RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

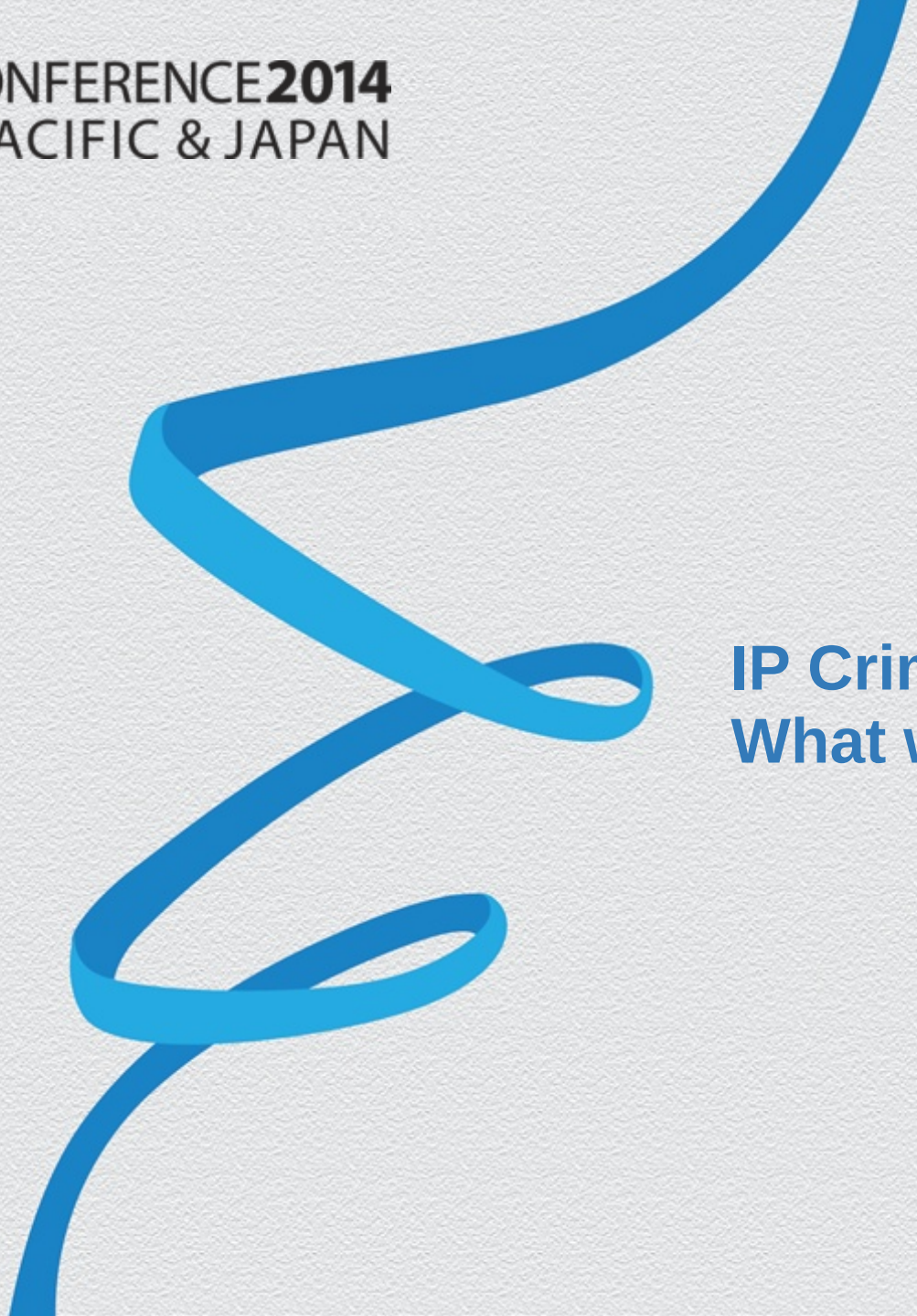
IP and telephony crime has converged – wake up, wise up & get protected!

SESSION ID: CLE-T07

Andy Dancer

Director
Evolved Intelligence
@_AndyDancer

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



IP Crime:
What we all know well

Malware Evolution

- Perpetrator
  - Out: Kids in their bedroom
  - In: Organised Crime
- Motive
  - Out: Proving how clever you are
  - In: Making money
- Timespan
  - Out: The “Outbreak”
  - In: Stealthy and Slow

Banking is usually a first target

- Professional attackers want cash
- Value of an exploit diminishes over time
  - AV software starts to detect it
  - Patches become available
- So first focus is on high value attacks
  - Close to cash

- Banking

100% defence is impossible

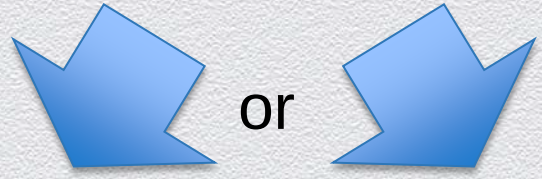
- Most defence is reactive
  - Cloud databases help AV to react really fast – but it's still reactive
- Anticipating attacks may prevent some
  - But every so often attackers will get through the defence

- Another layer of defence is required

Focus: Banking defence systems

Nature of attacks

- Target Log-in credentials
  - If the Cybercriminals can steal log-in credentials they can get full control over the cash in an account



- Steal by Phishing
  - Draw the user to a fake website
  - Pretend to be the Bank
  - Capture user Credentials as they are entered
- Steal by Key-logging
  - Get some malware on the users machine
  - Intercept key strokes / data as the user logs in to the genuine bank site

IP Banking fraud is familiar…

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Zeus Bank Malware Surges On Facebook

Old threat makes a comeback, targeting Facebook users' bank credentials and more.

By Mathew J. Schwartz, InformationWeek
June 05, 2013
URL: http://www.informationweek.co.uk/security/attacks/zeus-bank-malware-surges-on-facebook/240156156

(click image for larger view)
The Syrian Electronic Army: 9 Things We Know
Zeus malware, long popular with the cybercrime underground, has seen a resurgence in the first half of 2013, becoming a weapon of choice for attacks distributed via spam emails as well as social networks such as Facebook.

That finding comes from security firm Trend Micro, which has reported seeing a spike in attempted Zeus Trojan application infections beginning in February 2013 and peaking in May. Zeus malware targets personal and financial data stored on Windows PCs and is controlled via a "Zbot" botnet.

"Old threats like Zbot can always make a comeback because cybercriminals profit from these," said Jay Yaneza, senior technical manager at Trend Micro, in a blog post. "Peddling stolen banking and other personal information from users is a lucrative business in the underground market. Plus, these crooks can use your login credentials to initiate transactions in your account without your consent."

…but keeps reinventing itself

Enhanced defence – partial data

- Entering the entire password is high risk
  - One interception gives the attacker the ability to log-in

- Requesting partial data reduces the risk
  - 3 characters from 9 can take seven entries to capture all 9 characters
  - But…
    - It can be done in three
    - The crook decides that – not the bank

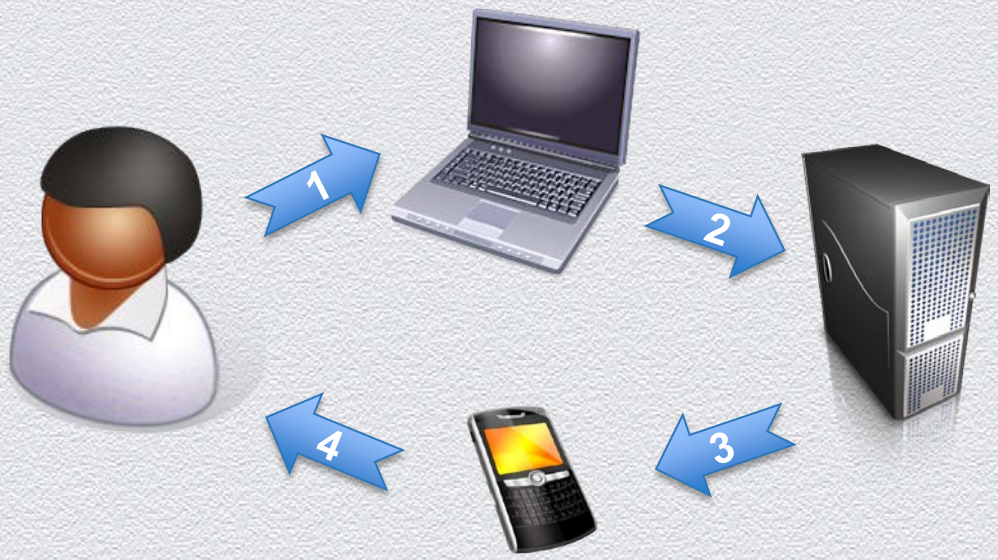
Secondary defence – Two step verification

- Something you have and something you know
  - Password is something you know
  - Need to add in something you have
    - Could be a token (ie RSA SecurID)
      - But people won't carry round a keychain full of them
    - Many banks are using the telephone
      - Provides a second, out of band way to check in with the customer

IP and Telephony combined

…Banks respond with “out of band” authentication…

- Using the Telephony channel
  - Voice or text
- Sometimes automatic
  - Part of the log on process
- Sometimes focused
  - New payee
  - High value transaction



…and the arms race moves on!

CRN

Malware Hijacks Two-Step Verification, Drains Bank Accounts

By Robert Westervelt, CRN 10:50 AM EST Tue. Jun. 11, 2013

Banking malware that has been notorious for stealing up to $200,000 a day for cybercriminal gangs has been updated to capture banking customer's text messages, hijacking a key verification service used in high-value transactions to validate the identity of customers.

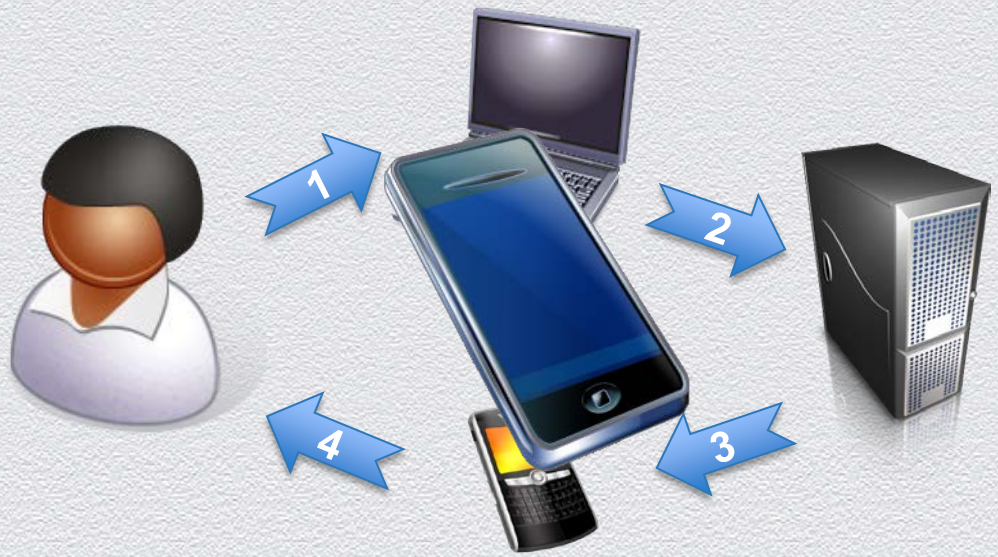
The Bugat Trojan, also known as Cridex, copied two-factor authentication hijacking from the Zeus and SpyEye malware families by adding a mobile text messaging capture feature. The malware is used by financially motivated cybercriminals that target individuals who conduct high-value transactions, according to Limor Kessem, a cybercrime and online fraud communications specialist at RSA's FraudAction Labs. The new technique actually is seen as good news, according to Kessem's analysis of the threat.

"It is very likely that Bugat's operators started seeing a diminished ability to target high-value accounts due to added authentication challenges, forcing them to resort to developing a malware component that is already used by many mainstream banking Trojans in the wild," Kessem wrote.

[**Related:** Top 5 Android Malware Threats]

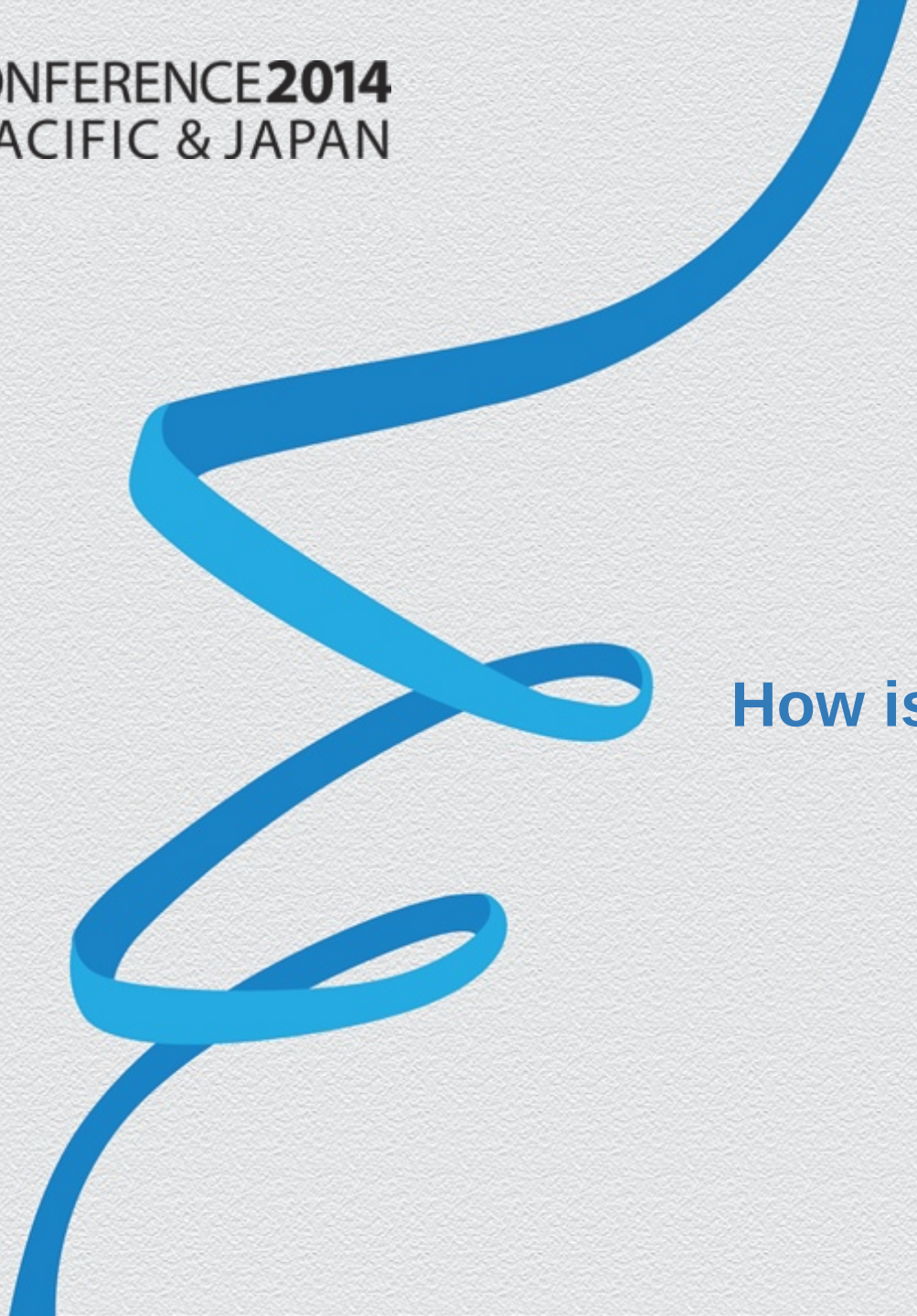
The authors of the Bugat Trojan are coming in late to the game, Kessem said. Zeus-in-the-mobile attacks are documented as far back as 2010. Security firms have been closely monitoring threats to mobile devices and see much of the mobile malware activity, a tiny fraction of the overall malware landscape, in Eastern Europe, Russia and Asia. Banking Trojans that hijack two-factor authentication are among the most dangerous attacks. Meanwhile, SMS Trojans that silently rack up premium text messaging charges are also a growing threat.

The main threat from Bugat and other banking malware is on the desktop, where the Trojan attempts to hijack the victim's browser session. It spreads via the Black Hole automated attack toolkit. The mobile functionality is triggered when two-factor authentication is requested to verify the victim's identity. Victims are then prompted by the cybercriminals to download the BitMo mobile malware to their Android, BlackBerry or Symbian phones as a result of a newly implemented data encryption policy instituted by the victim's bank.



Especially vulnerable if channels recombine

When the same device is used for web access and telephony



How is it done?

Malware

- New generation of Trojans emerging
- Keystroke logging, screen grabbing and call forwarding
- Examples:
  - ZitMo (Zeus in the Mobile)
  - SMS Zombie
  - Perkel
  - Wroba
- Lots of people talking about malware
  - But it's only one of several techniques being employed!

Call Victim
Pretend to be from their phone company

Sell a Story
"You have a problem on your phone line…"

Offer a Solution
Please type in the following numbers for me…

Numbers entered divert phone
Calls and texts

Execute Fraud
Security codes now sent to fraudster

Social Engineering of Victim

Classic fraud with a new spin

Insider Fraud

- Accomplice in phone company remotely redirects incoming calls and texts
  - Cross Operator?
- Can re-set the phone after a fraud
  - Very difficult to track after the event

SIM Swap

- Several legitimate reasons for changing your SIM card
  - New type of phone
  - Failure or loss
  - Moving service provider
- On inserting a new SIM the old SIM is locked out

Phish Victim
Research likely security Q&A

https://www.youtube.com/watch?v=F7pYHN9iC9I

Acquire Utility Bill
Shared hallway, dustbin or online billing

Go to Phone shop
Choses least experienced agent

Show mangled SIM card
"My dog ate it"

Insert new SIM
Victim's phone is now Pwned

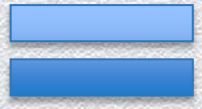
Execute Fraud
Security codes now sent to fraudster

SIM Swap Fraud

Social Engineering in the supply chain

“Pwn” both channels

- Capture the password
  - Malware
  - Phishing
- Capture the phone
  - Malware
  - SIM Swap
  - Network Call diversion



- Pwn both channels

A chilling tale

- http://www.bbc.co.uk/programmes/p00ylgk7

- I noticed that my mobile phone had no signal
- "£4,500 ($7,500 US) was taken from my bank account"
- "I rang home and the phone was answered by a man with an Eastern European accent"

Another example in the news…

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

Money › Banks and building societies

Hacking case exposes potential flaw in Halifax and Lloyds' security

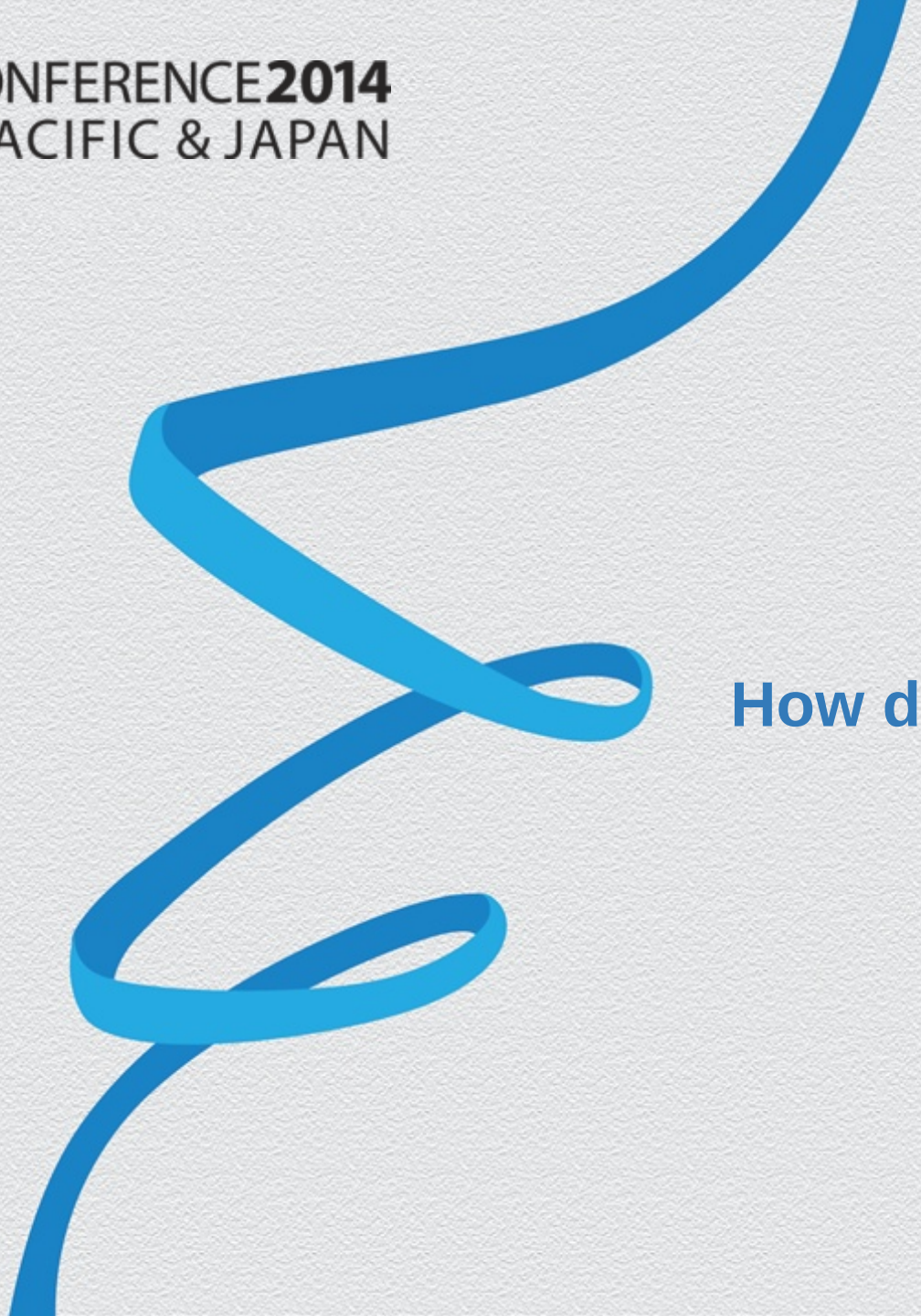
Hackers have found a way to get round a crucial step in Halifax and Lloyds online safety check

Miles Brignall
The Guardian, Friday 30 May 2014 10.43 BST
Jump to comments (42)

A reader exposes a bank security flaw. Photograph: Alastair Grant/AP

A Guardian Money reader has exposed a potentially major flaw in the security of the 22m current accounts operated by Lloyds and Halifax after hackers attempted to empty his account of £7,200.

- http://www.theguardian.com/money/2014/may/30/halifax-lloyds-banking-online-security-hacker
- Fraudsters have developed a way to get round one of the banks' crucial security checks for online account holders.
- Because they had earlier contacted BT (local phone company) to request a call divert to their own mobile and because they had already hacked into the account, the fraudsters could input the code.



How do you defend?

Telephony Fraud Check

What does the “Live Fraud Check” do?

SIM Swap

- Each SIM card has a unique code
  - IMSI – “International Mobile Subscriber Identity”
- If this code has changed then it’s because a new SIM card has been issued
- There are legitimate reasons why that happens
- But extra caution should be taken if it has

Call Divert

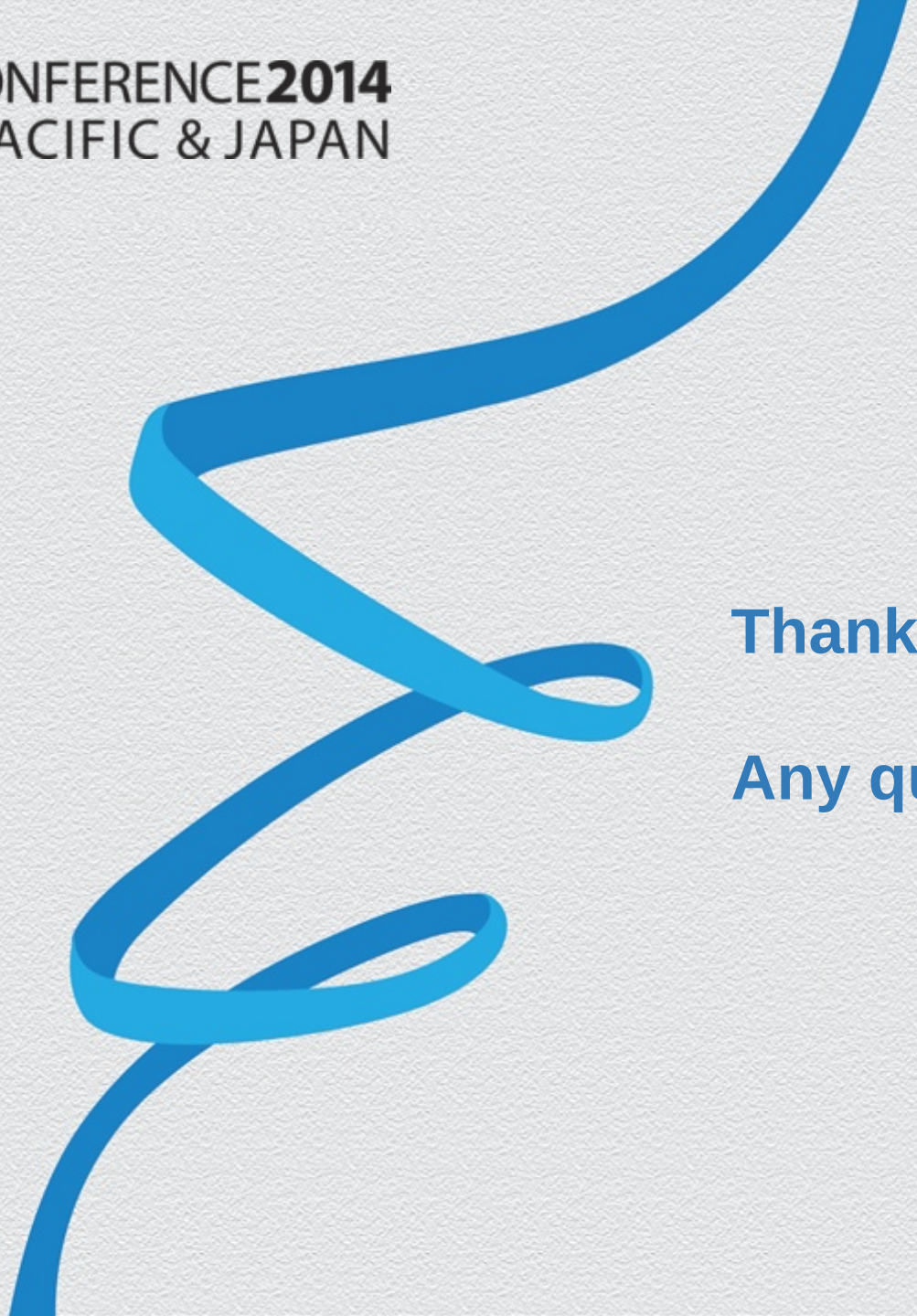
- The phone network switching system knows if a phone is diverted
  - There is no need to actually place a call to tell
- There are legitimate reasons for that
  - Divert to Answerphone
  - Divert landline to your mobile
- But it’s a caution flag

The good news

- You don’t need to be a phone system expert
  - No need to have low level access to the phone system
  - No need to understand the low level switching protocols
  - No need to integrate to lots of different Telco's
- You can now use a SaaS solution
  - Make a SOAP call before placing the customer call
  - Get back a confidence factor on how trustworthy that call is
- Also some Call Centre software providers are integrating the Telephony Fraud Check as an option from within their software

Conclusion

- Many banks and other secure services feel that customers prefer Telephony to separate security tokens for secondary authentication
- Fraudsters have responded with a series of techniques to compromise the Telephony channel
- Techniques now exist to secure the Telephony channel and get back ahead of the fraudsters
- What's next?



Thank you

Any questions?