Inhaltsverzeichnis

Secure QR Code

Oder Fun mit QR Codes..

Es gibt eine Erweiterung im QR Code, der hinter dem `Terminator` noch weitere Daten integriert. Diese werden mit normalen QR Lesern normalerweise nicht ausgelesen. Darin können zusätzliche Informationen wie z.B. ein signierter Hash der Daten im QR Code eingebettet werden. So kann die Authentizität der Daten im QR Code überprüft werden.

QR Hack

Finde ich eine Coole Idee, nicht unbedingt für Stegano aber eben z.B. für eine Digitale Signatur oder ähnliches.

Der folgende Text habe ich direkt von der Homepage übersetzt und ist nur zur Info hier abgelegt. Die Bilder fehlen, aber ich finde den Artikel interessant und möchte später darauf zurückkommen.

https://fukuchi.org/works/qrhack/qrhack2.html

Übersetzung

Kurze Erläuterung der Methode der Universität Kobe Seit dem 25. Juni 2018 macht ein Nachrichtenartikel mit dem Titel „QR Code Vulnerability“ Schlagzeilen.

Untersuchungen einer Gruppe an der Universität Kobe haben ergeben, dass der QR-Code, der häufig für elektronische Zahlungen und Werbung verwendet wird, eine Sicherheitslücke aufweist, die das Einfügen gefälschter Informationen ermöglicht. Durch Ausnutzen dieser Schwachstelle ist es möglich, Benutzer auf einen bestimmten Prozentsatz nicht autorisierter Websites zu leiten, und die Gruppe sagt, es sei notwendig, die Sicherheitsmaßnahmen zu verstärken.

Sicherheitslücken im QR-Code Anleitung zu nicht autorisierten Websites [NHK NEWS WEB] Es gab einen Artikel, in dem der Gruppenleiter, Professor Morii von der Universität Kobe, dies erklärte.

Kurz gesagt, der exakt gleiche QR-Code springt manchmal auf URL A (Website) und manchmal auf URL B, sozusagen, wir haben einen "skurrilen QR-Code" entwickelt. .

Achtung! Schwachstelle im QR-Code? Seine Ernsthaftigkeit und Maßnahmen zur Vermeidung von Täuschung (Masakatsu Morii) – Einzelperson – Yahoo!-Nachrichten Diese Methode nutzt den Fehlerkorrekturmechanismus des QR-Codes. Nehmen wir als Beispiel den im Artikel gezeigten QR-Code. Ein QR-Code besteht aus weißen und schwarzen Punkten, aber wenn ein grauer Punkt, der die Zwischenfarbe darstellt, in den QR-Code gemischt wird, ist es dem QR-Code-Lesegerät nicht möglich, ihn als weiß oder schwarz zu interpretieren. , variiert abhängig von verschiedenen Bedingungen. Wenn es sich um einen nicht speziell erstellten QR-Code handelt, wird er unverändert durch Fehlerkorrektur korrigiert, unabhängig davon, wie er interpretiert wird, aber in dem von Professor

Morii auf der obigen Website gezeigten QR-Code sind bestimmte Punkte ausgegraut dabei wirkt die Korrektur unterschiedlich, je nachdem, ob sie als weiß oder schwarz interpretiert wird.

Lassen Sie mich ein wenig näher darauf eingehen. Die schwarzen und weißen Punkte im QR-Code haben je nach Standort unterschiedliche Rollen. In dem unten abgebildeten QR-Code werden die einzubettenden Daten in den violett eingefärbten Bereichen in binäre Daten umgewandelt. Zusätzlich sind in den gelb eingefärbten Bereich Informationen zur Fehlerkorrektur geschrieben. (Die roten Bereiche sind Formatinformationen, Positionsmarkierungen etc.)

In dem von Morii et al. gezeigten Beispiel ist die URL der bösartigen Website (http://srv.prof-morii.net/~lob) als Daten eingebettet (violetter Bereich). Andererseits sind die Fehlerkorrekturinformationen Korrekturinformationen, wenn die eingebetteten Daten die korrekte Site-URL (http://srv.prof-morii.net/~lab) (gelber Bereich) sind. Daher lesen diese Fehlerkorrekturinformationen gemäß dem normalen Verhalten eines QR-Code-Lesegeräts die korrekte Website-URL.

Hier geht es darum, dass in diesem Fehlerkorrektur-Informationsbereich graue Punkte gesetzt werden. Wenn die grauen Punkte als schwarz interpretiert werden, funktioniert die Fehlerkorrektur, aber wenn sie als weiß interpretiert werden, funktioniert sie nicht und die im violetten Bereich eingebettete URL der schädlichen Website wird unverändert ausgegeben. (Es sollte beachtet werden, dass es nicht nur darum geht, jeden Punkt der Fehlerkorrekturinformationen auszugrauen, es ist notwendig, den Punkt basierend auf dem Fehlerkorrekturmechanismus zu spezifizieren.) Übrigens, wenn Sie sich nur das im Artikel gezeigte Beispiel ansehen, denken Sie vielleicht, dass Sie erkennen können, ob ein Verdacht besteht, indem Sie sich das Vorhandensein grauer Punkte ansehen, aber wenn alle schwarzen Punkte dunkelgrau sind, scheint es menschlich zu sein möglich, es dem Auge schwer zu machen, zwischen ihnen zu unterscheiden. Es kann auch möglich sein, andere Bilder dünn über den QR-Code zu legen, um ihn zu verschleiern.

Darüber hinaus geht es darum, einen mehrdeutigen Punkt zu erzeugen, der als weiß oder schwarz beurteilt werden kann, sodass es möglich zu sein scheint, ihn geschickter zu verbergen. Zum Beispiel würde das Ändern der Form der Punkte statt ihrer Farbe, wie sie beispielsweise dreieckig zu machen, wahrscheinlich einen ähnlichen Effekt erzeugen. Außerdem kann es möglich sein, mehrdeutige Punkte zu erzeugen, indem man die Größe jedes Punkts unregelmäßig macht oder seine Positionen verschiebt. Es gibt sogar QR-Codes mit unauffälligen Punkten , sodass Sie sie so undurchsichtig gestalten können, wie Sie möchten. Es scheint möglich, an andere Methoden zu denken, wie z. B. Blinken oder das Ändern der Punktfarbe für einen sehr kurzen Zeitraum, damit die Menschen es nicht bemerken. Freuen wir uns auf weitere Berichte aus der Gruppe der Kobe University.

Zudem lässt sich das Verfahren von Morii et al. prinzipiell auch auf andere 2D-Barcodes anwenden. Obwohl dies nicht verifiziert wurde, sind ähnliche Angriffe wahrscheinlich gegen DataMatrix und Aztec Code wirksam. Ich würde auch gerne weitere Berichte zu diesem Bereich abwarten.

Wie man Sekundärinformationen einfach einbettet Die Methode der Kobe University ist eine ausgezeichnete Methode, die sehr schwer zu erkennen ist, da sie auf der Grundlage einer Analyse von QR-Code-Fehlerkorrekturmethoden präzise entwickelt wurde. Wenn es Ihnen andererseits nichts ausmacht, sofort erwischt zu werden, gibt es eine Möglichkeit, dies einfacher zu tun, also werde ich sie vorstellen.

Versuchen Sie, den folgenden QR-Code zu scannen.

Nach mehreren Versuchen sollten Sie in der Lage sein, die folgenden beiden URL-Typen zu lesen.

https://fukuchi.org/qrhack/qrhack2.html HTTPS://FUKUCHI.ORG/merry.html Wenn es nicht funktioniert, versuchen Sie es mit einem anderen QR-Code-Lesegerät oder ändern Sie den Winkel der Kamera.

Dieser Mechanismus ist so einfach, dass er nicht mit der Methode der Universität Kobe verglichen werden kann. Die folgende Abbildung macht dies deutlich.

Es ist nur ein kleiner QR-Code, der in einen großen QR-Code wie diesen eingebettet ist. Der große QR-Code hat die höchste Fehlerkorrekturfähigkeit, sodass selbst dann, wenn der untere rechte Bereich stark mit anderen QR-Codes bedeckt ist, die ursprünglichen Daten wiederhergestellt werden können.

Bei einer so einfachen Methode hat der QR-Code an den drei Ecken charakteristische Positionsmarkierungen. Wenn Sie es also wissen, können Sie es sofort sehen, aber wenn Sie es mit jemandem zu tun haben, der die Situation nicht kennt, denke ich, dass es so ist eine gute Chance, dass es missbraucht werden kann.

Beachten Sie, dass der Teil der Positionsmarkierung auch dann erkannt werden kann, wenn seine Form leicht verzerrt ist. Die folgende Abbildung ist ein Beispiel für eine leicht beschädigte Version. Mit etwas Mühe gelingt es Ihnen vielleicht, sich besser einzufügen.

Die Verwendung eines Mikro-QR-Codes für den eingebetteten QR-Code führt zu einer zusätzlichen Positionsmarkierung, was es noch verwirrender macht. Es gibt jedoch nicht viele Lesegeräte, die Mikro-QR-Codes unterstützen, sodass die Auswirkungen gering sein werden.

Wenn Sie einen Mikro-QR-Code verwenden, können Sie den gesamten Code verkleinern, aber wenn Sie ihn verkleinern, ist es einfacher, den gesamten einzubettenden QR-Code zu scannen, sodass es etwas schwierig ist, dem Lesen Priorität einzuräumen Mikro-QR-Code. Das wird schwierig.

Diskussion

Er erläuterte die Schwächen von QR-Codes, auf die Prof. Morii von der Universität Kobe und andere hingewiesen haben, und stellte eine Methode vor, die diese auf einfache Weise nachahmt.

Im Vergleich zu der zuvor vorgestellten Methode, versteckte Daten in den QR-Code einzubetten , ist diese Methode deutlich anfälliger für Missbrauch. Auf den ersten Blick kann ich mir keinen wirksamen Weg vorstellen, dies zu verhindern. Im obigen Artikel erwähnt Professor Morii die visuelle Bestätigung der gelesenen URL. Es ist nicht mehr möglich, die Manipulation visuell zu erkennen, wenn eine unordentliche und lange Zeichenkette wie das Ziel ist.

Andererseits ist es dem QR-Code-Leser möglich, Codes abzulehnen, die mehrfach interpretiert werden können.

Die Nachfrage nach kameralesbaren Barcodes wie QR-Codes wächst weiter. Es scheint, dass Code der nächsten Generation mit verbesserter Sicherheit erforderlich ist.