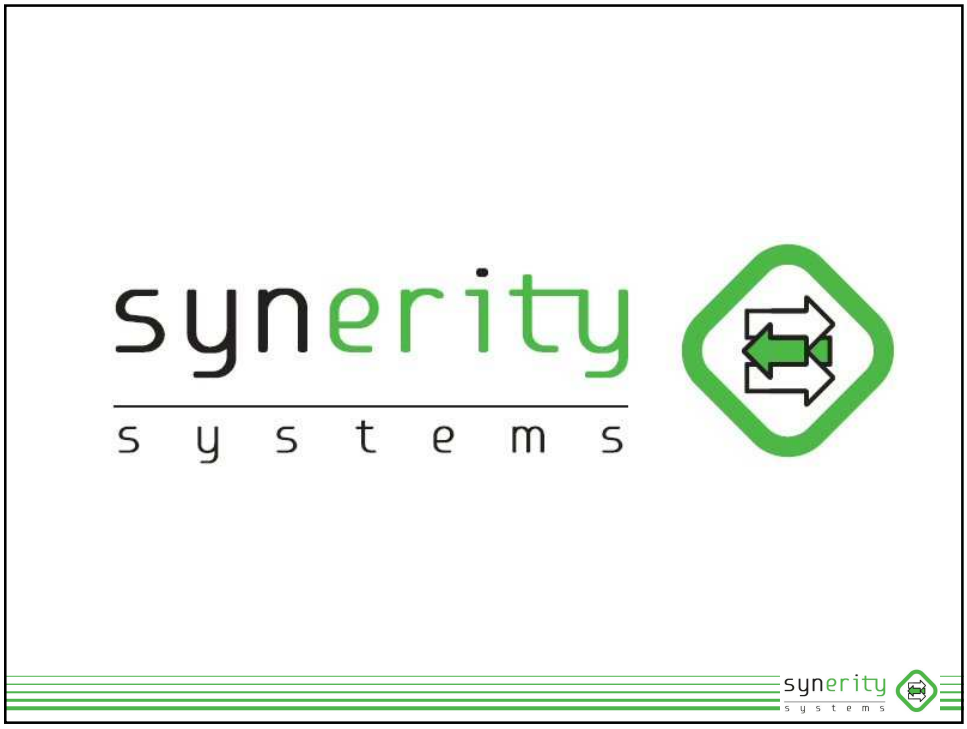
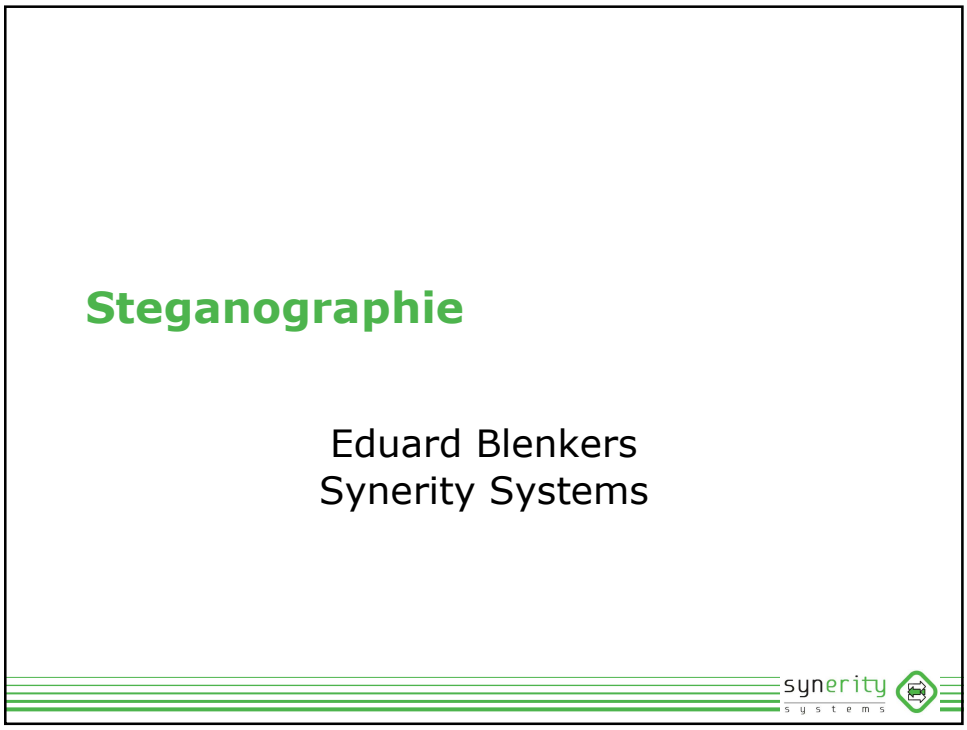


Steganographie

Eduard Blenkers
Synerity Systems



Steganographie

- Abgeleitet aus dem Griechischen für „Verdeckte Schrift“
- Verschleiert eine Nachricht in einem beliebigen Container
- Bereits in der Antike genutzt
  - Wachs-Tafeln
  - Tätowierungen auf der Kopfhaut

synerity systems

Einfache Anwendung per Computer

- Zahlreiche Programme verfügbar
  - Freeware
  - Lizenzpflichtig
  - Quelltext und Bibliotheken für Entwickler
- Übliche Container:
  - Grafiken: .BMP, .JPG, .GIF
  - Audio-Dateien: .WAV und .MP3

synerity systems

Stego != Krypto

- Steganographie = Verdeckte Nachricht
- Kryptographie = Sichtbare Nachricht
- Steganographie ist häufig mit Verschlüsselung gekoppelt
  - Nachricht wird durch Kennwort geschützt

synerity systems

Stegoanalyse (Steganalyse)

- Suche nach Steganographie
- Nachrichten erkennen
- Nachrichten extrahieren
- Auch: Untersuchung digitaler Wasserzeichen

synerity systems

Steganografie

synerity systems

Speicherorte

- Unterscheidung nach Thompson / Monroe
- Out of band
  - Ausserhalb definierter Regeln
  - Beispiel: Sektoren als „Bad" markiert, Slackspace, HPA
- In band
  - Innerhalb definierter Regeln
  - Beispiel: Sektoren als „belegt" markiert, aber nicht zugewiesen
- Application layer
  - In Anwendungsdaten
  - Beispiel: .jpg, .wav ...

synerity systems

Trägermedien

- Üblich
  - Bilder: .JPG, .BMP und .GIF
  - Audio-Dateien: .WAV und .MP3
- Ungewöhnlich
  - Zip-Archive
  - Video-Dateien
  - Registry
  - NTFS Metadaten
  - Ausführbaren Dateien

synerity systems

Null Cipher

- Telegramm der Deutschen Botschaft 1914
- PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW, STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY

synerity systems

Null Cipher

- Telegramm der Deutschen Botschaft 1914
- **P**RESIDENT'S **E**MBARGO **R**ULING **S**HOULD **H**AVE **I**MMEDIATE **N**OTICE. **G**RAVE **S**ITUATION **A**FFECTING **I**NTERNATIONAL **L**AW, **S**TATEMENT **F**ORESHADOWS **R**UIN **O**F **M**ANY **N**EUTRALS. **Y**ELLOW **J**OURNALS **U**NIFYING **N**ATIONAL **E**XCITEMENT **I**MMENSELY
- **PERSHING SAILS FROM NY JUNE I**

synerity systems

Steganographie Heute

- Hunderte von Programmen verfügbar
- S-tools, jphs, gif-it-up, wbstego, bmp-secrets, data-stash, Contraband, Texthide, Stealthencrypt, Steganos, In Plain View, Encrypt Pic, Camouflage, MP3stego, Xidie, Puff, StegoMagic, ...

synerity systems

Stegoanalyse

synerity systems

Suche nach Steganografie

Untersuchung in 2001:

- E-Bay:
  - > 2 Million Bilder getestet
  - Ca. 17.000 verdächtige Bilder
- Usenet:
  - > 1 Million Bilder getestet
  - Ca. 20.000 verdächtige Bilder
- 1.8 Million Passworte und Phrasen getestet: Kein Ergebnis

synerity systems

Out of Band Steganografie

- Stärken
  - Wird gewöhnlich übersehen
  - Entdeckung benötigt besondere Werkzeuge
  - Erlaubt oft große Speicherbereiche (HPA, DCO)
- Schwächen
  - Speicherung bricht Standards
  - „Security through obscurity"
  - Kann durch Anomalie-Erkennung gefunden werden
  - Speicherung fällt erfahrenen Forensikern auf

synerity systems

In Band Steganografie

- Stärken
  - Wird gewöhnlich übersehen
  - Entdeckung benötigt besondere Werkzeuge
  - Speicherung hält sich an Standards
- Schwächen
  - Gewöhnlich kleine Speichermengen
  - „Security through obscurity"
  - Kann durch Anomalie-Erkennung gefunden werden
  - Speicherung fällt erfahrenen Forensikern auf

synerity systems

Application Layer Steganografie

- Stärken
  - Etabliert: Zahlreiche Programme verfügbar
  - Einfache Anwendung
- Schwächen
  - Stego-Programme werden bei forensischer Untersuchung erkannt
  - Stego-Container werden zunehmend erkannt

synerity systems

Analyseprogramme

- Gargoyle
  - Sucht nach Stego-Programmen und Artefakten
  - „Spezialisierter Virenscanner"
- StegSpy
  - Erkennt einige Stego-Artefakte in Bildern
- Outguess
  - Erkennt einige Stego-Artefakte
  - Wörterbuch-Attacke gegen ausgewählte Programme

synerity systems

Mehr Auswertung

- Stego Analysis Suite
  - Systematische Suche nach Artefakten in Containern
  - Erkennt „Fingerabdrücke“ von Stego-Programmen
  - Programme zur visuellen Auswertung
  - Wörterbuch- und Brute-Force Angriff auf ausgesuchte Stego-Programme

synerity systems