



Risk Based Authentication in the Enterprise

ISSA Phoenix
Q3 Chapter Meeting
July 8th, 2014

Rupert Scammell
Principal Consultant
rupert.scammell@rsa.com

Talking Points

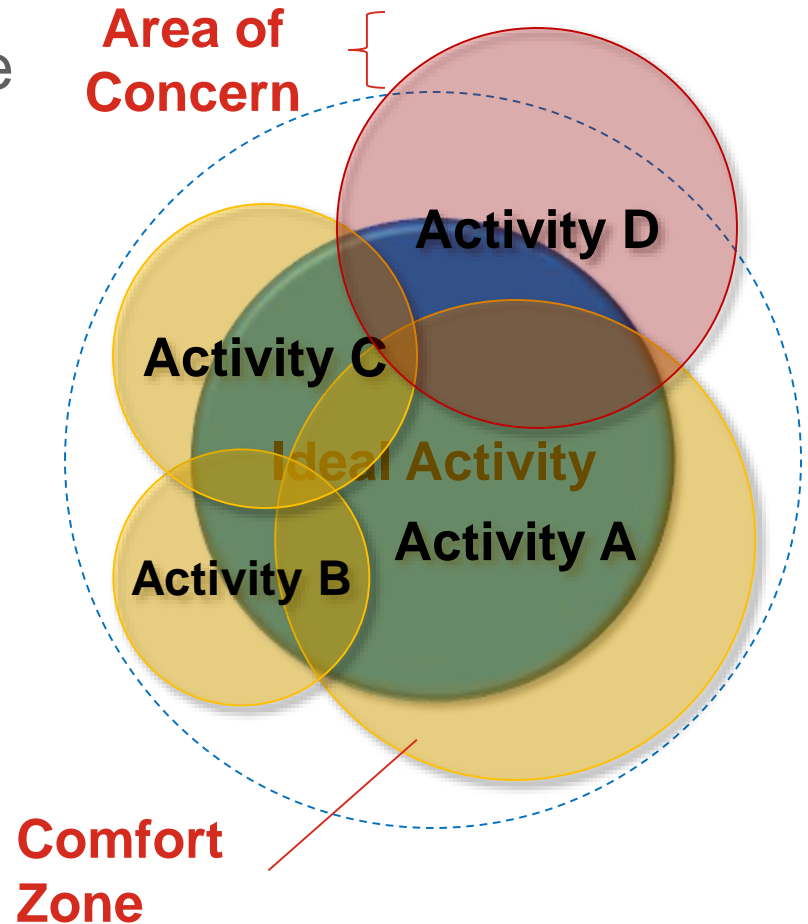
- A quick introduction to your presenter
- How we got here – a brief history of risk-based authentication
- Techniques, tools & threats
- RBA's 'enterprise leap' – a few stories from the field
- Enterprise integration strategies
 - Overcoming common objections and concerns
 - Design patterns
- What's next

Rupert Scammell

- First 'real job' was as a QA engineer for a dot-com era server software company
- 12 years with RSA, initially as a developer
- Left to join an startup focused on RBA for financial services companies
- Rejoined RSA (through acquisition!)
- Many roles since – pro services, pre-sales...
- Most recently as global SE for several major RSA customers

RBA – A quick definition

- Start with an Ideal Activity
 - Allow some degree of variance
- Define activities in comfort zone
 - Opportunity to control costs if comfort zone activities can be reliably identified
- Identify and flag only those activities which fall outside of comfort zone

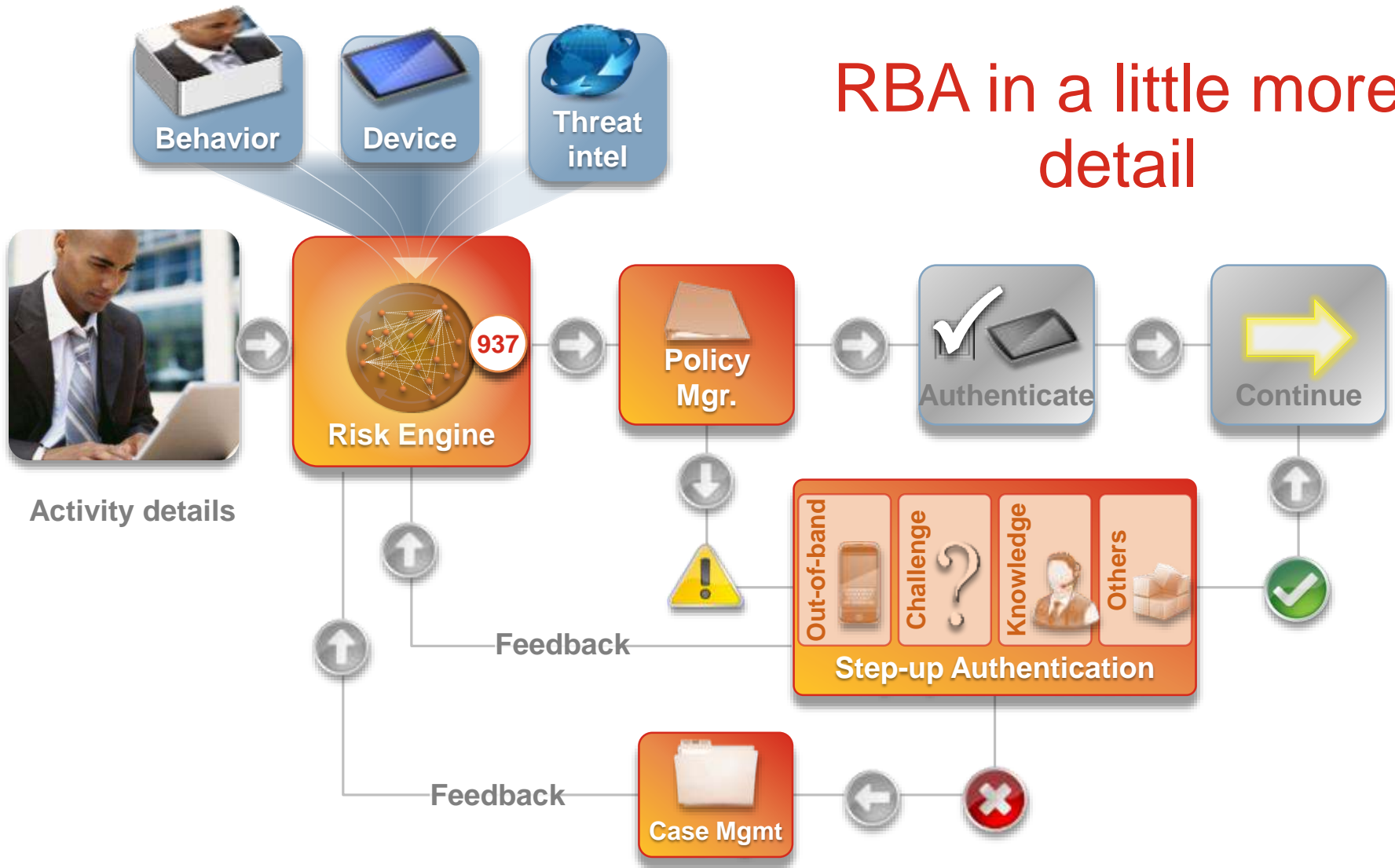


Risk Based Authentication

- Transparent detection of malicious behavior **without sacrificing user experience**
- Monitor and authenticate both **login and post login activities (ideally)**
- Use a risk based self-learning engine **(minimize admin cost & overhead, quickly detect new threats)**
- **Retain control** over institutional policy
- **Incorporate knowledge** of what's occurring beyond the castle walls!



RBA in a little more detail



A brief history of RBA


- Prior to 2005-2006, usernames and passwords were king in the consumer space
 - Insecure but convenient
 - Fear of alienating customers
 - Relatively few compelling threats (at least on the surface)
- FFIEC (regulator for banks and credit unions in the US) was the first to mandate stronger authentication
 - Phishing attacks were top of mind
 - Drove adoption of challenge questions as a commonly used enhanced auth method
 - Set the stage for a shift in the online security posture of financial institutions globally (copied by other regulators, used as a standard by many unregulated FIs)

A brief history of RBA – part II

- Threats evolved remarkably quickly
 - Phishing remained (and remains) a concern, but...
 - Cheap, sophisticated malware became readily available
 - No need to build own infrastructure – Fraud as a Service
 - Obscure source of attacks via botnets
 - Focus on device takeover (MITM/MITB attacks) over simple credential collection
- Very long gap (5+ years) between original FFIEC guidance and revised rules for banks
 - New regs have met with a mixed reaction – sensible response to threats vs. worries about introducing yet more authentication steps

Botnets for hire...

Senior Member



is offline

Join Date: Dec 2011

Posts: 106

Reputation: 26 +/-

welcome to [redacted]'s botnet all in one shop !
here I will be offering you the services regarding the botnet field.

// **webinjects**
i can code any kind of webinject for any kind of botnet to grab all the info that you require. professional work you can r
you can check my work, lr inject i coded [here](#)

// **exploit packs**
i can rent you access to my already hosted, live exploit packs.
packages that i have available :
1 week access for BlackHole
1 week access for Phoenix Exploit pack

// **FUD crypter**
custom coded from scratch on VC++, Fully Undetectable on all antivirus, antimalware engines, bypassing KIS.

// **installs**
at the moment I'm selling clean US, CA, UK and EU mix, Asia mix and Australia installs. min 1k

// **BP hosting and domain**
i present you the opportunity of hosting your botnet or spam project, child porn etc on true offshore hosting. contact m
linux VPS starting from \$50, VDS from \$100
domain registration for all extentions \$70 per year

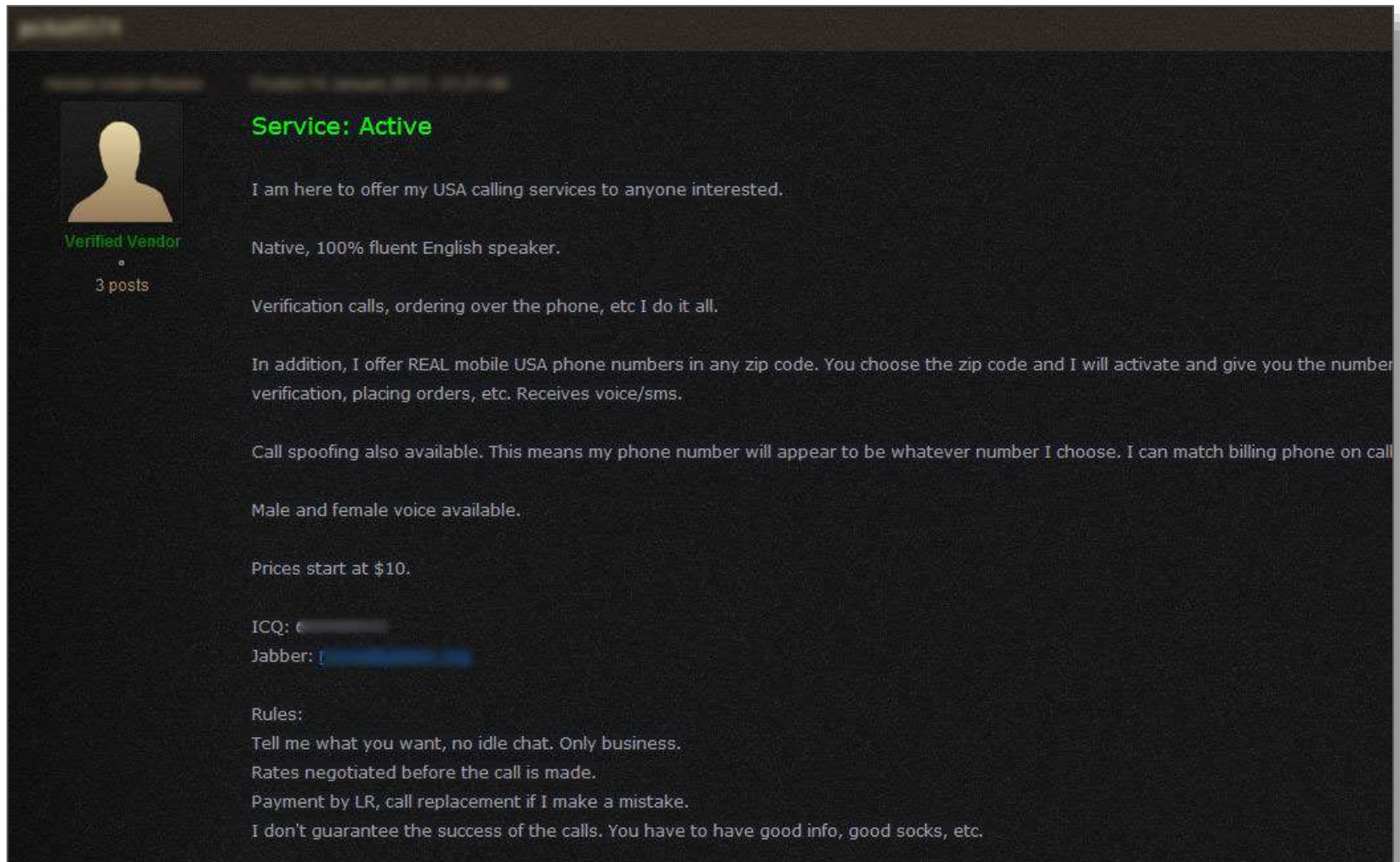
// **botnet turnkey solution**
latest version of Citadel botnet can be setup and configured for any kind of work you want, we discuss in private.
if you want basic idea of botnet you can refer to my little tut [here](#)

My only JID is [redacted] at jabber dot org
accept all forum escrows and payment by LR WU

looking forward to working with you!

Citadel botnet Setup:
[www.\[redacted\].ad.php?p=388916](http://www.[redacted].ad.php?p=388916)

The human element – a fraudster callcenter



Service: Active

I am here to offer my USA calling services to anyone interested.

Native, 100% fluent English speaker.

Verification calls, ordering over the phone, etc I do it all.

In addition, I offer REAL mobile USA phone numbers in any zip code. You choose the zip code and I will activate and give you the number verification, placing orders, etc. Receives voice/sms.

Call spoofing also available. This means my phone number will appear to be whatever number I choose. I can match billing phone on call

Male and female voice available.

Prices start at \$10.

ICQ: e [redacted]

Jabber: [redacted]

Rules:

- Tell me what you want, no idle chat. Only business.
- Rates negotiated before the call is made.
- Payment by LR, call replacement if I make a mistake.
- I don't guarantee the success of the calls. You have to have good info, good socks, etc.

A ever-growing menagerie of malware...

#3156, WAITING ANSWER

Name: with token
URL: .com
Referer: .com

Time:	Creation	Modification	Activity
	09.04.2012 15:28:41	09.04.2012 15:31:39	09.04.2012 15:33:22

Bot: IPv4 ID Botnet

Servers: **Socks 4/4a/5** **VNC**

Token Questions Custom dialog


- 09.04.2012 15:28:41, Login
ID:
Password:
Token:
- 09.04.2012 15:29:07, Questions
What is your youngest child's middle name?:
In which city were you born?:
- 09.04.2012 15:30:32, Token
Secure Token Token Code:
- 09.04.2012 15:31:39, Questions
What is your youngest child's middle name?:
When is your youngest child's birthday (MM/DD)?:

LE	BITID	OS	TIME	SET	ACC	AGENT
66	...	XP SP 3	27.12.2011 13:22:38	264	paypal	SET
67	...	XP SP 2	28.12.2011 16:23:07	2998	paypal	SET
68	...	XP SP 2	25.12.2011 16:21:38	3000	paypal	SET
69	...	Seven	24.12.2011 10:19:11	499	paypal	SET
70	...	XP SP 3	22.12.2011 15:21:46	809	paypal	SET
71	...	Seven	20.12.2011 18:24:13	953	paypal	SET
72	...	XP SP 3	20.12.2011 01:49:22	1464	paypal	SET
73	...	XP SP 3	19.12.2011 21:09:27	1706	paypal	SET
74	...	XP SP 3	19.12.2011 21:55:33	1906	paypal	SET
75	...	XP SP 3	19.12.2011 21:48:54	1404	paypal	SET
76	...	Vista SP 2	19.12.2011 21:28:34	899	paypal	SET
77	19.12.2011	SET


The present day

- Diversification of attacker types and motives
 - State sponsored actors
 - No 'safe industries'
- Attackers no longer purely focused on financial gain
- Increase in underground market sophistication has enabled monetization of intellectual property and (sometimes obscure) corporate assets
- Increasing use of ransomware to hold acquired information hostage – very much an enterprise play

One example...



National Fraud Intelligence Bureau






Action Fraud
Report Fraud & Internet Crime

INTERNET CRIME ATTEMPT FROM IP: 84.110.49.252

This operating system is locked due to the violation of the laws of the United Kingdom! Following violations were detected:

Your IP address is "**84.110.49.252**". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with Pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.






To unlock the computer you are obliged to pay a fine of £ 100.

You could pay the forfeit in two ways:

- 1) Paying through Ukash:
To do this, you should enter the 19 digits code in the payment form and press "PAY A FINE" (if you have several codes, enter them one after the other and press "PAY A FINE").
- 2) Paying through Paysafecard:
To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press "PAY A FINE" (if you have several codes, enter them one after the other and press "PAY A FINE").





Ukash or **paysafecard**

You could buy **Ukash** in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). **Paysafecard** is available from 350,000 sales outlets worldwide, in the United Kingdom, exclusively from all **PayPoint** outlets.



I guarantee that my personal information entered during the process is correct

PAY A FINE



All NFIB related enquiries should be directed to nfib@cityoflondon.pnn.police.uk or to PO Box 38451 London EC2M 4WN

RBA's leap into the enterprise space

- It was a rainy afternoon in San Mateo, CA, c ~2007
- Received a call from a long-time RSA SecurID token customer in the hospital management industry
- Demanded an alternative to 'token necklaces' for physicians and clinical staff who had admitting privileges at the hospitals
- Led us to think creatively about how to adapt our RBA portfolio for other use cases
- Initial partnership with enterprise infrastructure vendors (e.g. SSL/VPN) was key

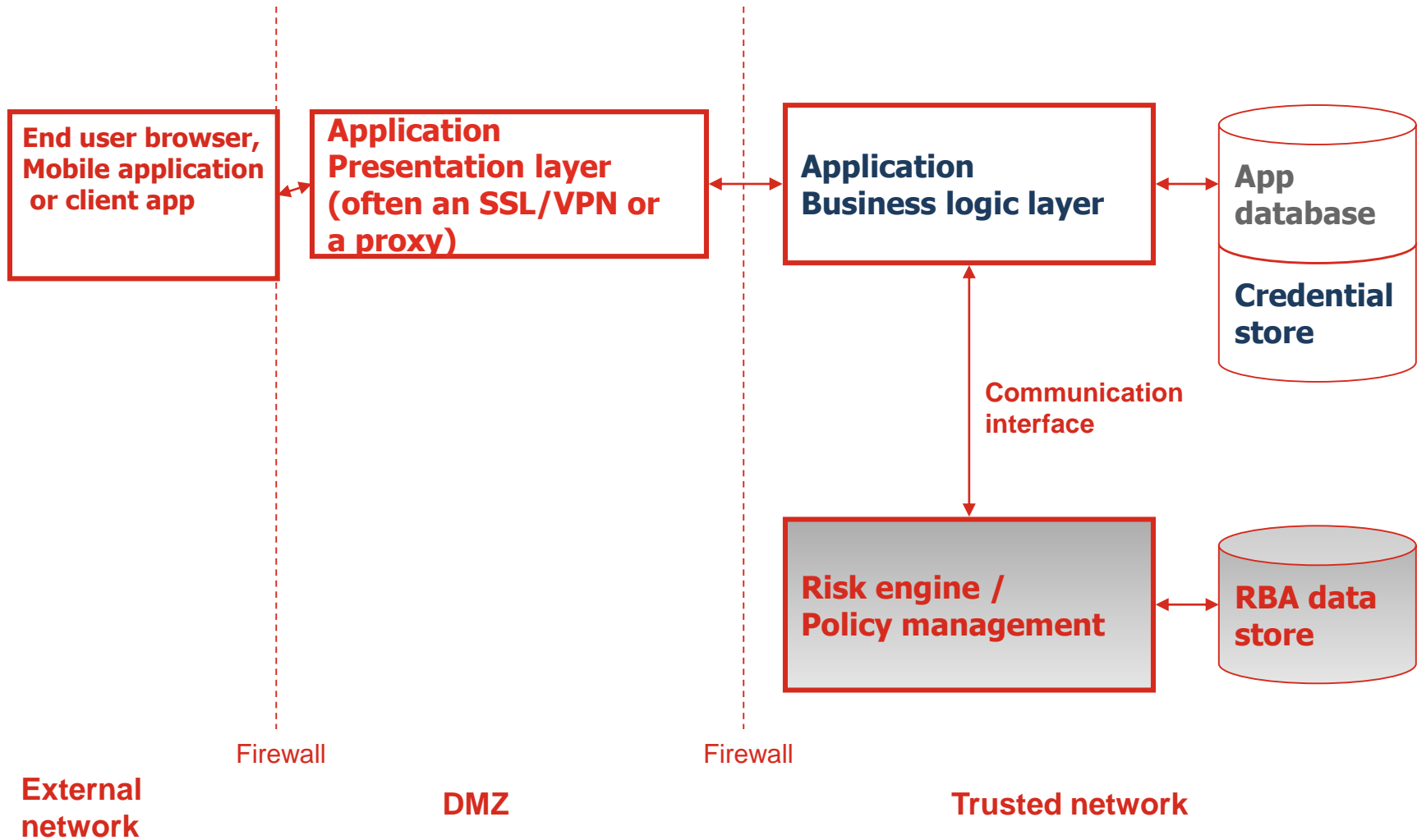
The leap, continued

- Developed vendor-specific middleware to interface with a back-end risk engine and secondary authentication server
- Took longer than expected – original requestor walked, but similar requests from non-traditional customers (esp. healthcare companies) began arriving from all sides
- Formerly disgruntled end-users / doctors became our best customers – viral marketing!

Overcoming objections & concerns

- Rock the boat, but do it gently
 - Find a champion with a well-scoped use case (e.g. an electronic medical records pilot implementation)
 - Be willing to co-exist with incumbent authentication methods to ease acceptance
 - Accept that you won't be able to integrate with everything – web apps are usually easier than dusty AS/400 green-screens!
 - Use consumer familiarity with authentication techniques outside the workplace (online banking) to explain threats & rationale
 - Provide a flexible toolbox
 - Centralize risk and policy functions on the back-end
 - Exercise caution re. customization requests – danger of one-offs and unmaintainable environments

Typical architecture (simplified)



Common enterprise design patterns

- **In all cases, you must have a risk engine that can ingest meaningful information from the access channel!**
- Intermediate it
 - Leverage existing proxy infrastructure
 - Alternatively, introduce a new entity to perform this function
 - Can dramatically reduce complexity by providing a single integration point for many applications
- Wrap it
 - Utilize a web-access management style agent/server model
 - May allow apps scattered through the enterprise to be tied to a central authentication / risk analysis source more easily
 - Generally requires deep integration with WAM/MDM systems, however
- Directly integrate with it
 - Preferred method for many banks
 - Provides maximal flexibility
 - Requires ability to modify presentation/business logic of app – often a rarity in enterprise settings
 - Apps must be integrated/supported/ upgraded individually

What's next

- Static authentication methods (challenge questions, passwords) must eventually die, but have a long half life
- Loosely connected populations – contractors, vendors, supply chain partners will often be first candidates for enterprise RBA
- Encouraging movement toward dynamic authentication in many contexts, consumer and enterprise
 - Often requires a compelling event such as a breach to spur action
 - Regulation is slowly producing positive changes in many industries, but can't always keep up
 - Users are often more willing to adopt new authentication methods than security staff realize
- Must secure multiple channels
 - Channel-friendly auth methods for web, mobile, tablets, voice
- Leverage what the user has
 - Biometrics
 - Device characteristics
 - Geolocation
 - Gestures



The Security Division of EMC

Thank you!