The Tenets of e-Banking Security

Classification**: Restricted to e-Crime Delegates**
Place & Date: London, 13-14 March 2012

sponsored by:

EISST Ltd
Fairfax House,
15 Fulwood Place
London WC1V 6AY, UK
T: +44 (0)20 79 695 688
F: +44 (0)20 77 483 273
E: info@eisst.com
W: www.eisst.com

HOW BAD IS IT REALLY?

The general consensus among IT security professional organizations regarding the pecentange of malware-infected PCs is:

A. Less than 20%

B. Less than 30%

C. More than 30%

Answer: C

79% of banks surveyed in 2011 said that malware was in their top three security concerns.
Gartner Report: The Five Layers of Fraud Prevention – April 2011

WORKING ASSUMPTION #1

The End User's computer is controlled by Malware

REALISTIC

RELEVANT

WHY IS IT STILL A PROBLEM?

Financial malware fraud is a major concern to Banks and causes considerable losses. The reason is:

A. we haven't still figured out the right security technology

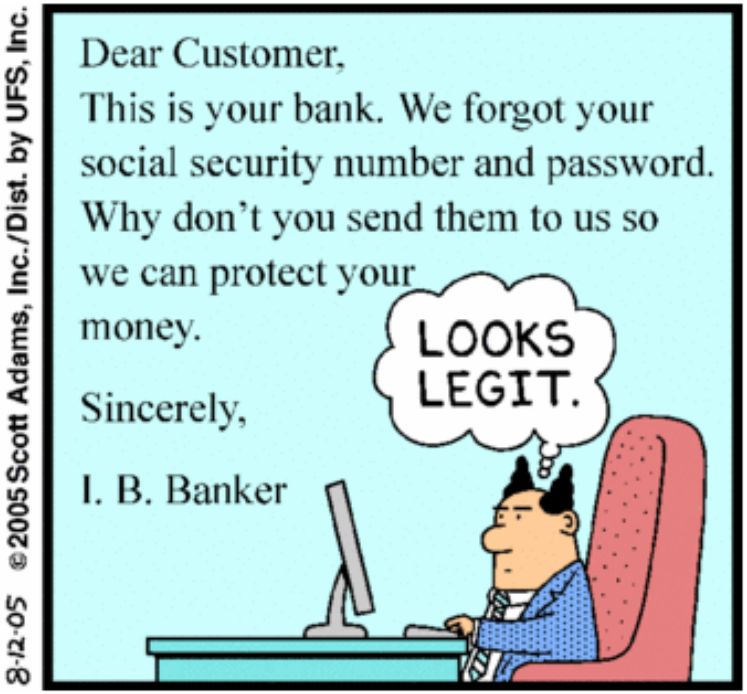
B. current solutions are too complex for a mass deployment

C. e-criminals are simply too smart and motivated

D. the security ROI doesn't justify the deployment costs

Answer: D (for the Banks – the End Users' perspective is obviously very different…)

WORKING ASSUMPTION #2



The End User trusts the Bank
(and whoever else claims to be the Bank)

WHAT ARE WE LOOKING FOR?

The main result of deploying best-of-breed e-Banking security solutions should be to:

A. maximize detection of malware and fraud attempts

B. raise the percentage of legitimate transactions

C. minimize financial losses due to online fraud

Answer: B (what use would it be to have perfect security but no transactions? Of course, the answer of choice when asking Bank officials is C...)

WORKING ASSUMPTION #3

A Security Solution should be evaluated based on how it performs under typical attack conditions

i.e. based on how well it supports the Internet banking business model (**encouraging customers to transact online**)

WHAT IS TRANSACTION EFFICIENCY?

The ability to reduce the level of exposure to online fraud while ***enabling*** a growing number of legitimate transactions.

→ By design, Web Fraud Detection methods can only lower the transaction efficiency: *i.e.* at best under attack the response is to abort the transaction

→ Web Fraud Prevention methods can actively protect against malware attacks, achieving higher security without degrading transaction efficiency by allowing to transact also using an infected PC.

ARE THINGS GOING TO GET BETTER?

Will malware detection techniques and active protections eventually thwart malware threats?

A. yes

B. no

C. don't know

Answer: B

In 2012 hackers will shift their focus to exploiting vulnerabilities in the browsers themselves (rather than in add-ons) in order to install malware. The reason is due to recently added browser functionalities, mainly driven by the adoption of HTML 5 standard.
Imperva: Security Trends 2012– December 2011

WHAT CAN WE DO ABOUT IT?

The best authentication method against attacks launched by financial malware (*e.g*. SpyEye) is:

A. biometric token

B. one time password token

C. out of band (*e.g.* mTAN)

D. None of the above

Answer: D

No authentication measure on its own, especially when communicating through a browser, is sufficient to counter today's threats. Additional fraud prevention layers must be utilized.
Gartner Report: The Five Layers of Fraud Prevention – April 2011

AN AUTHENTIC ILLUSION

The use of biometric or multi-factor authentication methods creates only the illusion of stronger security, while attackers have since long focused on exploiting the vulnerabilities to be found *down-stream* of the authentication step.

In other words, the character and details of the sole authentication step cannot be considered to be linked in any meaningful way to the practical security of online e-banking transactions.

WHAT ABOUT MOBILE OUT-OF-BAND?

Transaction verification using the mobile phone as out-of-band secure channel has not yet been hacked

A. true

B. false

C. don't know

Answer: B

The number of Android malware increased by 800 % from February to May of 2011 alone! …. Google estimates that there are currently 100 million active Android-based mobile devices, which is expected to continue increasing at an estimated 400,000 devices per day.
TrendLabs: Android Malware acts as SMS Relay - August 2011

BEYOND AUTHENTICATION

In order to be linked in a meaningful way to the practical security of online transactions, the acts of identification and authentication must be integrated and stretched across a single coherent process inclusive of the various information and components necessary for a specific transaction to take place.

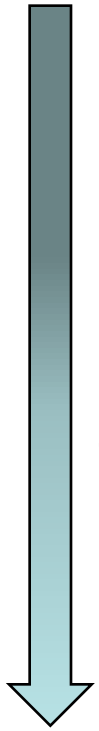
The **INDIVIDUATION** act extends *beyond* the identification and authentication factors to include information on *what you use and do* to transact, most noticeably the details of the client application(s) and device(s), the network location, the operating system's context and your online behavioral patterns.

TRANSACTION INDIVIDUATION

FACTOR DESCRIPTION	EXAMPLE
a secret known only to the user	PASSWORD
a hardened client application	SECURE BROWSER
a unique digital secret	PRIVATE KEY
an external crypto processor	SMART CARD
an external tamper-proof storage	USB DEVICE
an external display	POS DEVICE
an external keyboard	POS DEVICE
behaviour analytics	SERVER APP
application analytics	SERVER APP

TRANSACTION INDIVIDUATION

FACTOR DESCRIPTION	EFFICIENCY
a secret known only to the user	high
a hardened client application	
a unique digital secret	
an external crypto processor	
an external tamper-proof storage	
an external display	
an external keyboard	
behaviour analytics	
application analytics	low



CLIENT

THIRD PARTY

SERVER

OTP DEVICE

FACTOR DESCRIPTION		
a secret known only to the user		PASSWORD
a hardened client application		
a unique digital secret		
an external crypto processor		OTP DEVICE
an external tamper-proof storage		
an external display		
an external keyboard		
behaviour analytics		
application analytics		

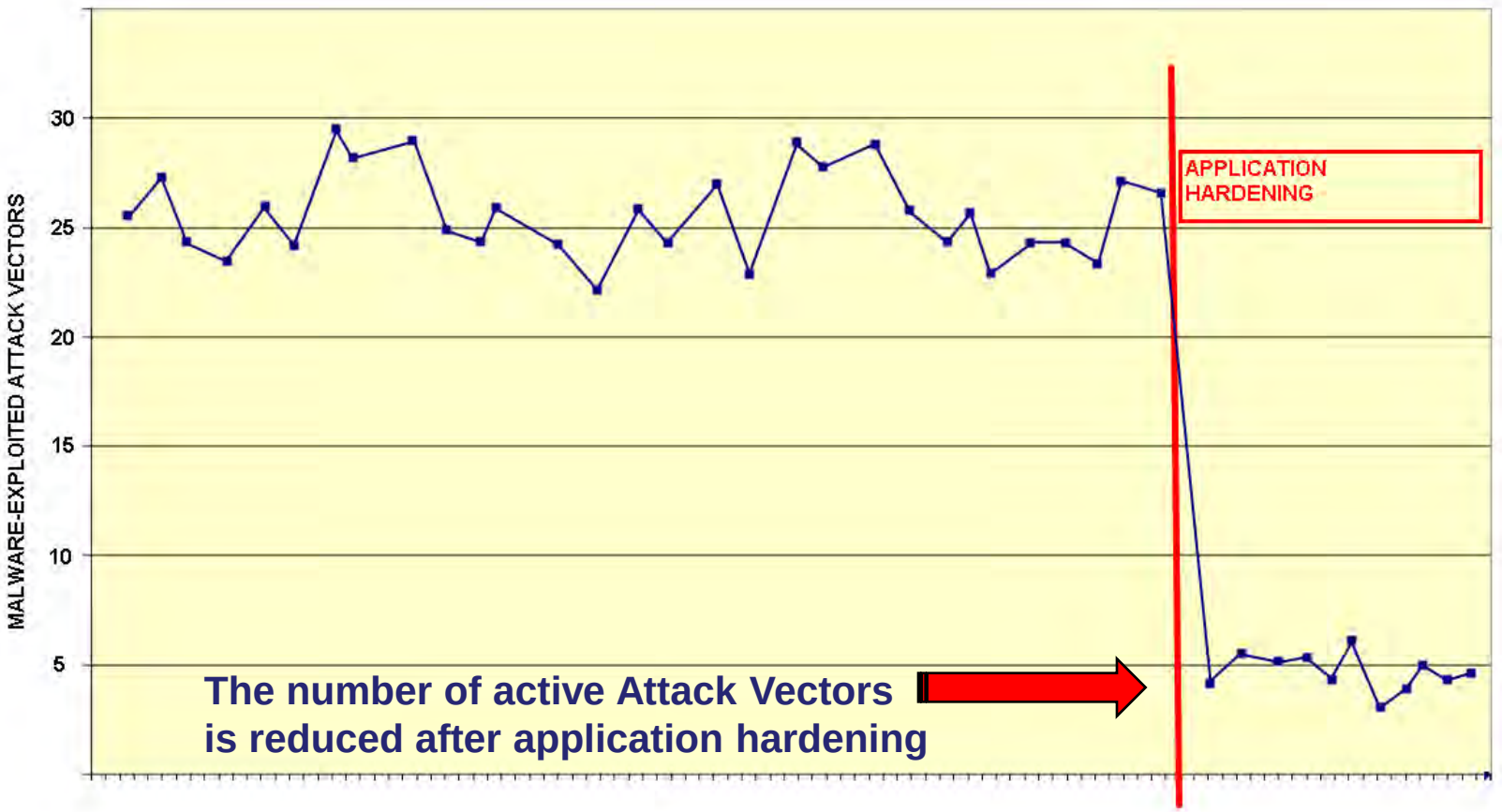
CHIP & PIN

FACTOR DESCRIPTION		
a secret known only to the user		PIN
a hardened client application		
a unique digital secret		PRIVATE KEY
an external crypto processor		SMART CARD
an external tamper-proof storage		KEY STORE
an external display		
an external keyboard		
behaviour analytics		
application analytics		

SECURE USB + BROWSER

FACTOR DESCRIPTION		
a secret known only to the user	✓	PIN
a hardened client application	✓	SECURE BROWSER
a unique digital secret	✓	PRIVATE KEY
an external crypto processor	✓	SMART CARD
an external tamper-proof storage	✓	KEY STORE FLASH MEMORY
an external display	✗	
an external keyboard	✗	
behaviour analytics	✗	
application analytics	✗	

Application Hardening Disables Malware



SESSION MONITORING

FACTOR DESCRIPTION		
a secret known only to the user	✓	PASSWORD
a hardened client application	✗	
a unique digital secret	✗	
an external crypto processor	✗	
an external tamper-proof storage	✗	
an external display	✗	
an external keyboard	✗	
behaviour analytics	✓	NAVIGATION PATTERNS
application analytics	✗	

SUMMARY OF FINDINGS

Banks consider malware their biggest immediate threat.

No single layer of fraud prevention or authentication is enough especially when communicating through a browser.

Multiple layers must be employed to defend against today's attacks. Fraud detection alone cannot grant high efficiency.

*Deploy **both** secure browsing **and** out-of-band or dedicated hardware transaction verification for high-risk transactions as complementary measures to existing authentication methods.*

→ By 2014, Gartner estimates that 15% of enterprises will adopt layered fraud prevention techniques to compensate for weaknesses inherent in using authentication methods only.

BEST OF BREED INDIVIDUATION

FACTOR DESCRIPTION		
a secret known only to the user	✓	PIN
a hardened client application	✓	SECURE BROWSER
a unique digital secret	✓	PRIVATE KEY
an external crypto processor	✓	SMART CARD
an external tamper-proof storage	✓	KEY STORE FLASH MEMORY
an external display	✓	DEDICATED HARDWARE
an external keyboard	✓	DEDICATED HARDWARE
behaviour analytics	✗	
application analytics	✓	BROWSER AUTHENTICATION

The FUTURE….. TODAY

- ✓ STRONGEST Security (HW+SW+FW)
- ✓ High Usability
- ✓ AES256 HW Encryption
- ✓ Smart Card (FIPS/CC)
- ✓ Firmware updates in the field
- ✓ On-board H-Applications™
- ✓ Display and Keypad integrated
- ✓ External slot for SIM-size smart cards
- ✓ GUI Enabled
- ✓ Up to 32GB Flash storage
- ✓ Multi Platform (Win, Mac, Linux)
- ✓ Stainless steel housing

EISST

H-Token Marco Polo

Flash Memory

- Flash memory: 2 GB (default) up to 32GB
- Multi-partitions support
  - CDROM and/or Read-Only
  - Public or Private (encrypted)
  - Hidden (raw access)
- AES-256 CBC hardware encryption
- Read performance
  - up to 10MB/s in single flash mode
  - up to 20MB/s in dual flash mode
- Write performance
  - up to 6MB/s in single flash mode
  - up to 10MB/s in dual flash mode

Smart Card

- Cryptographic smart card chip
- Common Criteria EAL 4+ for the chip
- NIST CAVP/FIPS approved hw implementation of: RSA1024, RSA2048, AES256, 3DES, RNG
- Memory Protection
  - Bus/memory encrypted
  - Memory access control and protection
- Secured against DPA/SPA attacks
- Secure channel with H-Token Middleware

Certifications

- USB 2.0, CE
- SSCD Certified
- FCC
- RoHS

Flash Controller

High performance flash memory controller with hardware accelerated AES-256 CBC encryption

Integrated Smart Card Reader

- slot for ID-000 cards

Interfaces and Standards

- Integrated keypad for secure PIN entry
- 1.8" TFT display (176x220, 65K colors)
- Keypad & display controlled by internal smart card

EISST

CONCLUSIONS

- Don’t rely on the “strength” of authentication, think endpoint identification and transaction **individuation**
- Hacking the endpoint client application (man-in-the browser) provides a devastating advantage to e-criminals and allows them to control the user experience (via the **social engineering** attack vector)
- Browser **architectural hardening** is essential to force malware attacks to be very complex and to reduce the criminals’ ROI
- Mobile out-of-band has been hacked and will become increasingly insecure as **mobile malware attacks grow in volume and sophistication**.
- **Multiple layers** must be employed to defend against today's attacks. Fraud detection alone cannot grant high efficiency.
- Secure browsing and hardware transaction verification on a dedicated secure channel is today a viable technology and is massively deployed by leading Banks in Switzerland: **www.crealogix.com/en/products/banking-products/e-banking-security/ clxsentineldisplay**

THANK YOU!

FOR FURTHER INFORMATION: cronchi@eisst.com

EISST Ltd
Fairfax House,
15 Fulwood Place
London WC1V 6AY, UK
T: +44 (0)20 79 695 688
F: +44 (0)20 77 483 273
E: info@eisst.com
W: www.eisst.com