



Criterion attack / QR-bit flip

Nicolas Collignon
<nicolas.collignon@synacktiv.com>

QRcode

- Technologie de code-barre 2D
 - Qrcode
 - Datamatrix
 - ...
- Utilisation
 - Publicité → URL
 - Carte de visite
 - Android: Access point Wifi (ESSID + clé)

La mission

- La mission
 - Patcher un Qrcode contenant l'URL d'un site Web
- Le problème
 - Pas d'imprimante pour réimprimer le code-barre
- Les outils
 - Un criterium (stylo noir BIC ou crayon conté 7B)
 - Un Tipp-Ex (ou une feuille blanche et un ciseau)

Criterium attack

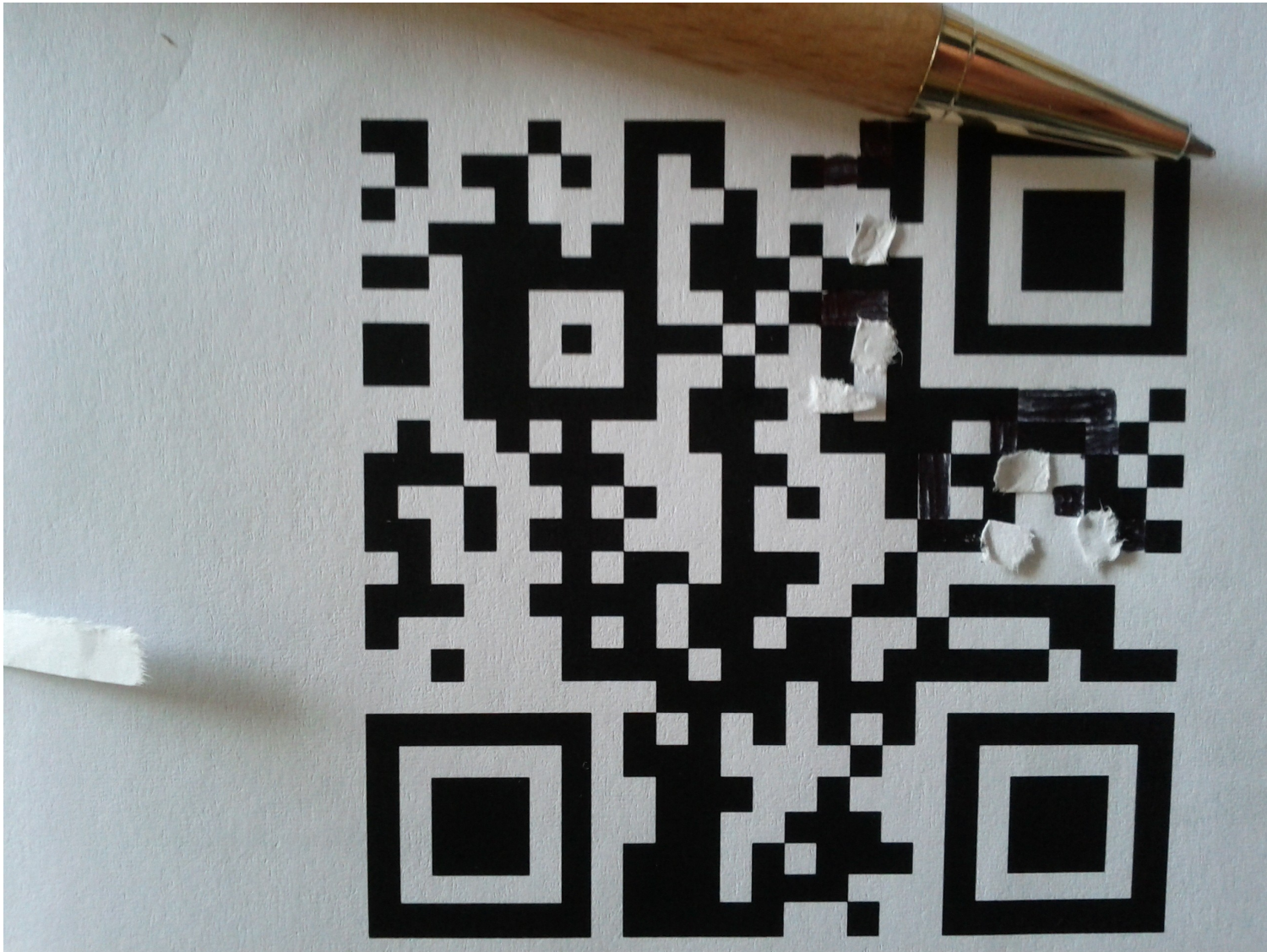
- Phase 1
 - Générer des collisions dans l'URL pour minimiser les transitions pixel “noir” → “blanc”.
- Phase 2
 - Réduire la surface de correction du Qrcode avec un algorithme maison “next-gen”
 - Générer des collisions dans la somme de contrôle Reed-Solomon
- Phase 3
 - Attaque manuelle (coloriage niveau maternelle grande section)

Criterion attack

- Avant / Après / Différentiel
- <https://www.sstic.org/2012>



L'attaque



Le résultat

