Security Engineering

Banking and Payment Security II

Contactless

- Tickets 1990s; cards 2005; phones 2011-14
- Various flavours, e.g. PED sends (N, d, X) and card answers with a MAC as the CVV
- EMV allows a few tap-and-pay transactions with a limit, then demands PIN
- Various bugs and blunders; most notably the limit may fail with foreign currency
- Now most sales, thanks to the pandemic!

TLS and online card payments

- Microsoft etc tried to create a proper payment protocol, SET, in 1994–5, but certifying keys for all banks, cardholders and merchants was too hard
- Netscape hacked together SSL; Verisign was set up to sell certificates to anyone with a website
- SSL became TLS and was ‘verified’, but remained open to middleperson attacks in too many ways
- Opened the floodgates to e-commerce; and also to phishing and card fraud

Carding forums

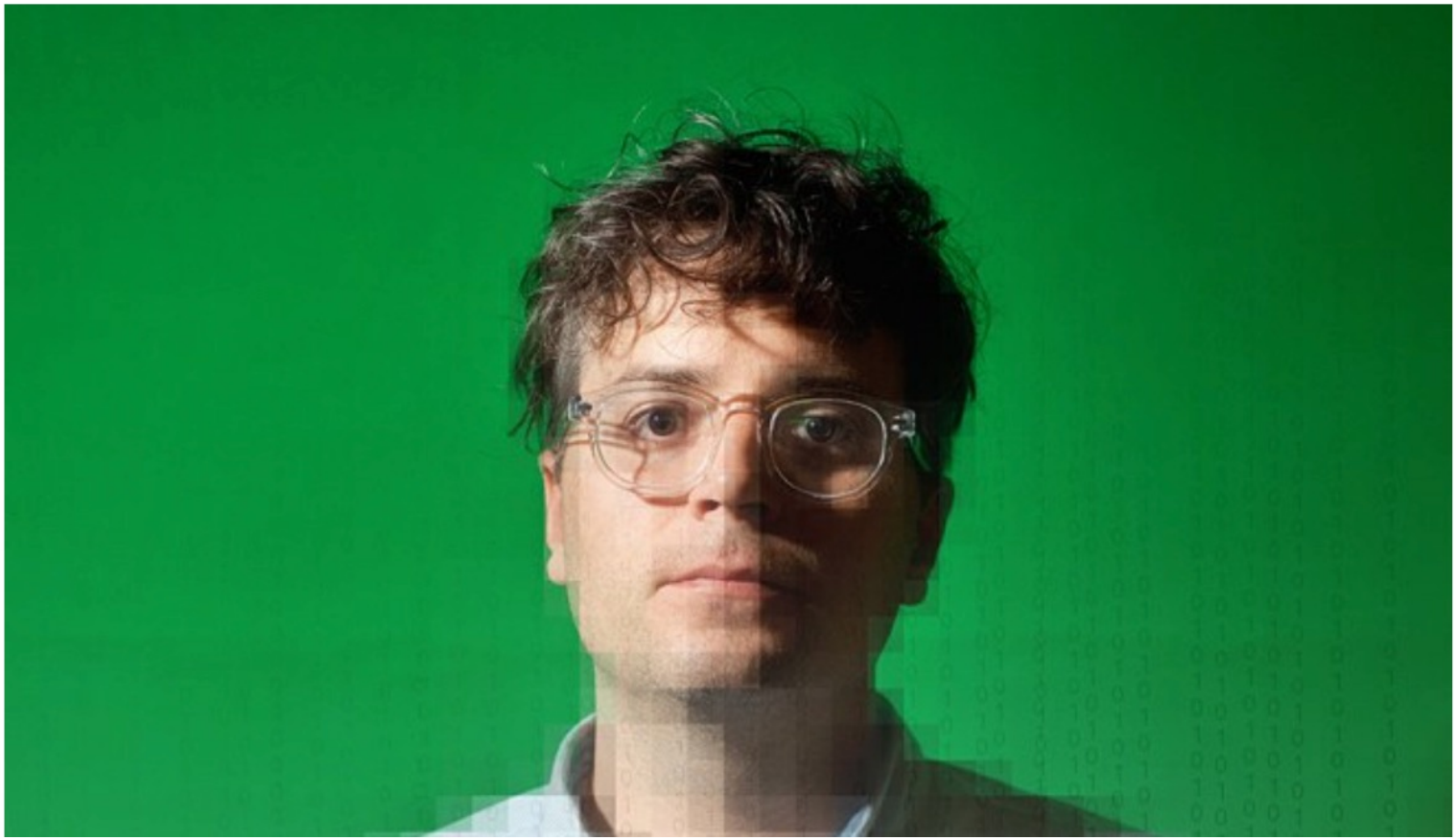
- In mid-2000s, banks used EMV to dump cardholder-not-present fraud on merchants
- Underground forums sprang up to trade card data, malware, cashout services...
- Cyber-crooks started to specialize and get good at their jobs
- Merchant websites got fraud engines that turned down several percent of baskets

PCI DSS

- Banks' response from 2004: Payment Card Industry Data Security Standards (PCI DSS)
- Fraud is cross-channel; e.g. card data stolen from stores / POS devices, then used online
- Merchants can't keep CVVs at all; they must protect cardholder data, patch their kit etc
- Assessors must be qualified; large firms need to report compliance (great for auditors!)

MAT HONAN GEAR 08.06.12 08:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING



Mat Honan hack

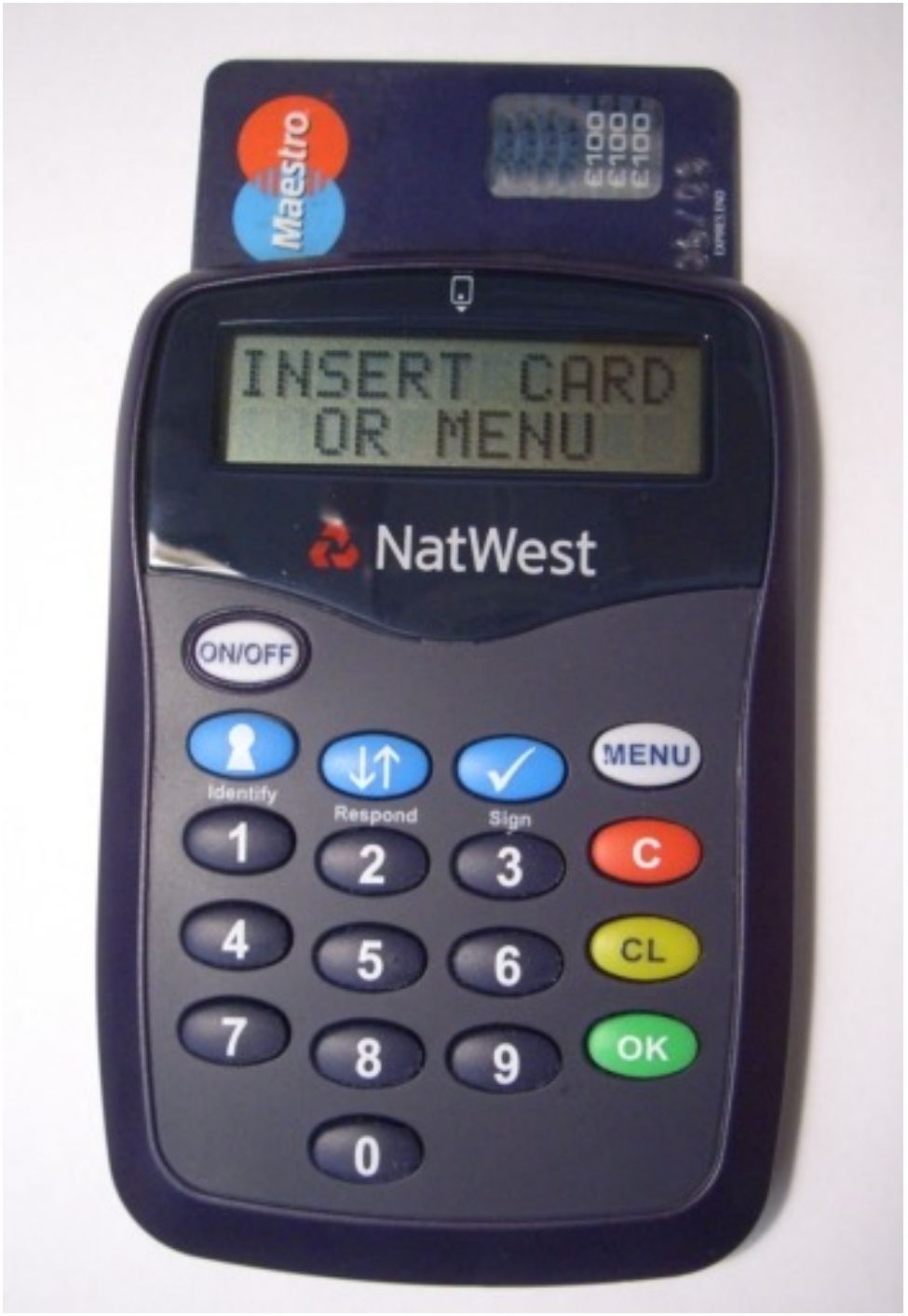
- Get Mat's billing address from whois
- Call Amazon to add a credit card (then you see last 4 digits of others), then again to add email
- Apple password reset needs billing address plus last 4 digits of credit card
- Gmail password reset: sends a message to the backup email (Matt's apple @me.com account)
- Hackers wiped Mat's phone, Macbook and Gmail, then sent racist tweets from his Twitter

Incremental guessing

- Of Alexa top 500 websites, 26 use primary account number + exp date
- 37 use PAN + postcode (numeric digits only for some, add door number for others)
- 291 ask for PAN + expdate + CVV
- Aamir Ali et al: iterated guessing works!
- Some paper receipts have PAN + expdate
- Some websites whitelist good customers

Online electronic banking

- Early pilots in 1980s; phone banking in 1990s
- Phishing from 2005 killed static passwords
- Complex password schemes for delegation
- Growth of two-factor authentication (2FA): custom password calculators, SMS
- Limiting factor: man-in-the-browser attacks


Maestro
INSERT CARD
OR MENU
NatWest
ON/OFF
Identify
Respond
Sign
MENU
1
2
3
C
4
5
6
CL
7
8
9
OK
0

Chip Authentication Program (CAP)

- 2FA to stop phishing attacks on electronic banking, now for big card payments too
- EMV version: each customer has a chipcard
- Easy mode:

  $U \rightarrow C$: PIN

  $C \rightarrow U$: $\{N, PIN\}_{KC}$
- Serious mode:

  $U \rightarrow C$: PIN, amt, last 8 digits of payee A/C…

What goes wrong…

guardian.co.uk

Police think French pair tortured for pin details

Matthew Taylor
The Guardian, Saturday July 5 2008

Laurent Bonomo and Gabriel Ferez, two French exchange students who were killed in London. Photographs: Met police/Getty

The two French students who were bound up and brutally murdered at a bedsit in south London may have been tortured for their bank and credit card pin numbers, police said yesterday.

Laurent Bonomo and Gabriel Ferez, both 23, were found at Bonomo's flat in New Cross, south London, on Sunday night. They had been stabbed more than 200 times, bound, gagged, and tortured over several hours.

SIM swapping

- ‘I lost my phone...’
- First seen in 2007 in Cape Town: someone got a SIM for the treasurer of the Ubuntu Foundation and stole about £10k
- 2010: widely used in Nigeria
- 2015: ‘OG’ Instagram heists in the USA
- Now: widely used to steal accounts at cryptocurrency exchanges

Other 2FA defeats

- SS7 is telco signaling; a phone company can say ‘Alice just joined my network, so please send me her SMS messages’
- SS7 hacking has been seen against German and UK banks (starting 2018)
- Governments might order telcos to install firewalls, but some rather like being able to abuse SS7…

Whither 2FA?

- People now do banking on their phone!
- They hate 2FA tokens, which cost money
- So banks lobbied for two apps on the same phone to be treated as two factors
- ECB said okay so long as one of them has runtime application security protection (RASP)

The Faster Payments System

- Designed to replace cheques for small payments, settling in 2h rather than 3d
  - First rolled out 2008
  - banks promote once interest rates fall
  - Access via online banking then phone apps
  - fintechs start to join from 2017
- Changed the fraud landscape too...

Authorised push payment

- Since 2020–1, the largest fraud type against retail customers is authorized push payment (APP) scams
- Often targets elderly and vulnerable
- ‘This is Lloyds bank. I’m afraid our security has been hacked, so we created an account at HSBC for you to keep your money safe...’
- The Payment Services Regulator ordered banks to refund customers, but most drag their heels...

AML/KYC

- Regulations on anti-money-laundering (AML), know-your-customer (KYC) since 1990s to counter drugs trade
- Boost after 9/11 for ‘counter-terrorism’
- Expensive and ineffective: of every $1000 in crime proceeds, $1 is stopped by AML but this costs the banking industry $100!
- Also, a real obstacle to financial inclusion...

Mobile payments in LDCs

- First large-scale system: Safaricom in Kenya
- Encrypted SMS / USSD, moving to apps
- Enabled everyone to send money home by building a cash-in cash-out agent network
- Because of KYC rules, only small sums in accounts, so only petty crime at user end
- Now replicated in dozens of other LDCs

Open banking

- Delegate some bank account access to payment services (e.g. Wise) or accounting (e.g. Sage)
- Fintechs mostly escape the regulatory cost of anti-money-laundering (AML) measures
- Delegated authentication replaced screen scraping; regulated by PSD2
- But it can get complex!
- Do you let your agent get data, or spend money?
- Edinburgh University hosts a centre of expertise...

Cryptocurrency

- Started 2009 among cypherpunks
- ‘Killer app’ was Silk Road, 2011–3
- Then capital flight, and drug money
- Investment scams: altcoins, ICOs
- Ransomware the new tactical pain point
- Strategic pain point: CO_2
- AML evasion drove the whole ecosystem!

Overall economic picture

- Fraud patterns much the same in 2018 as in 2011 (our ‘costs of cybercrime’ surveys)
- This was despite move from PCs to phones, from on-prem to cloud, and to social
- Conclude: dynamics of cybercrime are not tech so much regulation / context / etc
- Exceptions: rising costs of APP, and of cryptocrime including ransomware