VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016

Delivering a SECURE customer experience within the banking and retail environment

Terence Devereux
Senior Trusted Advisor, Wincor Nixdorf International

ISACA® Istanbul Chapter
Bilgi sistemlerinde güven ve katma değer

www.btyd.org.tr

while this is still a dream for some companies

it is actually closer that some people think

touch

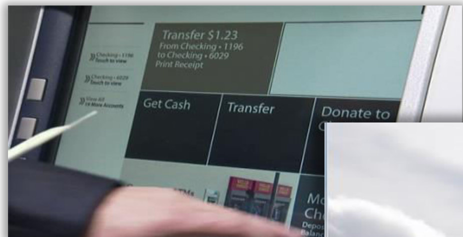
tap

cash

Cardless cash with existing mobile apps.

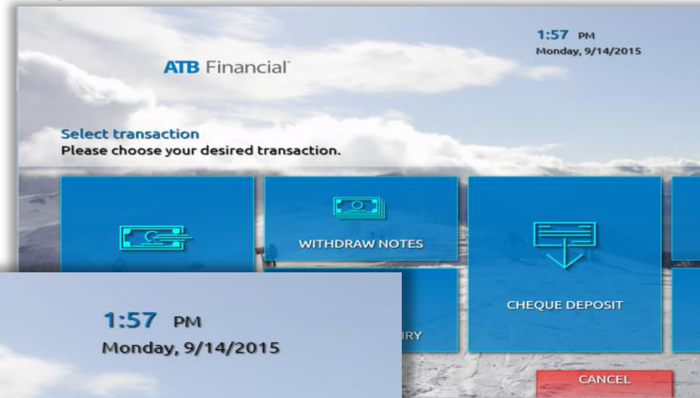
MyATM - Fast and Easy…

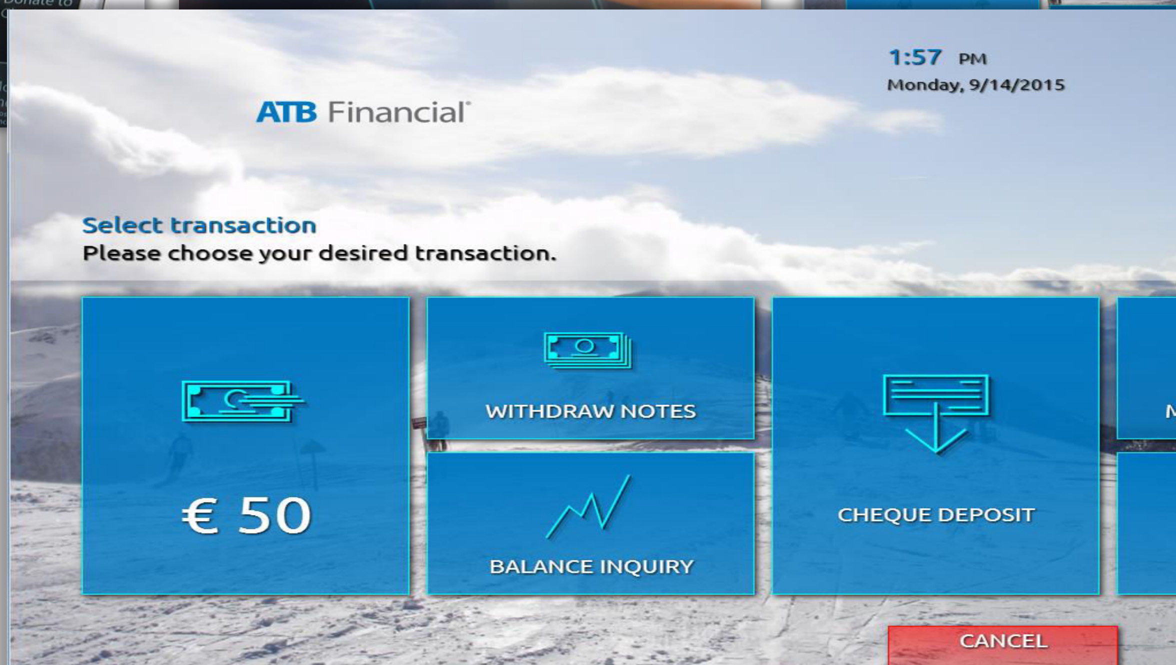
Functionally
enriched interface



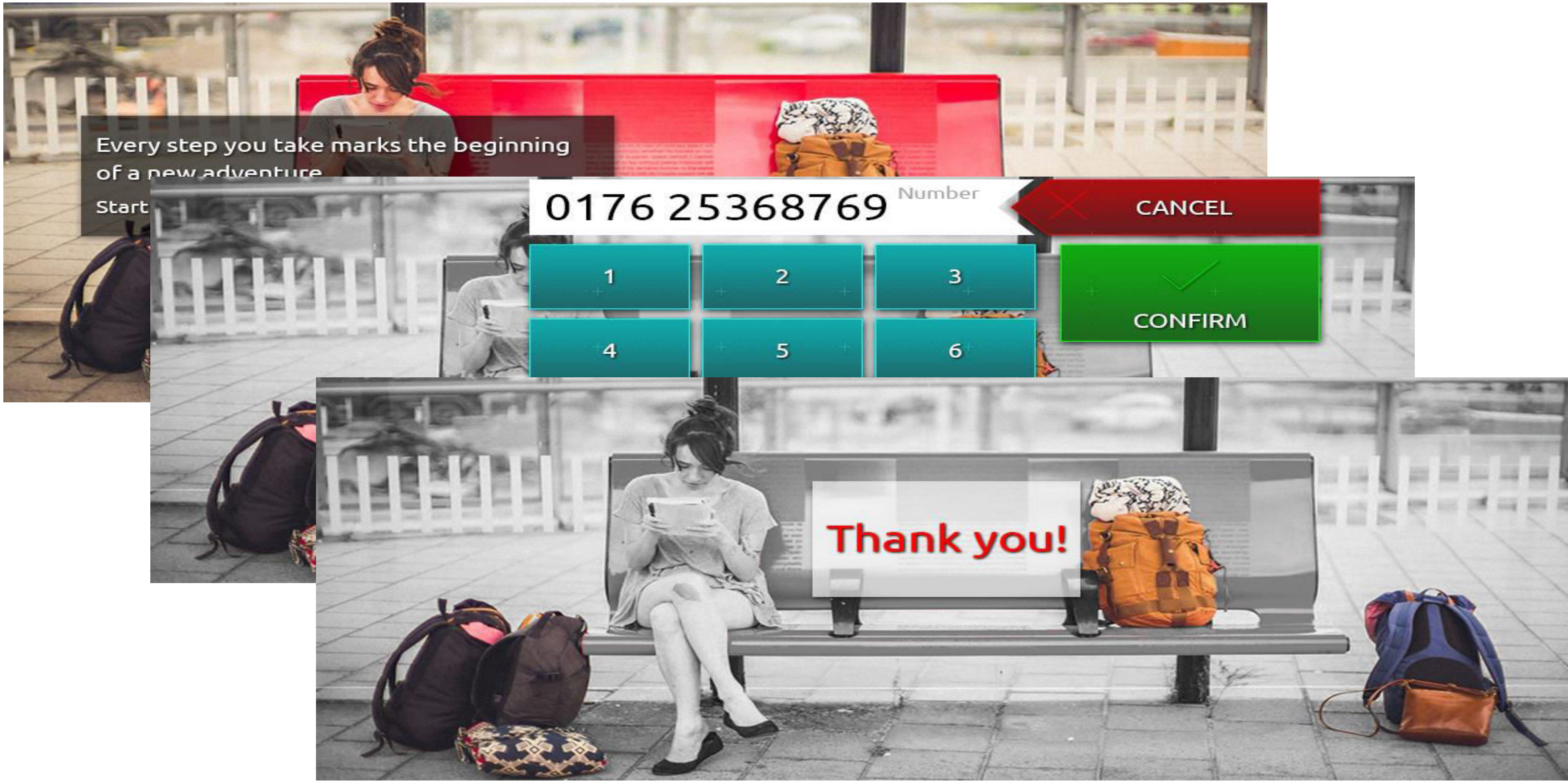
Usability
enriched interface

MyATM





in an attempt to connect, banks and retailers have deployed the google / apple strategy



this is happening everyday somewhere

Target

$162 million – 70M cards exposed

Home Depot

Cost $62M - 56M cards exposed

Hilton Hotels

Hilton identified and taken action to eradicate unauthorized malware that targeted payment card information in some point-of-sale systems.

Trump Hotels

Memory-scraping malware *Punkey* infect POS systems. Infection latest for more than a year.

this is happening every day somewhere

Canada

variant of the known “Tyupkin” attacks Canadian ATM’s,

Malaysia

Hackers steal approx. US$1.2 million from ATMs belonging to 4 different banks

England

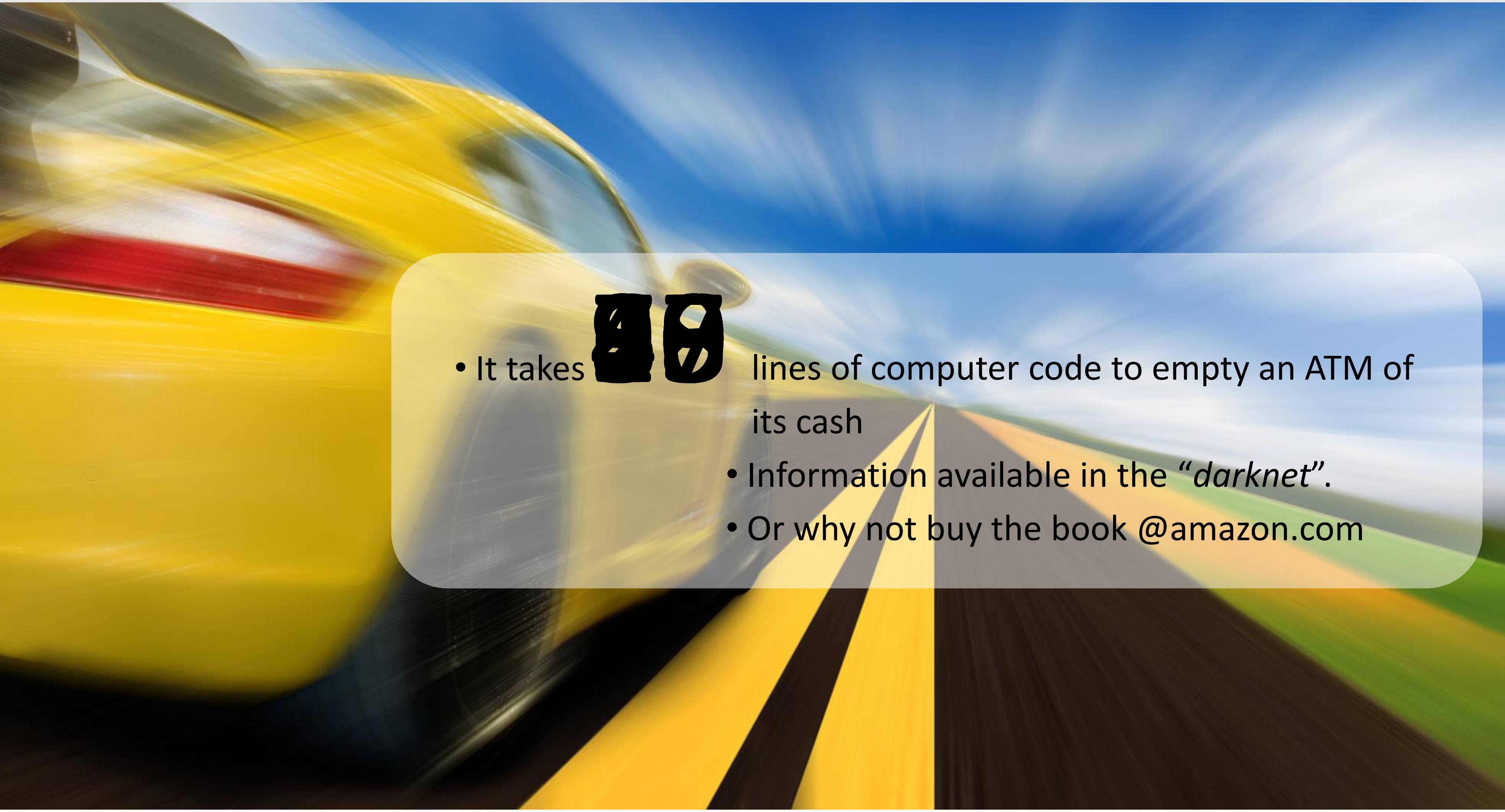
Hackers 'ordered ATM to dispense UK£10 of millions from UK banks’

Mexico

Proofpoint research discovered yet another variant of ATM malware dubbed GreenDispenser.


EVERYTHING IS UNDER CONTROL
DENZEL WASHINGTON
MERYL STREEP
LIEV SCHREIBER
THE MANCHURIAN CANDIDATE

these attacks have been made possible due to the emergence of the Internet, the Darknet etc. Knowledge has become freely available.



- It takes [illegible] lines of computer code to empty an ATM of its cash
- Information available in the "*darknet*".
- Or why not buy the book @amazon.com

open (commoditize) driven environment which also enable criminals to commoditize their malware

Europol Unclassified - Basic Protection Level (BPL)

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

The Hague, September 2015
Intelligence Notification 30 -2015

CYBER BITS
Series: Trend

New ATM malware targeting credit card holders: SUCEFUL

What happened?

A new piece of ATM malware has been detected [1] named as Backdoor.ATM.Suceful (the name comes from a typo made by the malware authors), which targets cardholders and is able to retain debit cards on infected ATMs, disable alarms, or read the debit card tracks. Based on its timestamp, it was likely created on August 25, 2015.

How does it work?

Similar to Ploutus [2] and PadPin[3], SUCEFUL interacts with a middleware called XFS Manager, which is part of the WOSA/XFS[4] Standard that major vendors comply with. The XFS Manager is the interface between the application (malware in this case) and the peripheral devices (e.g. dispenser, card reader and pin pad).

Once a session has been opened, the malware will request specific operations to the peripheral devices such as:

1

what the security industry has identified over he years

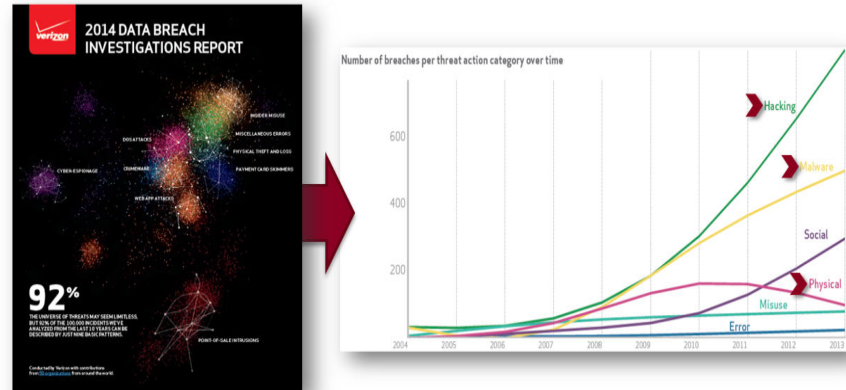
Analysis shows that the preferred attack of choice is Malware and Hacking with ATM's and PoS (Point of Sales) being the preferred targeted assets

WINCOR NIXDORF

Source : http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

This trend was restated in the 2014 report which also showed the shift and usage of Malware – Hacking is in comparison to physical e.g. Skimming, Trapping, explosions etc.

WINCOR NIXDORF



Source : http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

From a timeline perspective, a clear shift to ATM malware began in 2006–2007

WINCOR NIXDORF

2006 Tranex machine reprogrammed to dispense $20 Bills Are $5 Bills. https://www.schneier.com/blog/archives/2006/09/programming_atm.html

2008 FBI Investigate theft of 1.5 million cards with loss of withdrew more than $9 million from automated teller machines (ATMs) worldwide. http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

2009 Rogue bank software develever develops malware on employee's ATM. http://www.wired.com/2010/04/malware-targeted-100-atms/

2009 US National Security Agency called in to investigate malware attacks on ATM attack carried out in Russia and Ukraine http://nakedsecurity.sophos.com/2009/03/17/credit-card-skimming-malware-targeting-atms/

2010 Barnaby Jack demonstrated the Scrooge Root Kit/Jackpotting at the Black Hat security conference in 2010. black hat http://www.wired.com/2010/07/atms-jackpotted/

2010 / 2011 Visa Alert motifying of Malware taking advantage of non-PCI Encrypted Pin Pads deployed in Russia –Ukraine.

2013 BlackBox attack executed in various countries in the South America (Brazil, Mexico etc.) http://www.ncr.com/newsroom/resources/mexico-black-box-attacks

2013 Initial version of Backdoor.Ploutus found in South America. http://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico

2013 VISA Visa issue alerted of new cases where ATM Cash-Out frauds have been successfully executed. Malware believed to be a variation of Backdoor.Ploutus. http://krebsonsecurity.com/wp-content/uploads/2013/01/DataSecurityAlert_ATM-CashOut_Jan2013_v1.pdf

2014 Cyber criminals armed with custom-built malware stole an estimated 56 million debit and credit card numbers from its customers between April and September 2014. http://krebsonsecurity.com/tag/home-depot-breach/

2014 Media outlets in Malaysia reported that organized crime gangs had stolen the equivalent of about USD $1 million with the help of malware they had installed on at least 18 ATMs across the country. Similar attacks have bee recorded in UK, France, Russia, Ukraine, China, Canada, USA Germany as well as in South America. http://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/

2015 Malware such as *SUCEFUL*, *GREENDISPENSE* and variations of Ploutus have been found on ATM's around the globe.

2016 **Industry is bracing themselves for potential even more sophisticated malware attacks.**

2017 ?

The spread of the recent ATM malware

WINCOR NIXDORF

- Principle development in Russia and Ukraine
- After a given brooding time it migrated across the Atlantic ocean to Latin America
- This and other strains of malware has been observed in various other countries e.g. Argentina, Colombia, Venezuela, Peru, China, UK, France, Russia, Ukraine, USA, China, Germany, Malaysia, Jordan, Canada etc.

from being a Closed (proprietary) based to a Open (commoditized) driven environment

X.25 – SNS	TCP IP
Client – Host	Web Services
Direct I/O.	CEN (J/)XFS
NDC, DDC, ….	IFX, XML, …
Fixed Screen	HTML 5, CSS

the commoditization of the banking / retail env. is supporting the criminals in the goal of achieving a greater Return of Investment

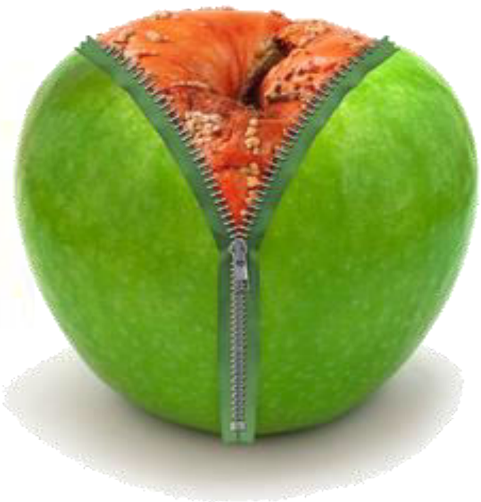
Over *727 vulnerabilities have been identified in the Microsoft XP operating system

****Up to now 481 vulnerabilities have been found in the Windows 7 operating system**

Microsoft

*http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html
**http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/Microsoft-Windows-7.html

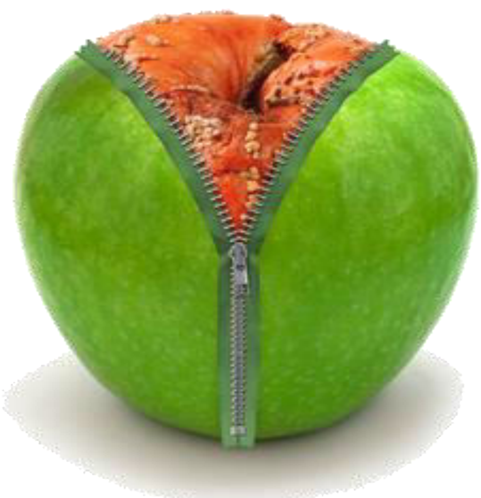
can you recognise the GOOD and BAD apple ?



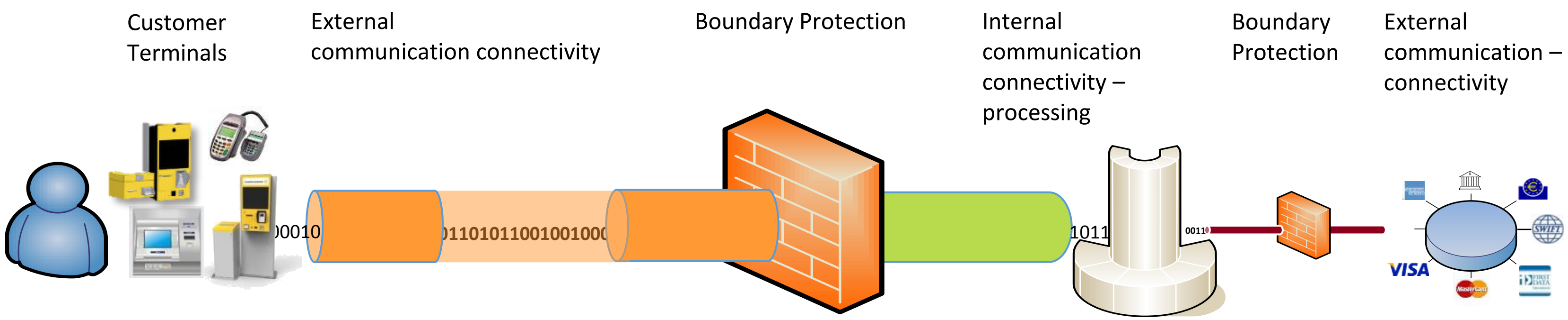
can you recognise the GOOD and BAD apple ?

The old adage “*never judge a book by its cover*”.

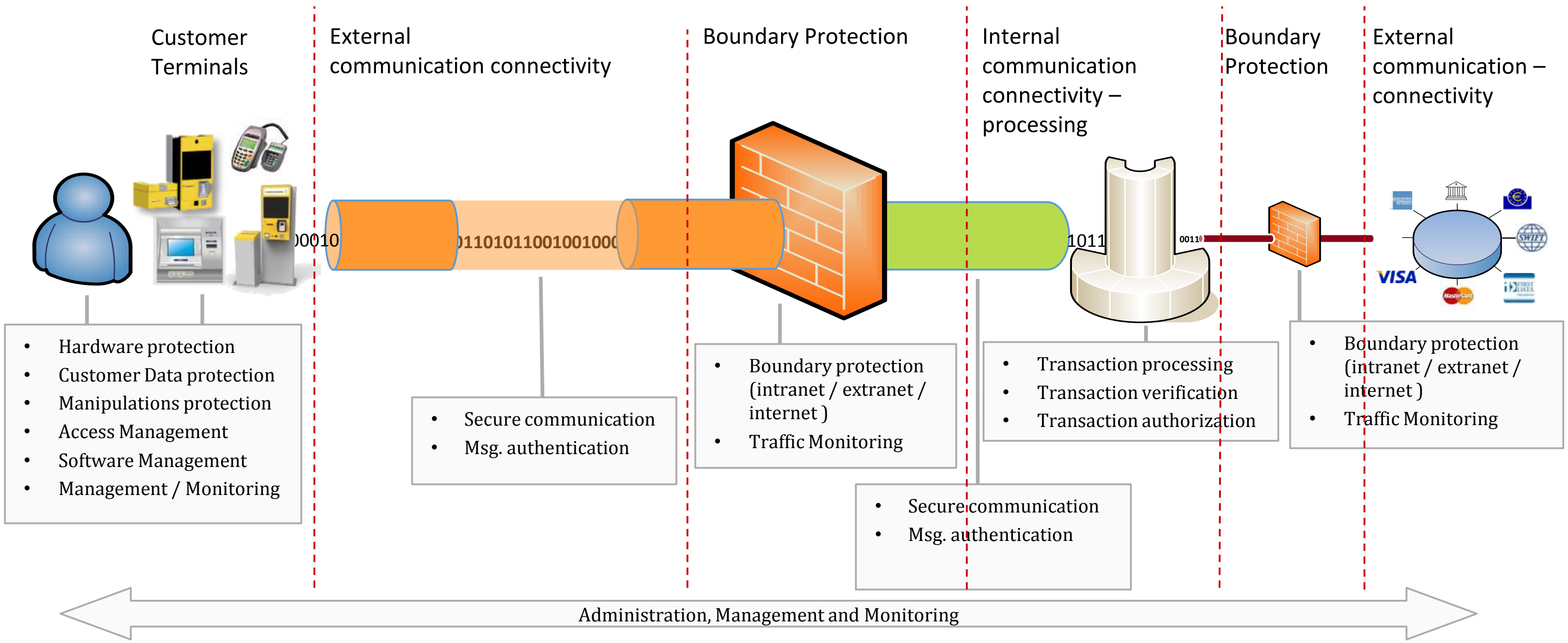
- Rogue bank software developers create and install malware inside employee’s ATM (http://www.wired.com/2010/04/malware-targeted-100-atms/)
- Framework POS derived from the **McAfee antivirus agent it impersonates**



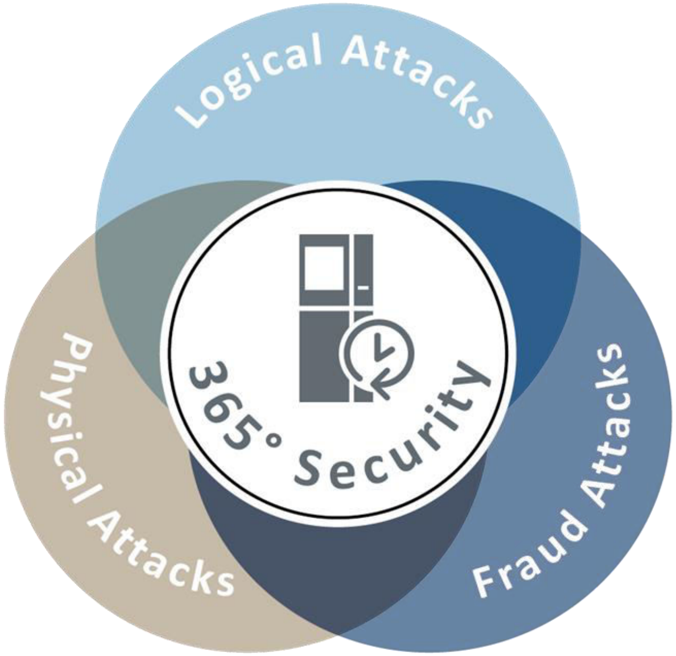
some elements within the payment chain which must be protected

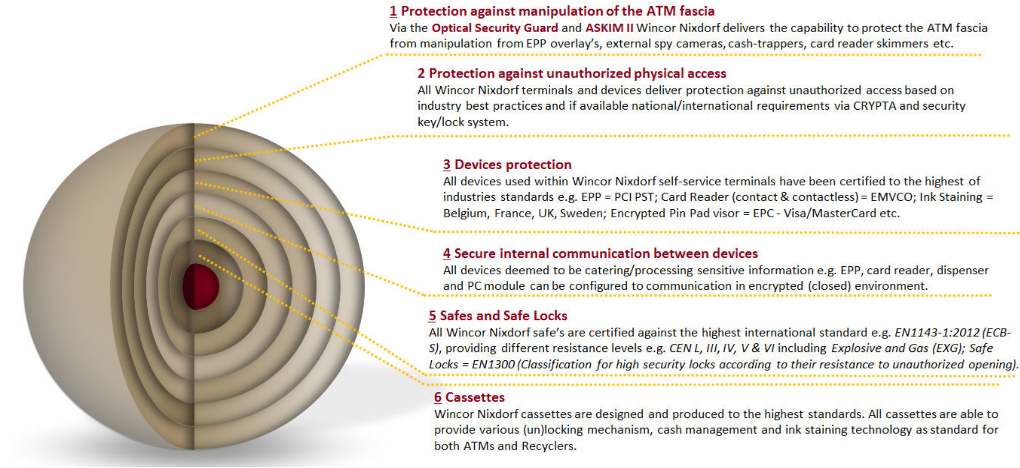


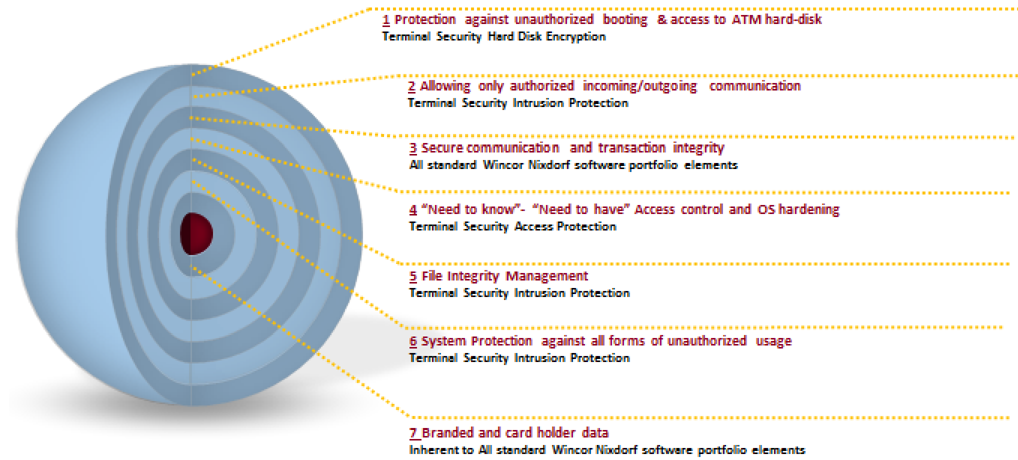
some elements within the payment chain which must be protected



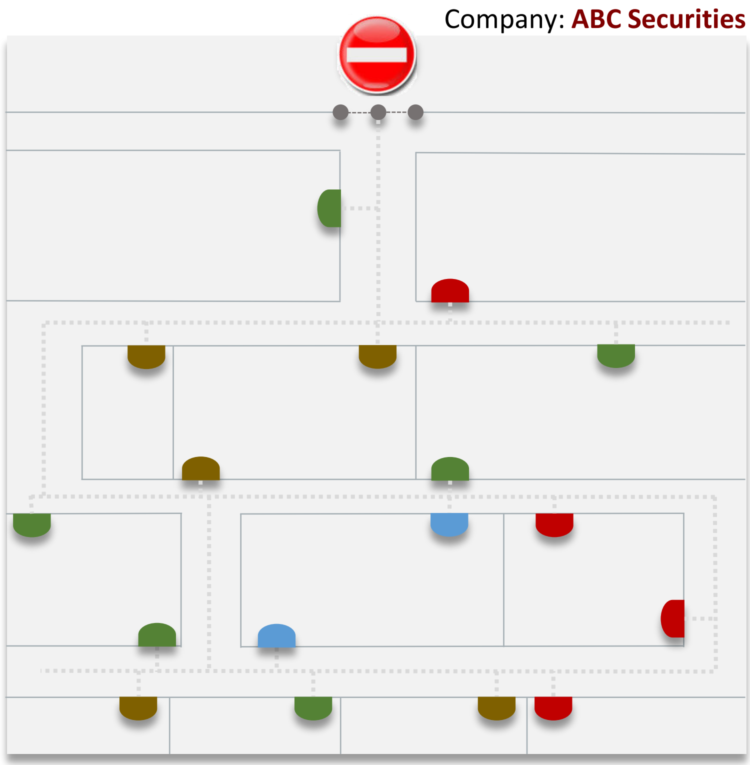
in form of a general company presentation by introducing the Onion model







traditional protection is lacking

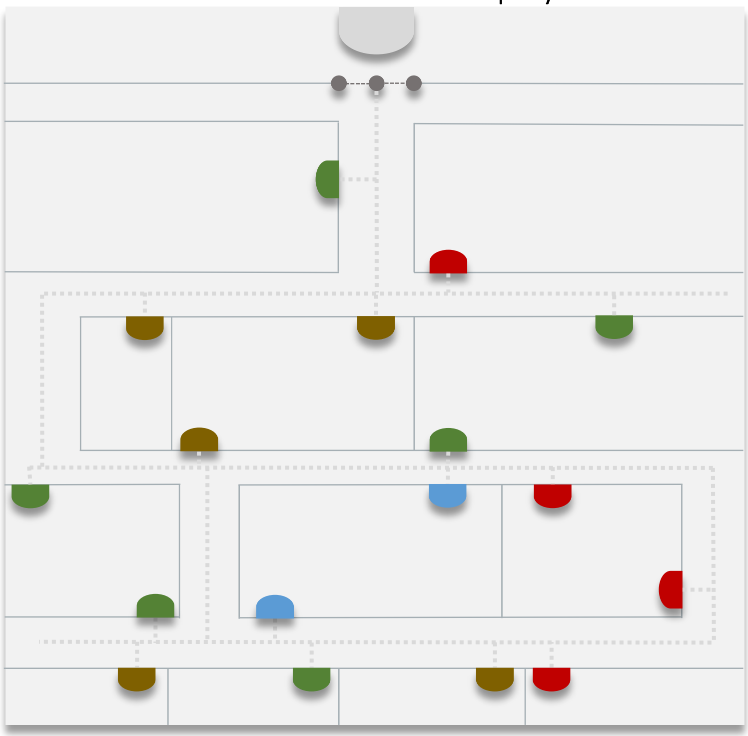


Blacklisting

- When somebody (***or something*** e.g. software component) is contained within a **Blacklist** they will be recognised blocked.
- However the electronic fingerprint of the malware has to recognised and a Blacklist entry created.

traditional protection is lacking

Company: **ABC Securities**

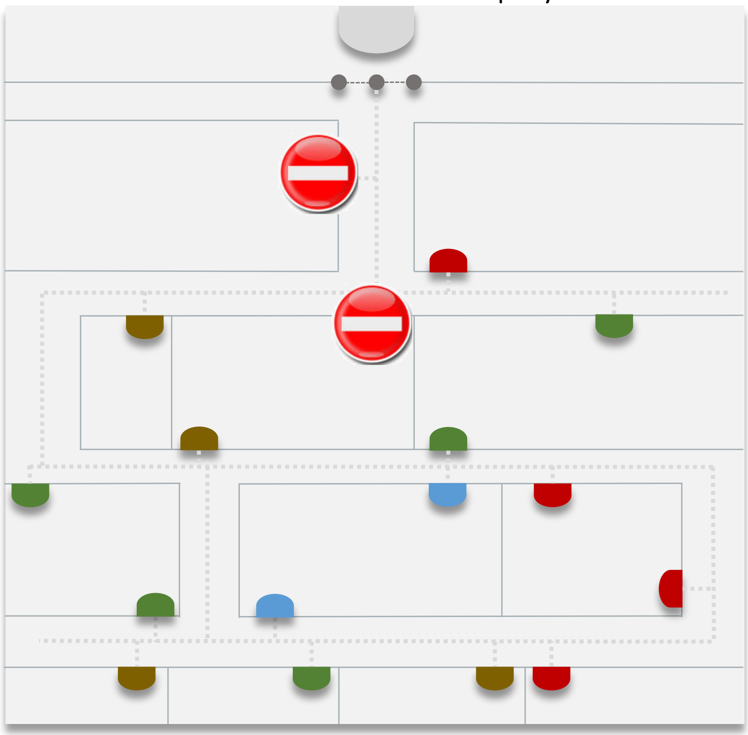


Whitelisting

- Access is given based on the person having a valid ID card (valid entry on the Whitelist).
- Unfortunately once they have an entry they have unlimited access.
- Detection of rogue software / behaviour, due to their TRUESTED status is near too impossible.

evolving security based on lessons learned with neural – fuzzy logic based solutions

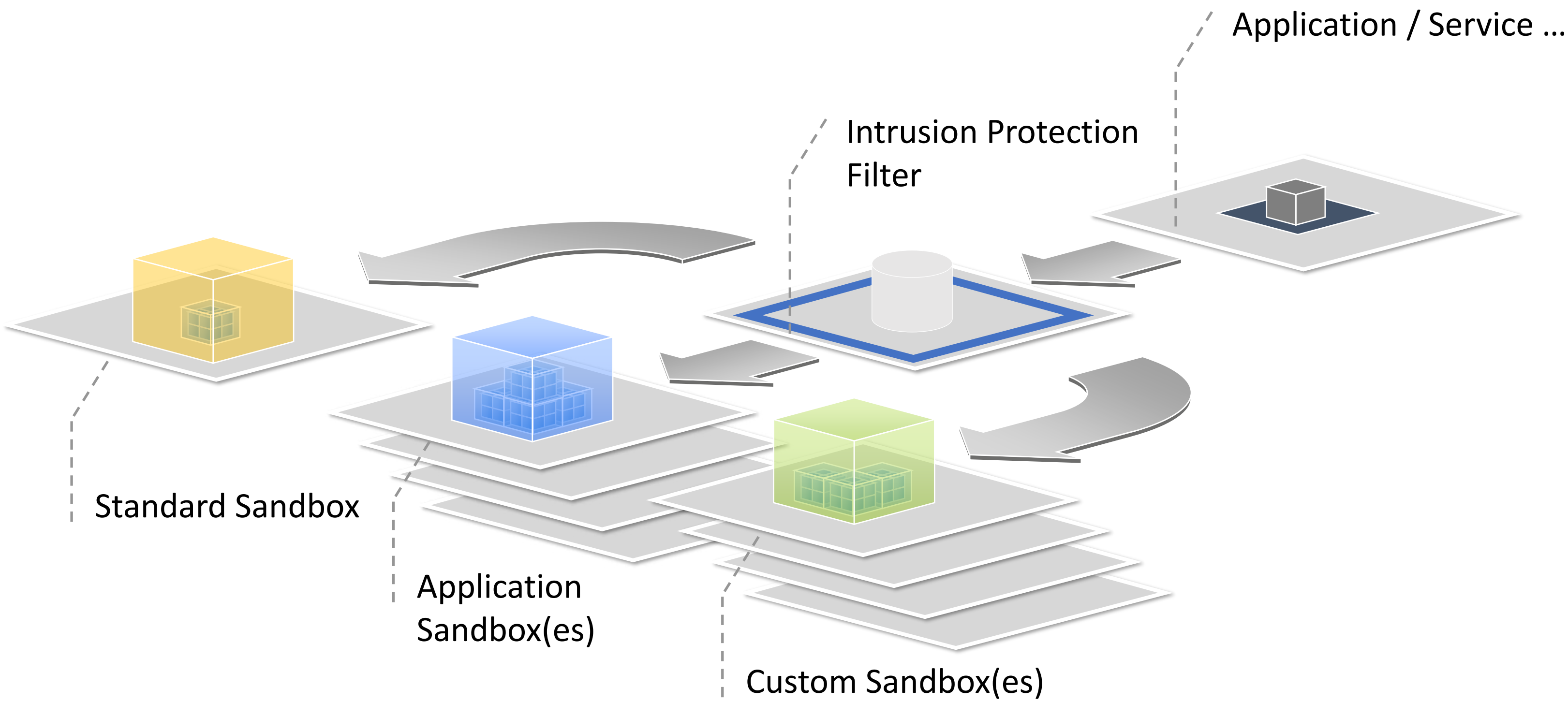
Company: **ABC Securities**



Behaviour based

- Security based on **TRUST**
- **TRUST** is allocated on individual requirements and constantly monitored
- All inclusive, incorporating the various software layers, device usage, software dist. – inst. and system servicing
- Real-time identification of anomalies

Wincor Nixdorf's **Zero Trust** concept



Wincor Nixdorf’s **Zero Trust** concept

- **Zero Trust** concept where there is no default trust for anything — incl. users, devices, applications, communication both internal and external etc…..
- establishes **Zero Trust** boundaries whereby everything is compartmentalize, isolated from it’s surroundings.
- a **Zero Tr**ust concept protects critical intellectual property from unauthorized applications and malware, Reducing the Exposure of vulnerable systems, Mitigating Risk and preventing lateral movement of malware throughout your network.

Wincor Nixdorf's **Zero Trust** concept for retail and banking terminals

Access Protection
Delivering Self-Service **Security Governance** and **Hardening** to the Microsoft Operating Systems based on Security, Industry and self-service best practice e.g. PCI, *SANS, *NIST, *FFIEC, ATMIA.

Intrusion Protection
Delivering protection against all forms of malware, unauthorized usages of and access to system resources e.g. software services, memory, registry, file system, communication, devices etc.

Terminal Security consists of **3 components** each delivering protection against inherent system exploits and vulnerabilities and the various forms of malware attacks

****Hard Disk Encryption**
Delivering protection to all contents on the Self-Service Terminals hard disk from booting via unauthorized mediums (CDROM, USB Sticks etc.) and access to if removed from original self-service terminal environment.

ISACA®

Bilgi sistemlerinde güven ve katma değer

Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016

Thank you for paying attention.

Terence Devereux
Senior Trusted Advisor, Wincor Nixdorf International

www.btyd.org.tr