certificate issued by the CA.

5.2 Certification Methodology

Ideally, Surety Bond Certificates would be issued just as any other certificate, with extensions indicating the type and value of the associated surety bond. CAs must ensure that RPs can readily access and understand the details of a particular surety bond in order to evaluate the assurances the CA is making.

Since the industry is slow to adopt new techniques, in section 6 we propose a method which allows immediate benefit for RPs, SPs and CAs, without waiting for the trilateral buy-in required for the commercial success of Surety Bond PKI using traditional methods.

5.3 Procedures for Default

Both the CA and SPs have an incentive to avoid defaulting on surety bonds. In the case of well-run SPs, avoiding default is a natural byproduct of following best business and security practices. CAs may wish to establish additional safeguards by which to safeguard the penal sums they guarantee in partnership with external funding sources. As section 3 suggests, CAs may wish to monitor SP sites and establish a reporting mechanism whereby RPs can report SP compromises. If the CA defines surety bonds with a grace period for addressing such compromises, the CA can ensure that bonds will not be broken by responding to reports itself within the grace period.

On the other hand, CAs must resist the temptation to leave loopholes in the surety bonds in order to avoid *ever* paying out a penal sum. A fraudulent website only has to be active for a few hours to execute a successful phishing attack, so CAs and SPs must be sure to keep grace periods as small as possible without incurring excessive losses when the inevitable compromises occur.

5.4 Revocation Methodology

Since Surety Bond PKI attempts to increase the utility of certificates by advertising significant guaranteed assurances, CAs have an increased (and indeed, explicitly calculatable) incentive to ensure that certificates are quickly revoked when those assurances can no longer be made. The proposal for an on-line service listed in section 6 has good characteristics in this respect, since RPs can query the service before each transaction, meaning that any transaction which takes place after the CA updates its revocation database will correctly show that the SP is no longer protected under the terms of the surety bond.

CAs must clearly establish what happens to a certificate's surety bond when a certificate is revoked. Using the example from 3, what happens if Bob's site is compromised the week after he purchases his certificate? If the CA revokes his certificate quickly and thus avoids breaking the terms of the surety bond, what happens to the $800 Bob paid for it? Perhaps the CA will have established terms under which Bob can obtain a new certificate and have his old bond automatically applied (but perhaps might stipulate that Bob won't get a full refund of the $600 he could have had if his site had remained secure). Such decisions are obviously important, and we leave specific recommendations based on good business and marketing practice for future work.

5.5 Certification

Once procedures for handling all aspects of the Surety Bond PKI have been established, the CA may begin issuing Surety Bond Certificates. As section 3 suggests, this process need not be significantly more costly or complicated than existing certificate issuing processes [2]. Section 6 describes how CAs can establish a user base of SPs and RPs for a reasonable investment, giving other SPs an incentive to register.

6 Gradual Buildup of Support

Issuing new certificates in the usual way requires cooperation between CA, SP and RP. The CA must be willing to issue the cert, the SP must be willing to pay for it and use it in its service, and the RP must run software which reports the implications of the certificate.

Until such a scenario becomes desirable for all parties, we propose leveraging the existing user base of the TrustBar plugin for the Firefox web browser. RPs already use TrustBar to help identify fraudulent sites, and it was relatively easy to augment TrustBar to identify and display data relating to Surety Bond Certificates from an on-line system instituted by a CA. Or, to address the privacy risks of signalling an external service every time an RP contacts an SP, the service could operate as an off-line service, distributing its database of certified and revoked SPs at regular intervals (noting the importance of revocation described in section 5.4). While neither of these solutions scales well, remember that they are designed to help bootstrap the system into widespread acceptance, at which point SPs could be expected to present signed Surety Bond Certificates directly to SPs in the usual way.

This helps lower the barriers to adoption for RPs, leaving CAs to try to sell Surety Bond Certificates to SPs already faced with a multitude of CAs to choose from as well as upsells such as high assurance certificates. To create a user base for Surety Bond Certificates and establish itself as the clear leader in the market, CAs could offer free certificates to well established sites which already have large incentives and clear track records in keeping their sites secure. But since even this sort of promotion can be difficult to implement, given the multitude of security solutions targeted at SPs, CAs may have difficulty convincing SPs to install even a free certificate. Consequently, we propose that a CA create an on-line service which the TrustBar can contact to retrieve information on the surety bond status of a given site.

So, given only cooperation between TrustBar authors and a single CA, Surety Bond Certificate support could be added to an application used by thousands of RPs on the open Internet. Then, the CA can invest in establishing a database of popular sites with sufficiently low risk of compromise to justify the CA's risk in creating its own surety bond without their input. At that point, the CA can offer SPs certificates for sale based on a PKI used by thousands of RPs and certifying hundreds or thousands of SPs.

If the notion of a CA unilaterally certifying hundreds of SPs just to create a market for Surety Bond Certificates sounds unlikely, consider the economics of the situation. 100 surety bonds valued at $100 creates a maximum liability of only $10,000 even in the unlikely scenario in which it had to pay each and every penal sum. If we assume payouts on 10% of the surety bonds (still a much higher rate of default than we would expect from reasonable terms), the CA could certify 1,000 SPs at $100 each, or 100 SPs for $1,000. Breaking a surety bond is the exception rather than the rule, so for properly constructed bonds we would expect a CA to be fully capable of unilaterally establishing a base of certifications for popular SPs for a relatively modest sum.

7 Risks

In any PKI, RPs must ultimately make intelligent decisions based on the assurances made by a CA, and unfortunately, CAs may ultimately offer only vague, poorly-enforced assurances. In the case of Surety Bond PKI, this may take the form

[2] For example, Comodo.com offers high assurance certificates priced at about $150 for two years as of March 2006

of bond terms which make payment of the penal sum easy to avoid for CAs and SPs, even in clear cases of negligence or abuse. Surety bonds have the advantage of at least making the promises explicit and attaching a concrete monetary value to them, but ultimately RPs are left with the task of evaluating their implications.

The presige offered by a $1,000,000 bond may lend significant credibility to a SP, but this increased credibility is also valuable to attackers. Attackers may target sites with unusually highly valued bonds in order to add credibility to fraudulent activities. Or, they may seek to damage the credibility and financial interests of the bond parties by attempting to force a default on the bond. This creates a challenge when establishing surety bond terms, since RPs need to have confidence that the assurances are significant, while SPs need to know that they can maintain intact bonds with high probability.

Widespread adoption of Surety Bond PKI leads to a large total liability in the combined penal sums from the bonds. This liability is particularly dangerous in scenarios in which many bonds could default at once. A widespread vulnerability, or a major attack on the CA as well as a large number of SPs could force the bond sureties to pay large penal sums. As a protection against this scenario, bonds could be devised with clauses which set a maximum penal sum to be paid in such a scenario.

8 Conclusion

We presented economic and practical arguments for the establishment of Surety Bond PKI, a system which allows certificates to include explicit assurances guaranteed by an explicit financial sum. We described how to build such a system, and further described an arrangment in which interested parties can build up the system gradually, mitigating the high hurdles normally associated with development of new PKI implementations.

Future work may focus on the technical and legal details of establishing such a system, or may further consider the holistic challenges faced in making it work for real users and real businesses.