Institution:

University of Cambridge

Unit of Assessment:

UoA11

Title of case study:

Electronic payment systems

1. Summary of the impact (indicative maximum 100 words)

Research examining the vulnerabilities in electronic payment systems conducted by Professor Ross Anderson and his research team at the University of Cambridge since 1995 has had profound impact on the current generation of payment systems. Research outcomes have (i) led existing businesses to redesign application programming interfaces (APIs) used by hardware security modules; (ii) created a new company, Cronto; (iii) convinced authorities to review certification systems so that products are more secure; and (iv) fuelled public awareness of, and discourse about, the security of electronic payment systems.

2. Underpinning research (indicative maximum 500 words)

The core foundation for the payment security research was conducted in the Cambridge University Computer Laboratory by a team led by Professor Ross Anderson, Lecturer from 1995, Reader from 2000, Professor from 2003 to present. This research enabled a deeper understanding of security protocols, extending first into the study of cryptographic application programming interfaces (APIs) and then into the analysis of deployed payment protocols. The security API research, which Anderson commenced in 2000 with Dr Mike Bond (postdoctoral researcher until he left to join Cryptomathic in 2006), found new vulnerabilities in almost all studied APIs [1].

Anderson, Bond and Dr Stephen Murdoch (postdoctoral researcher from 2006, now Royal Society Research Fellow in the Laboratory) analysed real-world payment protocols including various electronic banking systems, 3D secure, and most significantly, Europay, Mastercard and Visa (EMV, or more commonly, “chip and PIN”). Anderson and colleagues’ research uncovered serious certification failures in 2008 [2] and a protocol failure in 2010 that allowed use of an EMV card without knowledge of the PIN [3]. Subsequent research in 2012 led to flaws being uncovered in the random number generators used in ATMs and also the discovery of ‘preplay’ attacks – hitherto undocumented man-in-the-middle attacks on EMV. In such attacks, the attacker pretends to be the card to the terminal, and the terminal to the card. Furthermore, Anderson’s team brought to bear the forensic expertise to elucidate and expose flaws in the system already exploited by criminals and to develop the necessary systems to curtail this activity.

Anderson’s team also analysed the hardware tamper-resistance of smart cards. This was carried out in the Cambridge Laboratory by Sergei Skorobogatov (postdoctoral researcher in the Laboratory from 2000, Senior Research Associate from 2006) with whom Anderson pioneered the field of semi-invasive attacks on semiconductor chips in 2000. These are attacks in which the target chip is manipulated directly, typically using a laser, but without physical interference (in the sense that the passivation layer is left intact). As feature sizes have shrunk, semi-invasive attacks have come into their own. This expertise in microelectronics has strongly supported the forensic work [4].

Research in 2009 analysed currently available authentication devices and identified a number of flaws including bad token reuse and lack of freshness, which were the result of over-optimisation of implementations, and proposed improved designs [5].

In 2012 the group demonstrated that many payment terminals generate insufficiently random numbers for the EMV protocol to be secure from attack [6].

This research has been informed by direct engagement with many technology platform vendors with a view to making existing platforms more secure, or creating new ones. In particular, Anderson has worked directly with Symbian, Google, and Samsung.

3. References to the research (indicative maximum of six references)

[1]* "API-Level Attacks on Embedded Systems", Mike Bond, Ross Anderson, *IEEE Computer* v 34 no 10 (Oct 2002) pp 67–75.
DOI: http://dx.doi.org/10.1109/2.955101

[2] "Thinking inside the box: system-level failures of tamper proofing" Saar Drimer, Steven Murdoch and Ross Anderson, at *2008 IEEE Symposium on Security and Privacy*, pp 281–295; outstanding paper award by IEEE Security & Privacy Magazine.
DOI: http://dx.doi.org/10.1109/SP.2008.16

[3]* "Chip and Pin is Broken", Steven Murdoch, Saar Drimer, Mike Bond and Ross Anderson, at *2010 IEEE Symposium on Security and Privacy* pp 433–444; outstanding paper award.
DOI: http://dx.doi.org/10.1109/SP.2010.33

[4]* "Optical Fault Induction Attacks", Sergei Skorobogatov, Ross Anderson, Cryptographic Hardware and Embedded Systems Workshop (CHES), San Francisco, USA. LNCS 2523, Springer-Verlag, August 2002, ISBN 3-540-00409-2, pp 2–12.
DOI: http://dx.doi.org/10.1007/3-540-36400-5_2

[5] "Optimised to fail: Card readers for online banking", Saar Drimer, Steven J Murdoch and Ross Anderson at *Financial Cryptography 2009*
URL: http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf

[6] "Chip and Skim", Mike Bond, Omar Choudary, Steven Murdoch, Sergei Skorobogotov and Ross Anderson, Workshop on Cryptographic Hardware and Embedded Systems 2012 (CHES 2012), Leuven, Belgium, 9–12 September 2012
URL: http://arxiv.org/abs/1209.2531

*Research references which best represent the quality of the underpinning research

4. Details of the impact (indicative maximum 750 words)

Impact can be demonstrated in many areas but these elements interact strongly with each other. Also, due to the immediate impact of research related to the security of deployed systems, there is a constant interaction between impact and the further development of the research. It is not a simple linear model of research leading to impact.

Impact on public interest and public discourse
The team developed and led by Anderson at Cambridge is widely acknowledged to be the most visible *independent* centre of expertise in payment systems worldwide. Other centres of expertise are centred on specific large suppliers (e.g., IBM, Gemalto, NXP) and rarely publish in the public domain. Anderson's team has a high profile not only for research and citations, but also in search engines and conventional media. Thus many victims of fraud failing to get refunds from payment service providers contact the Cambridge team, providing interesting cases for further research and new insights into fraud patterns. The results have impact on the world through product redesign, improvements in operational procedures, and in the policy field.

Impact on public policy
During the REF period, Anderson's research uncovered wide variations between countries in rates of electronic fraud (and also in the fear of fraud). The group has unearthed systemic failures in the Financial Ombudsman Service, in the implementation of the Payment Services Directive, and in online consumer protection generally. These examples of bad practice have had impact not just within Europe (the group has advised both the FSA and the European Commission, and has also given evidence to various parliamentary committees) but also globally. The US Federal Reserve commissioned papers by Anderson for their biennial Payment Systems Economics conferences in 2008, 2010 and 2012 [9]. The conferences were "distinctive in attracting participation of policymakers, industry leaders, and academics from around the world" and were attended by key policy makers including Federal Reserve current and former Presidents, FVPs and COOs (Senior Economist in the Payments System function of the Economic, Research Department at the Federal Reserve Bank of Kansas City [8]).

Impact on performance of existing businesses

Anderson's group's research into API security rapidly established that most cryptographic hardware security modules (HSMs) used by banks and certification authorities (CAs) were highly vulnerable to simple attacks. This led Anderson to propose design changes to the APIs presented by most HSMs. Cryptomathic took a particular interest in this work, hiring Dr Bond as a security architect in 2006.

"*One of our latest products, CSG, the Crypto Service Gateway … would not have been built without the great insights that arose from the Anderson group*." [7]

Cryptomathic's CSG has substantially increased security levels for Barclays, while increasing performance and saving the bank more than £1M per year on development of new applications. The CSG is now the default at Barclays for any new application requiring cryptographic services. Reference [7].

Impact on business technology, public discourse, and public awareness

Anderson's research on EMV vulnerabilities in certification of PIN entry devices – ref [2] above – was used to explain why supposedly secure devices in the mid-2000s were compromised almost immediately, and on a large scale, by criminals after the rollout of EMV ("chip and pin"). Anderson's research reported in ref [3], informed by patterns of customer complaints, was used to uncover a previously unknown protocol failure whereby enabled stolen chip and pin cards could be used in merchant terminals without knowledge of the PIN (the "no-PIN attack"). Both of these findings received extensive media coverage, particularly long pieces on Newsnight (Feb 2008 and Feb 2010)[10]. The research also resulted in industry being more open about vulnerabilities. A particular example is the random number analysis reported in ref [6], which was reported in confidence earlier in 2012 to EMV and led to changes in test requirements issued by EMV in April of that year [12].

Impact on creation of new businesses

The Anderson group's research has been at the core of technology developed and commercialized by Cronto Limited, a spin-out company providing authentication systems for online banking. Dr Murdoch is the Chief Security Architect of Cronto in addition to his research role at the Laboratory. Cronto's products are now securing online banking in Chile (Corpbanca), Switzerland (Raiffeisen) and Germany (Commerzbank). The Cronto system was launched to all of Commerzbank's 11 million retail customers in February 2013. On May 20th 2013, VASCO Data Security International announced their acquisition of Cronto for £17M. [11]

The group's research has contributed to the commercial success of Cronto in two main ways. First, the demonstration of the weakness of banking hardware (ref [2] above) motivated the move to performing authentication on personal devices, which the customer can protect against tampering. Second, improvements to authentication devices proposed in ref [5] have been incorporated into the Cronto authentication system and have led to its high levels of usability and security.

5. Sources to corroborate the impact (indicative maximum of 10 references)

Individual sources

[7]. Letter from CEO, Cryptomathic

[8]. Senior Economist in the Payments System function of the Economic Research Department at the Federal Reserve Bank of Kansas City

Published sources

[9]. "Risk and privacy implications of consumer payment innovation", Ross Anderson, in *Consumer Payment Innovation in the Connected Age*, Kansas City Federal Reserve Bank, March 2012, ISBN 978-0-9744809-4-7. Commissioned by the Federal Reserve Bank.
http://www.kc.frb.org/publicat/pscp/2012/anderson.pdf

[10]. Newsnight programme 2010:
http://www.bbc.co.uk/blogs/newsnight/susanwatts/2010/02/new_flaws_in_chip_and_pin_syst.html

[11]. Acquisition of Cronto
http://www.prnewswire.com/news-releases/vasco-announces-acquisition-of-cronto-united-kingdom-208131501.html

[12]. Changes to EMV testing requirements since Anderson's work on faulty unpredictable numbers:
"SB-103 : Unpredictable Number generation (Spec Change), 1st Edition, April 2012"
http://www.emvco.com/download_agreement.aspx?id=702
"Bulletin nº127, Terminal Level 2 Test Cases, Unpredictable Number testing Update, 1st Edition, November 2012"
http://www.emvco.com/download_agreement.aspx?id=744