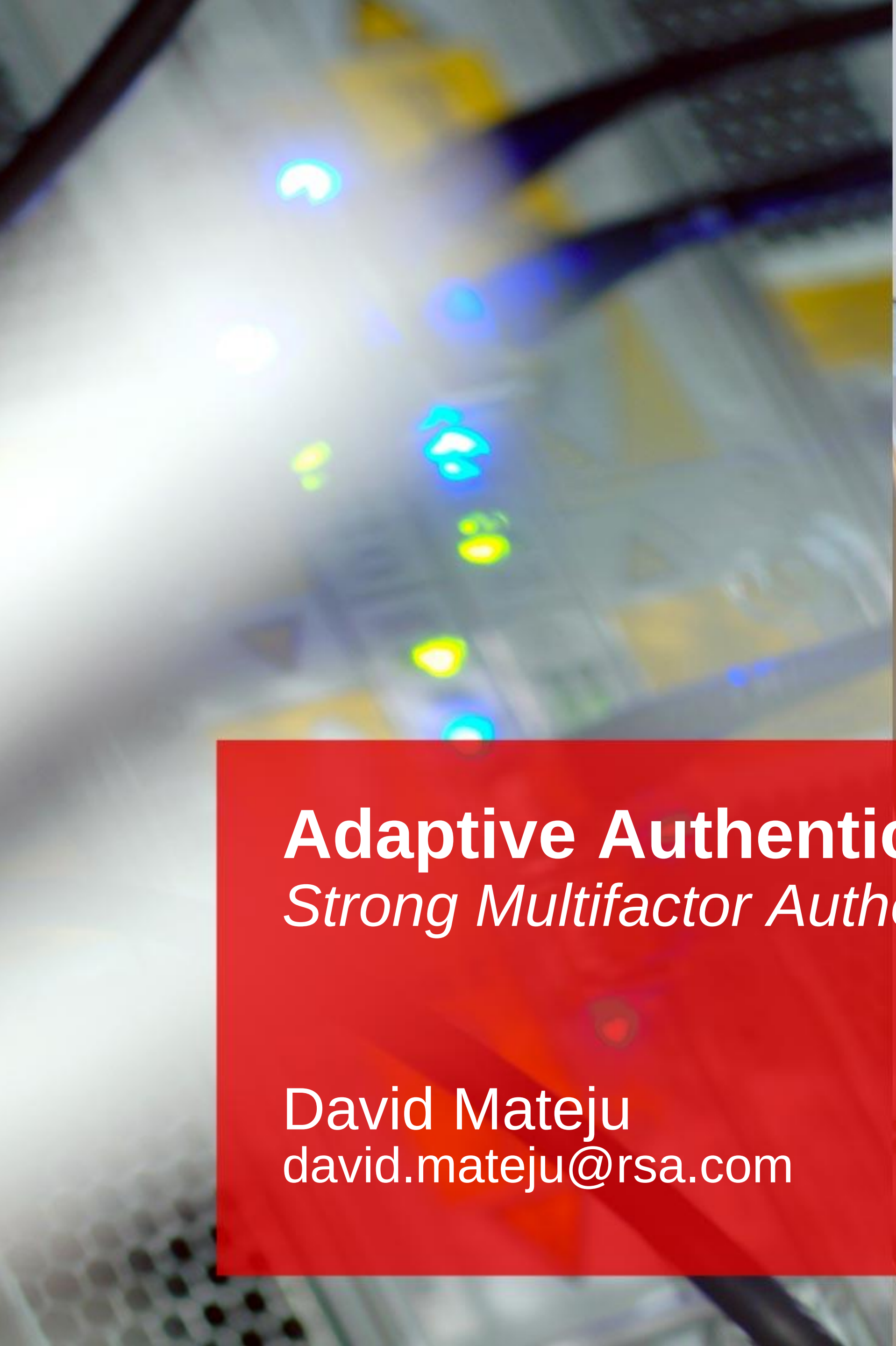


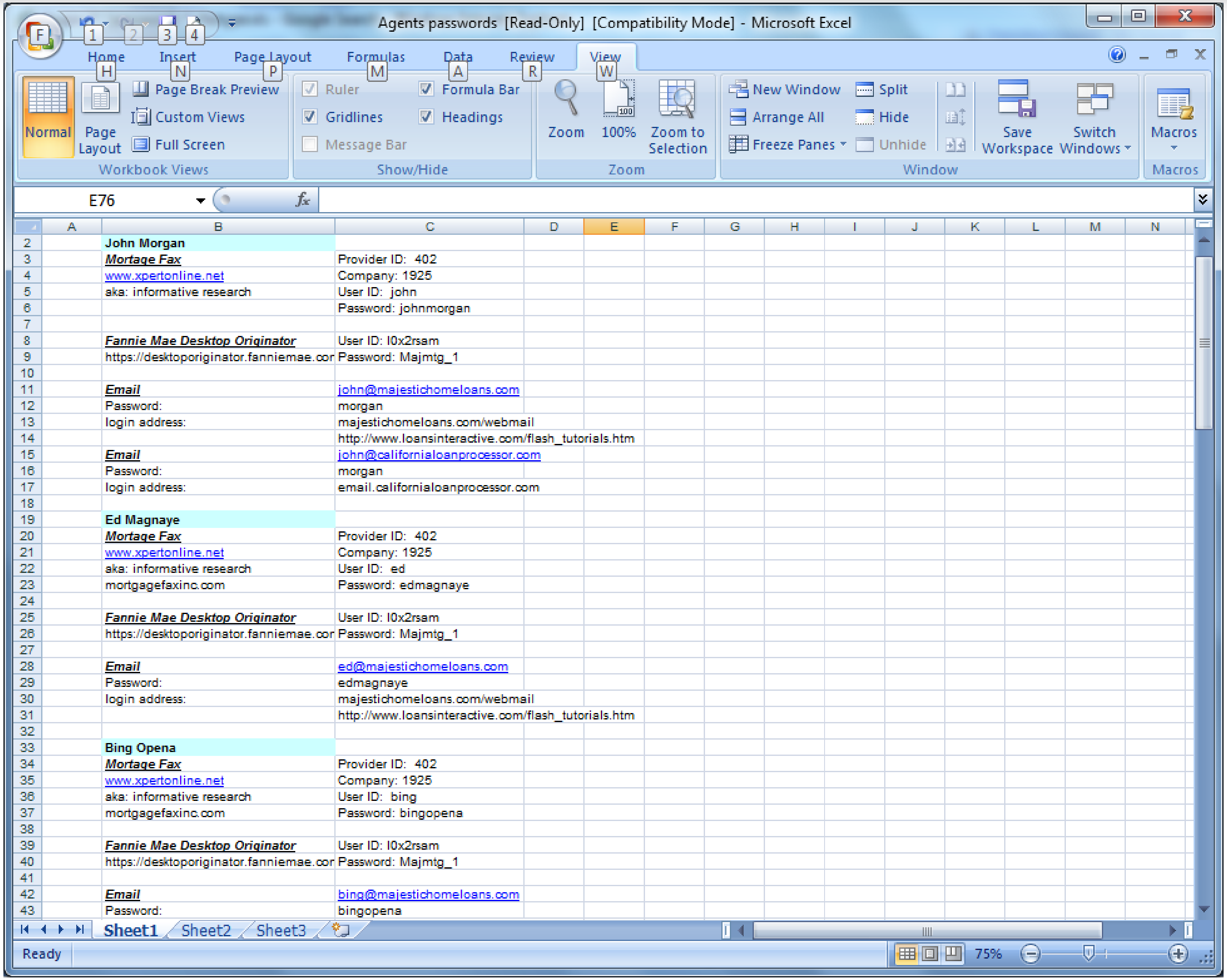
RSA
The Security Division of EMC

Adaptive Authentication

Strong Multifactor Authentication

David Mateju
david.mateju@rsa.com

Google Hacking

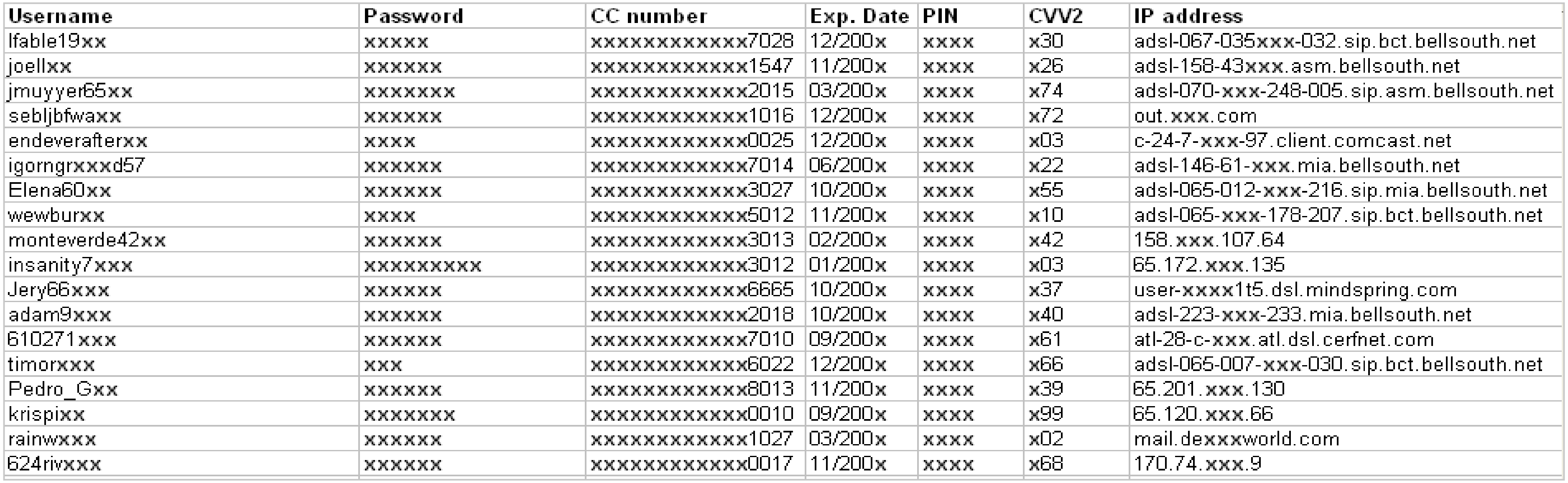


	A	B	C
2		John Morgan	
3		***Mortage Fax***	Provider ID: 402
4		www.xpertonline.net	Company: 1925
5		aka: informative research	User ID: john
6			Password: johnmorgan
7			
8		***Fannie Mae Desktop Originator***	User ID: I0x2rsam
9		https://desktoporiginator.fanniemae.cor	Password: Majmtg_1
10			
11		***Email***	john@majestichomeloans.com
12		Password:	morgan
13		login address:	majestichomeloans.com/webmail
14			http://www.loansinteractive.com/flash_tutorials.htm
15		***Email***	john@californialoanprocessor.com
16		Password:	morgan
17		login address:	email.californialoanprocessor.com
18			
19		Ed Magnaye	
20		***Mortage Fax***	Provider ID: 402
21		www.xpertonline.net	Company: 1925
22		aka: informative research	User ID: ed
23		mortgagefaxinc.com	Password: edmagnaye
24			
25		***Fannie Mae Desktop Originator***	User ID: I0x2rsam
26		https://desktoporiginator.fanniemae.cor	Password: Majmtg_1
27			
28		***Email***	ed@majestichomeloans.com
29		Password:	edmagnaye
30		login address:	majestichomeloans.com/webmail
31			http://www.loansinteractive.com/flash_tutorials.htm
32			
33		Bing Opena	
34		***Mortage Fax***	Provider ID: 402
35		www.xpertonline.net	Company: 1925
36		aka: informative research	User ID: bing
37		mortgagefaxinc.com	Password: bingopena
38			
39		***Fannie Mae Desktop Originator***	User ID: I0x2rsam
40		https://desktoporiginator.fanniemae.cor	Password: Majmtg_1
41			
42		***Email***	bing@majestichomeloans.com
43		Password:	bingopena

RSA®
The Security Division of EMC

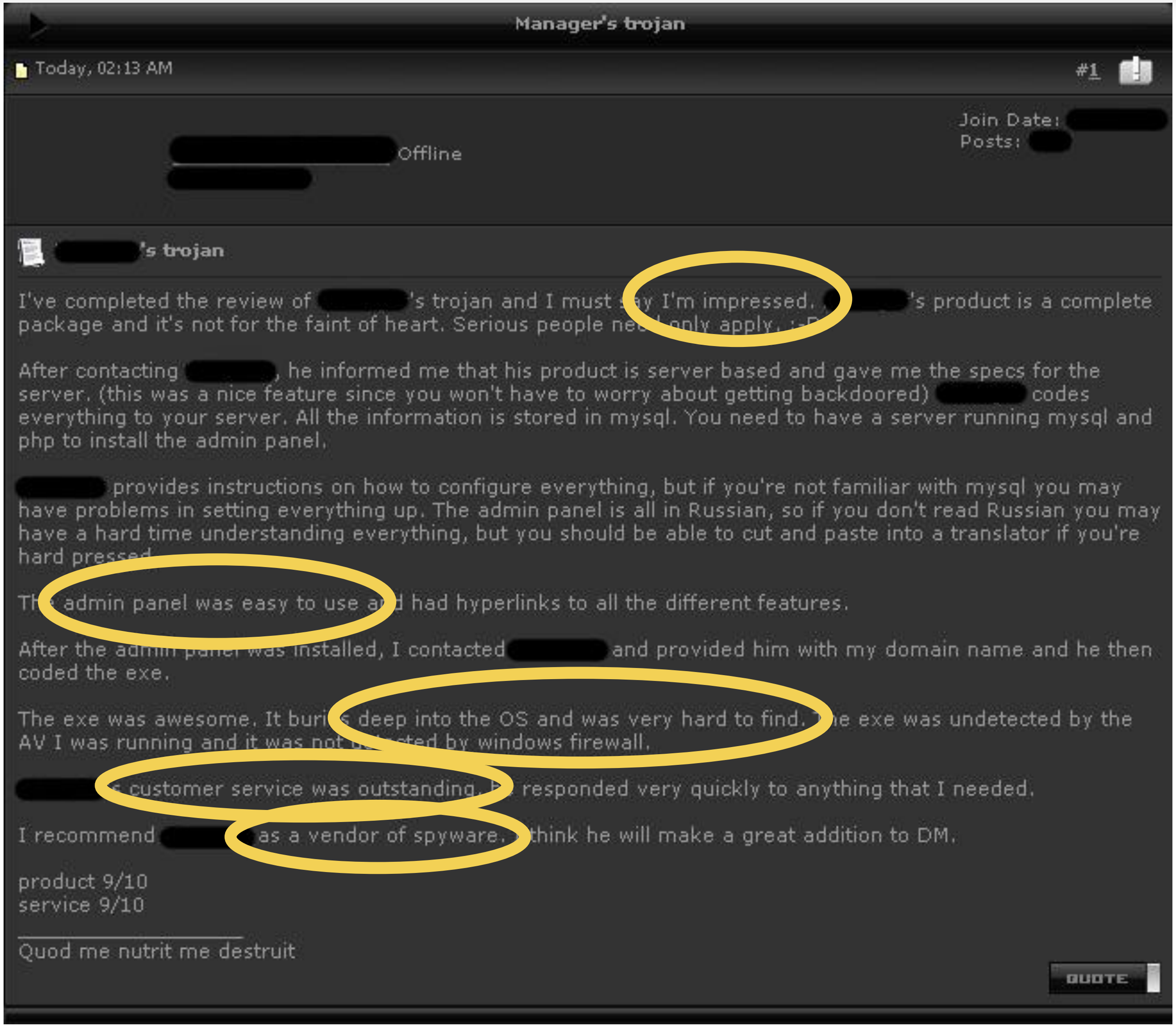
Phishing, Keyloggers, Trojans

Example of stolen credentials extracted from a phishing site by RSA AFCC team:



Username	Password	CC number	Exp. Date	PIN	CVV2	IP address
lfable19xx	xxxxx	xxxxxxxxxxxx7028	12/200x	xxxx	x30	adsl-067-035xxx-032.sip.bct.bellsouth.net
joellxx	xxxxxx	xxxxxxxxxxxx1547	11/200x	xxxx	x26	adsl-158-43xxx.asm.bellsouth.net
jmuyyer65xx	xxxxxxx	xxxxxxxxxxxx2015	03/200x	xxxx	x74	adsl-070-xxx-248-005.sip.asm.bellsouth.net
sebljbfwaxx	xxxxxx	xxxxxxxxxxxx1016	12/200x	xxxx	x72	out.xxx.com
endeverafterxx	xxxx	xxxxxxxxxxxx0025	12/200x	xxxx	x03	c-24-7-xxx-97.client.comcast.net
igorngrxxxd57	xxxxxx	xxxxxxxxxxxx7014	06/200x	xxxx	x22	adsl-146-61-xxx.mia.bellsouth.net
Elena60xx	xxxxxx	xxxxxxxxxxxx3027	10/200x	xxxx	x55	adsl-065-012-xxx-216.sip.mia.bellsouth.net
wewburxx	xxxx	xxxxxxxxxxxx5012	11/200x	xxxx	x10	adsl-065-xxx-178-207.sip.bct.bellsouth.net
monteverde42xx	xxxxxx	xxxxxxxxxxxx3013	02/200x	xxxx	x42	158.xxx.107.64
insanity7xxx	xxxxxxxxx	xxxxxxxxxxxx3012	01/200x	xxxx	x03	65.172.xxx.135
Jery66xxx	xxxxxx	xxxxxxxxxxxx6665	10/200x	xxxx	x37	user-xxxx1t5.dsl.mindspring.com
adam9xxx	xxxxxx	xxxxxxxxxxxx2018	10/200x	xxxx	x40	adsl-223-xxx-233.mia.bellsouth.net
610271xxx	xxxxxx	xxxxxxxxxxxx7010	09/200x	xxxx	x61	atl-28-c-xxx.atl.dsl.cerfnet.com
timorxxx	xxx	xxxxxxxxxxxx6022	12/200x	xxxx	x66	adsl-065-007-xxx-030.sip.bct.bellsouth.net
Pedro_Gxx	xxxxxx	xxxxxxxxxxxx8013	11/200x	xxxx	x39	65.201.xxx.130
krispixx	xxxxxxx	xxxxxxxxxxxx0010	09/200x	xxxx	x99	65.120.xxx.66
rainwxxx	xxxxxx	xxxxxxxxxxxx1027	03/200x	xxxx	x02	mail.dexxxworld.com
624rivxxx	xxxxxx	xxxxxxxxxxxx0017	11/200x	xxxx	x68	170.74.xxx.9

Want to be a fraudster? Buy Trojan!



Manager's trojan

Today, 02:13 AM #1

[redacted] Offline
[redacted]

Join Date: [redacted]
Posts: [redacted]

[redacted]'s trojan

I've completed the review of [redacted]'s trojan and I must say I'm impressed. [redacted]'s product is a complete package and it's not for the faint of heart. Serious people need only apply. :-D

After contacting [redacted], he informed me that his product is server based and gave me the specs for the server. (this was a nice feature since you won't have to worry about getting backdoored) [redacted] codes everything to your server. All the information is stored in mysql. You need to have a server running mysql and php to install the admin panel.

[redacted] provides instructions on how to configure everything, but if you're not familiar with mysql you may have problems in setting everything up. The admin panel is all in Russian, so if you don't read Russian you may have a hard time understanding everything, but you should be able to cut and paste into a translator if you're hard pressed.

The admin panel was easy to use and had hyperlinks to all the different features.

After the admin panel was installed, I contacted [redacted] and provided him with my domain name and he then coded the exe.

The exe was awesome. It buries deep into the OS and was very hard to find. The exe was undetected by the AV I was running and it was not detected by windows firewall.

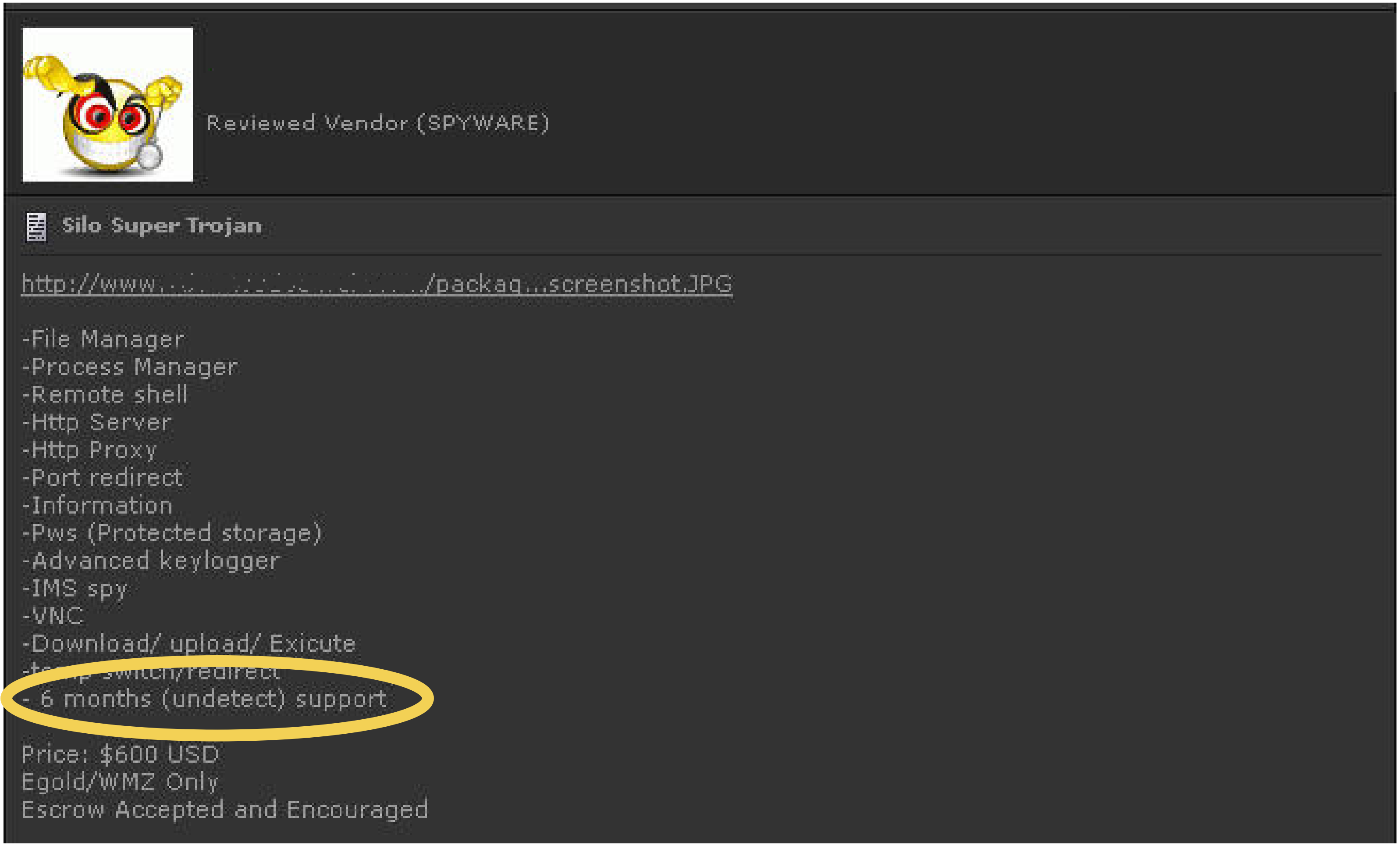
[redacted]'s customer service was outstanding. He responded very quickly to anything that I needed.

I recommend [redacted] as a vendor of spyware. I think he will make a great addition to DM.

product 9/10
service 9/10

Quod me nutrit me destruit

Don‘t want to be detected? Buy undetection service!



Reviewed Vendor (SPYWARE)

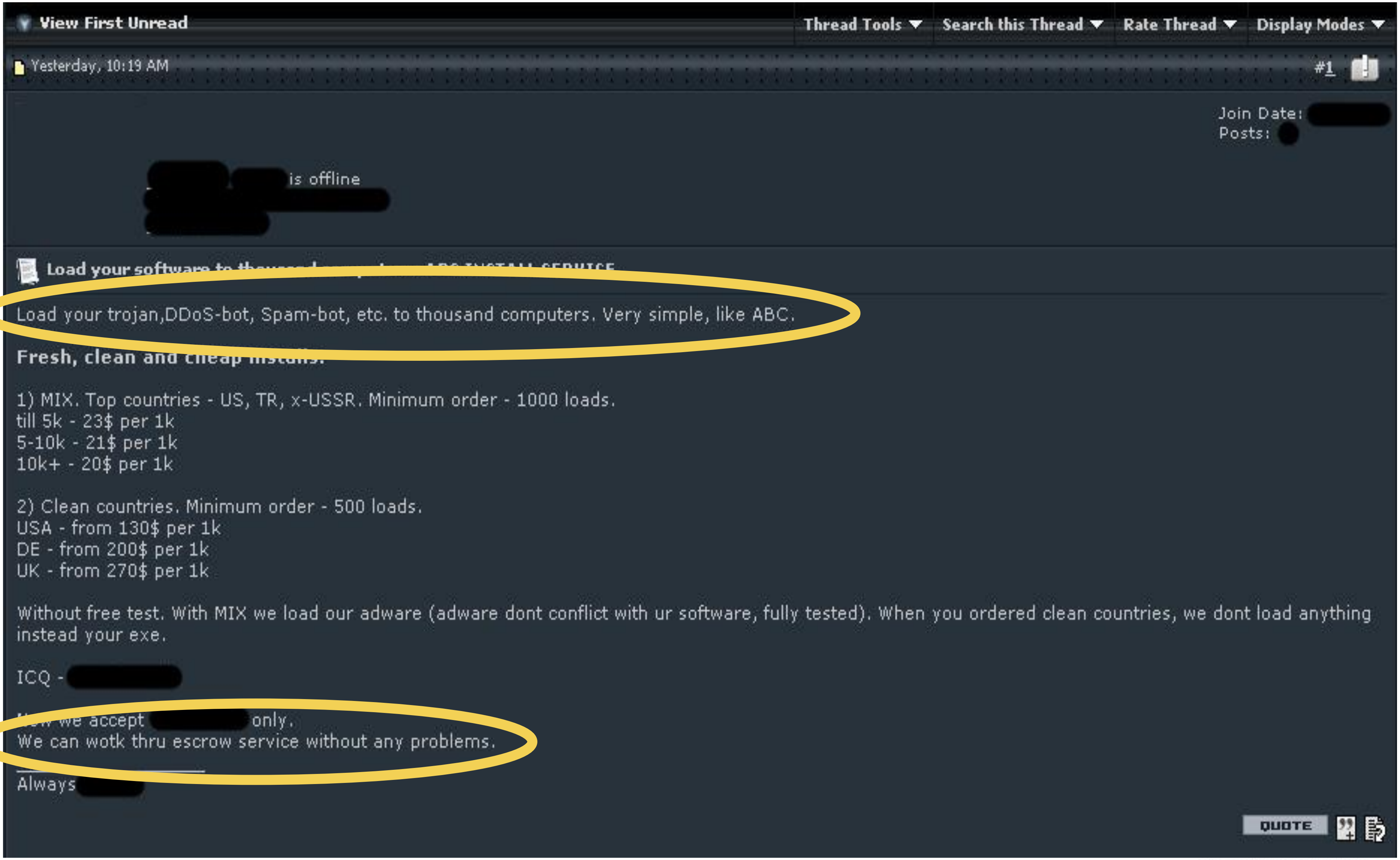
Silo Super Trojan

http://www.[redacted]/packag...screenshot.JPG

-File Manager
-Process Manager
-Remote shell
-Http Server
-Http Proxy
-Port redirect
-Information
-Pws (Protected storage)
-Advanced keylogger
-IMS spy
-VNC
-Download/ upload/ Exicute
-tcp switch/redirect
- 6 months (undetect) support

Price: $600 USD
Egold/WMZ Only
Escrow Accepted and Encouraged

Cannot distribute? Buy Trojan distribution service!



Yesterday, 10:19 AM #1

Join Date: [redacted]
Posts: [redacted]

[redacted] is offline
[redacted]

Load your software to thousand computers - ABC INSTALL SERVICE

Load your trojan,DDoS-bot, Spam-bot, etc. to thousand computers. Very simple, like ABC.

Fresh, clean and cheap installs.

1) MIX. Top countries - US, TR, x-USSR. Minimum order - 1000 loads.
till 5k - 23$ per 1k
5-10k - 21$ per 1k
10k+ - 20$ per 1k

2) Clean countries. Minimum order - 500 loads.
USA - from 130$ per 1k
DE - from 200$ per 1k
UK - from 270$ per 1k

Without free test. With MIX we load our adware (adware dont conflict with ur software, fully tested). When you ordered clean countries, we dont load anything instead your exe.

ICQ - [redacted]

Now we accept [redacted] only.
We can wotk thru escrow service without any problems.

Always [redacted]

Zeus Trojan as an example outcome…

- Tracking one variant of a very popular tool-kit
- In first two weeks infected 32,000 computers
  - Roughly 4,000 infections a day
- No effective anti-virus update available
  - Highly polymorphic, no consistent binary signature
- To Q2/2009 we have recovered 60,000 compromised users and their credentials from this tool-kit alone
- **Are YOU sure you don't have one in your PC?**

How to fight? Strong multifactor authentication!

Two-factor Authentication via One-time Password

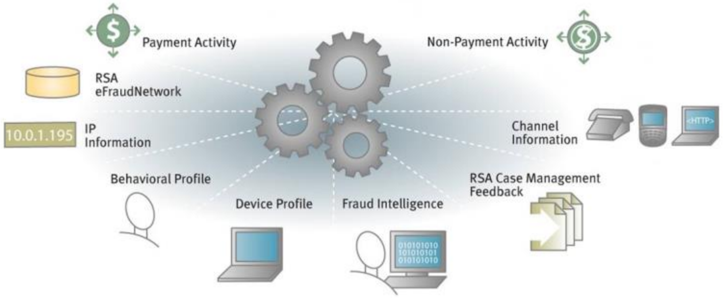
- Username
- PIN + OTP

Two-factor Authentication via PKI

- Username
- Password + Certificate

Adaptive Authentication

- Username
- Password
- Only in case of high risk
  - Step-up Authentication



RSA®
The Security Division of EMC

OTP and PKI Authentication

Advantages

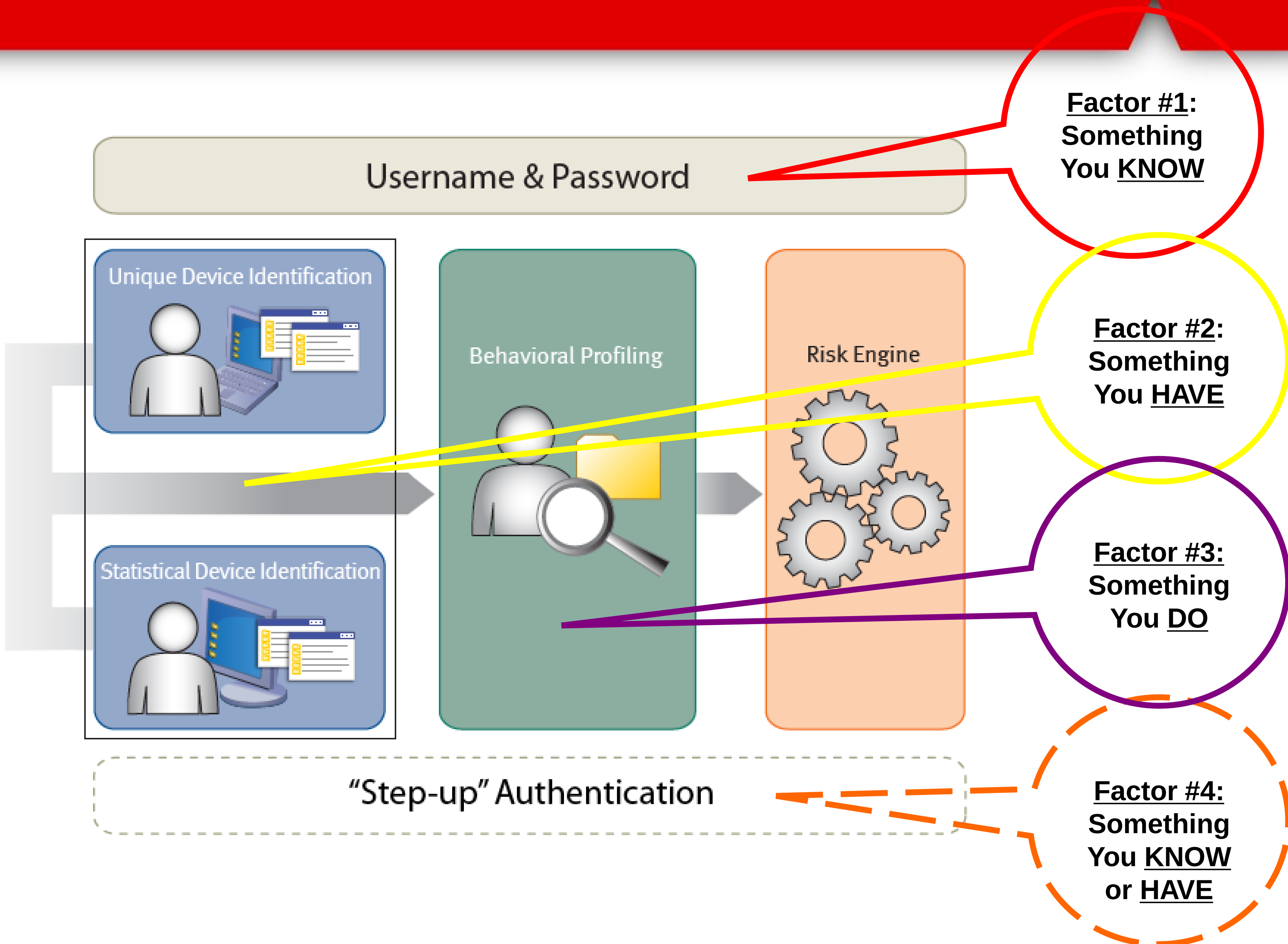
- Much more secure than static passwords
- Easy to use for users
- Users “own” something, they feel more secure – psychology

Challenges

- Distribution process of hardware/software tokens and certificates
- Managing tokens’ and certificates’ life-cycle (expiration, renewals)
- Can be vulnerable to on-line financial fraud
  - Man-in-the-middle, Trojans

Multi-factor Adaptive Authentication

Adaptive Authentication Concept



Username & Password

Unique Device Identification

Statistical Device Identification

Behavioral Profiling

Risk Engine

"Step-up" Authentication

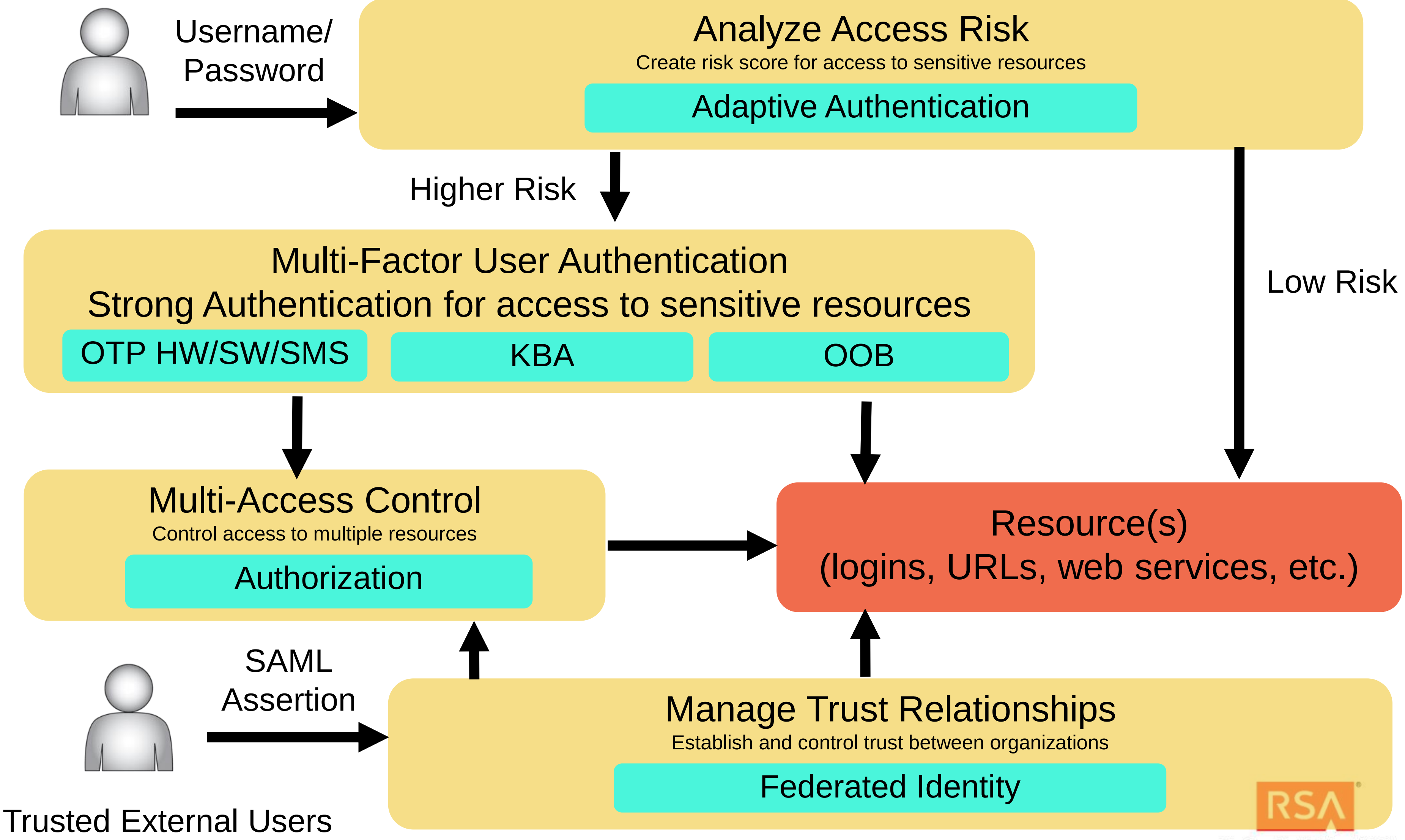
Factor #1: Something You **KNOW**

Factor #2: Something You **HAVE**

Factor #3: Something You **DO**

Factor #4: Something You **KNOW** or **HAVE**

Adaptive Authentication Concept



Username/ Password

Analyze Access Risk

Create risk score for access to sensitive resources

Adaptive Authentication

Higher Risk

Low Risk

Multi-Factor User Authentication

Strong Authentication for access to sensitive resources

OTP HW/SW/SMS

KBA

OOB

Multi-Access Control

Control access to multiple resources

Authorization

Resource(s)

(logins, URLs, web services, etc.)

SAML Assertion

Manage Trust Relationships

Establish and control trust between organizations

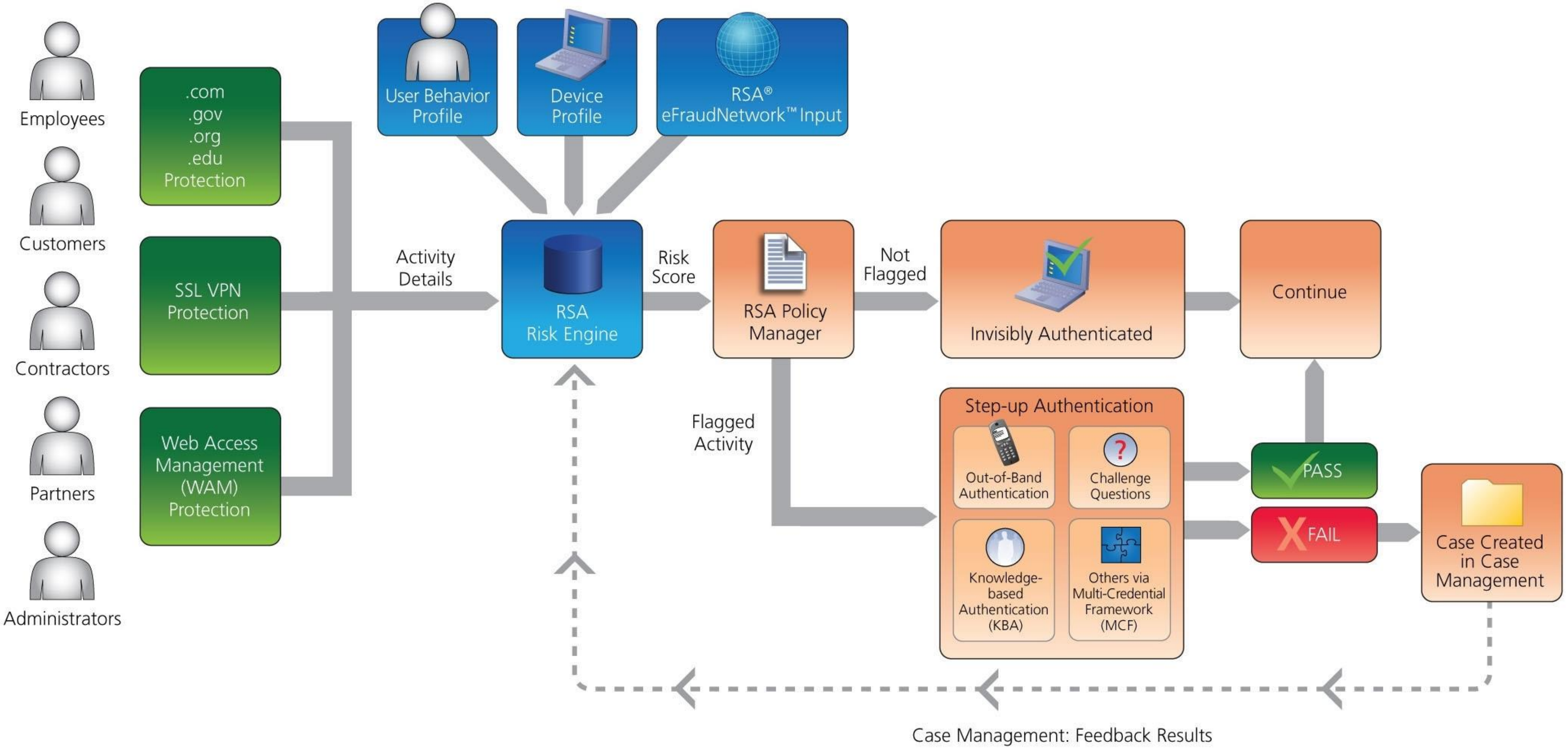
Federated Identity

Trusted External Users

RSA

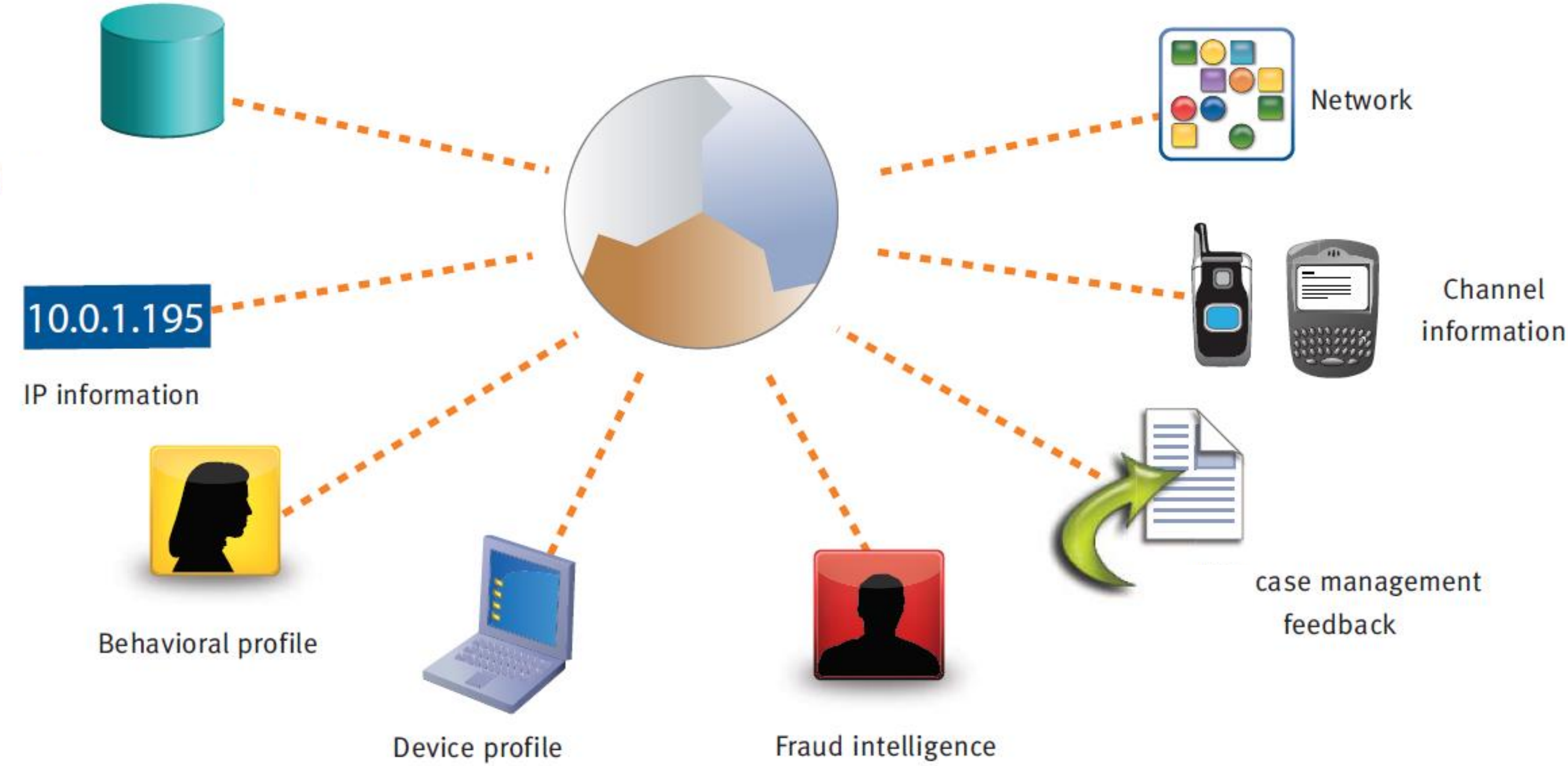
The Security Division of EMC

Adaptive Authentication Process



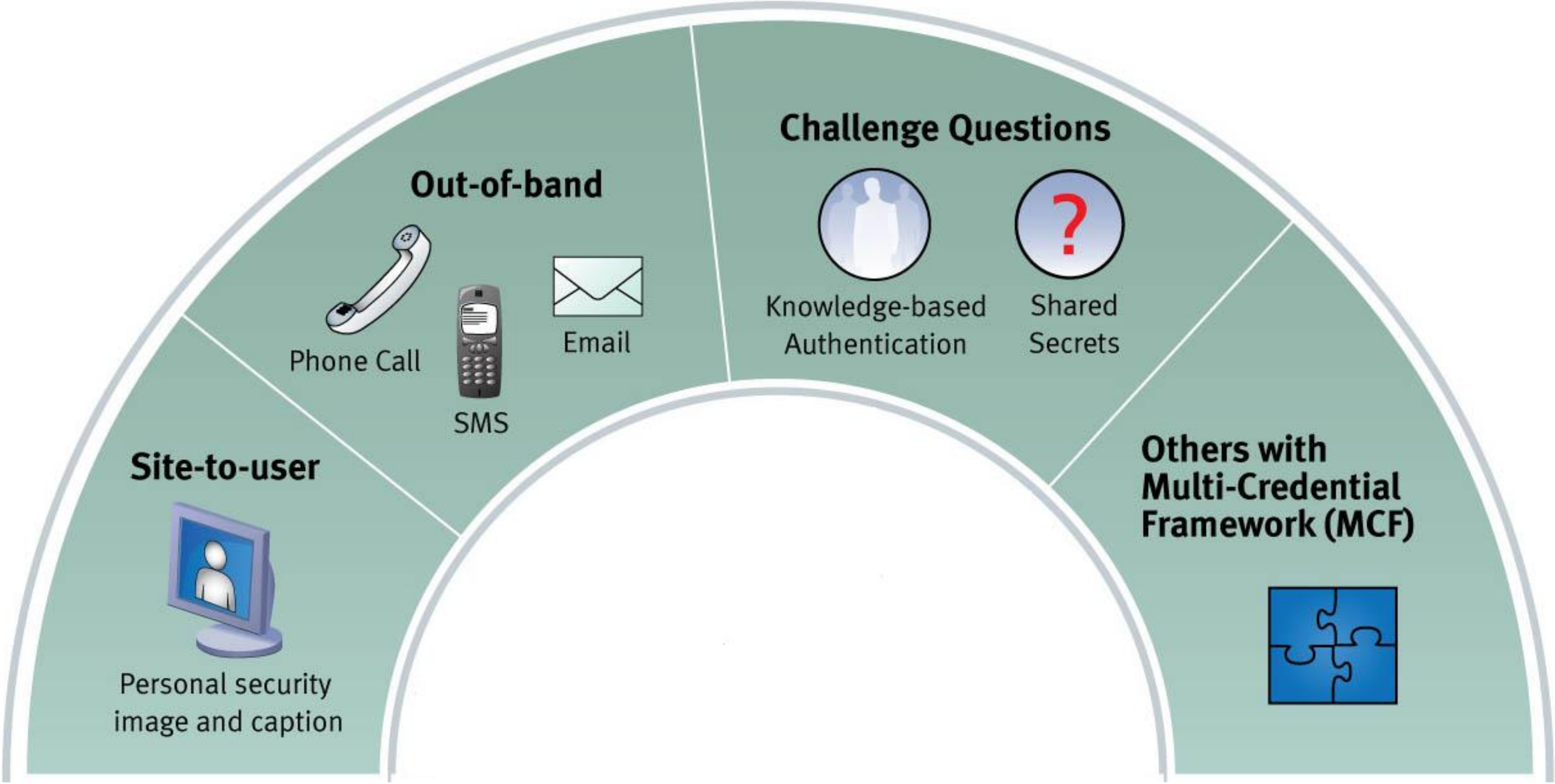
RSA
The Security Division of EMC

The Risk Engine Details

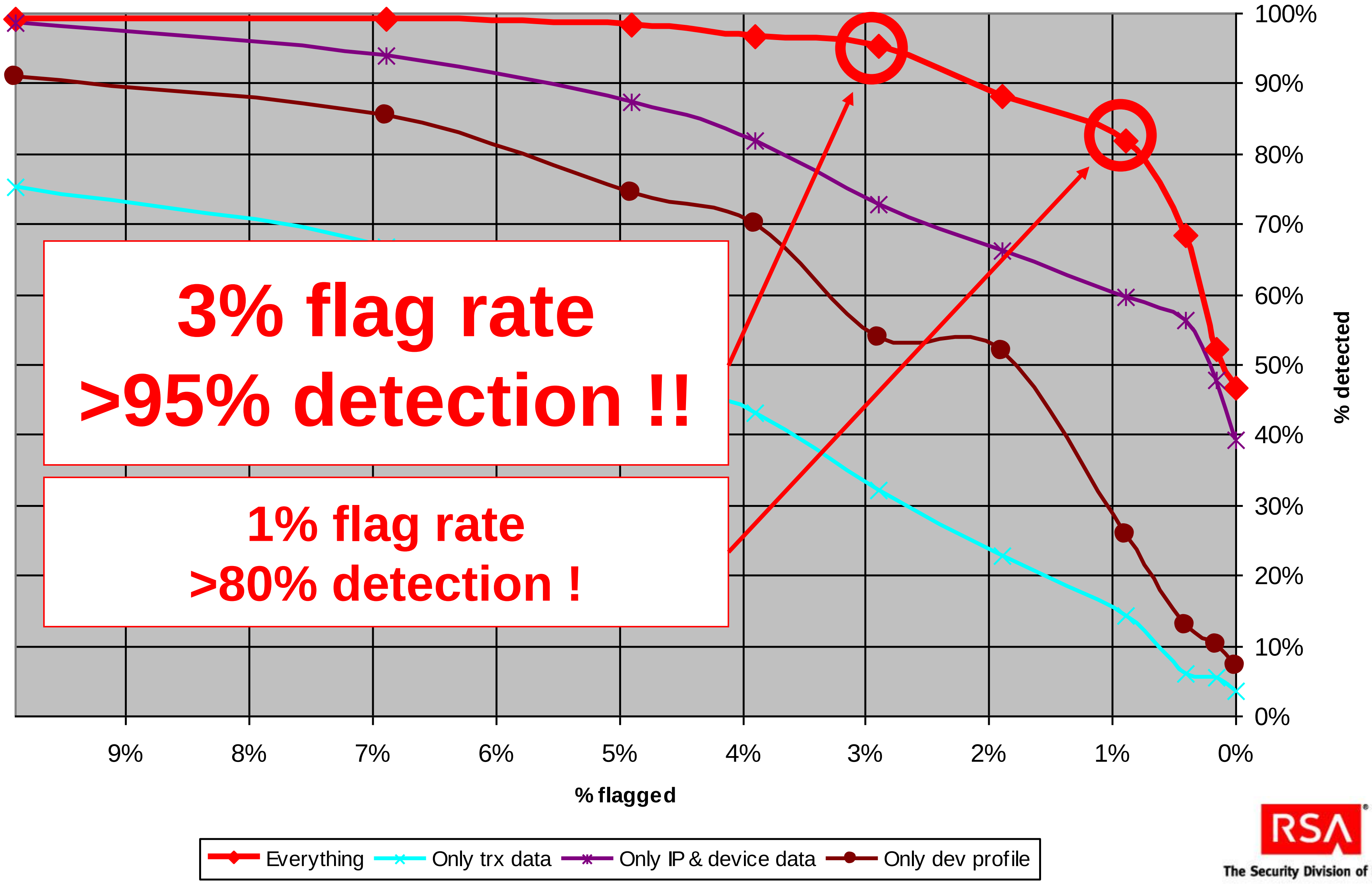


RSA
The Security Division of EMC

Step-up Authentication Options


Out-of-band
Phone Call
SMS
Email
Challenge Questions
Knowledge-based Authentication
Shared Secrets
Site-to-user
Personal security image and caption
Others with Multi-Credential Framework (MCF)

Adaptive Authentication – Identity Theft Detection



3% flag rate
>95% detection !!

1% flag rate
>80% detection !

RSA®
The Security Division of EMC

Why Adaptive Authentication?

- More secure than OTP and PKI alone
  - Can be (as is frequently) used with SMS code
- No impact to user experience
- No HW, SW or Certificate distribution process
- No token/certificate life-cycle management
- Much less vulnerable to online identity fraud
- Integration with SSL VPN, etc.
- Already protecting more than **200.000.000** identities!

RSA®

The Security Division of EMC