The Convergence of Anti-Counterfeiting and Computer Security

Steven J. Murdoch[1] Ben Laurie[2]

[1]University of Cambridge, Computer Laboratory,
15 JJ Thompson Avenue, Cambridge CB3 0FD, United Kingdom
http://www.cl.cam.ac.uk/users/sjm217/

[2]http://www.apache-ssl.org/ben.html

21st Chaos Communication Congress, December 27–29 2004
Berliner Congress Center, Berlin, Germany

Outline

Introduction

- Optical security features used to protect many "documents"
  - Anti-tamper seals, tickets, gift vouchers, ID documents, currency, etc. . .
- Many similarities between Optical Document Security and Computer Security
  - Both communities can learn from each other
- Largest threat is now from computers, so fields are converging
  - The long term consequences of this are unclear

What is Optical Document Security?

- Canonical reference is "Optical Document Security" by Rudolf L. van Renesse [1]
- Main goals
  - Protect document against adequate duplication (counterfeiting)
  - Protect document against adequate modification (forgery)
- Both issuing bodies and counterfeiters have costs
  - Attacker wants cheapest fake which gets past first inspection
  - Issuing body wants cheapest document which will (mostly) prevent them

Document Inspection

- Documents must be designed to be checked in a variety of situations
- First line
  - Limited time, poor environment, little equipment
- Second line
  - More training, simple equipment, automated checks
- Third line
  - Forensic specialists, sophisticated equipment, special knowledge

Duplication Resistance

- Defences designed to prevent certain types of duplication
- Largest problem was colour photocopier, now scanner/inkjet printer
- Under a microscope, copies look very different from the original, but at normal distance they are difficult to distinguish
  - Dithering and half-toning is applied – but resolution is high enough
- Use the difference between human and computer vision to deter copying

Optically Variable Devices (OVDs)

- Printers can only produce images which look identical regardless of the angle of inspection
- So use features which change depending on the position of the viewer and of light source
- Watermarks are the simplest example, look different with transmitted vs. reflected light
- Iridescent effects can be achieved through diffraction and interference of thin films and micro-structures
- Holograms and Kinegrams extend these effects

Security against Digital Copying

- Printers and scanners have resolution limit tuned to human perception
- Security printing techniques can print at much higher resolution
- Use Nyquist limit to cause distortion when image is sampled
- SAM (Screen Angle Modulation) changes the angle of lines printed at higher resolution than human perception
  - But when sampled these cause moiré effects

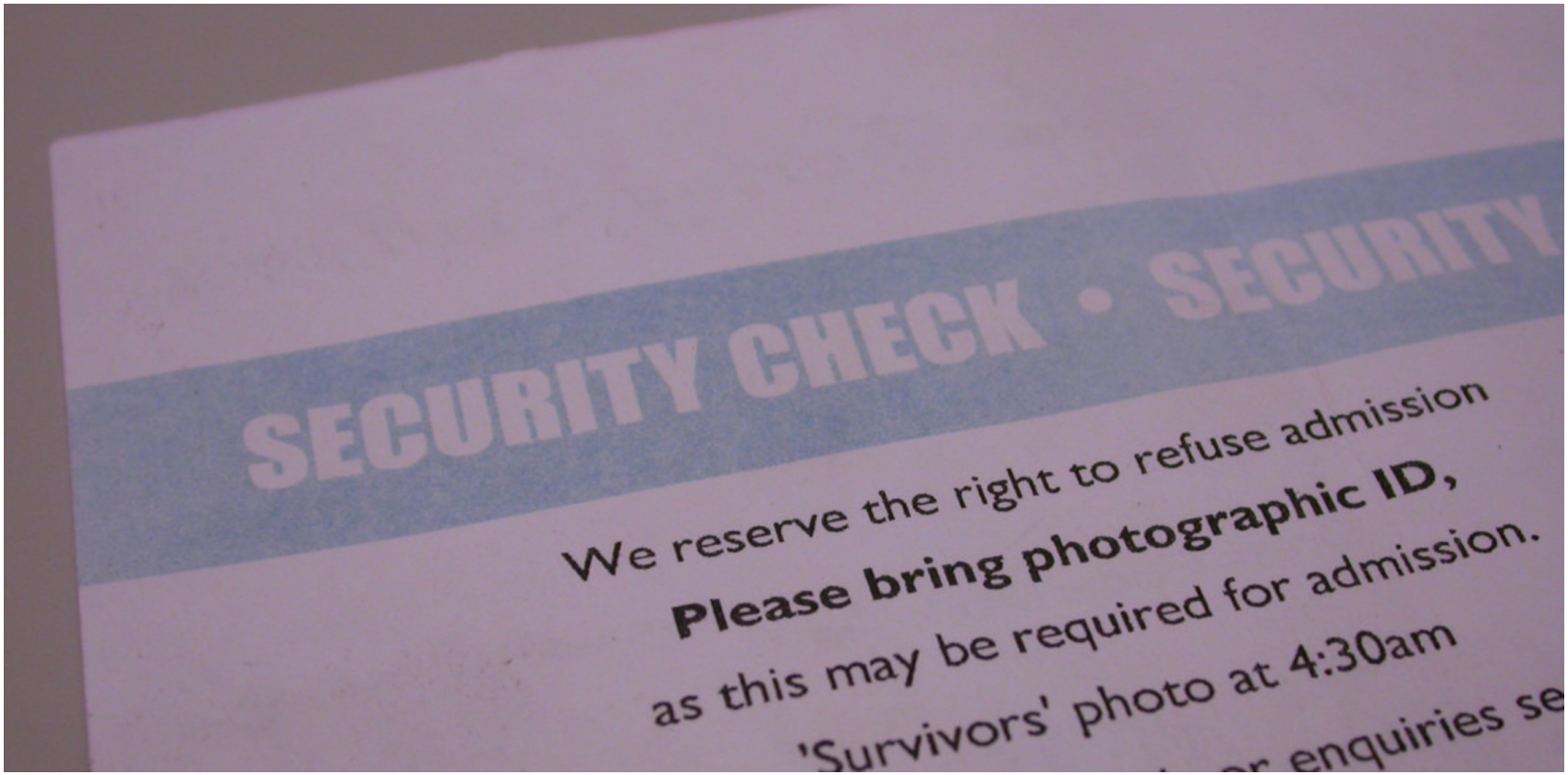
Screen Angle Modulation

Screen Angle Modulation

Other techniques

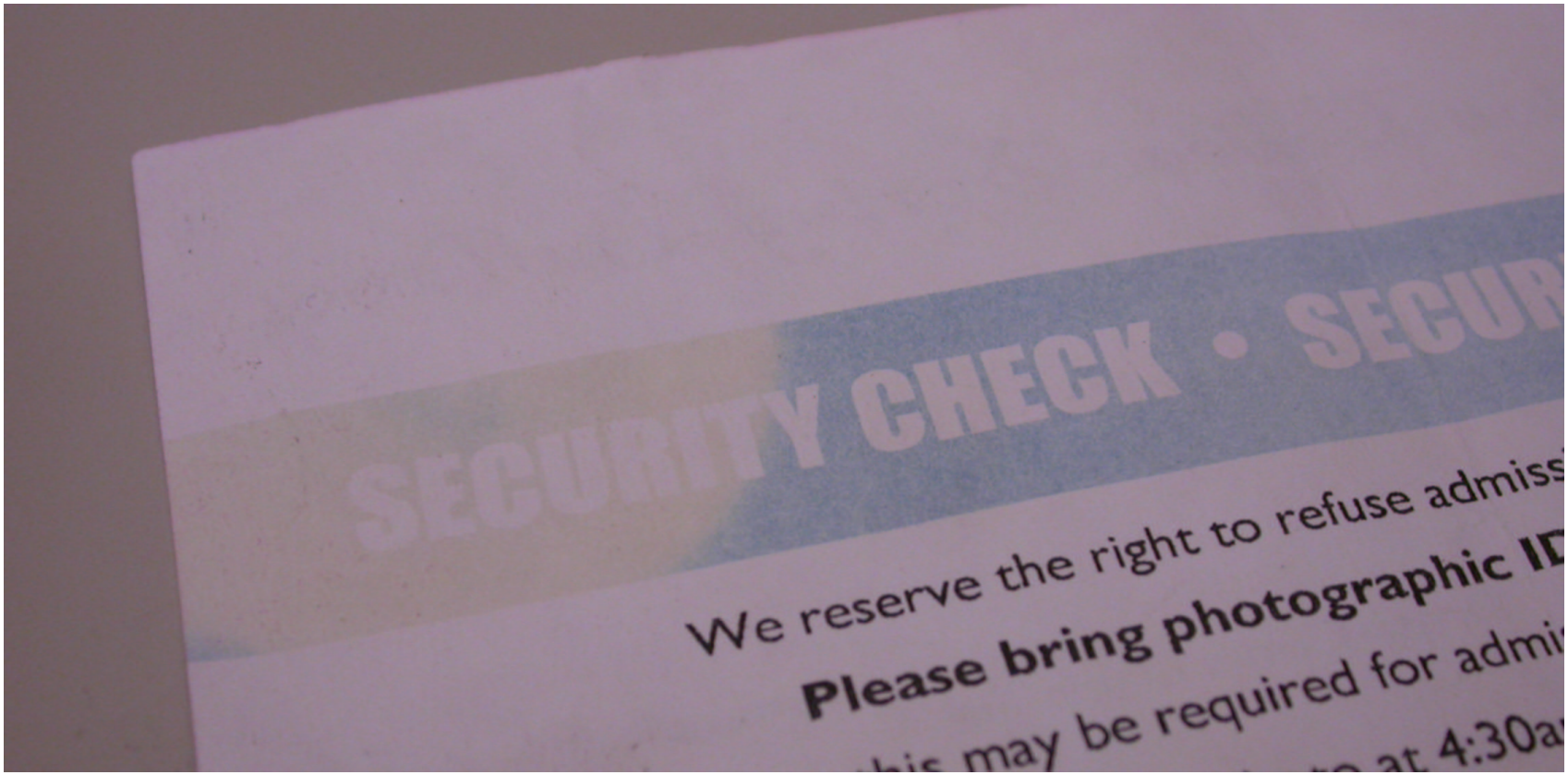
- Use special non-fluorescent paper, include fluorescent security fibres
- Include colour pairs difficult to reproduce in a 4 colour process (e.g. bright orange/light brown)
- Specialised printing techniques
  - Intaglio (tactile effect)
  - Registration windows
  - Serial numbers
- Thermochromic ink (durability problems)

Thermochromic Ink



Thermochromic Ink

Thermochromic Ink



Binding and Integrity

- Keep information unchanged and linked to other information
  - Photo & name/nationality, banknote & value
- Biometrics are example of binding a person and some other information
  - If you can't change the photo on an ID card, can you change your own appearance to match the photo on a stolen card?
- Similar to integrity constraints in crypto-systems
  - Kerberos ticket and expiry time, key and type information

Forgery prevention and detection

- Paper which shows attempts to alter or remove ink
  - Washing – add ink which bleeds
  - Oxidising and Reducing agents – include chemical which reacts with these
  - Mechanical removal – coat with chromagen, vulnerable layer
- More difficult when document producer cannot control type of ink used (cheques)
- Detect different types of ink (also identifies addition)
  - UV and IR light
  - Microspectrography
  - Chemical analysis such as gas chromatography, mass spectography (destructive)
  - Second/third line checks only

Anti Tamper Ink on Cheques

- Water, 2-Propanol, Cyclohexane

Other techniques

- Cover document with a thin film
  - Use standard techniques to make film difficult to duplicate
  - Film is weaker than glue, so cannot be removed intact (durability problems)
  - Transferable ink which leaves film if removed
- Problems if attacker applies film, or has access to document soon after cold seal
- Bind chip and card by having cryptographic key in a machine readable hologram

Risk Analysis

- Similar process to design of safety critical systems and security
- Identify threat model and refine into *S*ecurity Target
- Integrate with other requirements (durability, aesthetics)
- Evaluate benefit of security features
  - Compare cost to risk (likelihood of attack $\times$ damage)
- Optimise all requirements simultaneously (probably need several iterations)

Defence in Depth

- No one feature is sufficient, creates a fragile system
- Different features for different inspection levels
  - Some provide moderate security but are easy to check, others provide better security but need more time/equipment.
- Prevention not always possible, so use punishment as deterrent
  - Colour photocopiers and laser printers have characteristic signatures, sometimes intentional (yellow dots), sometimes not [2]
  - More difficult for cheap inkjet printers, buy with cash and destroy once used
  - Similar to audit logs in security systems

Human-Scale Security Protocols

- There are many similarities between computer security and "real-life" security [3]
  - In a restaurant – ordering wine, paying the bill
  - Airport security
  - Voting
- Where there are differences, both can learn from each other [4]
- As with locks, the fields of computer security and anti-counterfeiting are merging

Burglary, Bribery and Blackmail

- One of the largest problems in computer security
- Firewalls and access control of limited use if the computer can be stolen
- Attackers will choose the easiest route
- Protecting against corrupt(ed) insiders is very difficult
- A counterfeit made from original material cannot usually be identified
  - Secret conventions in filling out documents can help, but can only be known to a few people
  - If original documents are numbered then stolen ones can be revoked, but this doesn't always work, in either field

Complexity

- The more difficult a system is to understand the harder it is to see flaws
  - The APIs of cryptographic co-processors are so complex, that combinations of operations may introduce a security vulnerability [5]
  - Complex protocols may hide vulnerabilities for a long time e.g. SSL3 [6]
- But when attackers have less sophisticated equipment than the producers then complexity can be an effective deterrent
  - Holograms, OVDs, intaglio, kinegrams
- Complexity introduces a problem with usability, the inspection procedure may be difficult to remember and hard to perform

The Composition Problem

- A cryptographic primitive can be secure in isolation, but if feedback is allowed, or if combined with others then it may become insecure [7]
- Similarly poor combinations of security devices can negate their benefit
  - Intaglio printing over a watermark will make the watermark difficult to see
  - OVDs may be distracting and prevent users from looking are other features, so removing the advantages of defence in depth

Security Usability

- A document is only as secure as the checking process, so usability is key
- Security Usability within computer systems is known to be important but is hard to do correctly [8]
- Education is important, but not much can be remembered, so make security features self evident
- Standardisation across different products aids memory
- Human factors should be considered at all points of design

Cultural Differences

- Awareness of cultural differences is necessary in computing
  - Microsoft had a product banned in India due to a mistake in colouring a map [9]
- Similarly for document security, culture must be considered
  - In Japan it is common to iron banknotes given to children as New Year presents, to make them look new
  - The new banknotes contain a hologram which is damaged by heat, so the central bank had to produce an advert discouraging this
- In some circumstances it may be considered insulting to be seen checking a banknote, so currency should include some way of covert checking

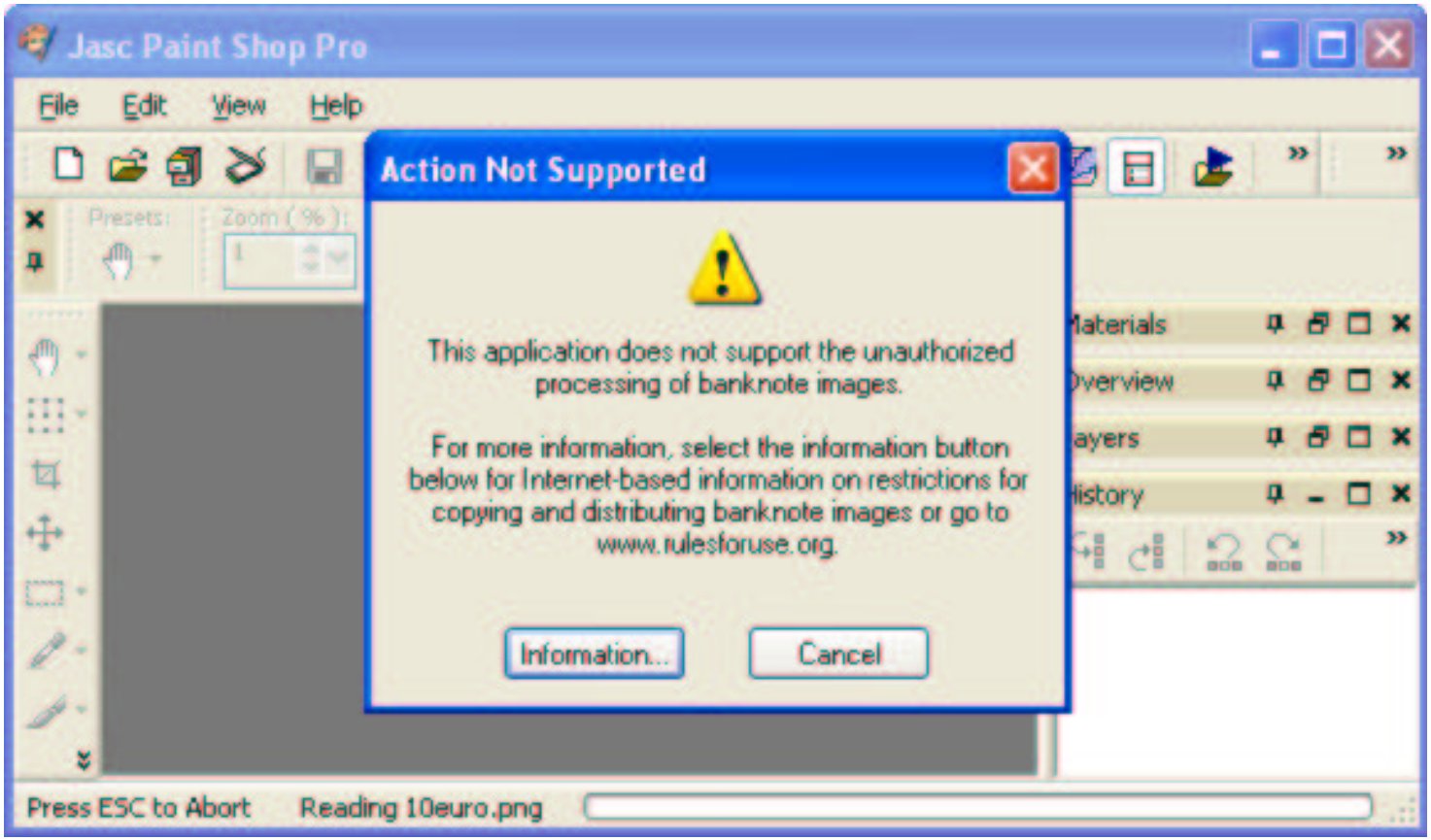
Security Through Obscurity

- Generally considered bad within computer security
  - While relying on security through obscurity is inadvisable, sometimes it is advantageous to keep some information hidden
- Within document security, opinions are mixed
  - Machine reading techniques are still quite carefully guarded
- Much information is public already
  - Intaglio and watermarking techniques are well known, but are still quite secure
  - Applying for a patent requires publishing information
  - Users need to know of features in order to recognise them

Counterfeit Detection System (CDS)

- Introduced to deter counterfeiting on banknotes on desktop PCs
  - Included in Adobe Photoshop, JASC Paint Shop Pro, HP printer Drivers, Canon scanner software, and others
- Existence became publicly known in January 2004
- Produced on behalf of the Central Banks Counterfeit Deterrence group (part of G10) by Digimarc
- Algorithm not disclosed, code is free of charge but closed source, even to companies who integrate it

rulesforuse.org



Eurion constellation

- Identified by Markus G. Kuhn in 2002 [10].
- Used by colour photocopiers

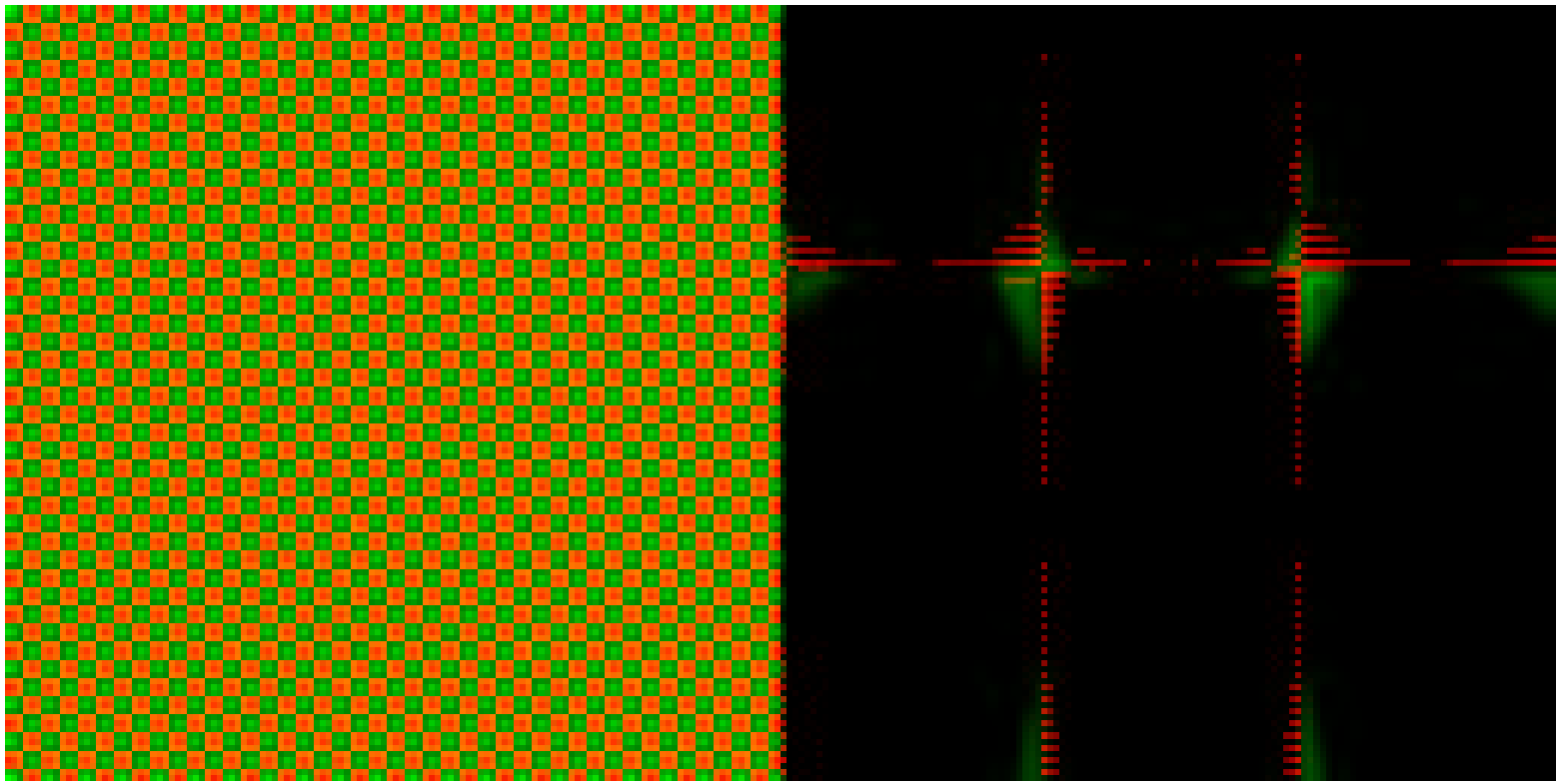
Black Box Analysis

- Eurion constellation neither necessary nor sufficient
- Not colour histogram
- The whole banknote is not required
- Some parts of the banknote are detected more strongly than others
  - Particularly areas using SAM like techniques

Reverse Engineering

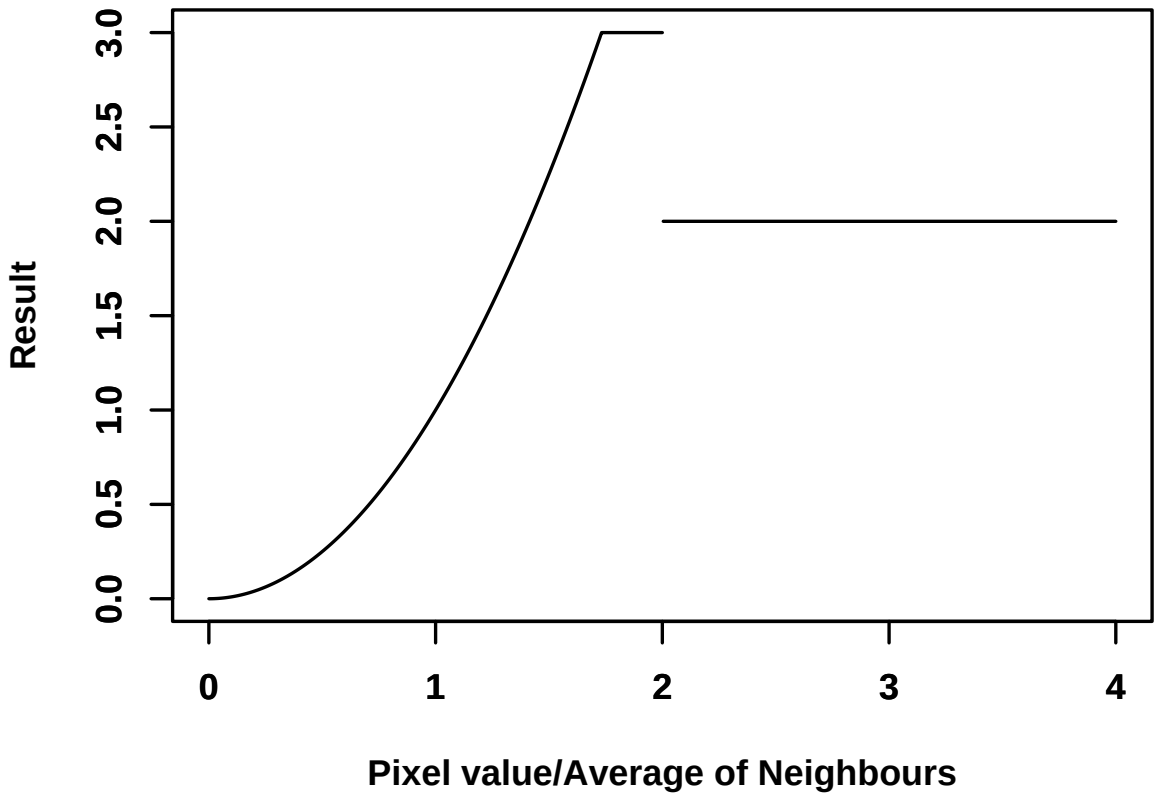
- IDA for static analysis, OllyDbg for dynamic
- Several techniques used, one of the most effective is to identify a function of interest and trace execution
  - Make trace for each different image, and run diff on the resulting files
- Break before a function call, replace arguments with chosen data and examine output.

Domain Transform



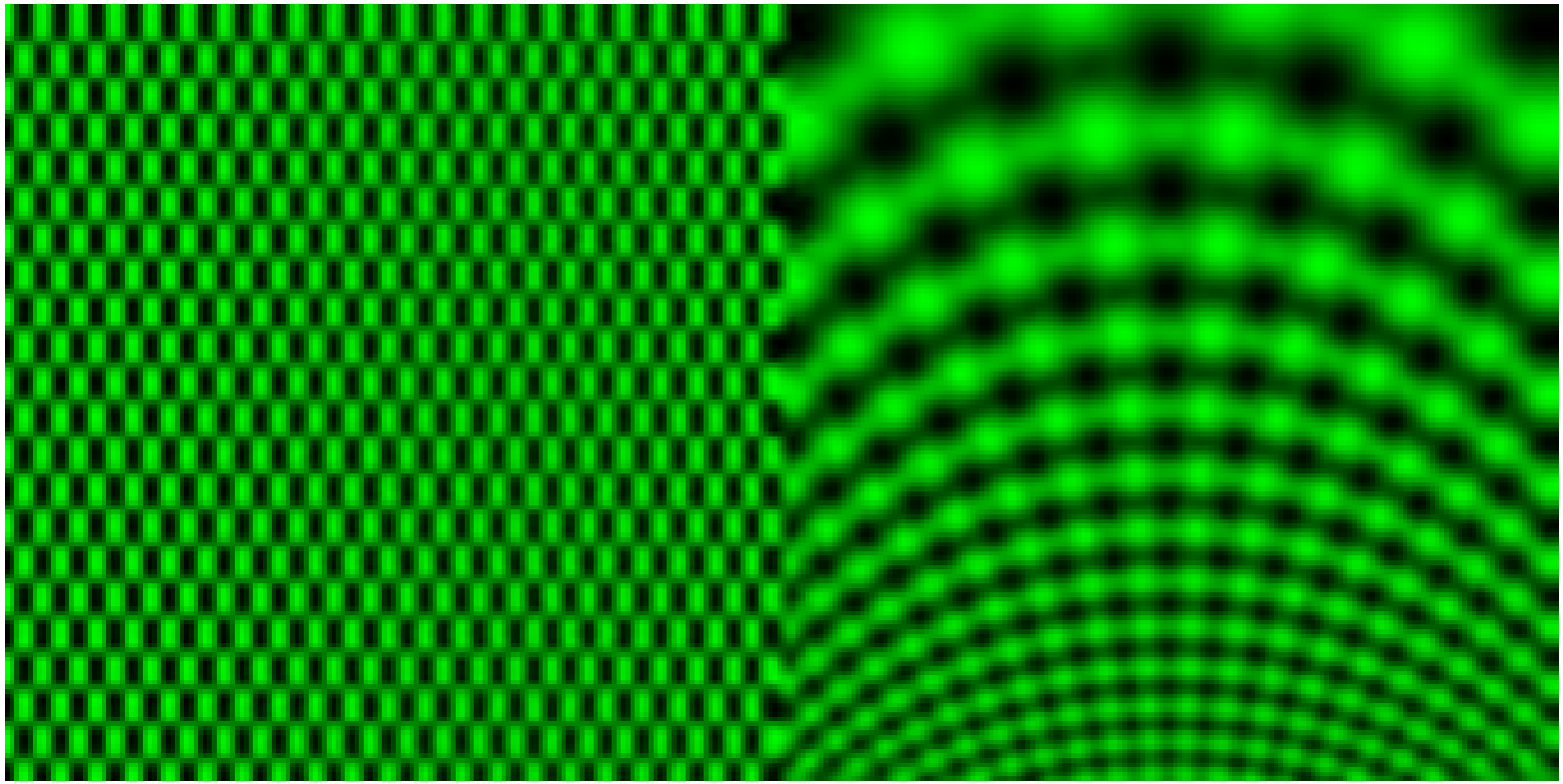
- Split image into segments, sharpen, then frequency transform

Normalisation



- Compare each pixel to the average of its neighbours

Coordinate Transform



- Convert from log-polar to Cartesian coordinates
- Finally extract two arrays the compare elements to 7.0 and 1.9

Proposed Legislation

- "legislation would require any equipment, software or other products manufactured, imported, distributed or sold within the EU that is capable of capturing images or transferring images into, or out of, computer systems or of manipulating or producing digital images for the purposes of counterfeiting, to incorporate counterfeit deterrence technology." [11]
- Consultation deadline was 19 December 2003
- According to newspaper reports the goal was to have such legislation in place by December 2004 [12]

Potential Problems

- Detection code is closed source, cannot be integrated with GPL products
- If source is available then potential counterfeiters could simply remove it
  - This may not be a problem if only casual counterfeiting is to be prevented
- Making copies of currency is legal in some circumstances, how will exceptions be handled?
- What products need this detection code, GIMP, Perl, the Linux kernel, GCC?

Conclusion

- Optical document security is a mature technology and has evolved to combat real world threats
- It may help computer security to learn from this field
- Due to the prevalence of IT both the attack and defence of counterfeiting, the two fields are converging
- While this could have significant gains for both, there may be damaging unintended consequences of applying the assumptions of one area to the other.

Acknowledgements

- Public Software Fund, Inc.
- Carnegie Trust for the Universities of Scotland

References I

[1] Rudolf L. van Renesse, editor.
Optical Document Security.
Artech House Publishers, second edition, 1992.

[2] Gazi N. Ali, Aravind K. Mikkilineni, Pei-Ju Chiang, Jan P. Allebach, George T. Chiu, and Edward J. Delp.
Application of principal components analysis and gaussian mixture models to printer identification.
In *International Conference on Digital Printing Technologies*, 2004.

[3] Matt Blaze.
Towards a broader view of security protocols.
In *Twelfth International Workshop on Security Protocols*, Lecture Notes in Computer Science (to be published). Springer-Verlag, April 2004.
http://dimacs.rutgers.edu/Workshops/Tools/slides/blaze.pdf.

[4] Matt Blaze.
Cryptology and physical security: Rights amplification in master-keyed mechanical locks.
IEEE Security and Privacy, March/April 2003.
http://www.crypto.com/papers/mk.pdf.

[5] Mike Bond.
Attacks on cryptoprocessor transaction sets.
In .K. Ko, D. Naccache, and Paar C., editors, *Cryptographic Hardware and Embedded Systems CHES 2001: Third International Workshop, Paris, France*, volume 2162 of *Lecture Notes in Computer Science*, page 220. Springer-Verlag, May 2001.
http://www.cl.cam.ac.uk/~mkb23/research/Attacks-on-Crypto-TS.pdf.

References II

[6] D. Wagner and B. Schneier.
Analysis of the SSL 3.0 protocol.
In *The Second USENIX Workshop on Electronic Commerce*, pages 29–40. USENIX Press, November 1996.
http://www.schneier.com/paper-ssl-revised.pdf.

[7] D. McCullough.
Noninterference and the composability of security properties.
In *IEEE Symposium on Security and Privacy*, pages 177–186. IEEE, April 1988.

[8] Alma Whitten and J. D. Tygar.
Why Johnny can't encrypt: A usability evaluation of PGP 5.0.
In *8th USENIX Security Symposium*, pages 169–184, August 1999.
http://www.usenix.org/publications/library/proceedings/sec99/whitten.html.

[9] Paul Brown.
Microsoft pays dear for insults through ignorance.
The Guardian, August 2004.
http://www.guardian.co.uk/online/news/0,12597,1286066,00.html.

[10] Markus G. Kuhn.
The EURion constellation.
http://www.cl.cam.ac.uk/~mgk25/eurion.pdf, February 2002.

References III

[11] European Central Bank.
Consultation announcement regarding possible legislation on the incorporation of counterfeit deterrence technology in products capable of handling digital images.
Official Journal of the European Union, 2003/C 255/13, October 2003.
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:C:2003:255:0008:0008:EN:PDF.

[12] Tony Thompson.
Security clampdown on the home PC banknote forgers.
The Observer, June 2004.
http://observer.guardian.co.uk/uk_news/story/0,6903,1232480,00.html.