illusoryTLS

illusoryTLS - Alfonso De Gregorio, illusorytls.com.

- Published: date not stated
- Original: <http://www.illusorytls.com/>
- Preserved from: http://www.illusorytls.com/ (live) on 2026-08-09
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

illusoryTLS

illusoryTLS

illusoryTLS is an elliptic-curve asymmetric backdoor in RSA key-generation and exploiting the universal implicit cross-certification adopted in the current Web PKI to break all the HTTPS security guarantees. One rotten apple spoils the whole barrel.

Video

illusoryTLS: Nobody But Us. Impersonate,Tamper and Exploit from Deepsec Conference on Vimeo.

Cryptographic backdoors are a timely topic often debated as a government matter to legislate on. At the same time, they define a space that some entities might have practically explored for intelligence purposes, regardless of the policy framework.

The Web Public Key Infrastructure (PKI) we daily rely on provides an appealing target for attack. The entire X.509 PKI security architecture falls apart if a single CA certificate with a secretly embedded backdoor enters the certificate store of trusting parties. Do we have sufficient assurance that this has not happened already?

Alfonso De Gregorio presented at DeepSec 2015 his findings and introduced illusoryTLS. Aptly named illusoryTLS, the entry is an instance of the Young and Yung elliptic curve asymmetric backdoor in the RSA key generation. The backdoor targets a Certification Authority public-key certificate, imported in the certificate store of a pretty standard HTTPS client and TLS server. The security outcome is the worst possible outcome, because the backdoor completely perverts the security guarantees provided by the TLS protocol, allowing the attacker to impersonate the endpoints (i.e., authentication failure), tamper with their messages (i.e., integrity erosion), and actively eavesdrop on their communications (i.e., confidentiality loss).

Abstract

illusoryTLS: Nobody But Us Impersonate, Tamper, and Exploit

The entire X.509 PKI security architecture falls apart, if a single CA certificate with a secretly embedded backdoor enters the certificate store of relying parties. Have we sufficient assurance that this did not happen already? This talk explores this scenario from both an experimental and speculative point of view.

From the experimental standpoint, the talk reports on illusoryTLS, an entry to the first Underhanded Crypto Contest. illusoryTLS is an instance of the Young and Yung elliptic curve asymmetric backdoor in RSA key generation. It targets a Certification Authority public-key certificate imported in the certificate store of a pretty standard HTTPS client and TLS server. The security outcome is the worst possible outcome, because the backdoor completely perverts the security guarantees provided by the TLS protocol, allowing the attacker to impersonate the endpoints (i.e., authentication failure), tamper with their messages (i.e., integrity erosion), and actively eavesdrop their communications (i.e., confidentiality loss).

illusoryTLS has been shortlisted to the final rounds of the contest, which is still ongoing. Being the backdoored public-key indistinguishable (under the ECDDH assumption) to all probabilistic polynomial time algorithms from genuine public-keys, illusoryTLS is expected to withstand the review and scrutiny of contest judges.

In the Internet X.509 PKI the security impact of such backdoor would extend further; the presence of a single CA certificate with a secretly embedded backdoor in the certificate store renders the entire TLS security fictional. In fact, the current practice of universal implicit cross-certification makes the whole X.509 PKI as weak as its weakest link.

Therefore, when dealing with this class of attacks in the context of X.509 PKIs, it might be not sufficient to avoid outsourcing the key generation. It becomes essential also to have assurance about the security of each implementation of vulnerable key-generation algorithms employed by trusted credential issuers. Have we sufficient assurance about the tens or hundreds CA certificate we daily entrust our business upon?

Q&A

Why it is called illusoryTLS?

Because, due to the current practice of universal implicit cross-certification, if a single CA certificate with a secretly embedded backdoor enters the certificate store of relying parties, the entire X.509 PKI security architecture falls apart, rendering the TLS security fictional.

Am I affected by the vulnerability?

As long as you entrust your business to today's PKI, you are likely to be affected either directly or indirectly. If risk can be understood as the price of dependence, this vulnerability can be understood as the price of a misplaced trust relationship. Unfortunately, today we do not have sufficient assurance about the tens or hundreds CA certificates we daily entrust our business upon. Therefore it is hard to tell if any of them contains a secretly embedded backdoor that can be actively exploited.

Who can detect the presence of the backdoor?

Experts with access to the target RSA key-generation might notice that something is amiss. The susceptibility to detection depends on the implementation details.

Who cannot detect the presence of the backdoor?

Entities with black-box access to the key-generation cannot distinguish a backdoored public-key from a genuine public-key. That is to say that there is no way to tell backdoored certificates apart from non-backdoored credentials. The backdoored keys remain indistinguishable, as long as a computational hardness assumption called Elliptic-Curve Decisional Diffie-Hellman (ECDDH) holds.

Who can exploit the vulnerability?

The vulnerability can be exploited by the backdoor designer and by whoever gains access to the backdoor elliptic-curve private-key or to the associated key-recovery system.

Who cannot exploit the vulnerability?

The vulnerability cannot be exploited by those without access to the backdoor private-key or to the key-recovery system.

Why did you submit illusoryTLS to the first Underhanded Crypto Contest?

The common view is that backdoors are symmetric in nature and require the presence of malicious logic in the target system code base (i.e., everyone with knowledge about the internals of the backdoor can exploit it and code review can spot their presence). This work challenges this view. Backdoors can be asymmetric (i.e., the complete code for the backdoored system does not enable anyone except the entities with access to the key-recovery system to exploit the backdoor) and be planted in data. Or: to paraphrase a popular quote on homoiconicity of some programming languages, backdoor is data, data is backdoor.

The backdoored code is written in Haskell. Are non functional programming languages affected by the vulnerability?

Oh, sure, they are! The vulnerability put forward in illusoryTLS is ecumenical. And all programming languages are no more and less affected. The illusoryTLS backdoor is planted in cryptographic credentials that are indistinguishable from genuine ones to all probabilistic polynomial time algorithms. Therefore no computer programming technique will help here. That said, making invalid states unrepresentable, functional programming is helpful in improving software security and should see wider adoption. In order to emphasize the orthogonality of this backdoor to programming languages, illusoryTLS builds upon the the code included as part of network-simple-tls — an Haskell library for simple network sockets usage patterns using TLS security — and uses it as-is, without any modification.

Talk

- HITB SecConf 2015 Amsterdam
- DeepSEC 2015 Vienna
- ZeroNights 2015 Moscow

- HITB SecConf 2015 slide deck
- DeepSEC 2015 slide deck
- ZeroNights 2015 slide deck
- Speech at HITB SecConf 2015 Amsterdam
- Speech at Zeronights 2015 Moscow
- DeepSEC 2015 recordings

Documentation

Backdoor Design

Code

- illusoryTLS
- An elliptic-curve asymmetric backdoor in RSA key-generation based on Elligator

---